CEH V10 EC-COUNCIL CERTIFIED ETHICAL HACKER

MOST DEMANDING COMPLETE HACKING GUIDE

EXAM: 312-50

"To beat a hacker, you need to think like a hacker

MOST ADVANCED HACKING COURSE

www.ipspecialist.net

Chapter 3: Scanning Networks

Technology Brief

After Footprinting phase, you may have enough information about the target. Now Scanning network phase requires some of this information to proceed further. Network Scanning is a method of getting network information such as identification of hosts, port information, and services by scanning networks and ports. The main Objective of Network Scanning is: -

- To identify live hosts on a network
- To identify open & closed ports
- To identify operating system information
- To identify services running on a network
- To identify running processes on a network
- To identify the presence of Security Devices like firewalls
- To identify System architecture
- To identify running services
- To identify vulnerabilities

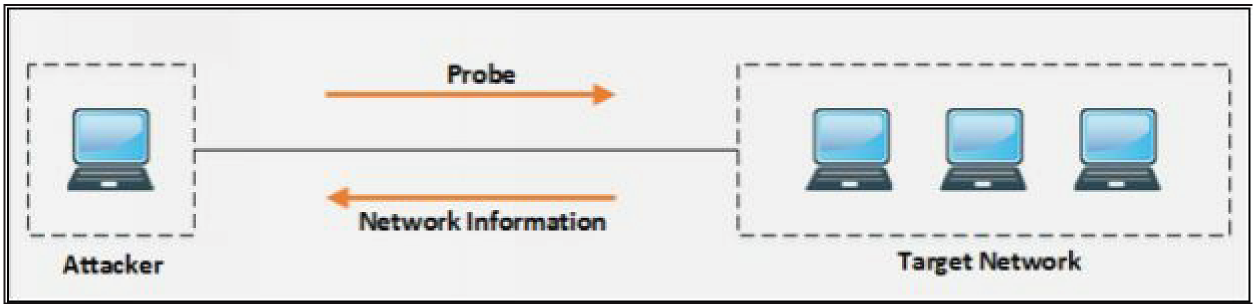


Figure 3-01 Scanning Network

Overview of Network Scanning

Scanning Network phase includes probing to the target network for getting information. When a user probes another user, it can reveal much useful information from the reply is received. In-depth identification of a network, ports and running services helps to create a network architecture, and the attacker gets a clearer picture of the target.

TCP Communication

There are two types of Internet Protocol (IP) traffic. They are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP is connection oriented. Bidirectional communication takes place after successful connection establishment. UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP. Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP packets. Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP. Following diagram shows the TCP header: -

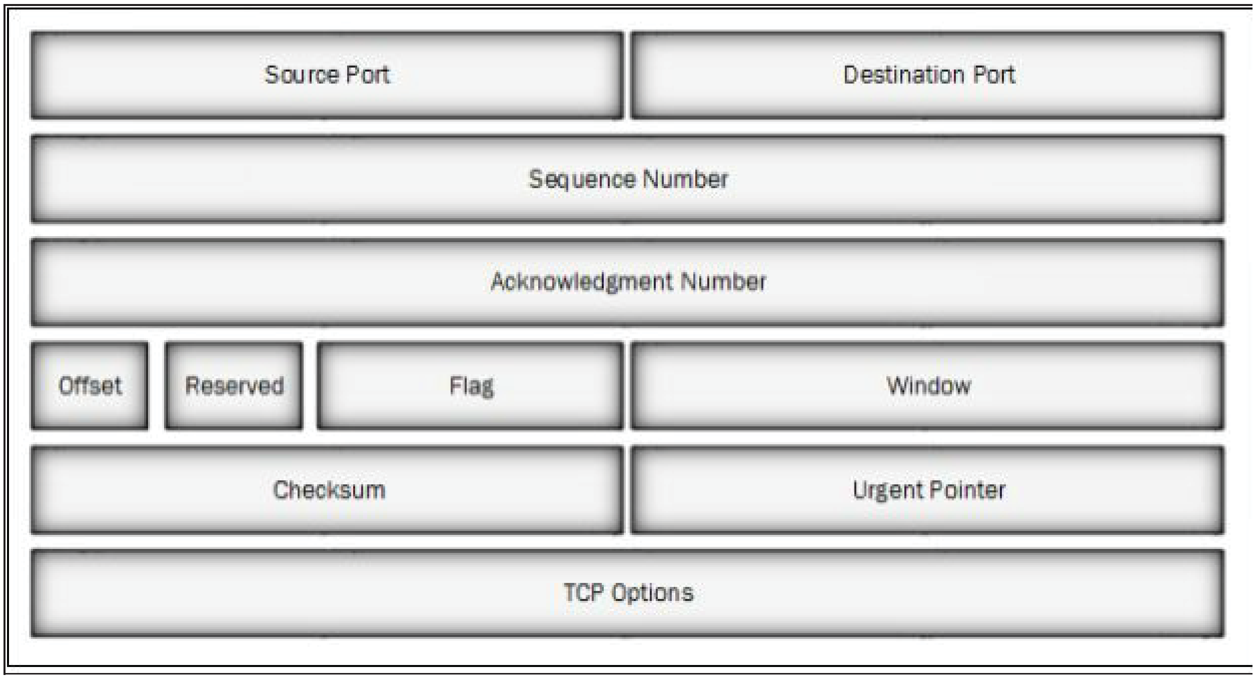


Figure 3-02 TCP Header

Flag filed in the TCP header is of 9 bits. Which includes the following 6 TCP flags: -

Flag	Use

SYN	Initiates a connection between two hosts to facilitate communication.
ACK	Acknowledge the receipt of a packet.
URG	Indicates that the data contained in the packet is urgent and should process immediately.
PSH	Instructs the sending system to send all buffered data immediately.
FIN	Tells the remote system about the end of the communication. In essence, this gracefully closes a connection.
RST	Reset a connection.

Table 3-01 TCP Flags

There is three-way handshaking while establishing a TCP connection between hosts. This handshaking ensures successful, reliable and connection-oriented session between these hosts. The process of establishment of a TCP connection includes three steps. As shown in the figure below: -

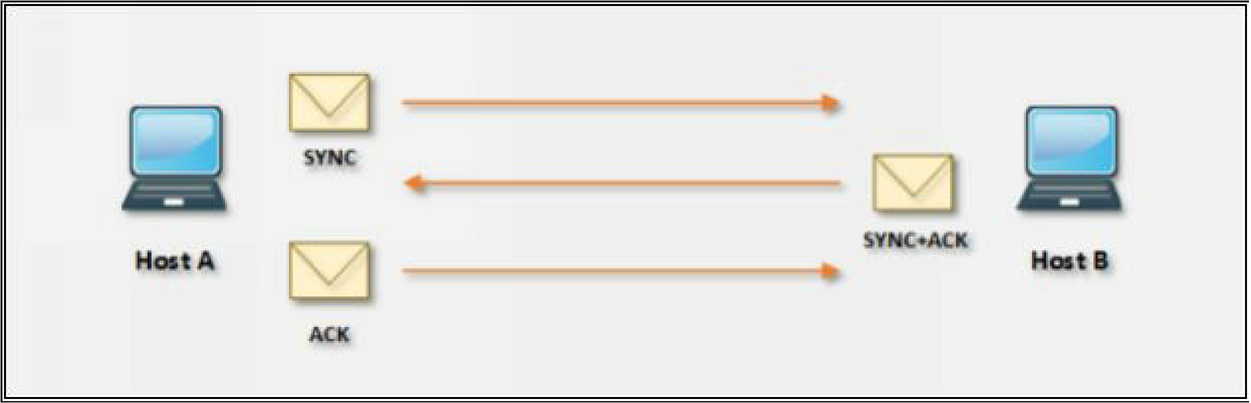


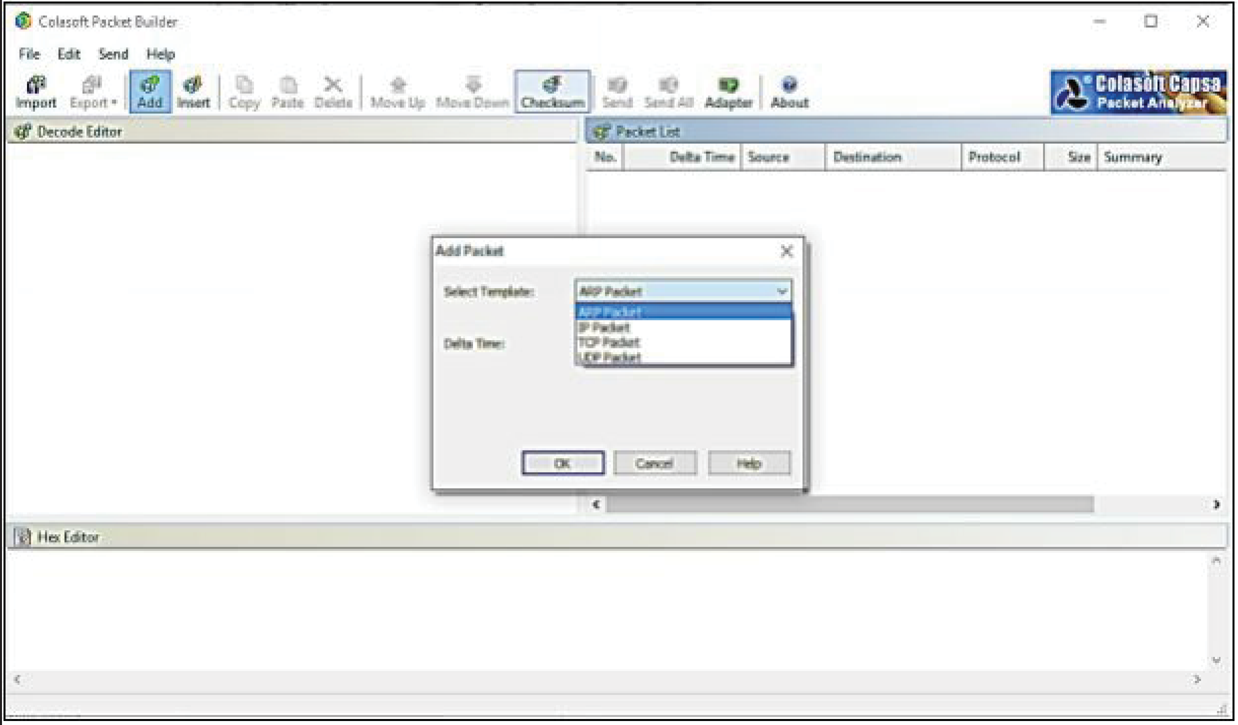
Figure 3-03 TCP Connection Handshaking

Consider Host A wants to communicate with Host B. TCP Connection establishes when host A sends a Sync packet to host B. Host B upon receipt of Sync packet from Host A, reply to Host A with Sync+Ack packet. Host A reply with Ack packet when it receives Sync+Ack packet from host B. After successful handshaking results in the establishment of TCP connection.

U.S Dept proposes TCP/IP model. Of Defence by combining OSI Layer Model and DOD. The Transmission Control Protocol (TCP) and the Internet Protocol (IP) are two of the network standards that define the Internet. IP defines how computers can get data to each other over a routed, interconnected set of networks. TCP defines how applications can create reliable channels of communication across such a network. IP defines addressing and routing, while TCP defines how to have a conversation across the link without garbling or losing data. Layers in TCP/IP model perform similar functions with similar specifications like in OSI model. The only difference is they combine top three layers into a single Application Layer.

Creating Custom Packet Using TCP Flags

Colasoft Packet Builder software enables to create the customized network packets. These Customized Network packets can penetrate the network for attacks. Customization can also use to create fragmented packets. You can download the software from www.colasoft.com.

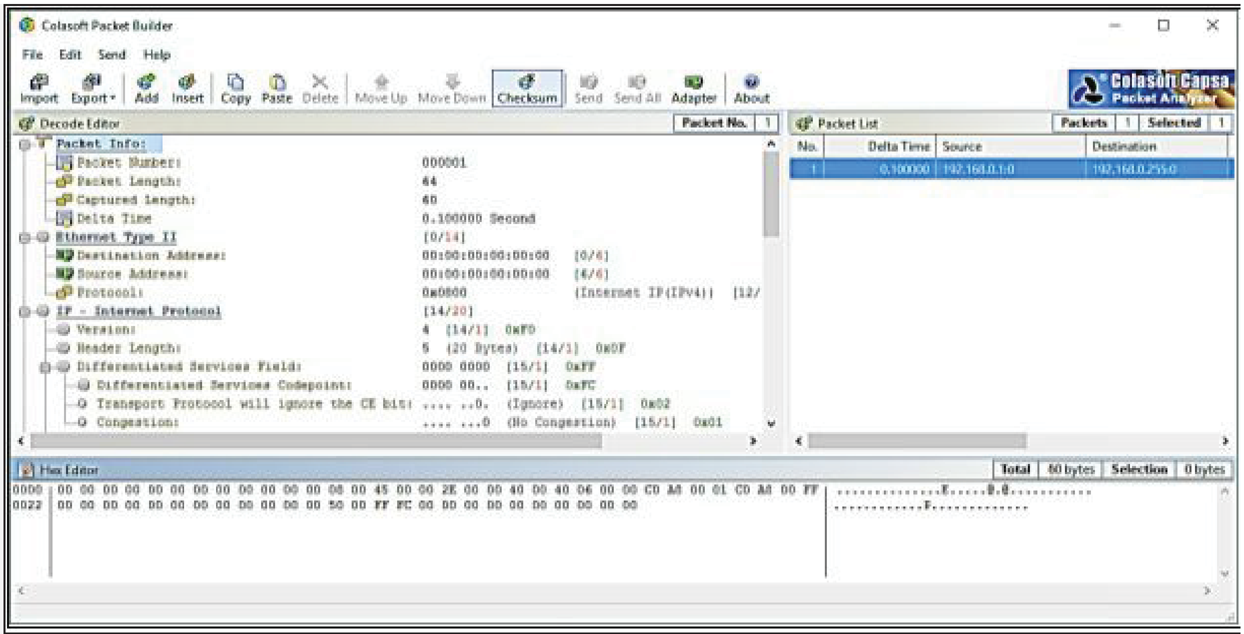


Select Template: ARP Packet

Figure 3-04 Packet Builder Software

Colasoft packet builder offers Import and Export options for a set of packets. You can also add a new packet by clicking **Add**/button. Select the Packet type from the drop-down option. Available options are: -

- ARP Packet
- IP Packet
- TCP Packet
- UDP Packet


Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter About
Colasoft Capsa Packet Analyzer
Decode Editor
Packet No. 1
Packet List
Packets 1 Selected 1
Hex Editor
Total 60 bytes Selection 0 bytes

```
Packet Info:
  Packet Number:                              000001
  Packet Length:                              64
  Captured Length:                            60
  Delta Time                                  0.100000 Second
Ethernet Type II                              [0/14]
  Destination Address:                        00:00:00:00:00:00   [0/6]
  Source Address:                             00:00:00:00:00:00   [6/6]
  Protocol:                                   0x0800              (Internet IP(IPV4))   [12/
IP - Internet Protocol                        [14/20]
  Version:                                    4  [14/1]  0xF0
  Header Length:                              5  (20 Bytes)  [14/1]  0x0F
  Differentiated Services Field:              0000 0000  [15/1]  0xFF
    Differentiated Services Codepoint:        0000 00..  [15/1]  0xFC
    Transport Protocol will ignore the CE bit: .... ..0.  (Ignore)  [15/1]  0x02
    Congestion:                               .... ...0  (No Congestion)  [15/1]  0x01
```

No.	Delta Time	Source	Destination
1	0.100000	192.168.0.1:0	192.168.0.255:0

```
0000 | 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 00 2E 00 00 40 00 40 06 00 00 C0 A8 00 01 C0 A8 00 FF | ..............E.....@.@...........
0022 | 00 00 00 00 00 00 00 00 00 00 00 00 50 00 FF FC 00 00 00 00 00 00 00 00 00 00                         | ............P.............
```

Figure 3-05 Creating Custom Packet

After Selecting the Packet Type, now you can customize the packet, Select the Network Adapter and Send it towards the destination.

Scanning Methodology

The Scanning Methodology includes the following step: -

- Checking for live systems
- Discovering open ports
- Scanning beyond IDS
- Banner grabbing
- Scanning Vulnerabilities
- Network Diagram
- Proxies

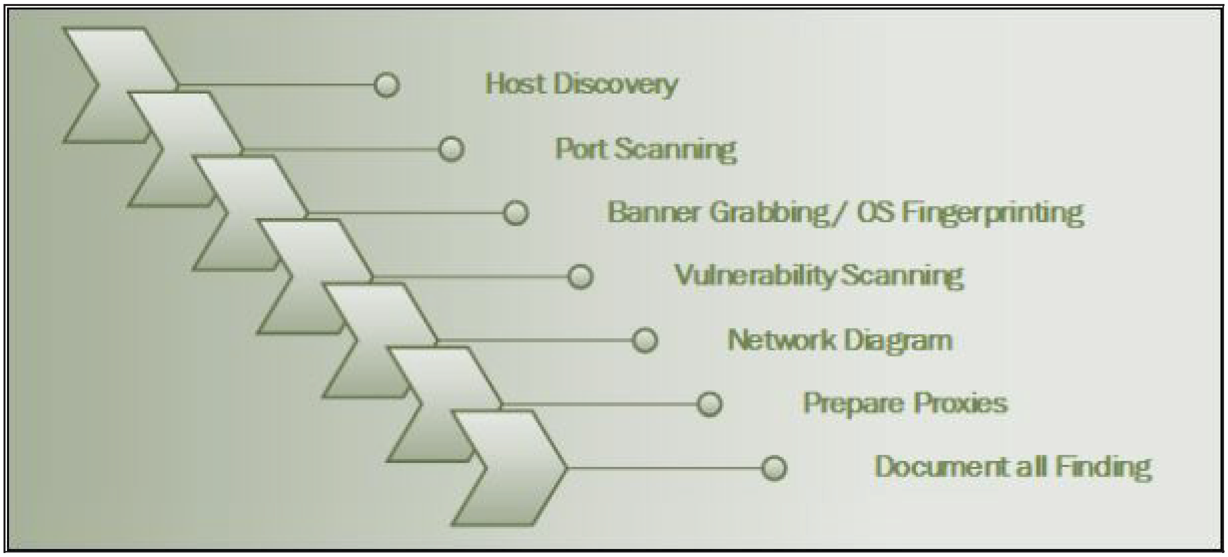


Figure 3-06 Scanning Pentesting

Checking for Live Systems

Initially, you must know about the hosts which are living in a targeted network. Finding live hosts in a network is done by ICMP Packets. The target replies ICMP Echo packets with ICMP echo reply. This response verifies that the host is live.

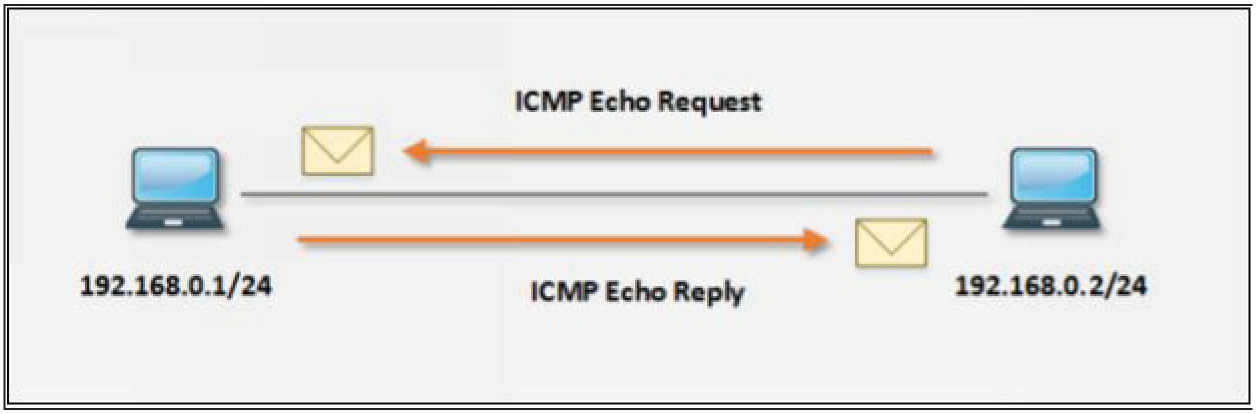
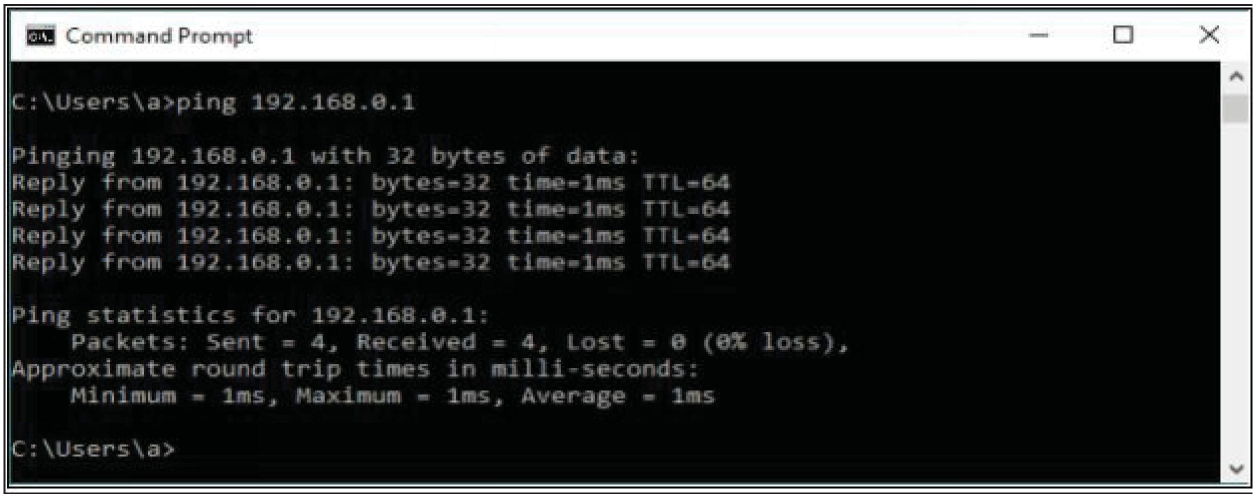


Figure 3-07 ICMP Echo Request & Reply Packets

The host having IP address 192.168.0.2/24 is trying to identify if the Host 192.168.0.1/24 is live by sending the ICMP Echo packets targeted to the destination IP address 192.168.0.1.

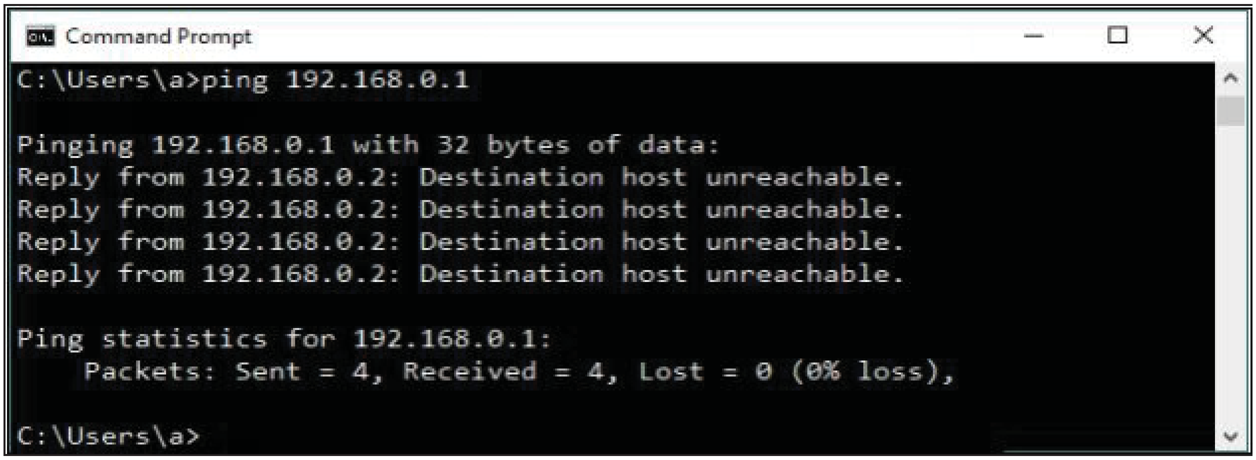


```
C:\Users\a>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\a>
```

Figure 3-08 ICMP Echo Reply Packets

If the destination host successfully responds to ICMP Echo packets, the host is live.

If the host is not live, Observe the following response of ICMP Echo packets.

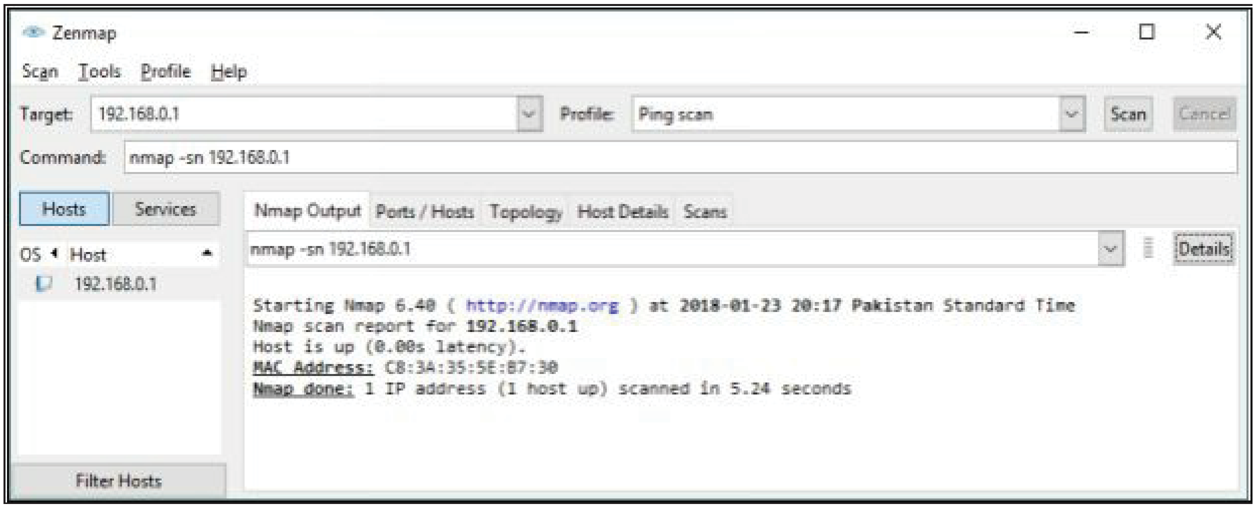


```
C:\Users\a>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\a>
```

Figure 3-09 ICMP Echo Reply Packets

ICMP Scanning

ICMP Scanning is a method of identifying live hosts by sending ICMP Echo requests to a host. ICMP Echo reply packet from host verify the host is live. Ping Scanning is a useful tool for not only identification of live host, but also for determining ICMP packet are passing through firewalls, and TTL value.



Target: 192.168.0.1
Profile: Ping scan
Command: nmap -sn 192.168.0.1

192.168.0.1

nmap -sn 192.168.0.1

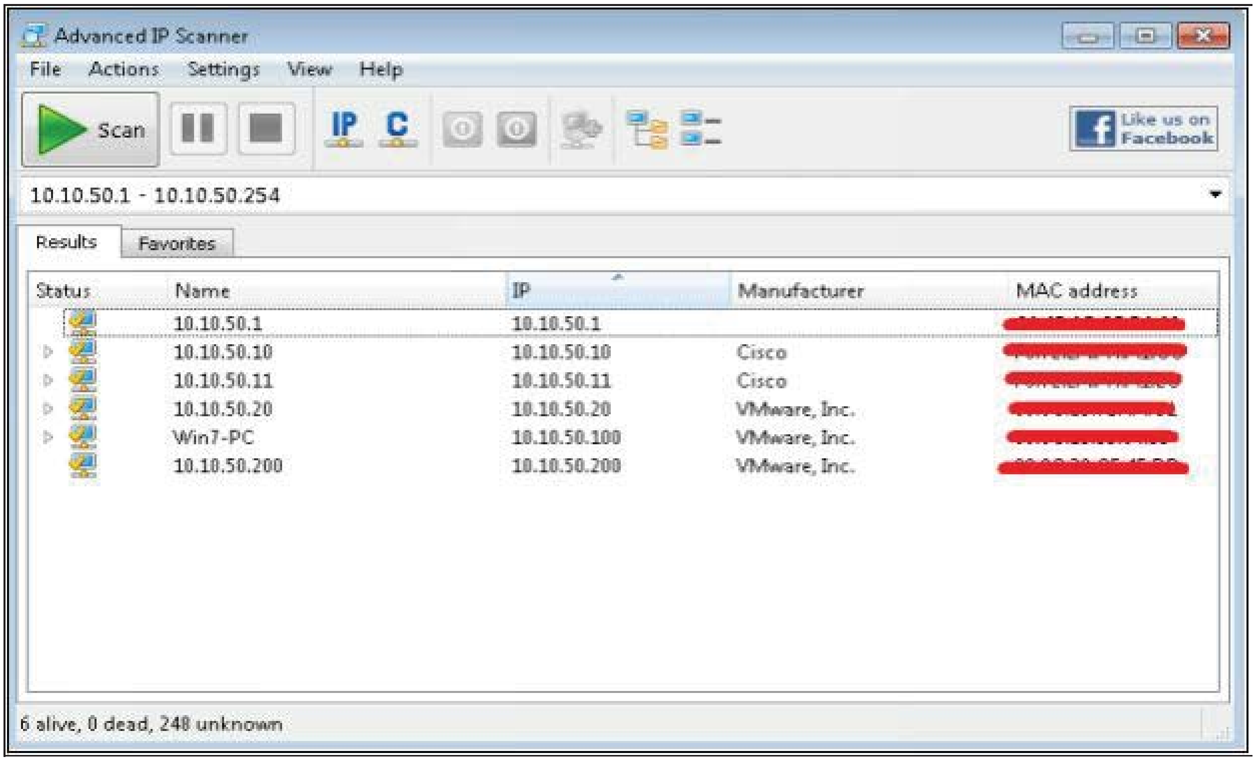
```
Starting Nmap 6.40 ( http://nmap.org ) at 2018-01-23 20:17 Pakistan Standard Time
Nmap scan report for 192.168.0.1
Host is up (0.00s latency).
MAC Address: C8:3A:35:5E:87:30
Nmap done: 1 IP address (1 host up) scanned in 5.24 seconds
```

Figure 3-10 ICMP Scanning

Ping Sweep

Ping Sweep determines live host on a large scale. Ping Sweep is a method of sending ICMP Echo Request packets to a range of IP addresses instead of sending one by one requests and observing the response. Live hosts respond with ICMP Echo Reply packets. Thus, instead of probing individually, we can probe a range of IPs using Ping Sweep. There are several tools available for Ping Sweep. Using these ping sweep tools such as SolarWinds Ping Sweep tool or Angry IP Scanner, you can ping the range of IP addresses.

Additionally, they can perform reverse DNS lookup, resolve hostnames, bring MAC addresses, and Scan ports.



10.10.50.1 - 10.10.50.254

Status	Name	IP	Manufacturer	MAC address
	10.10.50.1	10.10.50.1		[redacted]
	10.10.50.10	10.10.50.10	Cisco	[redacted]
	10.10.50.11	10.10.50.11	Cisco	[redacted]
	10.10.50.20	10.10.50.20	VMware, Inc.	[redacted]
	Win7-PC	10.10.50.100	VMware, Inc.	[redacted]
	10.10.50.200	10.10.50.200	VMware, Inc.	[redacted]

6 alive, 0 dead, 248 unknown

Figure 3-11 Ping Sweep

Check for Open Ports

SSDP Scanning

Simple Service Discovery Protocol (SSDP) is a protocol used for discovery of network services without the assistance of server-based configuration like Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) and static network host configuration. SSDP protocol can discover Plug & Play devices, with UPnP (Universal Plug and Play). SSDP protocol is compatible with IPv4 and IPv6.

Scanning Tool

1. **Nmap**

Another way to ping a host is by performing a ping using nmap. Using Windows or Linux command prompt, enter the following command: -

```
nmap –sP –v <target IP address>
```

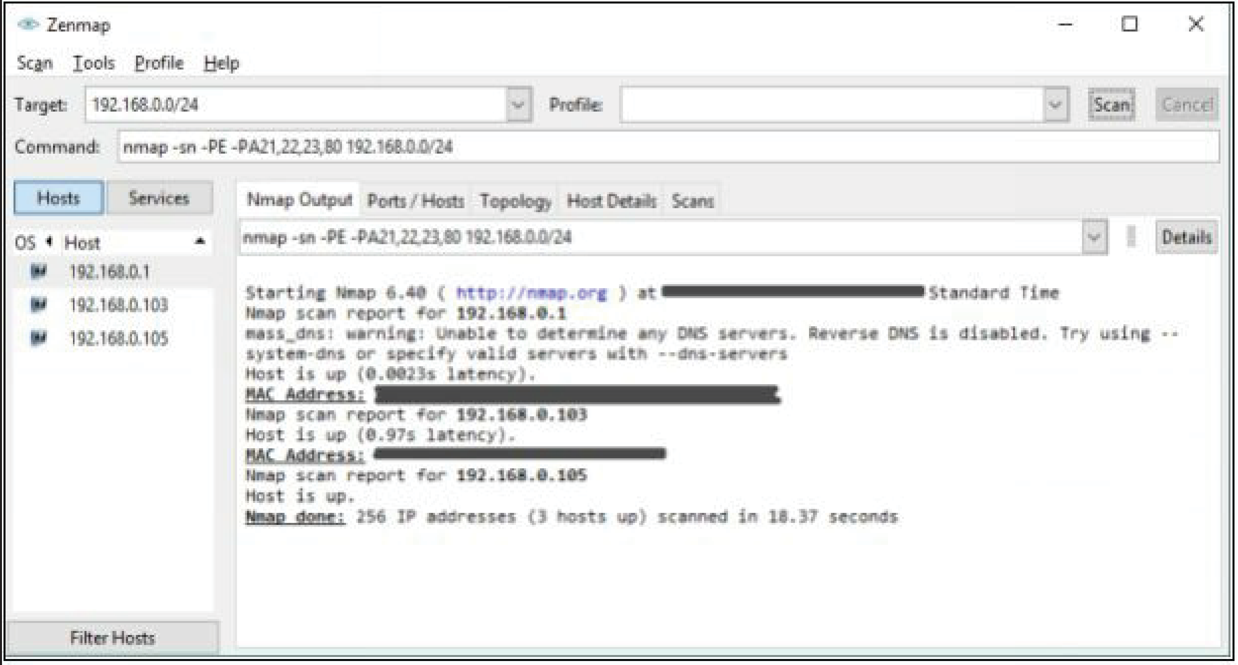
Upon successful response from the targeted host, If the command successfully finds a live host, it returns a message indicating that the IP address of the targeted host is up, along with the media access control (MAC) address and the network card vendor.

Apart from ICMP Echo Request packets and using ping sweep, nmap also offers a quick scan. Enter the following command for quick scan: -

nmap –sP –PE –PA<*port numbers*> <*starting IP/ending IP*>

For example,

nmap –sP –PE –PA 21,23,80,3389 <192.168.0.1-50>


Zenmap
Scan Tools Profile Help
Target: 192.168.0.0/24
Profile:
Scan
Cancel
Command: nmap -sn -PE -PA21,22,23,80 192.168.0.0/24
Hosts
Services
OS Host
192.168.0.1
192.168.0.103
192.168.0.105
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sn -PE -PA21,22,23,80 192.168.0.0/24
Details
Filter Hosts

```
Starting Nmap 6.40 ( http://nmap.org ) at [redacted] Standard Time
Nmap scan report for 192.168.0.1
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-servers
Host is up (0.0023s latency).
MAC Address: [redacted]
Nmap scan report for 192.168.0.103
Host is up (0.97s latency).
MAC Address: [redacted]
Nmap scan report for 192.168.0.105
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 18.37 seconds
```

Figure 3-12 Nmap

Nmap in a nutshell, offers Host discovery, Port discovery, Service discovery. Operating system version information. Hardware (MAC) address information, Service version detection, Vulnerability & exploit detection using Nmap scripts (NSE).

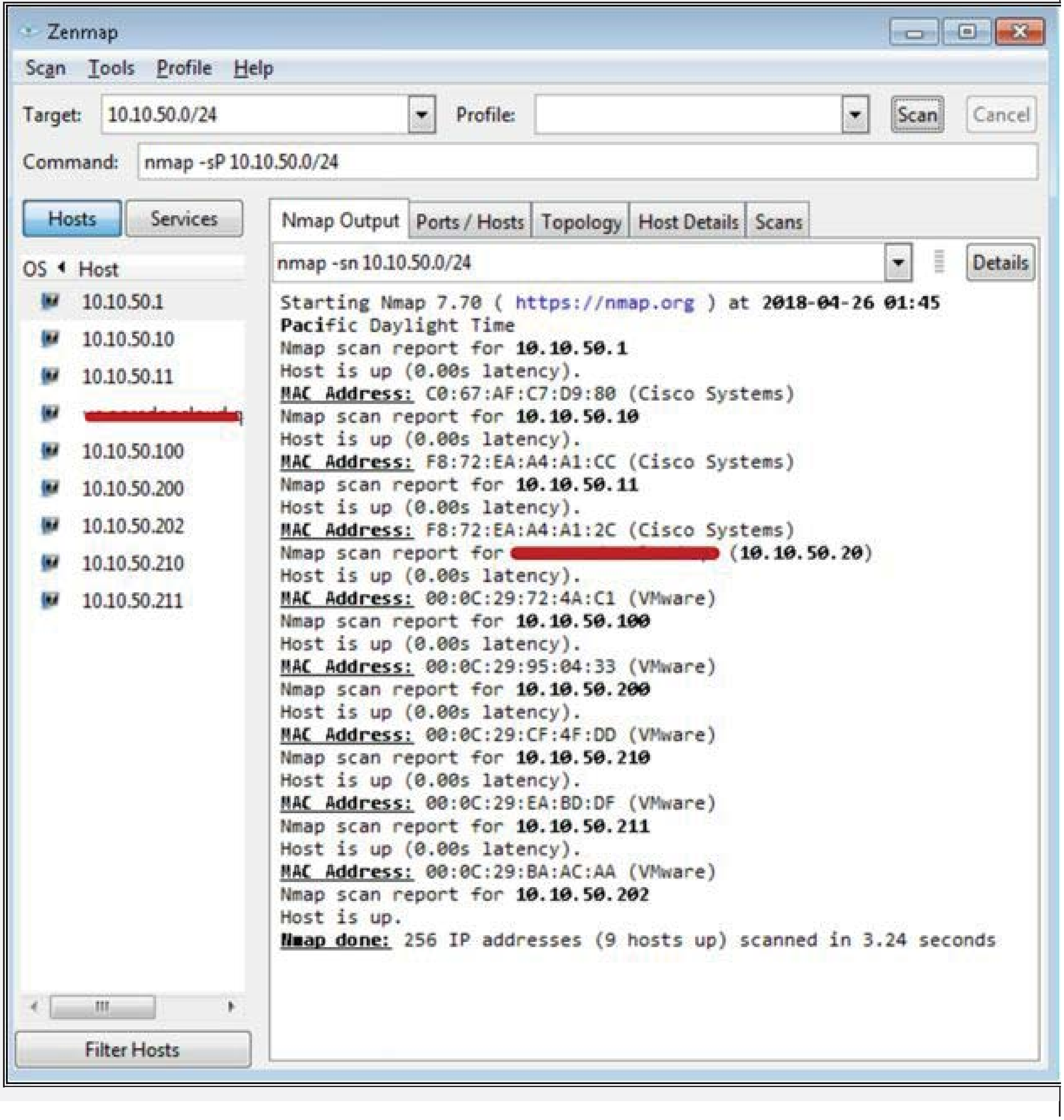
Lab 3-1: Hping Commands:

Case Study: Using Zenmap application, Performing Nmap scanning with its different options. We are using a Windows 7 PC for scanning the network.

Procedure:

Performing ping scans the network 10.10.50.0/24, listing machines that respond to ping.

Command: **nmap –sP 10.10.50.0/24**



Target: 10.10.50.0/24

Profile:

Command: nmap -sP 10.10.50.0/24

- 10.10.50.1
- 10.10.50.10
- 10.10.50.11
- [redacted]
- 10.10.50.100
- 10.10.50.200
- 10.10.50.202
- 10.10.50.210
- 10.10.50.211

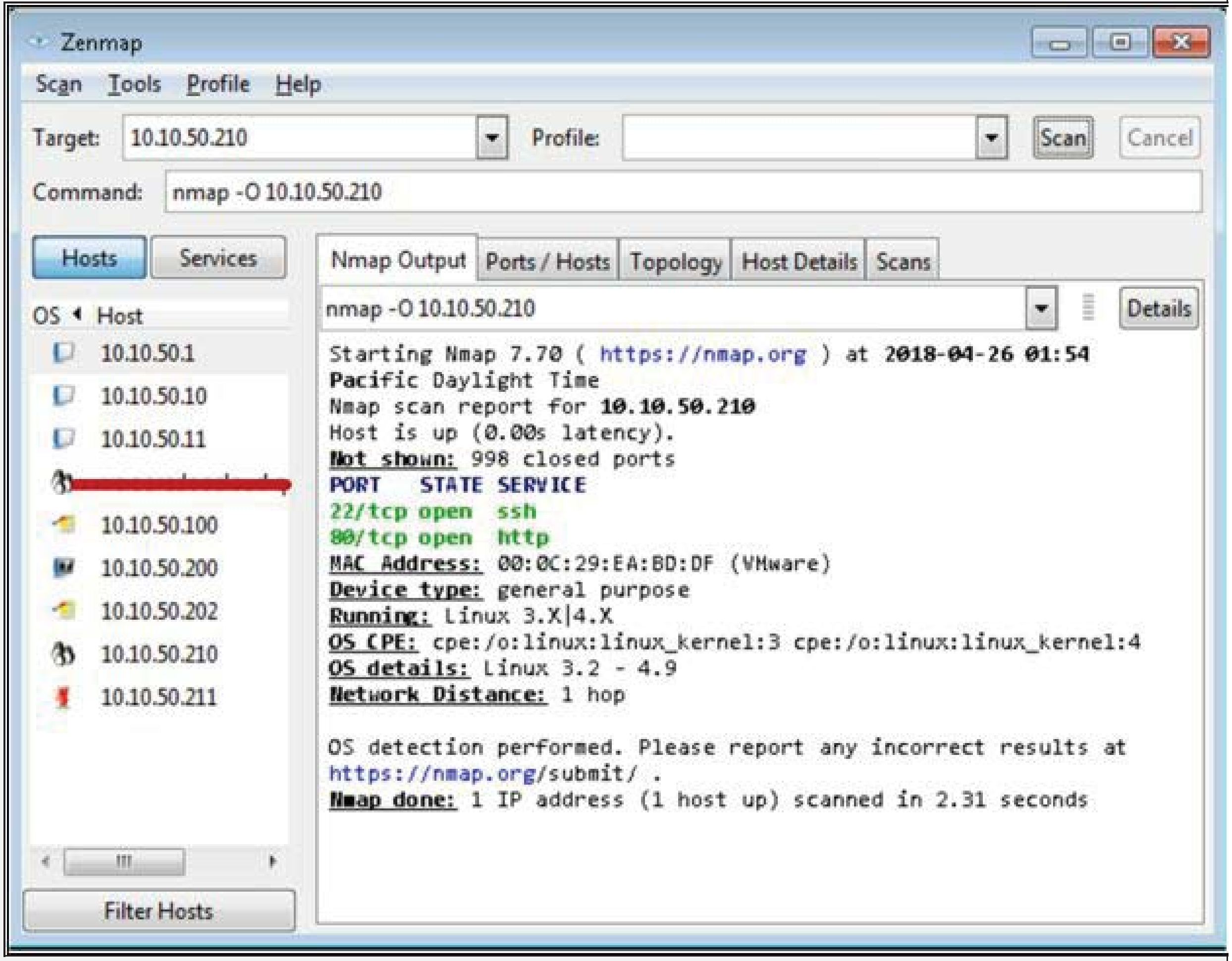
nmap -sn 10.10.50.0/24

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-26 01:45
Pacific Daylight Time
Nmap scan report for 10.10.50.1
Host is up (0.00s latency).
MAC Address: C0:67:AF:C7:D9:80 (Cisco Systems)
Nmap scan report for 10.10.50.10
Host is up (0.00s latency).
MAC Address: F8:72:EA:A4:A1:CC (Cisco Systems)
Nmap scan report for 10.10.50.11
Host is up (0.00s latency).
MAC Address: F8:72:EA:A4:A1:2C (Cisco Systems)
Nmap scan report for [redacted] (10.10.50.20)
Host is up (0.00s latency).
MAC Address: 00:0C:29:72:4A:C1 (VMware)
Nmap scan report for 10.10.50.100
Host is up (0.00s latency).
MAC Address: 00:0C:29:95:04:33 (VMware)
Nmap scan report for 10.10.50.200
Host is up (0.00s latency).
MAC Address: 00:0C:29:CF:4F:DD (VMware)
Nmap scan report for 10.10.50.210
Host is up (0.00s latency).
MAC Address: 00:0C:29:EA:BD:DF (VMware)
Nmap scan report for 10.10.50.211
Host is up (0.00s latency).
MAC Address: 00:0C:29:BA:AC:AA (VMware)
Nmap scan report for 10.10.50.202
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 3.24 seconds
```

Figure 3-13 Nmap ping Sweep

Now, scanning for Operating System details of target host 10.10.50.210. We can scan for all host using command **nmap –O 10.10.50.***

Command: **nmap –O 10.10.50.210**



Target: 10.10.50.210

Command: nmap -O 10.10.50.210

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-26 01:54
Pacific Daylight Time
Nmap scan report for 10.10.50.210
Host is up (0.00s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:EA:BD:DF (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
```

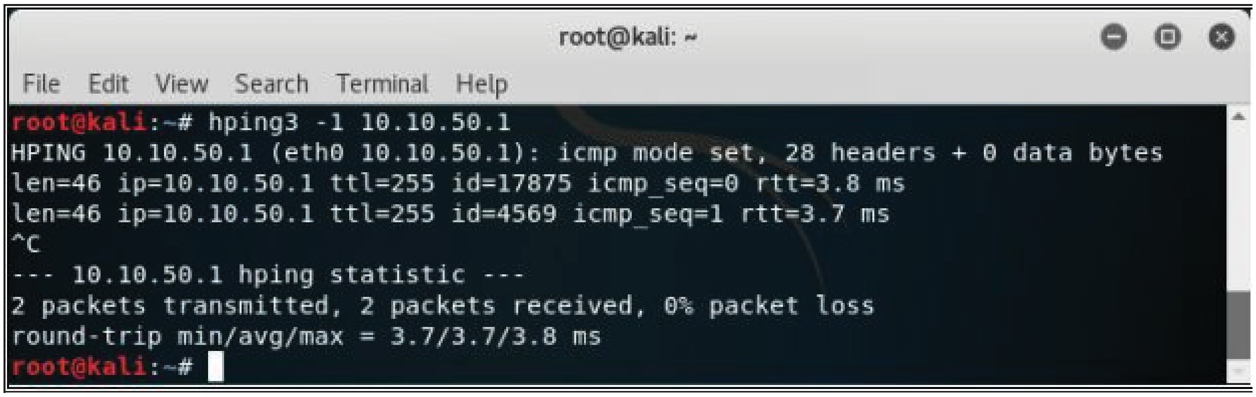
Figure 3-14 Nmap OS Scanning

2. Hping2 & Hping3

Hping is a command-line TCP/IP packet assembler and analyzer tool that is used to send customized TCP/IP packets and display the target reply as ping command display the ICMP Echo Reply packet from targeted host. Hping can also handle fragmentation, arbitrary packets body, and size and file transfer. It supports TCP, UDP, ICMP and RAW-IP protocols. Using Hping, the following parameters can be performed: -

- Test firewall rules.

- Advanced port scanning.
- Testing net performance.
- Path MTU discovery.
- Transferring files between even fascist firewall rules.
- Traceroute-like under different protocols.
- Remote OS fingerprinting & others.



```
root@kali:~# hping3 -1 10.10.50.1
HPING 10.10.50.1 (eth0 10.10.50.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.10.50.1 ttl=255 id=17875 icmp_seq=0 rtt=3.8 ms
len=46 ip=10.10.50.1 ttl=255 id=4569 icmp_seq=1 rtt=3.7 ms
^C
--- 10.10.50.1 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.7/3.7/3.8 ms
root@kali:~# 
```

Figure 3-15 Hping3

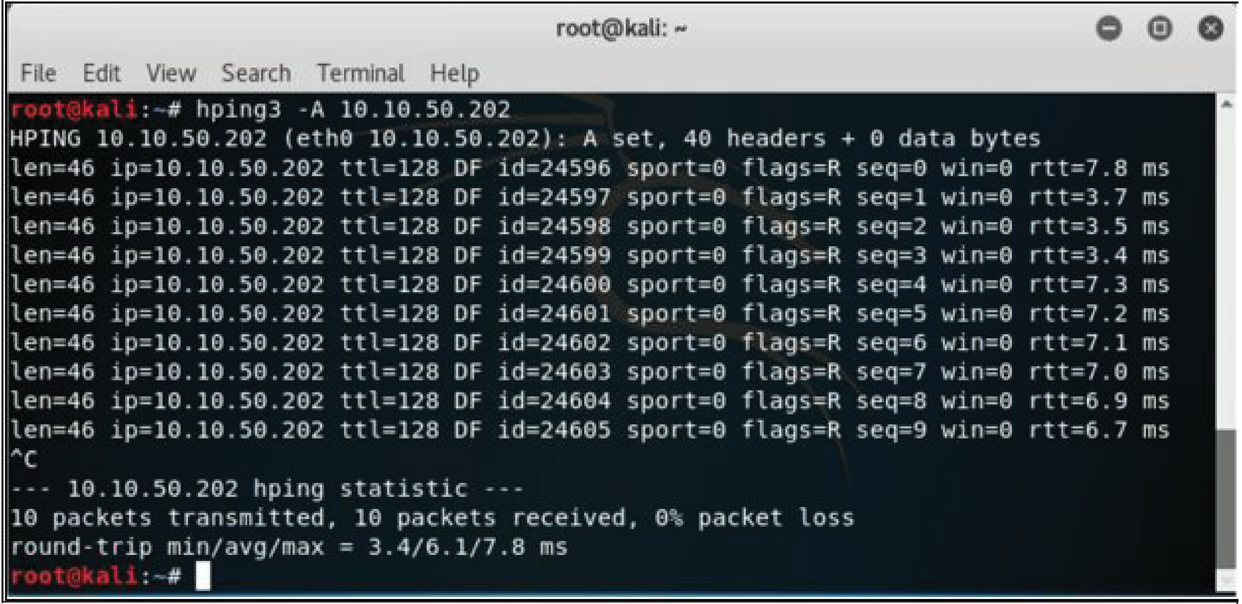
Lab 3-2: Hping Commands:

Case Study: Using Hping commands on Kali Linux, we are pinging a Window 7 host with different customized packets in this lab.

Commands:

To create an ACK packet:

root@kali:~# **hping3 –A 192.168.0.1**

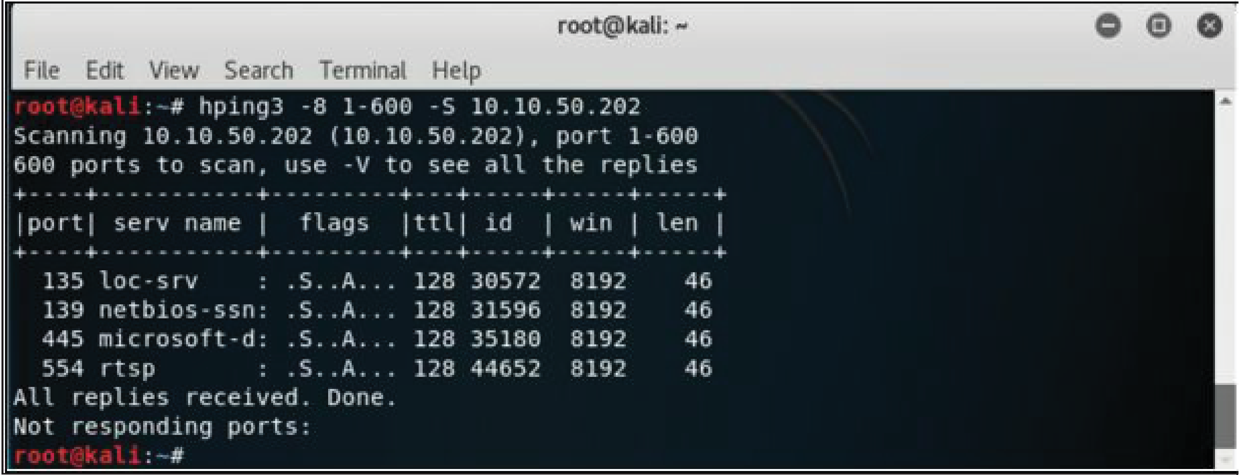


```
root@kali:~# hping3 -A 10.10.50.202
HPING 10.10.50.202 (eth0 10.10.50.202): A set, 40 headers + 0 data bytes
len=46 ip=10.10.50.202 ttl=128 DF id=24596 sport=0 flags=R seq=0 win=0 rtt=7.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24597 sport=0 flags=R seq=1 win=0 rtt=3.7 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24598 sport=0 flags=R seq=2 win=0 rtt=3.5 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24599 sport=0 flags=R seq=3 win=0 rtt=3.4 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24600 sport=0 flags=R seq=4 win=0 rtt=7.3 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24601 sport=0 flags=R seq=5 win=0 rtt=7.2 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24602 sport=0 flags=R seq=6 win=0 rtt=7.1 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24603 sport=0 flags=R seq=7 win=0 rtt=7.0 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24604 sport=0 flags=R seq=8 win=0 rtt=6.9 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24605 sport=0 flags=R seq=9 win=0 rtt=6.7 ms
^C
--- 10.10.50.202 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 3.4/6.1/7.8 ms
root@kali:~#
```

Figure 3-16 Sending customized packet using the Hping3 command

To create SYN scan against different ports:

root@kali:~# **hping3 -8 1-600 –S 10.10.50.202**

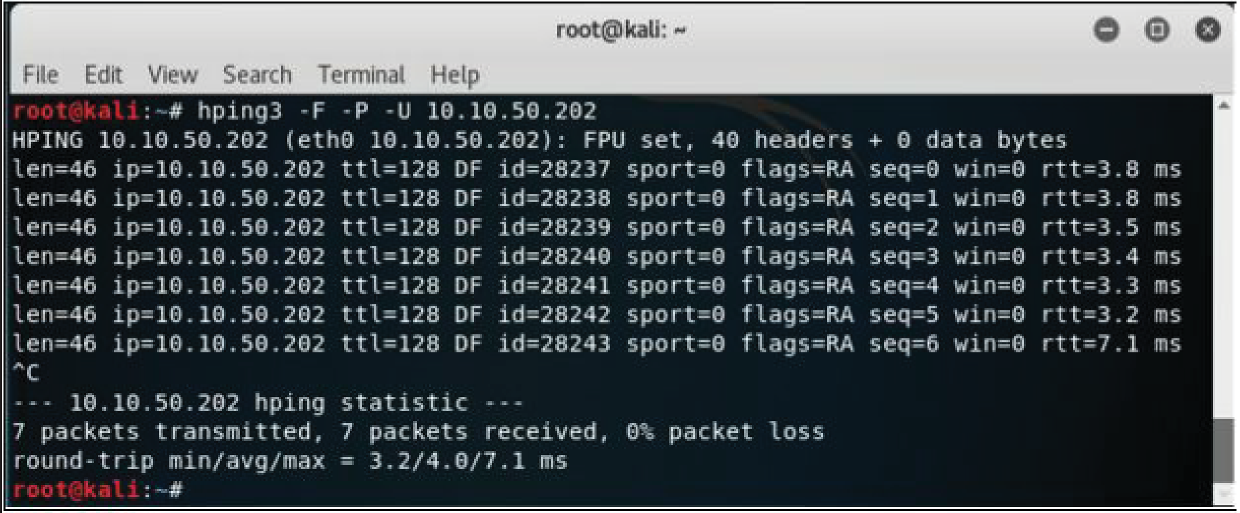


```
root@kali:~# hping3 -8 1-600 -S 10.10.50.202
Scanning 10.10.50.202 (10.10.50.202), port 1-600
600 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
  135 loc-srv    : .S..A... 128 30572  8192    46
  139 netbios-ssn: .S..A... 128 31596  8192    46
  445 microsoft-d: .S..A... 128 35180  8192    46
  554 rtsp       : .S..A... 128 44652  8192    46
All replies received. Done.
Not responding ports:
root@kali:~#
```

Figure 3-17 Sending customized packet using the Hping3 command

To create a packet with FIN, URG, and PSH flags sets

root@kali:~# **hping3 –F –P -U 10.10.50.202**



```
root@kali:~# hping3 -F -P -U 10.10.50.202
HPING 10.10.50.202 (eth0 10.10.50.202): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.50.202 ttl=128 DF id=28237 sport=0 flags=RA seq=0 win=0 rtt=3.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28238 sport=0 flags=RA seq=1 win=0 rtt=3.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28239 sport=0 flags=RA seq=2 win=0 rtt=3.5 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28240 sport=0 flags=RA seq=3 win=0 rtt=3.4 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28241 sport=0 flags=RA seq=4 win=0 rtt=3.3 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28242 sport=0 flags=RA seq=5 win=0 rtt=3.2 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28243 sport=0 flags=RA seq=6 win=0 rtt=7.1 ms
^C
--- 10.10.50.202 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 3.2/4.0/7.1 ms
root@kali:~#
```

Figure 3-18 Sending customized packet using the Hping3 command

The following are some options used with Hping command: -

-h	--help	Show help
-v	--version	Show Version
-c	--count	Packet Count
-I	--interface	Interface Name
	--flood	Send packets as fast as possible. Don't show replies.
-V	--verbose	Verbose Mode
-0	--rawip	RAW IP Mode
-1	--icmp	ICMP Mode
-2	--udp	UDP Mode
-8	--scan	Scan Mode
-9	--listen	Listen Mode
	--rand-dest	Random Destination Address Mode
	--rand-source	Random Source Address Mode
-s	--baseport	base source port (default random)
-p	--destport	[+][+]<port> destination port(default 0) ctrl+z

		inc/dec
-Q	--seqnum	Shows only TCP sequence number
-F	--fin	Set FIN flag
-S	--syn	Set SYN flag
-P	--push	Set PUSH flag
-A	--ack	Set ACK flag
-U	--urg	Set URG flag
	--TCP-timestamp	Enable the TCP timestamp option to guess the HZ/uptime

Table 3-02 Hping3 Command Options

Scanning Techniques

Scanning techniques include UDP & TCP Scanning technique. Observe the following figure showing the classification of Scanning techniques: -

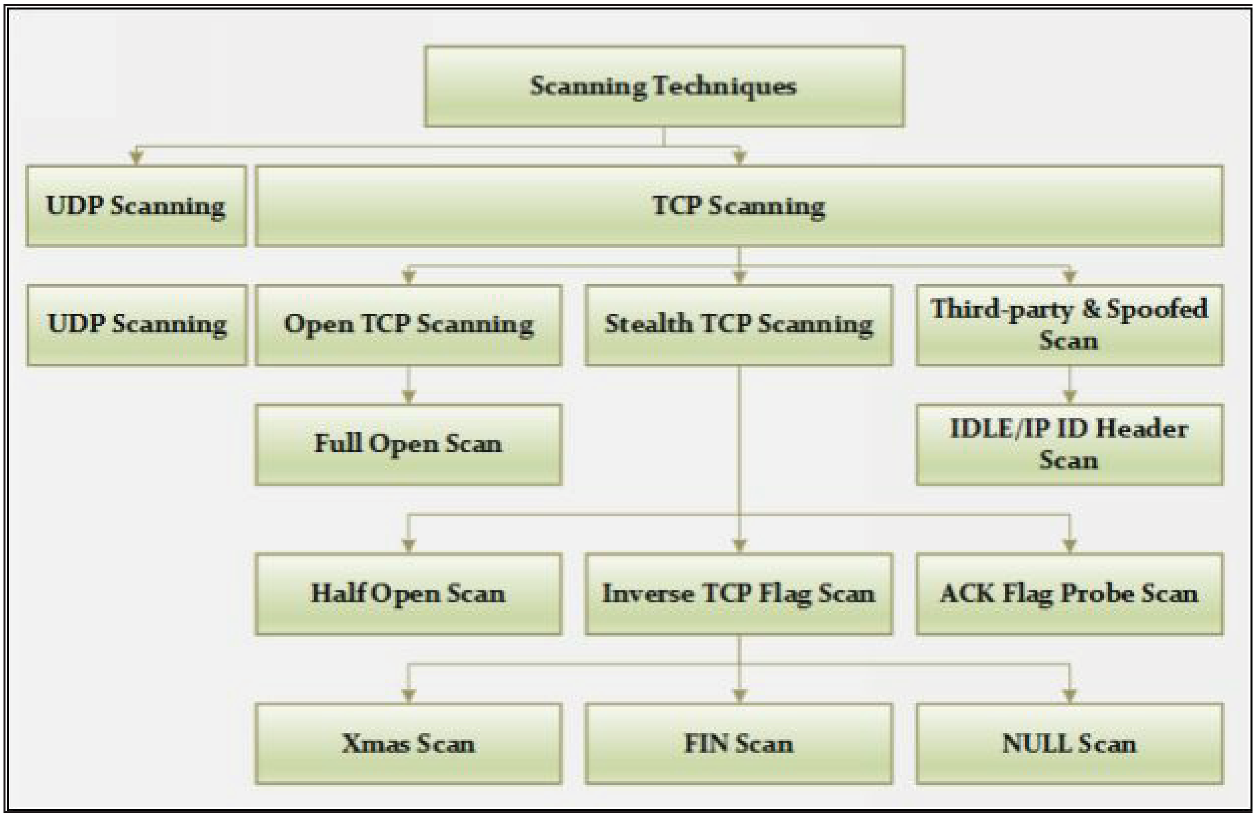


Figure 3-19 Scanning Techniques

TCP Connect / Full Open Scan

Full Open Scan is the type of Scanning technique in which Three-way handshaking session initiates and completed. Full Open Scanning ensures the response that the targeted host is live and the connection is complete. It is a major advantage of Full Open Scanning. However, it can be detected, logged by security devices such as Firewalls and IDS. TCP Connect / Full Open Scan does not require Super User Privileges.

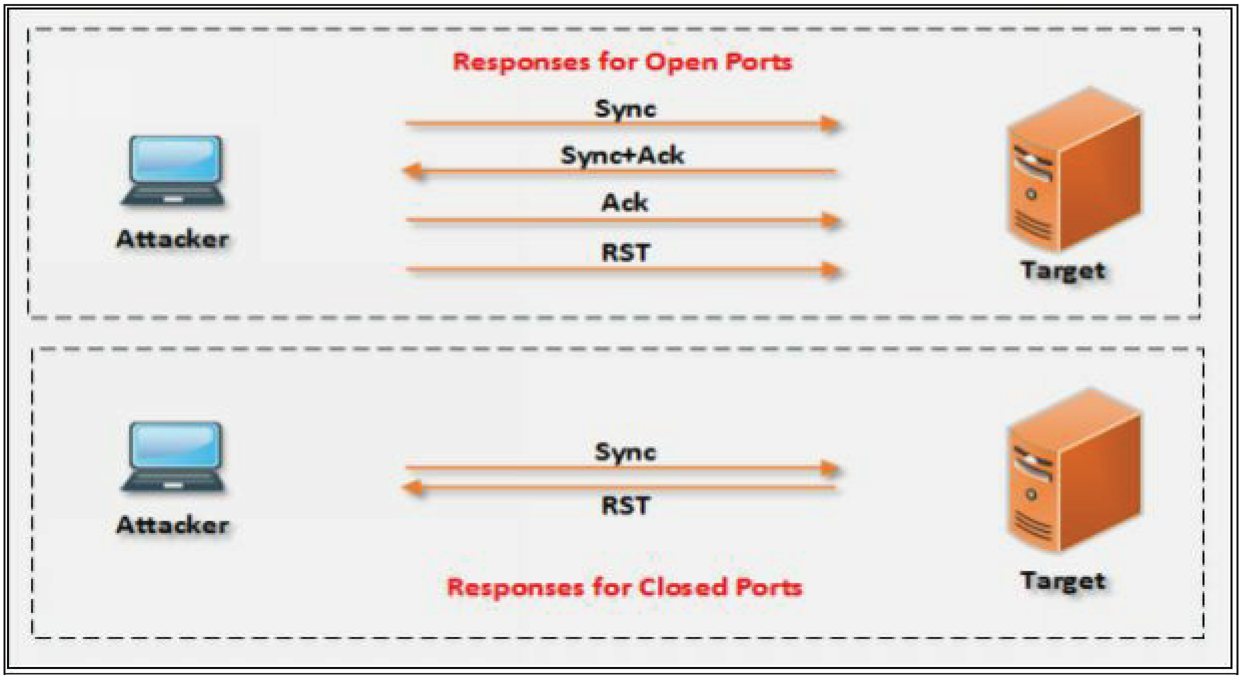


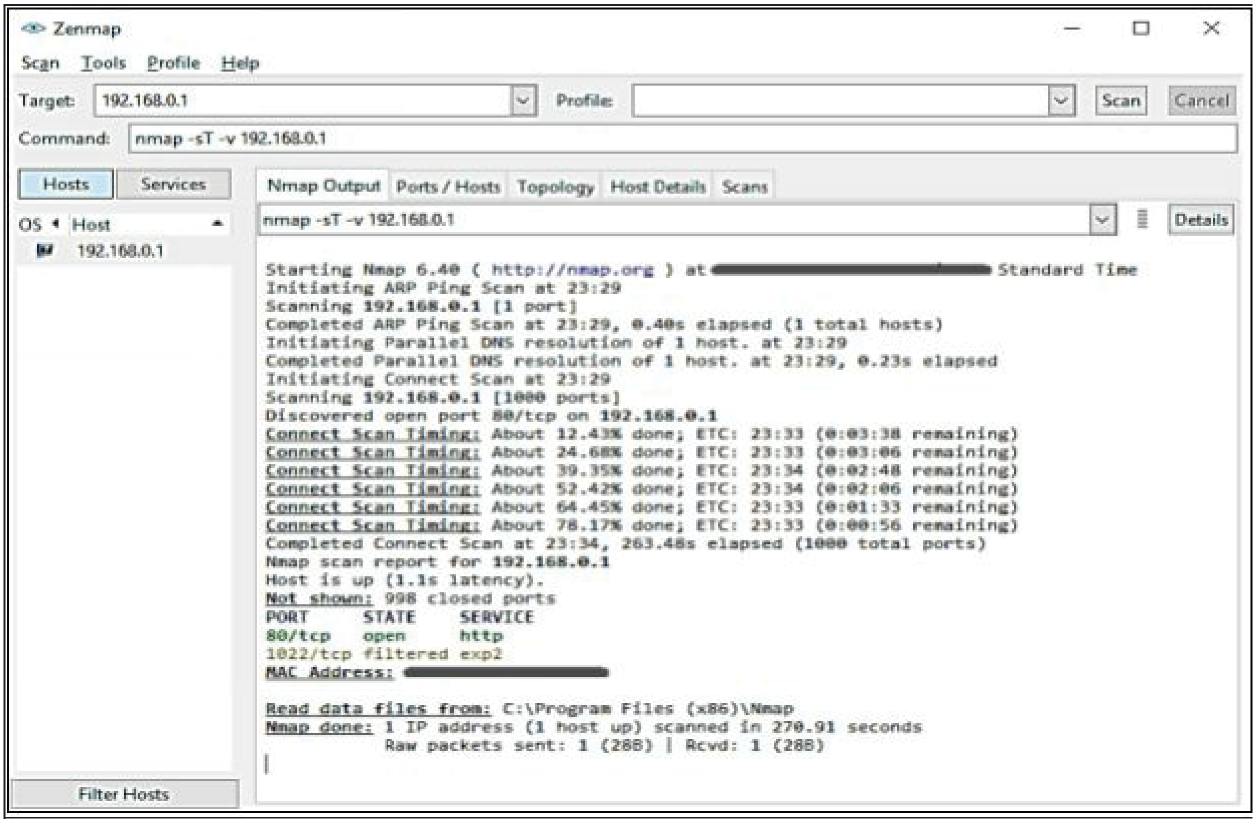
Figure 3-20 TCP Connection Responses

While using Full Open Scanning and a Closed port is encountered, RST response is sent to the incoming request to terminate the attempt. To perform Full Open Scan, you must use -sT option for Connect Scan.

Type the command to execute Full Open Scan: -

```
nmap –sT <ip address or range>
```

For example, observe the output shown in the figure below, using Zenmap tool to perform Full Open Scan.



```
nmap -sT -v 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at [redacted] Standard Time
Initiating ARP Ping Scan at 23:29
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 23:29, 0.40s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:29
Completed Parallel DNS resolution of 1 host. at 23:29, 0.23s elapsed
Initiating Connect Scan at 23:29
Scanning 192.168.0.1 [1000 ports]
Discovered open port 80/tcp on 192.168.0.1
Connect Scan Timing: About 12.43% done; ETC: 23:33 (0:03:38 remaining)
Connect Scan Timing: About 24.68% done; ETC: 23:33 (0:03:06 remaining)
Connect Scan Timing: About 39.35% done; ETC: 23:34 (0:02:48 remaining)
Connect Scan Timing: About 52.42% done; ETC: 23:34 (0:02:06 remaining)
Connect Scan Timing: About 64.45% done; ETC: 23:33 (0:01:33 remaining)
Connect Scan Timing: About 78.17% done; ETC: 23:33 (0:00:56 remaining)
Completed Connect Scan at 23:34, 263.48s elapsed (1000 total ports)
Nmap scan report for 192.168.0.1
Host is up (1.1s latency).
Not shown: 998 closed ports
PORT      STATE    SERVICE
80/tcp    open     http
1022/tcp filtered exp2
MAC Address: [redacted]

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 270.91 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

Figure 3-21 Full Open Scan

Stealth Scan (Half-open Scan)

Half-Open Scan is also known as Stealth Scan. To understand the Half-Open Scan processes, Consider the scenario of two hosts, Host A & Host B. Host A is the initiator of the TCP connection handshaking. Host A sends the Sync packet to initiate the handshaking. Receiving host (Host B) replies with Sync+Ack packet. Host A, Instead of Acknowledging the Host B with Ack packet, it responds with RST.

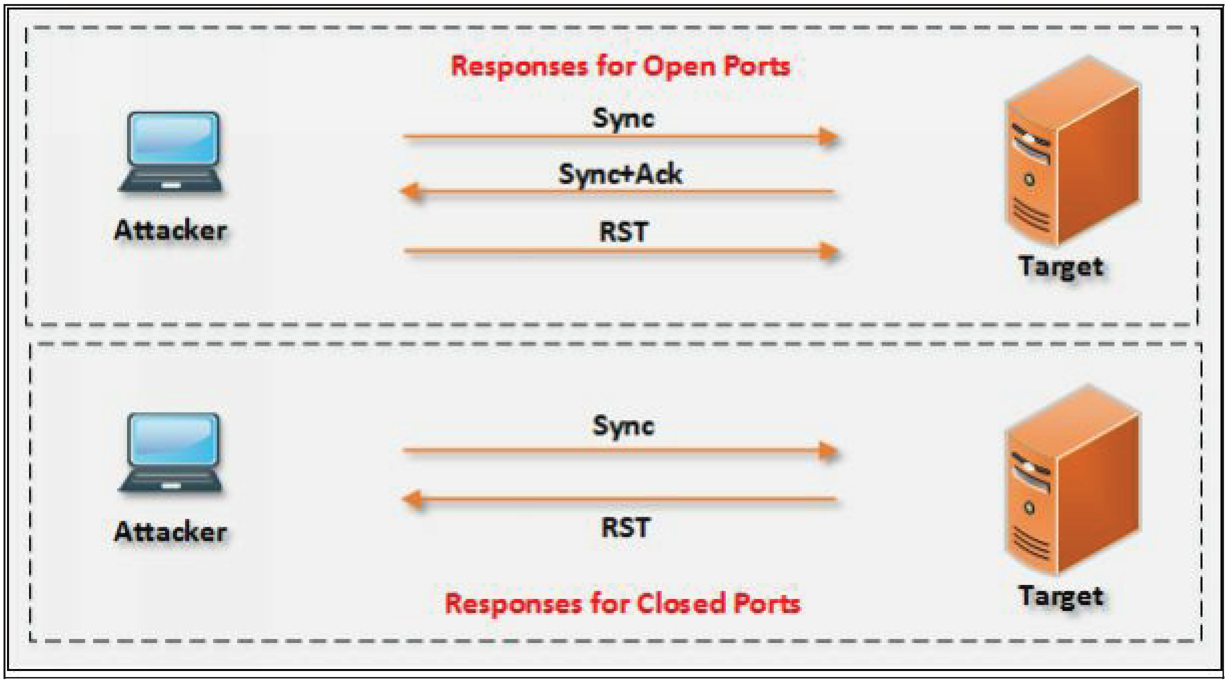
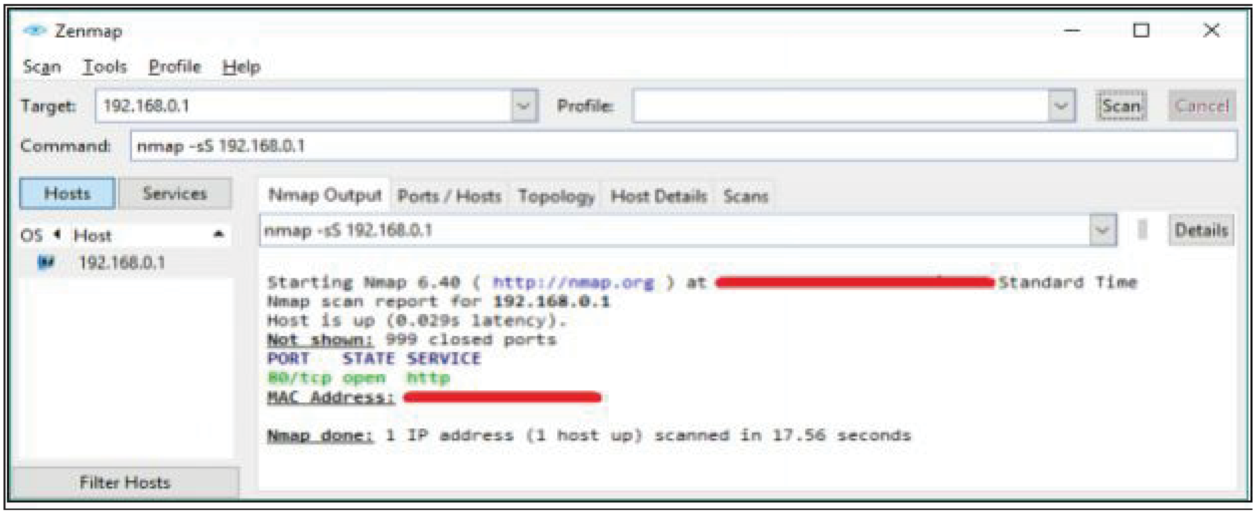


Figure 3-21 Half-Open Scan

To perform this type of scan in nmap use the syntax:

nmap –sS <*ip address or range*>

Observe the result in the following figure: -



Target: 192.168.0.1

Profile:

Command: nmap -sS 192.168.0.1

```
nmap -sS 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at [redacted] Standard Time
Nmap scan report for 192.168.0.1
Host is up (0.029s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
80/tcp open  http
MAC Address: [redacted]

Nmap done: 1 IP address (1 host up) scanned in 17.56 seconds
```

Figure 3-22 Half-Open Scan

Inverse TCP Flag Scanning

Inverse TCP Flag Scanning is the Scanning process in which Sender either send TCP probe with TCP flags, i.e. FIN, URG, and PSH or without Flags. Probes with TCP flags is known as XMAS Scanning. In case, if there is no flag set, it is known as Null Scanning.

Xmas Scan

Xmas Scan is the type of scan in which contains multiple flags. Packet sent to the target along with URG, PSH & FIN; or a packet having all flags creates an abnormal situation for the receiver. Receiving system has to take a decision when this condition occurs. Closed port responds with single RST packet. If the port is open, some systems respond as an open port, but the modern system ignores or dropped these requests because the combination of these flags is bogus. FIN Scan works only with Operating Systems with RFC-793 based TCP/IP Implementation. FIN Scan does not work with any current version of Windows typically Windows XP or later.

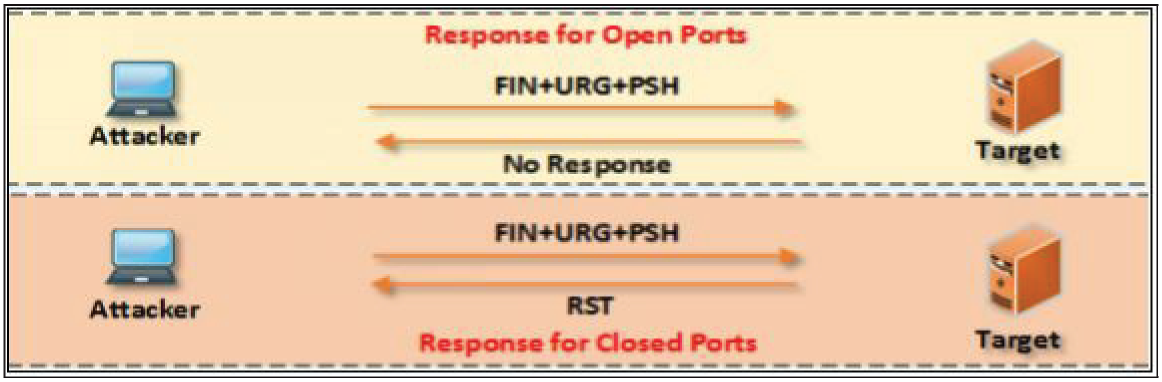


Figure 3-23 Xmas Scan

To perform this type of scan, use the syntax:

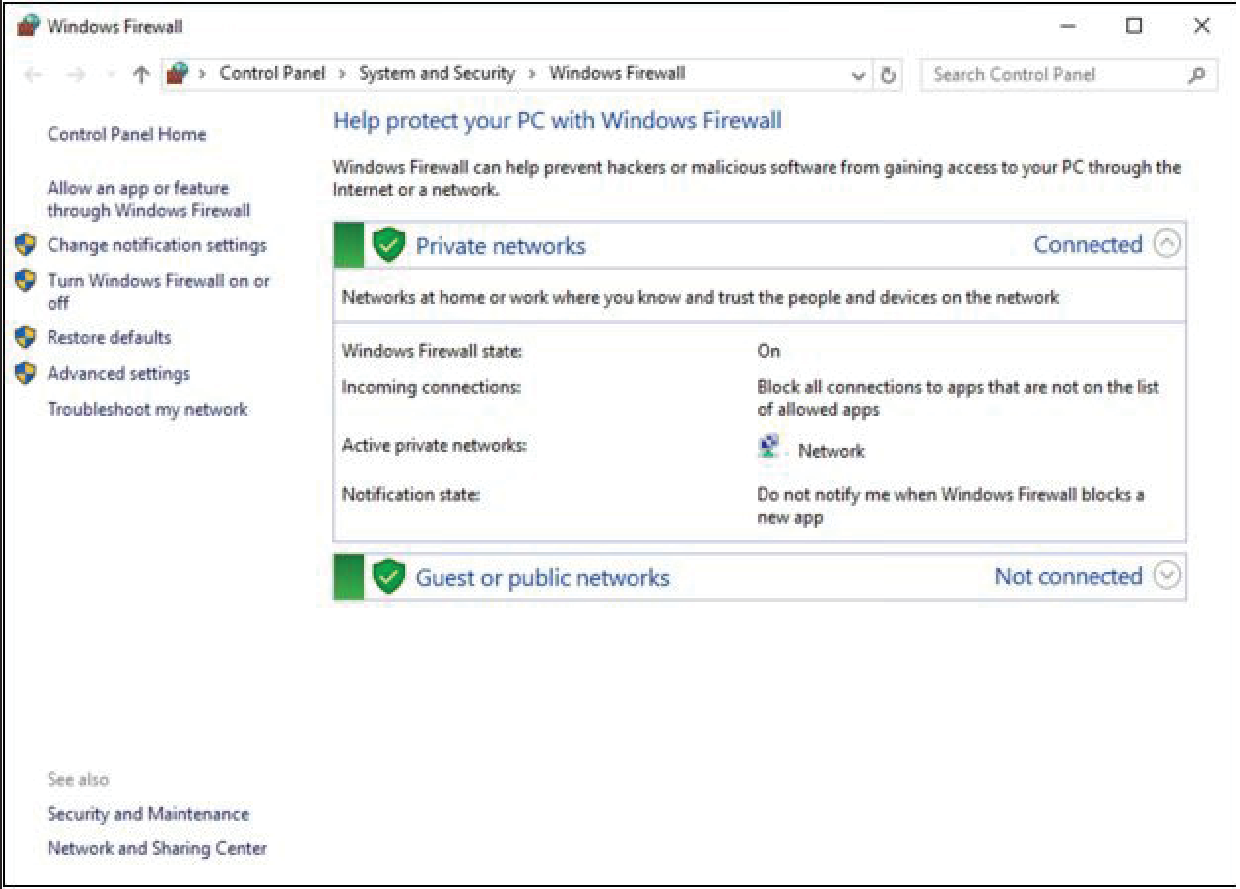
```
nmap –sX -v <ip address or range>
```

Lab 3-3: Xmas Scanning

Case Study: Using Xmas Scanning on Kali Linux, we are pining a Window Server 2016 host with firewall enabled & disabled state to observe the responses.

Procedure:

Open Windows Server 2016 & verify if the firewall is enabled.



Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — 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 apps that are not on the list of allowed apps

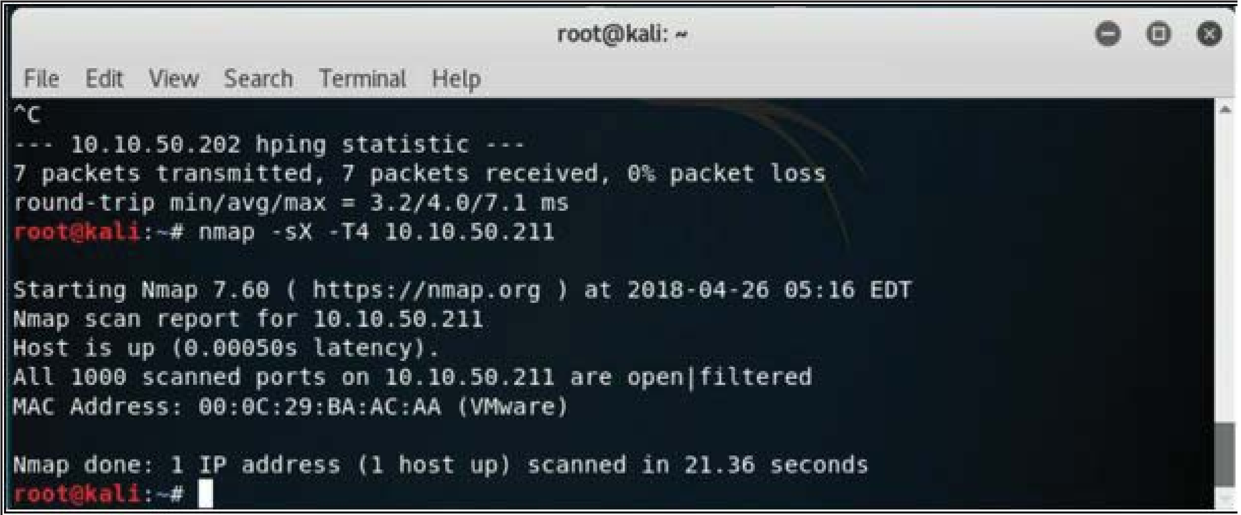
Active private networks: Network

Notification state: Do not notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

Figure 3-24 Windows Firewall settings

Open a terminal on your Kali Linux & enter the following command:

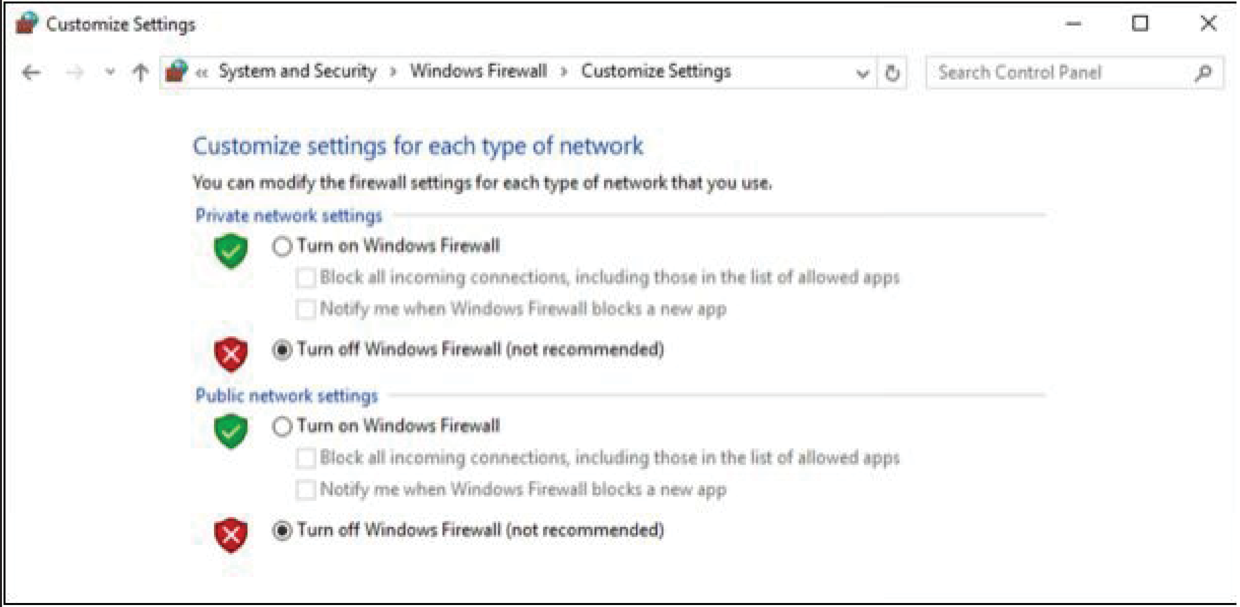


```
^C
--- 10.10.50.202 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 3.2/4.0/7.1 ms
root@kali:~# nmap -sX -T4 10.10.50.211

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-26 05:16 EDT
Nmap scan report for 10.10.50.211
Host is up (0.00050s latency).
All 1000 scanned ports on 10.10.50.211 are open|filtered
MAC Address: 00:0C:29:BA:AC:AA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.36 seconds
root@kali:~#
```

Figure 3-25 Xmas Scanning

Observe the output as shown above in the figure, all scanned ports are **Open** & **Filtered**. It means the firewall is enabled. A firewall basically not respond these packet hence assumed as Open & filtered ports.

Now, go back to Windows Server 2016 and disable the Firewall.



Customize Settings
« System and Security › Windows Firewall › Customize Settings
Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall

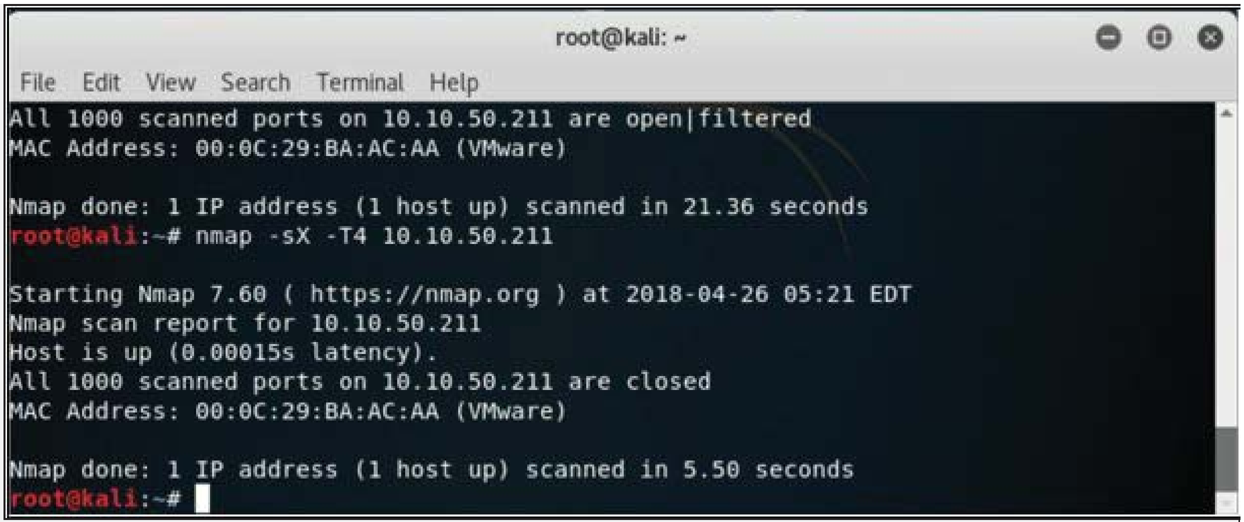
□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Figure 3-26 Disabling Firewall

Now again, run the scan.



```
All 1000 scanned ports on 10.10.50.211 are open|filtered
MAC Address: 00:0C:29:BA:AC:AA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.36 seconds
root@kali:~# nmap -sX -T4 10.10.50.211

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-26 05:21 EDT
Nmap scan report for 10.10.50.211
Host is up (0.00015s latency).
All 1000 scanned ports on 10.10.50.211 are closed
MAC Address: 00:0C:29:BA:AC:AA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.50 seconds
root@kali:~#
```

Figure 3-27 Xmas Scanning

In this case, the firewall is disabled, hence showing all ports as closed.

FIN Scan

FIN Scan is the process of sending the packet having only FIN flag set. These packets can reliably pass the firewall. FIN Scan packets, when sent to the target, the port is considered to be open if there is no response. If the port is closed, RST is returned.

To perform this type of scan, use the syntax:

nmap –SF <*ip address or range*>

NULL Scan

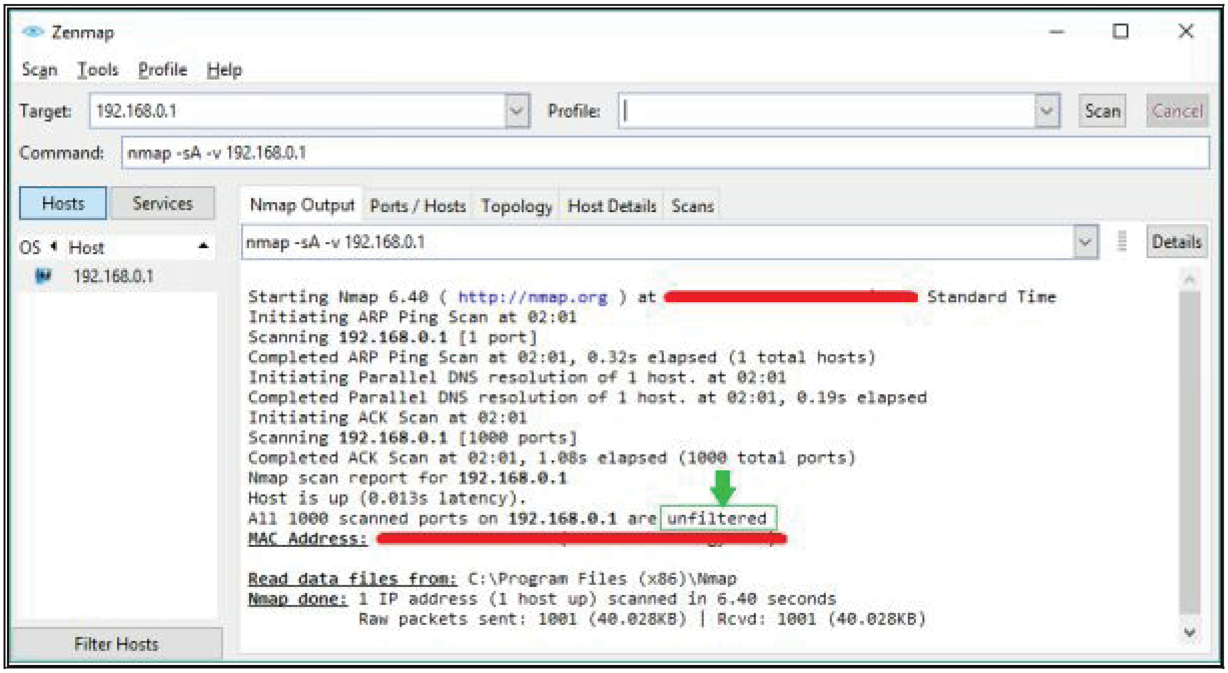
NULL Scan is the process of sending the packet without any flag set. Responses are similar to FIN and XMAS Scan. If Null Scan packet sends to an open port, it brings no response. If Null Scan packet sends to the closed port, it brings RST packet. Performing this scan is comparatively easier to be detected as there is logically no reason to send a TCP packet without any flag.

To perform this type of scan, use the syntax:

nmap –sN <*ip address or range*>

ACK Flag Probe Scanning

ACK flag Scanning technique sends TCP packet with ACK flag set towards the target. Sender Examine the header information because even when ACK packet has made its way to the target, it replies with RST packet either the port is open or closed. After Analyzing the header information such as TTL and WINDOW fields of RST packet, the attacker identifies if the port is open or closed.



Target: 192.168.0.1

Command: nmap -sA -v 192.168.0.1

Hosts: 192.168.0.1

```
nmap -sA -v 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at [redacted] Standard Time
Initiating ARP Ping Scan at 02:01
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 02:01, 0.32s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:01
Completed Parallel DNS resolution of 1 host. at 02:01, 0.19s elapsed
Initiating ACK Scan at 02:01
Scanning 192.168.0.1 [1000 ports]
Completed ACK Scan at 02:01, 1.08s elapsed (1000 total ports)
Nmap scan report for 192.168.0.1
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.0.1 are unfiltered
MAC Address: [redacted]

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 6.40 seconds
           Raw packets sent: 1001 (40.028KB) | Rcvd: 1001 (40.028KB)
```

Figure 3-28 Ack Flag Probe Scanning

ACK Probe scanning also helps in identifying the filtering system. If RST packet receives from the target, it means that packets toward this port are not filtering. If there is no response, it means Stateful firewall is filtering the port.

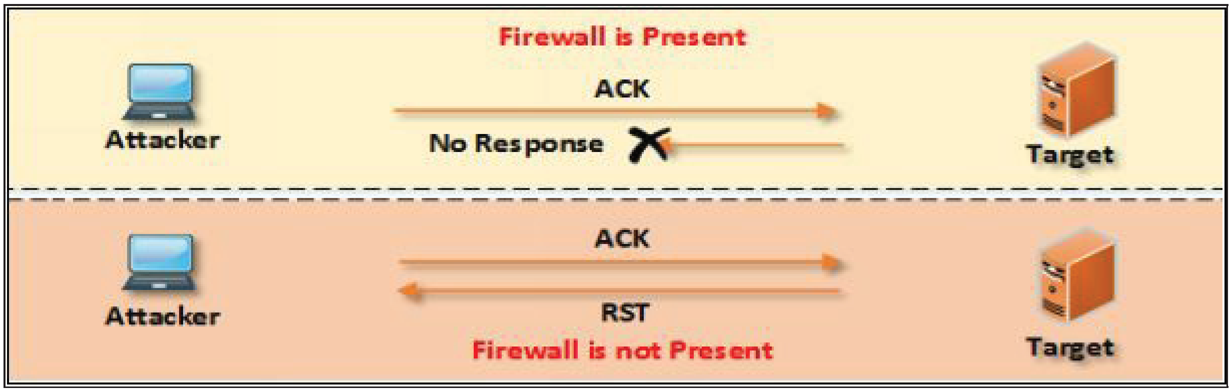


Figure 3-29 Ack Flag Probe Scanning Response

IDLE/IPID Header Scan

IDLE / IPID Header Scan is a unique and effective technique to identify the target host port status. Using this scan is capable of remaining low profile. Idle scanning describes the hiding ability of attacker. Attacker hides its identity by instead of sending the packet through its system, the scanning process done by bouncing packets from Zombie's system. If target investigates the threat, it traces Zombie instead of tracing the attacker.

Before understanding the Step required for IDLE/IPID Scan, you must know recall some important point: -

- To determine an Open port, send SYN packet to the port.
- Target machine responds with SYN+ACK packet if the port is open.
- Target Machine responds with RST packet if the port is closed.
- The unsolicited SYN+ACK packet is either ignored, responded with RST.
- Every IP packet has Fragment Identification Number (IPID).
- OS increments IPID for each packet.

Step: 01

- Send Sync+Ack packet to Zombie to get its IPID Number.
- Zombie is not waiting for Sync+Ack, hence respond with RST packet. Its Reply discloses the IPID.
- Extract IPID from Packet.

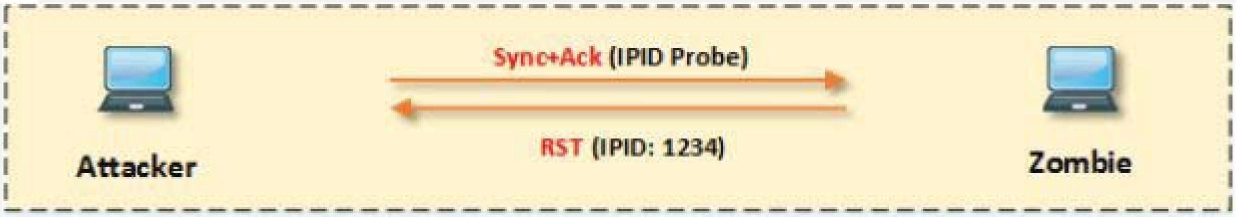


Figure 3-30 Step#01 Idle Scanning

Step: 02

- Send Sync packet to target spoofing the IP address of Zombie.
- IP port is open; Target reply with Sync+Ack to Zombie & Zombie reply back to target with RST packet.

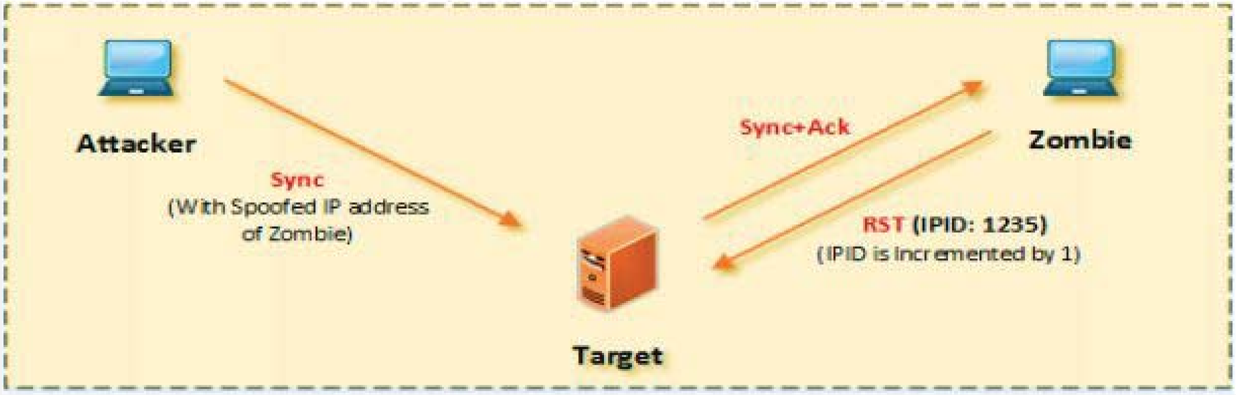

Attacker
Sync
(With Spoofed IP address of Zombie)
Target
Sync+Ack
Zombie
RST (IPID: 1235)
(IPID is Incremented by 1)

Figure 3-31 Step#02 Idle Scanning

- If the port is closed; Target reply with RST to Zombie & Zombie reply nothing back to target. IPID of Zombie is not incremented.

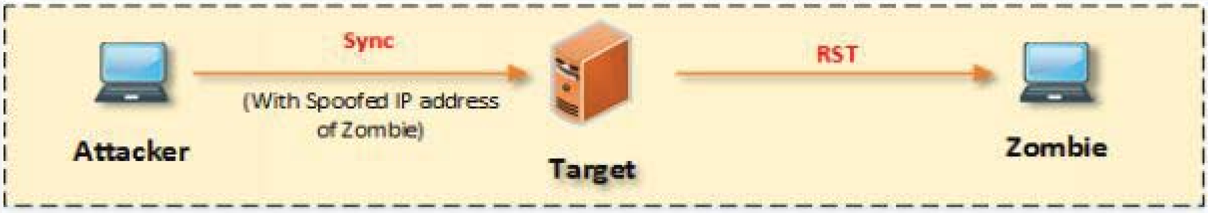


Figure 3-32 Step#02 Idle Scanning

Step: 03

- Send Sync+Ack packet to Zombie again, to get & compare its IPID Numbers to IPID extracted in step 01 (i.e. 1234).
- Zombie responds with RST packet. Its Reply discloses the IPID.
- Extract IPID from Packet.
- Compare the IPID.
- Port is open if IPID is incremented by 2.

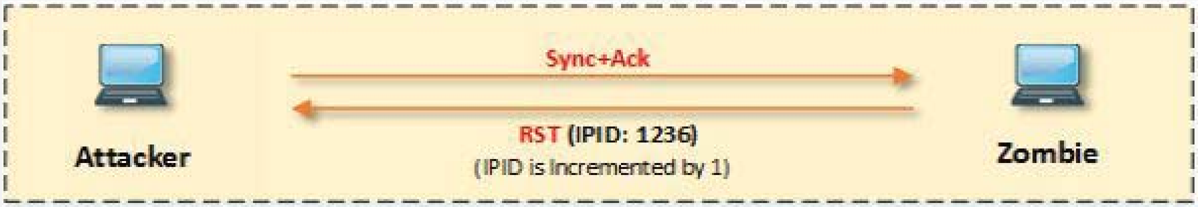


Figure 3-33 Step#03 Idle Scanning

- Port is close if IPID is incremented by 1.

UDP Scanning

Like TCP-based scanning techniques, there are also UDP Scanning methods.

Keeping in mind, UDP is a connectionless protocol. UDP does not have flags. UDP packets are working with ports; no connection orientation requires. No response if the targeted port is open however if the port is closed, the response message of "Port unreachable" returned. Most of the Malicious Programs, Trojans, Spywares uses UDP ports to access the target.

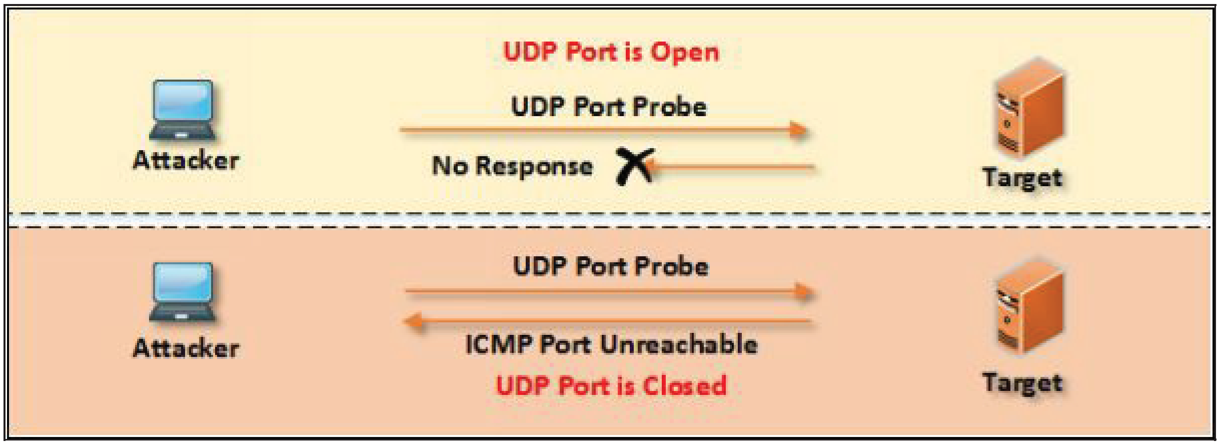
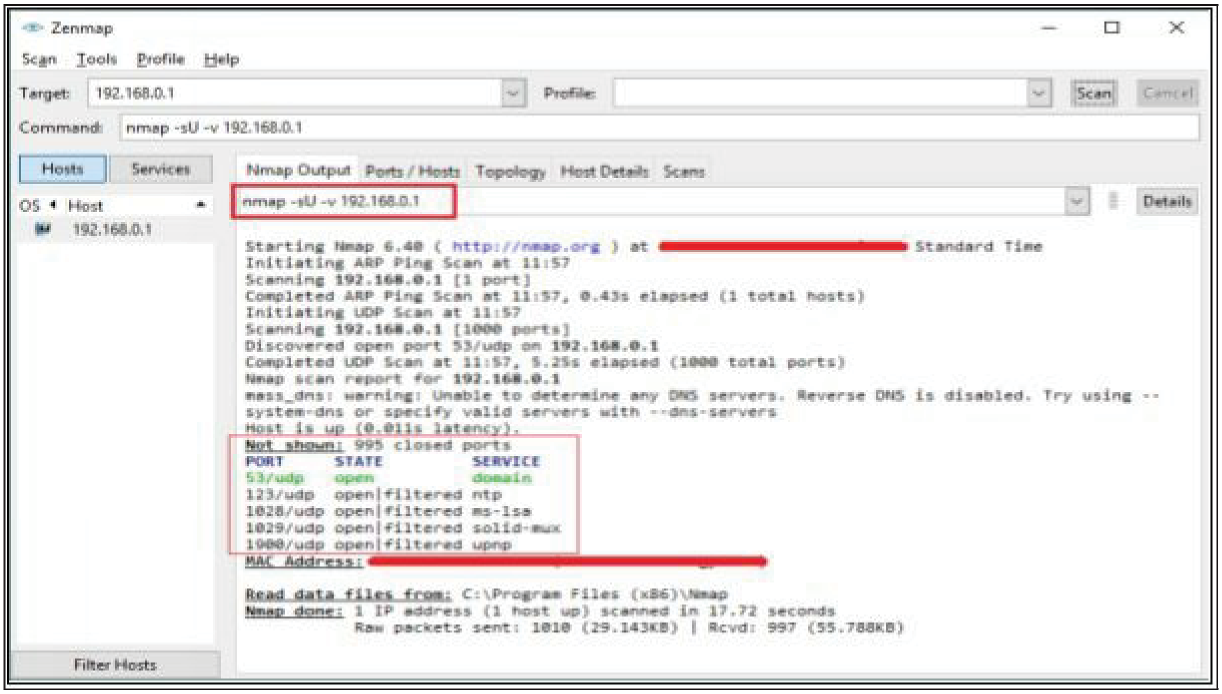


Figure 3-34 UDP Scanning Response

To perform this type of scan in nmap use the syntax:

nmap –sU –v *<ip address or range>*

Observe the result in the following figure: -



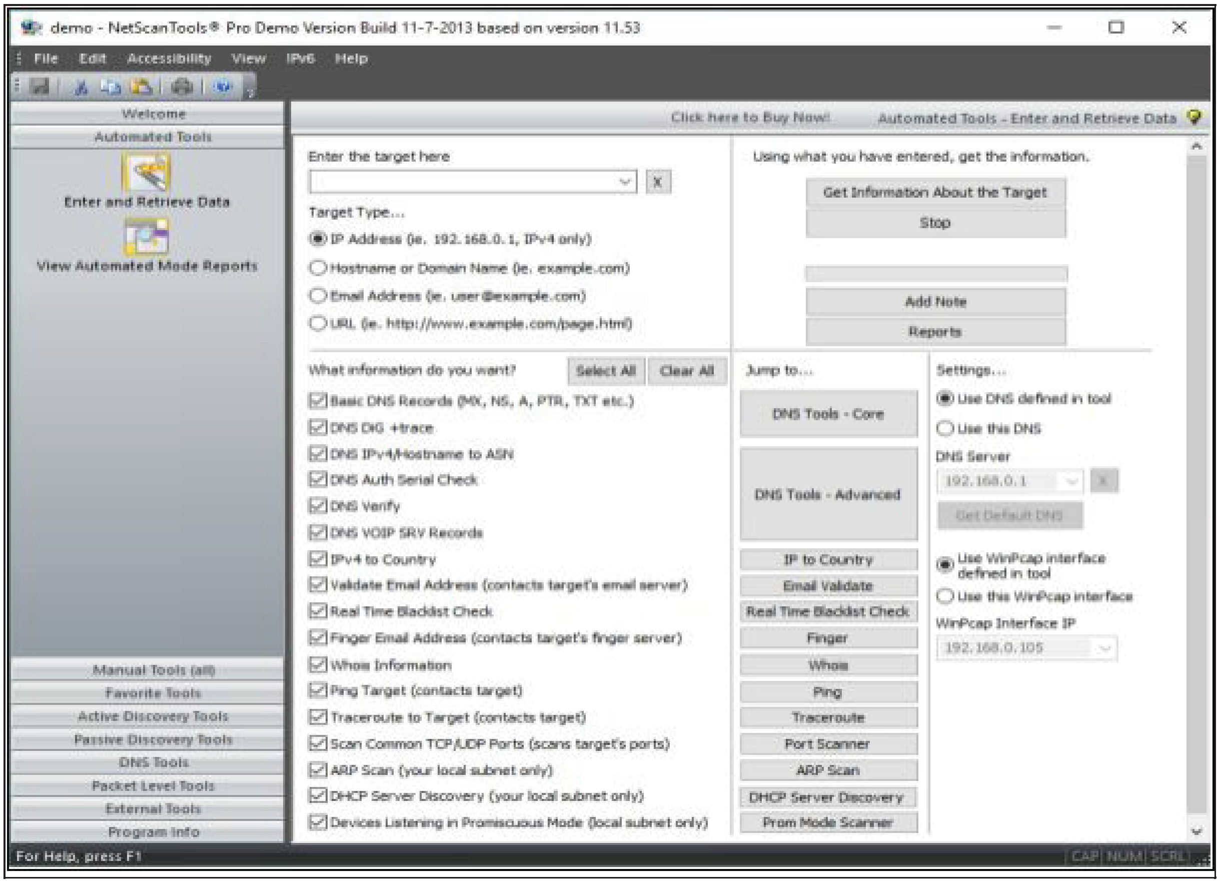
Command: nmap -sU -v 192.168.0.1

```
nmap -sU -v 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at [redacted] Standard Time
Initiating ARP Ping Scan at 11:57
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 11:57, 0.43s elapsed (1 total hosts)
Initiating UDP Scan at 11:57
Scanning 192.168.0.1 [1000 ports]
Discovered open port 53/udp on 192.168.0.1
Completed UDP Scan at 11:57, 5.25s elapsed (1000 total ports)
Nmap scan report for 192.168.0.1
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-servers
Host is up (0.011s latency).
Not shown: 995 closed ports
PORT      STATE         SERVICE
53/udp    open          domain
123/udp   open|filtered ntp
1028/udp  open|filtered ms-lsa
1029/udp  open|filtered solid-mux
1900/udp  open|filtered upnp
MAC Address: [redacted]

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 17.72 seconds
           Raw packets sent: 1010 (29.143KB) | Rcvd: 997 (55.788KB)
```

Figure 3-35 UDP Port Scanning

Scanning Tool

NetScan Tools Pro is an application which collects information, perform network troubleshooting, monitors, discover and diagnose with its integrated tools designed for Windows Operating system offering a focused examination of IPv4, IPv6, Domain names, Email and URL using Automatic and Manual Tool.



Enter the target here

Target Type...

● IP Address (ie. 192.168.0.1, IPv4 only)

○ Hostname or Domain Name (ie. example.com)

○ Email Address (ie. user@example.com)

○ URL (ie. http://www.example.com/page.html)

Using what you have entered, get the information.

What information do you want?

☑ Basic DNS Records (MX, NS, A, PTR, TXT etc.)
☑ DNS DIG +trace
☑ DNS IPv4/Hostname to ASN
☑ DNS Auth Serial Check
☑ DNS Verify
☑ DNS VOIP SRV Records
☑ IPv4 to Country
☑ Validate Email Address (contacts target's email server)
☑ Real Time Blacklist Check
☑ Finger Email Address (contacts target's finger server)
☑ Whois Information
☑ Ping Target (contacts target)
☑ Traceroute to Target (contacts target)
☑ Scan Common TCP/UDP Ports (scans target's ports)
☑ ARP Scan (your local subnet only)
☑ DHCP Server Discovery (your local subnet only)
☑ Devices Listening in Promiscuous Mode (local subnet only)

Settings...

● Use DNS defined in tool

○ Use this DNS

DNS Server: 192.168.0.1

● Use WinPcap interface defined in tool

○ Use this WinPcap interface

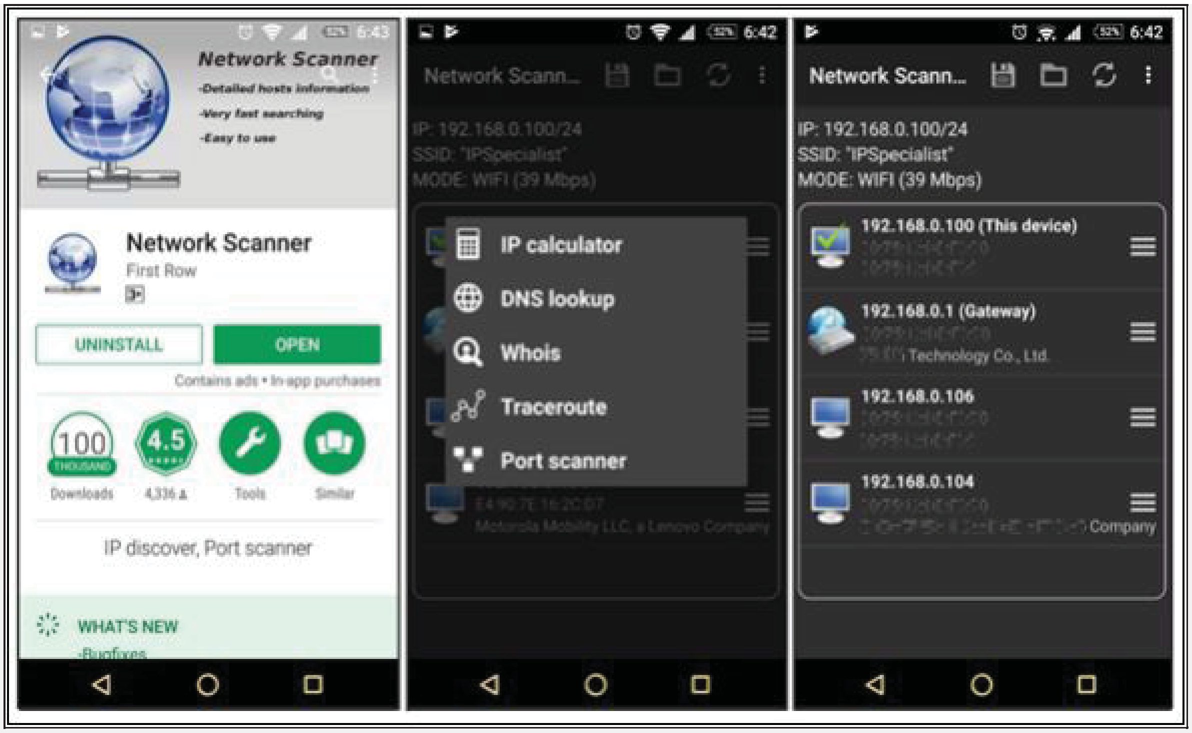
WinPcap Interface IP: 192.168.0.105

Figure 3-36 UDP Port Scanning

Scanning Tools for Mobile

There are several basic and advanced network tools available for the Mobile device on application stores. The following are some effective tools for network Scanning.

Network Scanner
"Network Scanner" tool offering IP Calculator, DNS lookup, Whois tool, Traceroute & Port Scanner option.



IP: 192.168.0.100/24
SSID: "IPSpecialist"
MODE: WIFI (39 Mbps)

Figure 3-37 Scanning Tool for Mobile

Fing- Network Tool

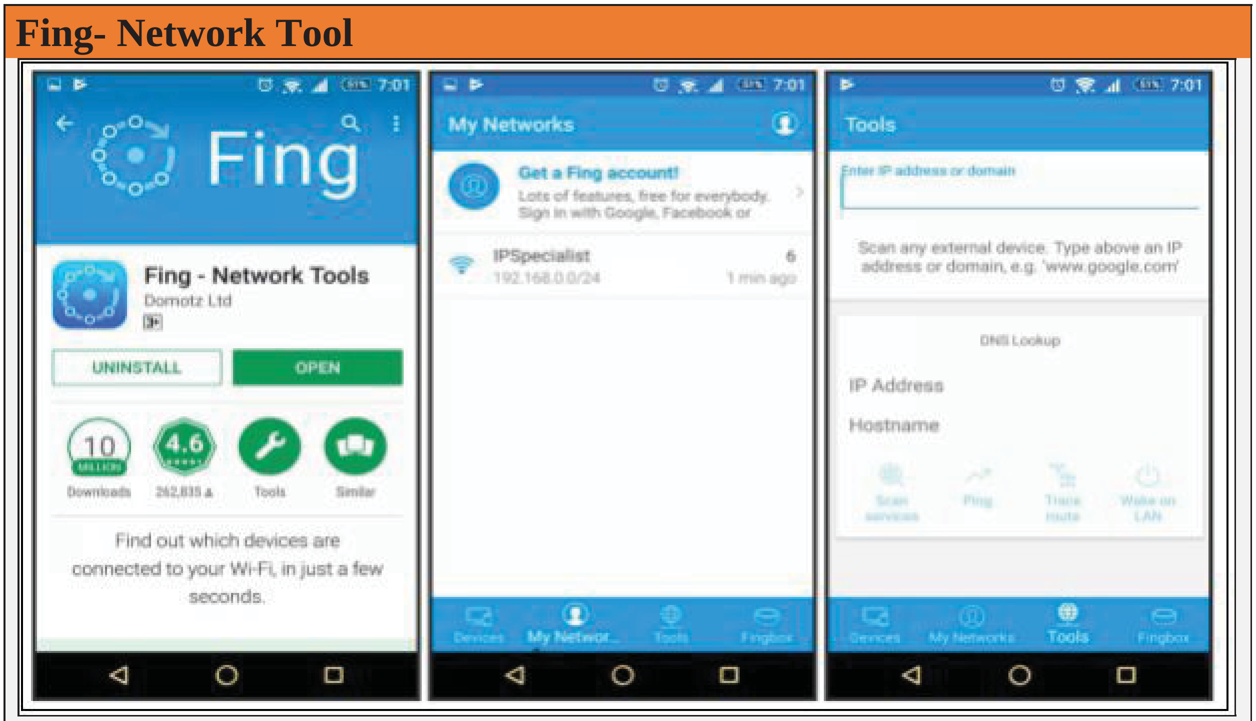
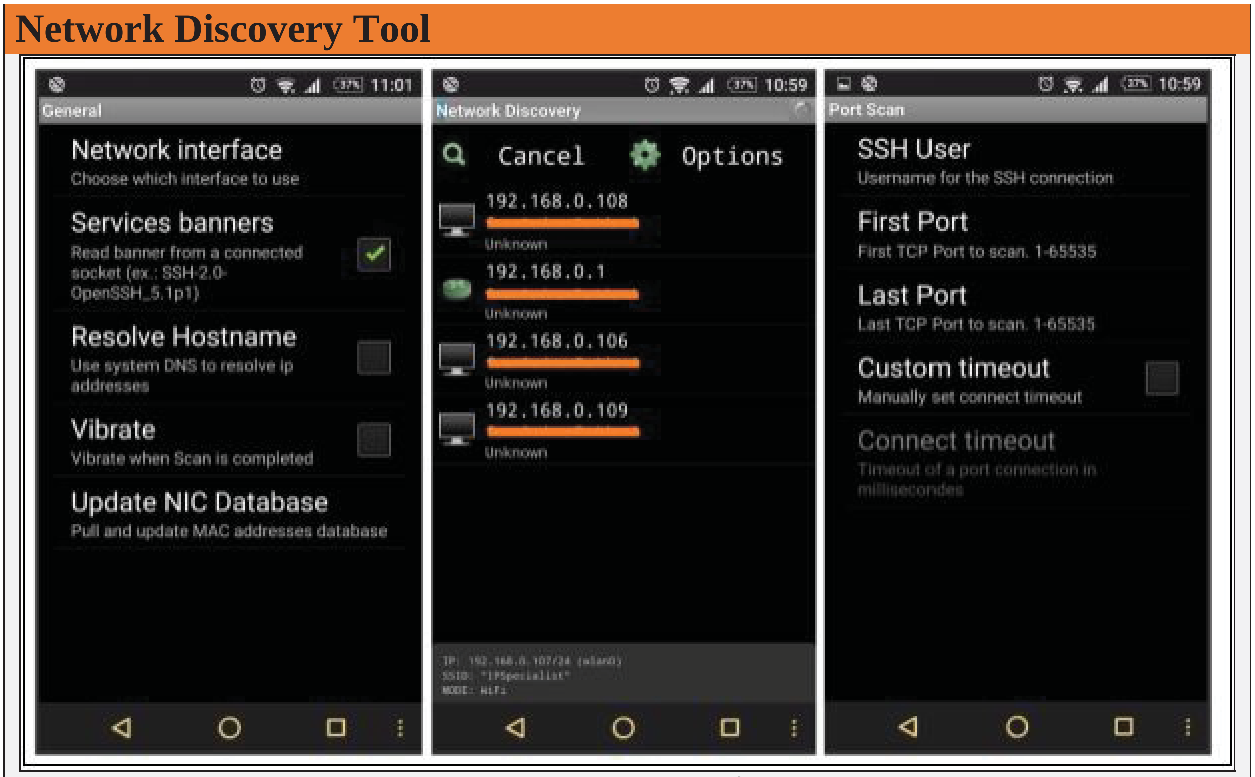


Figure 3-38 Scanning Tool for Mobile

Network Discovery Tool



General

Network interface
Choose which interface to use

Services banners ☑
Read banner from a connected socket (ex.: SSH-2.0-OpenSSH_5.1p1)

Resolve Hostname □
Use system DNS to resolve ip addresses

Vibrate □
Vibrate when Scan is completed

Update NIC Database
Pull and update MAC addresses database

Network Discovery

Cancel Options

192.168.0.108
Unknown

192.168.0.1
Unknown

192.168.0.106
Unknown

192.168.0.109
Unknown

```
IP: 192.168.0.107/24 (wlan0)
SSID: "IPSpecialist"
MODE: WiFi
```

Port Scan

SSH User
Username for the SSH connection

First Port
First TCP Port to scan. 1-65535

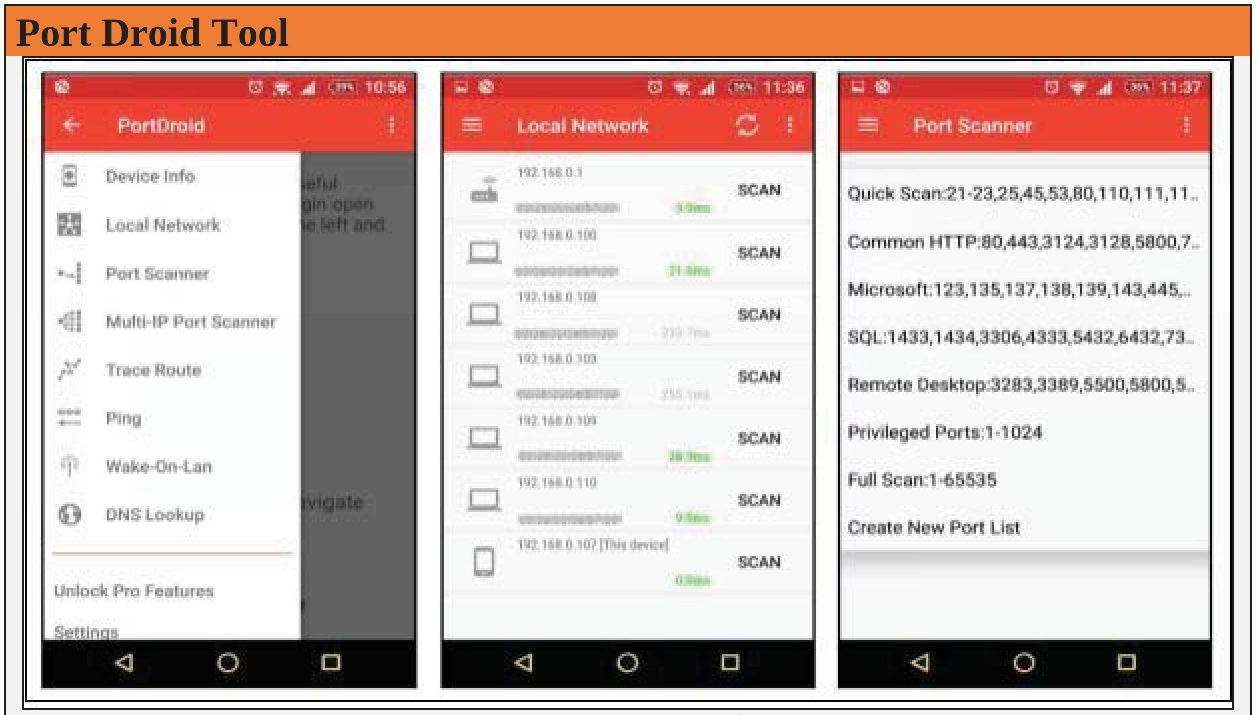
Last Port
Last TCP Port to scan. 1-65535

Custom timeout □
Manually set connect timeout

Connect timeout
Timeout of a port connection in milliseconds

Figure 3-39 Scanning Tool for Mobile

Port Droid Tool



192.168.0.1 3.9ms SCAN
192.168.0.100 21.4ms SCAN
192.168.0.108 213.7ms SCAN
192.168.0.103 255.1ms SCAN
192.168.0.109 38.3ms SCAN
192.168.0.110 9.9ms SCAN
192.168.0.107 [This device] 0.0ms SCAN

Quick Scan:21-23,25,45,53,80,110,111,11..
Common HTTP:80,443,3124,3128,5800,7..
Microsoft:123,135,137,138,139,143,445,..
SQL:1433,1434,3306,4333,5432,6432,73..
Remote Desktop:3283,3389,5500,5800,5..
Privileged Ports:1-1024
Full Scan:1-65535
Create New Port List

Figure 3-40 Scanning Tool for Mobile

Scanning Beyond IDS

The attacker uses Fragmentation and Small packets to evade Security devices such as Firewalls, IDS, and IPS. The basic technique that is most commonly & popularly used is splitting the payload into the smaller packet. IDS must have to reassemble these incoming packet stream to inspect and detect the attack. The small packet is further modified to be more complicated to reassemble and detect by packet reassemble. Another way of using fragmentation is by sending these fragmented packets out of order. These fragmented out of order packets are sent with pauses to create a delay. These packets are sent using proxy servers, or through compromised machines to launch attacks.

OS Fingerprinting & Banner Grabbing

OS Fingerprinting is a technique, used to identify the information of Operating System running on a target machine. By gathering information about running operating system, attacker determines the vulnerabilities and possible bugs that an operating system may possess. The two types of OS Fingerprinting are as follows: -

1. Active OS Fingerprinting
2. Passive OS Fingerprinting

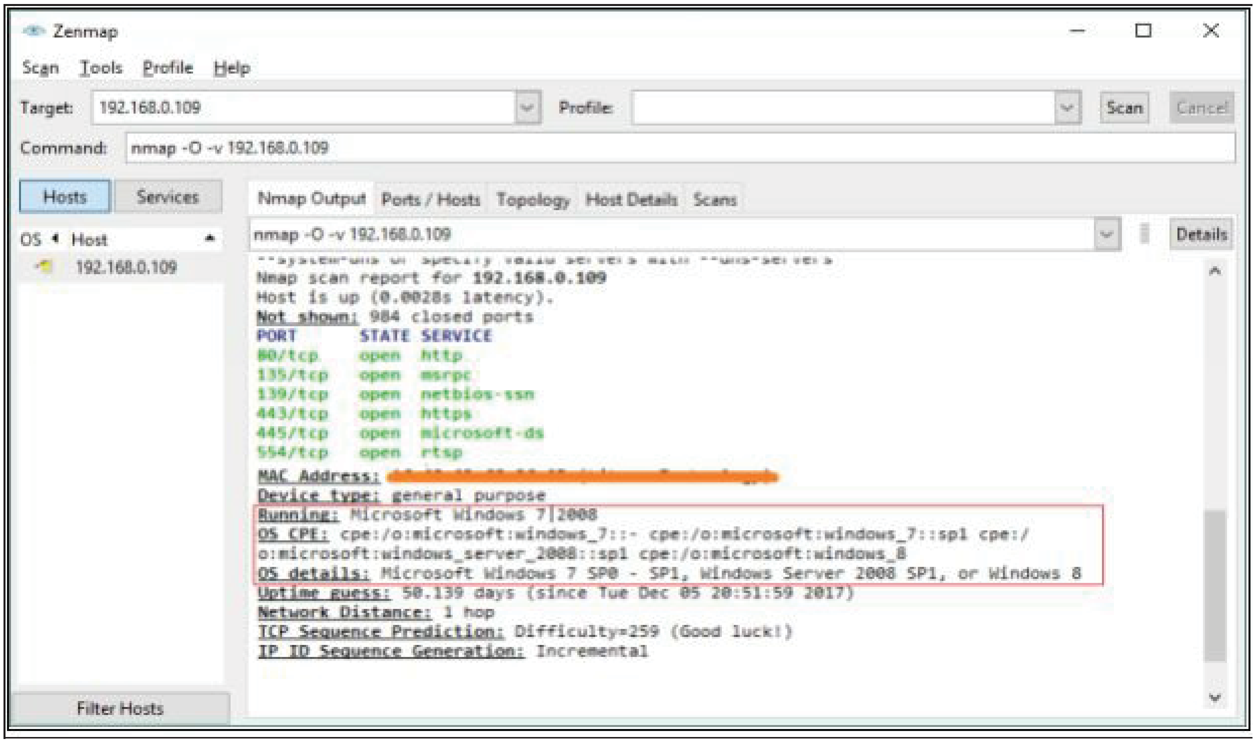
Banner Grabbing is similar to OS fingerprinting, but actually, Banner grabbing is determining the services that are running on the target machine. Typically, Telnet is used to retrieve information of banner.

Active OS Fingerprinting or Banner Grabbing

NMPA can perform Active Banner grabbing with ease. NMAP, as we know, is a powerful networking tool which supports many features and commands. Operating System detection capability allows to send TCP and UDP packet and observe the response from the targeted host. A detailed assessment of this response bring some clues regarding nature of an operating system disclosing the type an OS.

To perform OS detection with nmap perform the following: -

```
nmap -O <ip address>
```



Target: 192.168.0.109

Command: nmap -O -v 192.168.0.109

```
nmap -O -v 192.168.0.109
--system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.109
Host is up (0.0028s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
MAC Address: [redacted]
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/
o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Uptime guess: 50.139 days (since Tue Dec 05 20:51:59 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
```

Figure 3-41 OS Fingerprinting

Passive OS Fingerprinting or Banner Grabbing

Passive OS Fingerprinting requires detail assessment of traffic. You can perform Passive banner grabbing by analyzing network traffic along with special inspection of Time to Live (TTL) value and Window Size. TTL value and Window Size are inspected from a header of TCP packet while observing network traffic. Some of the common values for operating systems are: -

Operating System	**TTL**	**TCP Window Size**
Linux	64	5840
Google customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows Vista, 7 and Server 2008	128	8192
Cisco Router (iOS 12.4)	255	4128

Table 3-03 Passive OS Fingerprinting Values

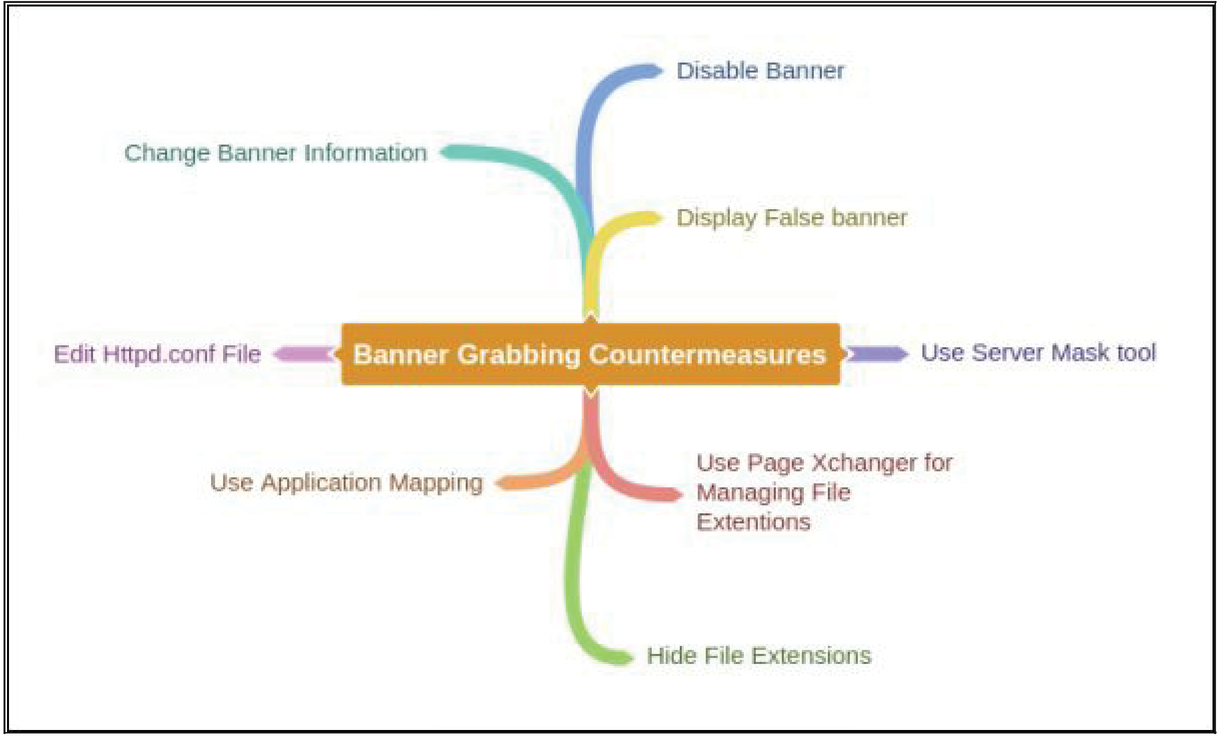
Banner Grabbing Tools

There are some tools available for banner grabbing. Some of them are: -

- ID Server

- Netcraft
- Netcat
- Telnet
- Xprobe
- pof
- Maltego

Mind Map



Draw Network Diagrams

To gain access to a network, deep understanding of the architecture of that network and detailed information is required. Having valuable network information such as security zones, security devices, routing devices, number of hosts, etc. helps an attacker to understand the network diagram. Once Network diagram is designed, it defines logical and physical path leading to the appropriate target within a network. Network diagram visually explains the network environment and provide an even more clear picture of that network. Network Mappers are the network mapping tools, which uses scanning and other network tools and techniques and draw a picture of a network. The thing that is important to care about is, these tools generate traffic which can reveal the presence of attacker or pentester on the network.

Network Discovery Tool

OpManager is an advanced network monitoring tool which offers fault management, supporting over WAN links, Router, Switch, VoIP & servers. It can also perform performance management. Network View is an advanced network discovery tools. It can perform discovery of routes, TCP/IP nodes using DNS, ports, and other network protocols. List of some popular tools are: -

1. Network Topology Mapper
2. OpManager
3. Network View
4. LANState Pro

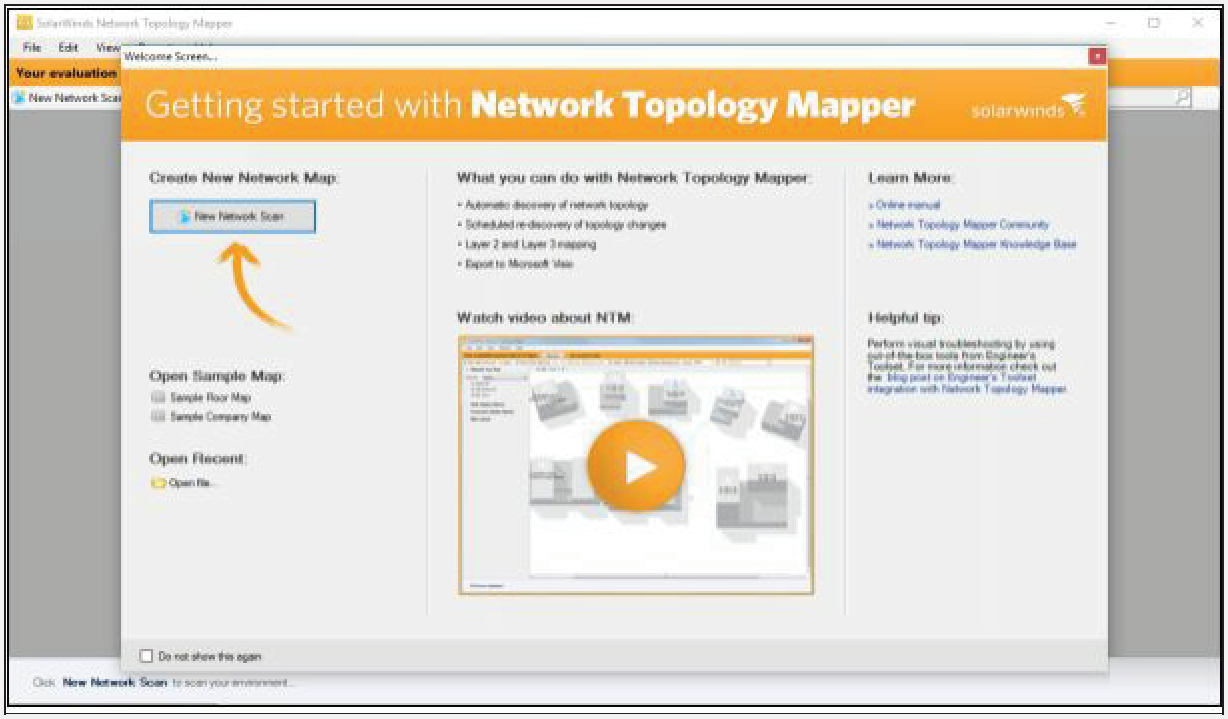
Drawing Network Diagrams

Solar Wind Network Topology Mapper can discover network & create a comprehensive network topology diagram. It also offers additional features like editing nodes manually, exporting diagram to Visio, multi-level network discovery, etc. Mapped topology can display Node name, IP Address, Hostname, System Name, Machine type, Vendor, System location, & other information.

Lab 3-4: Creating Network Topology Map using Tool

Creating Network Topology Map

With Solar Wind Network Topology Mapper tool, start scanning the network by clicking on New Network Scan/button.



Getting started with **Network Topology Mapper**

Create New Network Map:

What you can do with Network Topology Mapper:

- Automatic discovery of network topology
- Scheduled re-discovery of topology changes
- Layer 2 and Layer 3 mapping
- Export to Microsoft Visio

Learn More:

- › Online manual
- › Network Topology Mapper Community
- › Network Topology Mapper Knowledge Base

Watch video about NTM:

Helpful tip:

Perform visual troubleshooting by using out-of-the-box tools from Engineer's Toolset. For more information check out the blog post on Engineer's Toolset integration with Network Topology Mapper

Open Sample Map:

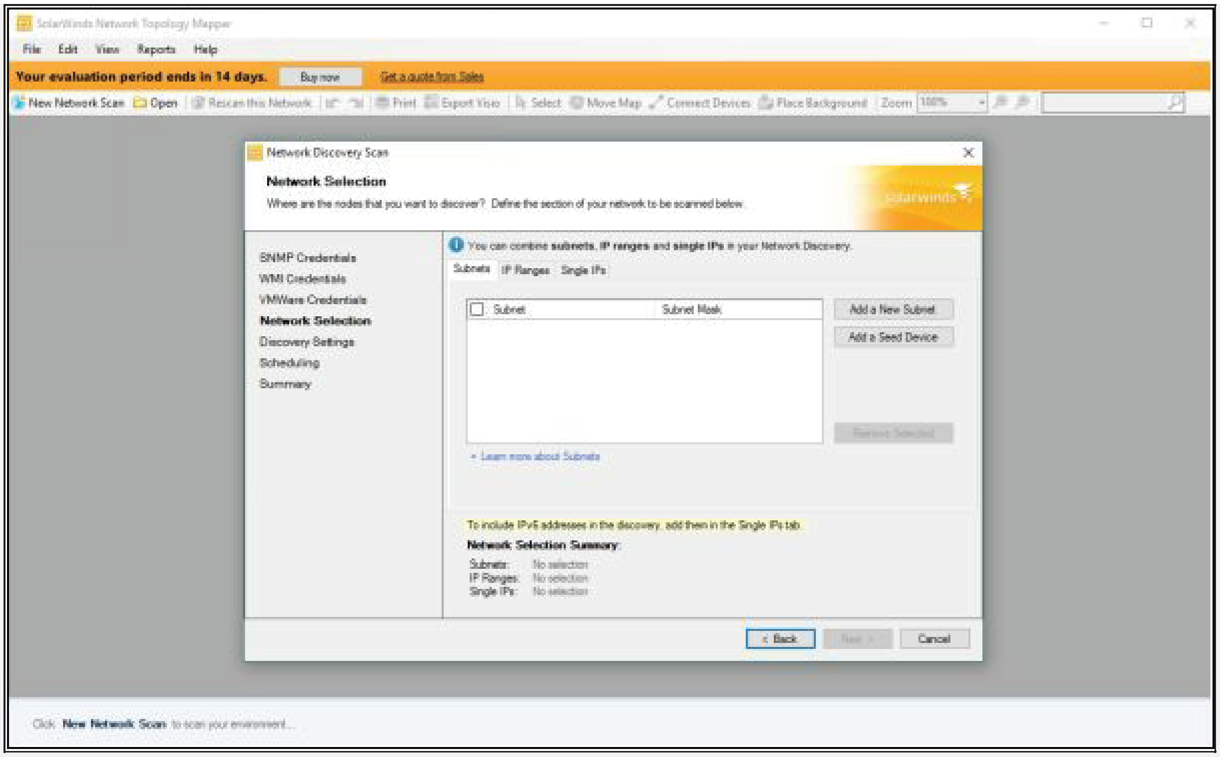
Open Recent:

□ Do not show this again

Click **New Network Scan** to scan your environment...

Figure 3-42 Network Topology Mapper Tool

Provide Network Information, Configure Discovery Settings, provide necessary credentials if required.



Your evaluation period ends in 14 days.

Network Selection

Where are the nodes that you want to discover? Define the section of your network to be scanned below.

You can combine **subnets**, **IP ranges** and **single IPs** in your Network Discovery.

To include IPv6 addresses in the discovery, add them in the Single IPs tab.

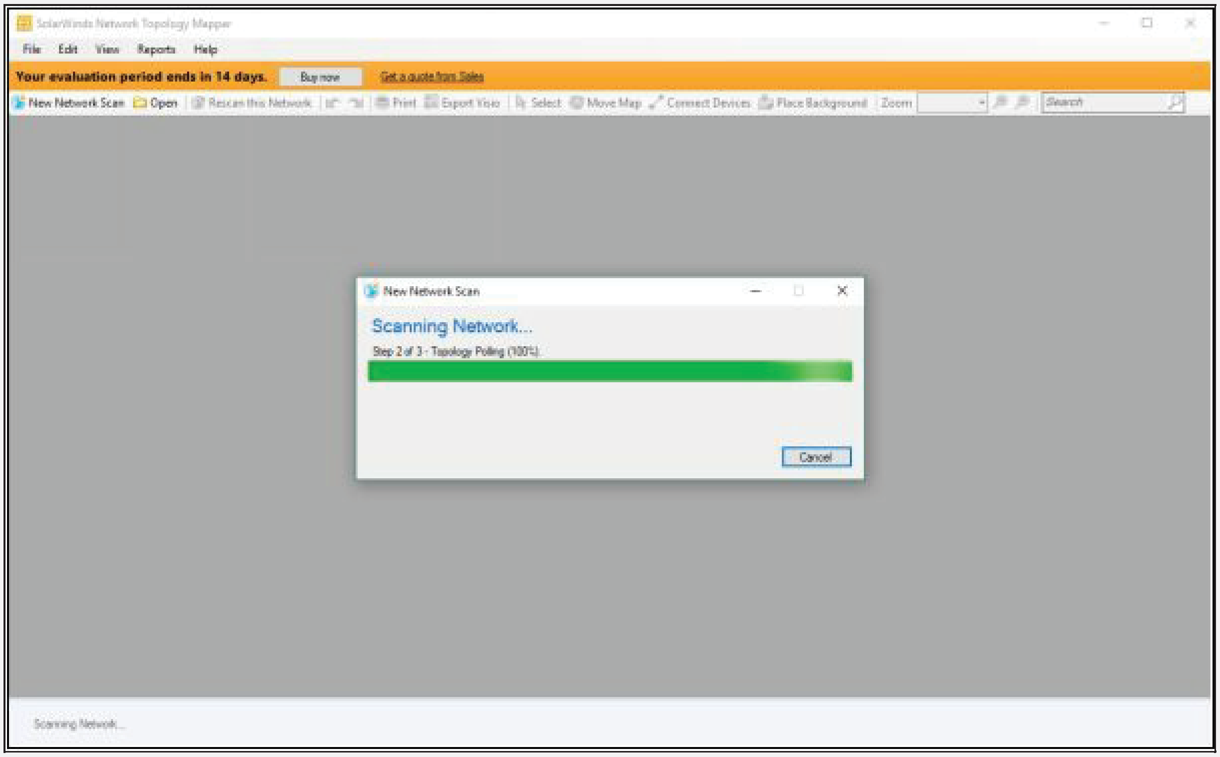
Network Selection Summary:

Subnets: No selection
IP Ranges: No selection
Single IPs: No selection

Click **New Network Scan** to scan your environment...

Figure 3-43 Configuring Scan

Once you configure all settings, Start the scan.



Your evaluation period ends in 14 days.

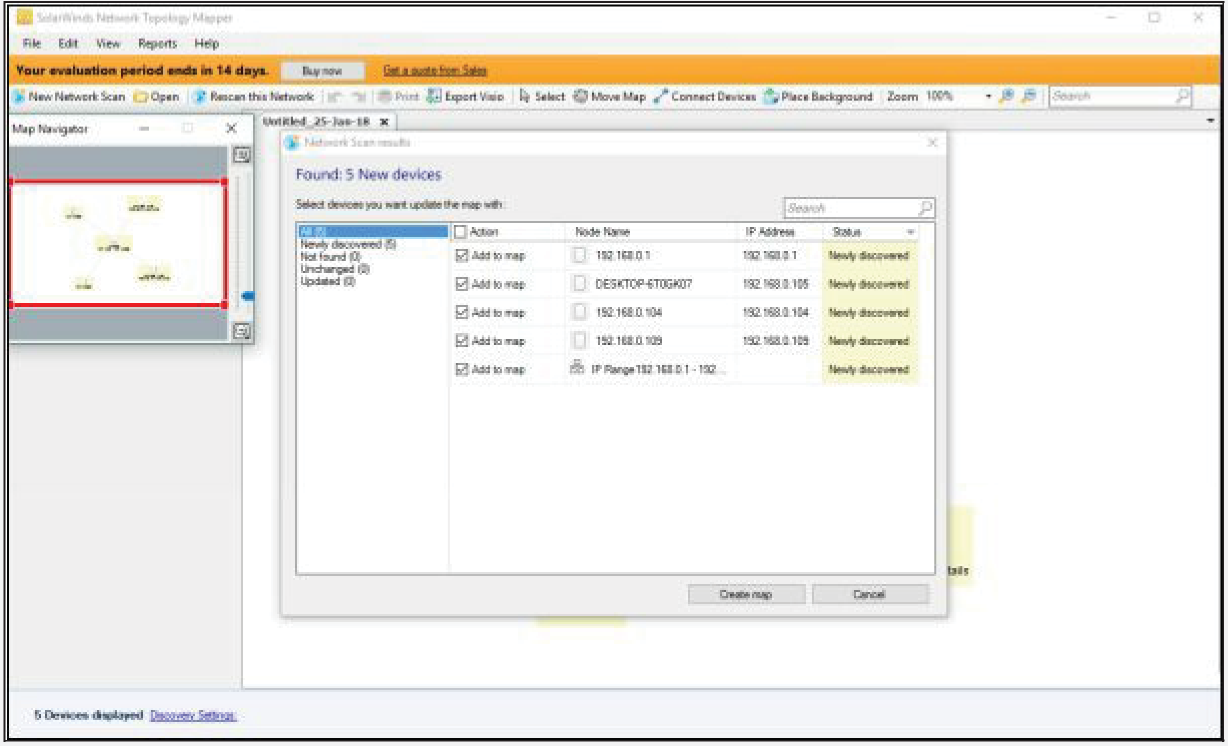
Scanning Network...

Step 2 of 3 - Topology Polling (100%)

Scanning Network...

Figure 3-44 Scanning Network

After complete scan process, it will show a list of detected devices to add into topology diagram. Select all or required devices to add to the topology.


SolarWinds Network Topology Mapper
File Edit View Reports Help
Your evaluation period ends in 14 days.
Buy now
Get a quote from Sales
New Network Scan Open Rescan this Network Print Export Visio Select Move Map Connect Devices Place Background Zoom 100%
Search
Map Navigator
Untitled_25-Jan-18
Network Scan results

Found: 5 New devices

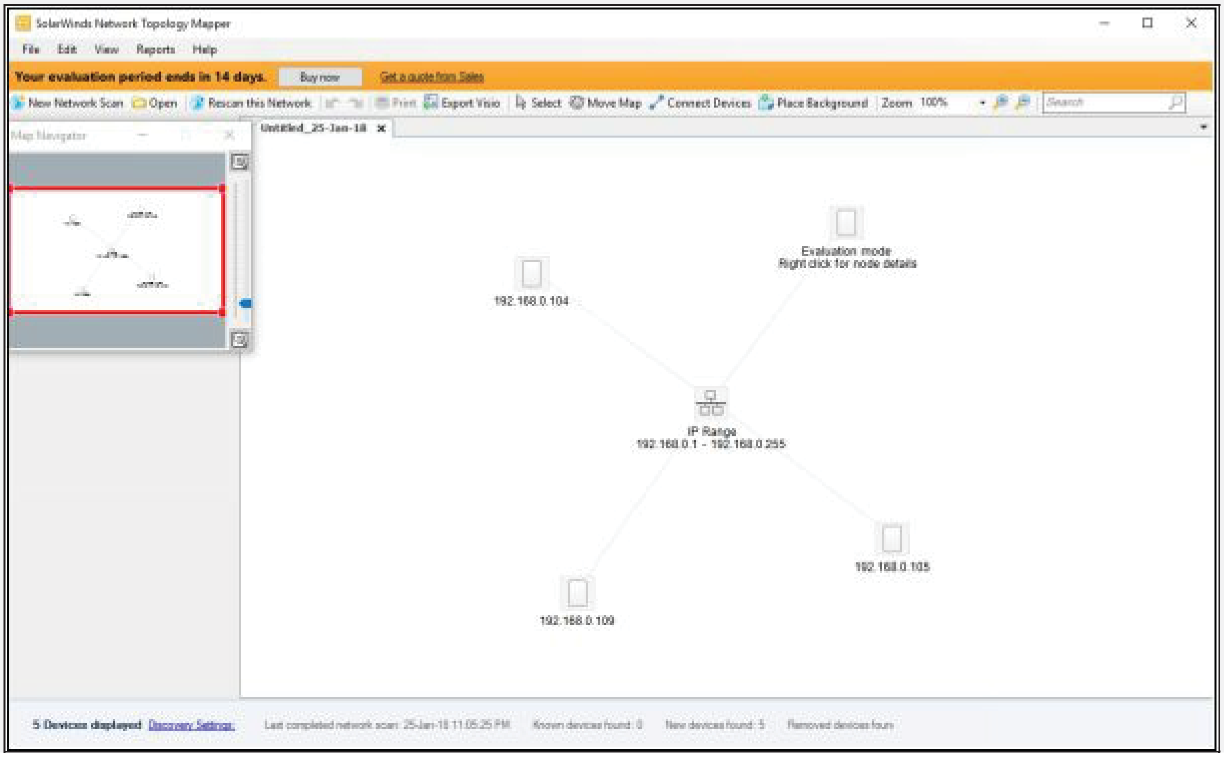
Select devices you want update the map with:

All (5)
Newly discovered (5)
Not found (0)
Unchanged (0)
Updated (0)

☐ Action	Node Name	IP Address	Status
☑ Add to map	192.168.0.1	192.168.0.1	Newly discovered
☑ Add to map	DESKTOP-6T0GK07	192.168.0.105	Newly discovered
☑ Add to map	192.168.0.104	192.168.0.104	Newly discovered
☑ Add to map	192.168.0.109	192.168.0.109	Newly discovered
☑ Add to map	IP Range 192.168.0.1 - 192...		Newly discovered

Figure 3-45 Discovered Devices List

Topology view of the scanned network. Now you can add nodes manually, export it to Vision and use other features of the tool.


SolarWinds Network Topology Mapper
File Edit View Reports Help
Your evaluation period ends in 14 days.
Buy now
Get a quote from Sales
New Network Scan Open Rescan this Network Print Export Visio Select Move Map Connect Devices Place Background Zoom 100%
Search
Map Navigator
Untitled_25-Jan-18
Evaluation mode
Right click for node details
192.168.0.104
IP Range
192.168.0.1 - 192.168.0.255
192.168.0.105
192.168.0.109

5 Devices displayed Discovery Settings: Last completed network scan: 25-Jan-18 11:05:25 PM Known devices found: 0 New devices found: 5 Removed devices foun

Figure 3-46 Topology

Prepare Proxies

Proxy is the system that is stands in between attacker and the target. Proxy systems play an important role in networks. Proxy systems are basically used by scanners to hide their identity to be traced back to the target.

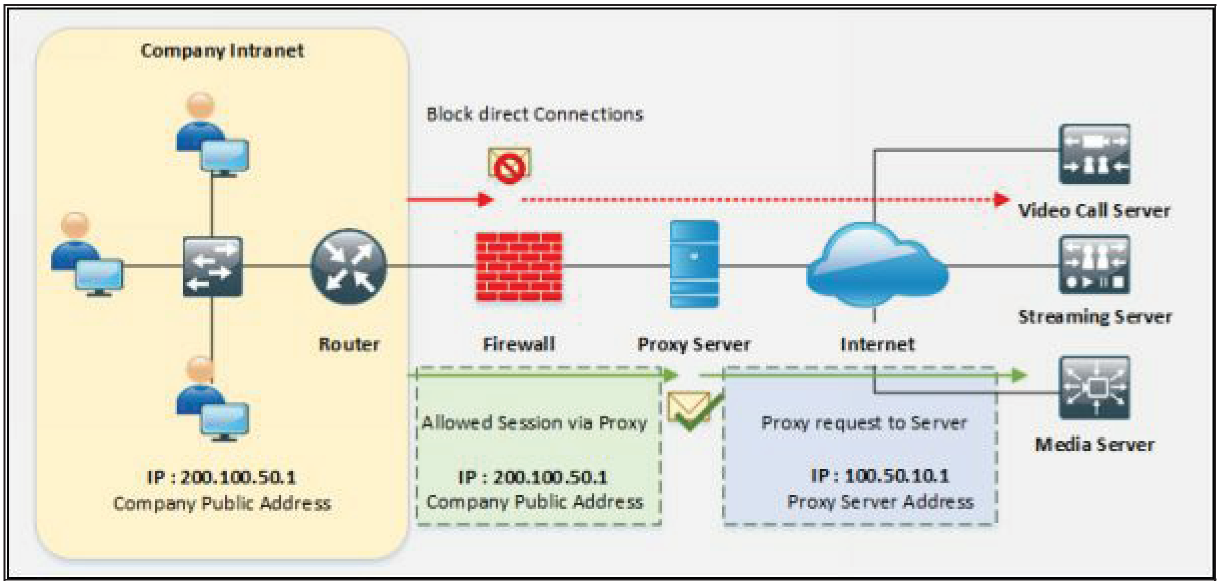


Figure 3-47 Proxy Server

Proxy Servers

Proxy server anonymizes the web traffic to provide anonymity. When a user sends a request for any resources to the other publically available servers, proxy server act as an intermediary for these requests. Users request is forwarded to proxy server first. the proxy server will entertain these requests like a web page, file download, connection to another server, etc. The most popular use of the proxy server is in terms of web proxy servers. These Web proxy servers are used to provide access to world wide web by bypassing the IP address blocking.

Uses Proxy server, in a nutshell, can be summarized as: -

- Hiding Source IP address for bypassing IP address blocking.
- Impersonating.
- Remote Access to Intranet.
- Redirecting all requests to the proxy server to hide identity.
- Proxy Chaining to avoid detection.

Proxy Chaining

Proxy Chaining is basically a technique of using multiple proxy servers. In addition to proxy servers, one proxy server forwards the traffic to next proxy server. This process is not recommended for production environments, or a long-term solution, however, this technique leverages your existing proxy.

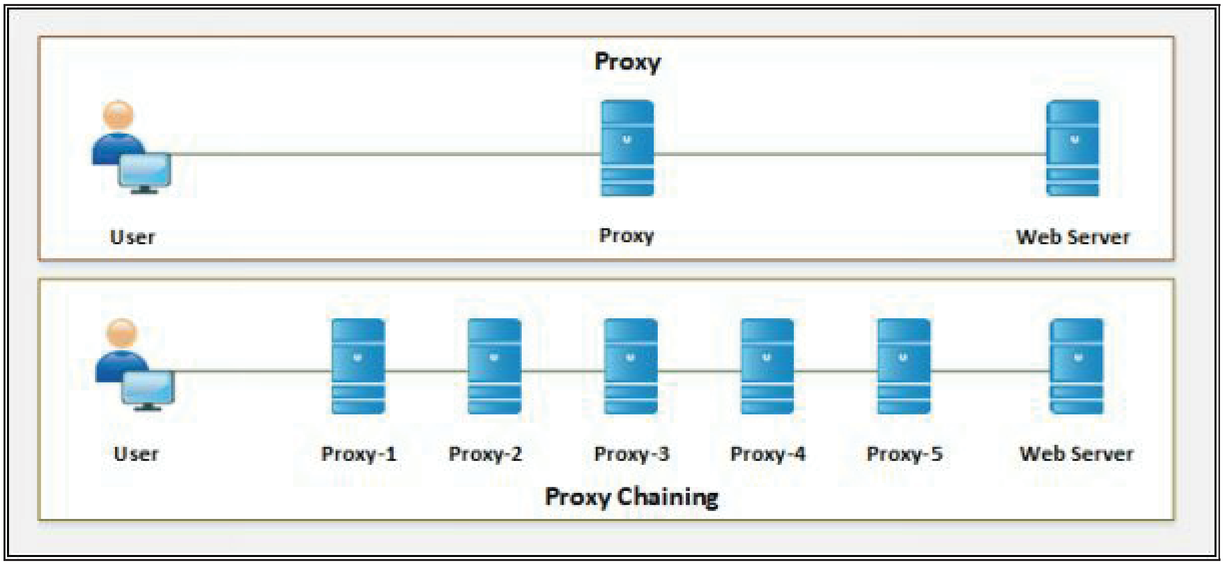


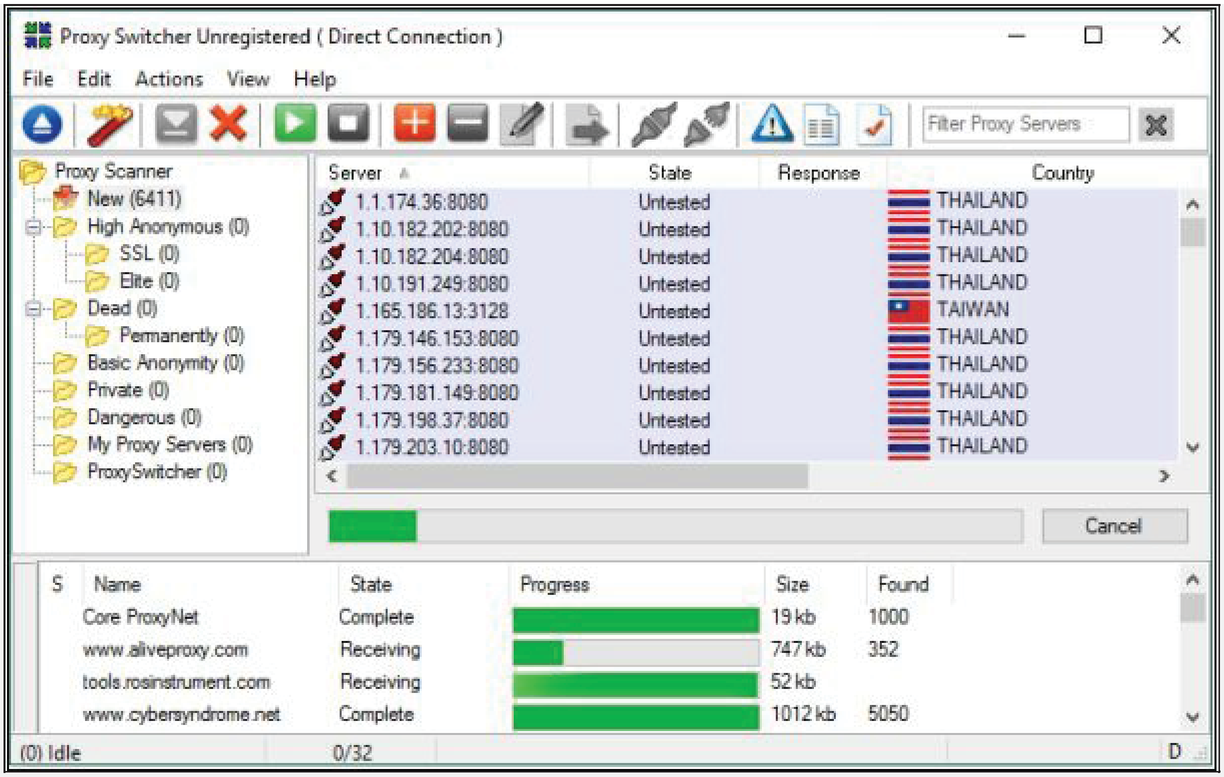
Figure 3-48 Proxy Chaining

Proxy Tool

There is a number of proxy tools available as well as you can online search for a proxy server and configure manually on your web browser. These tools include: -

1. Proxy Switcher
2. Proxy Workbench
3. TOR
4. CyberGhost

Proxy Switcher
Proxy Switcher tool scans for Available proxy servers. You can enable any proxy server to hide your IP address. The following figure is showing the searching process of Proxy servers using Proxy Switcher tool.



Server	State	Response	Country
1.1.174.36:8080	Untested		THAILAND
1.10.182.202:8080	Untested		THAILAND
1.10.182.204:8080	Untested		THAILAND
1.10.191.249:8080	Untested		THAILAND
1.165.186.13:3128	Untested		TAIWAN
1.179.146.153:8080	Untested		THAILAND
1.179.156.233:8080	Untested		THAILAND
1.179.181.149:8080	Untested		THAILAND
1.179.198.37:8080	Untested		THAILAND
1.179.203.10:8080	Untested		THAILAND

S	Name	State	Progress	Size	Found
	Core ProxyNet	Complete		19 kb	1000
	www.aliveproxy.com	Receiving		747 kb	352
	tools.rosinstrument.com	Receiving		52 kb	
	www.cybersyndrome.net	Complete		1012 kb	5050

Figure 3-49 Proxy Switcher

Proxy Tools for Mobile

There are several proxy applications available on google play store and App store for iOS devices.

Application	**Download URL**
Proxy Droid	https://play.google.com
Net Shade	https://itunes.apple.com

Table 3-04 Proxy Tools for Mobile

Introduction to Anonymizers

Anonymizer is a tool that completely hides or removes identity-related information to make the activity untraceable. The basic purpose of using anonymizers are: -

- Minimizing risk
- Identity theft prevention
- Bypass restrictions and censorship
- Untraceable activity on the Internet

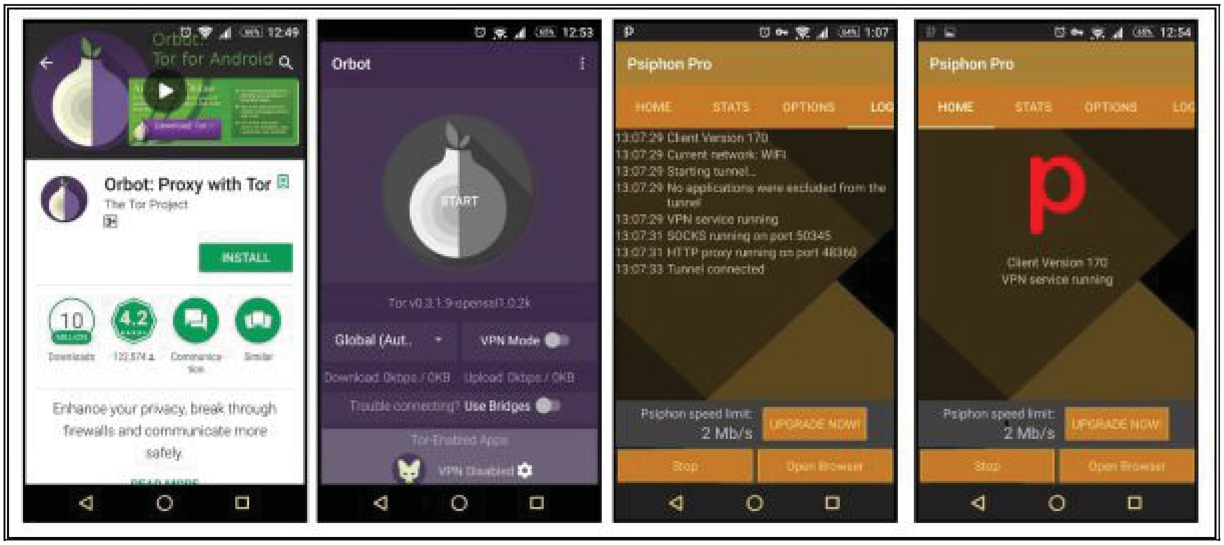
Censorship Circumvention Tool

- **Tails**

  Tails (The Amnesic Incognito Live System) is a popular censorship circumvention tool based on Debian GNU/Linux. It is basically a live operating system that can run on almost every computer from USB or DVD. It is an operating system that is specially designed to help you to use the internet anonymously leaving no trace behind. Tails preserve privacy and anonymity.

Anonymizers for Mobile

- Orbot
- Psiphon
- Open door



```
13:07:29 Client Version 170
13:07:29 Current network: WiFi
13:07:29 Starting tunnel...
13:07:29 No applications were excluded from the
         tunnel
13:07:29 VPN service running
13:07:31 SOCKS running on port 50345
13:07:31 HTTP proxy running on port 48360
13:07:33 Tunnel connected
```

Figure 3-50 Anonymizers for Mobile

Spoofing IP Address

IP Address Spoofing is a technique, that is used to gain unauthorized access to machines by spoofing IP address. An attacker illicitly impersonates any user machine by sending manipulated IP packets with spoofed IP address. Spoofing process involves modification of header with a spoofed source IP address, a checksum, and the order values. Packet-switched networking causes the packets arriving at the destination in different order. When these out of order packets are received at the destination, these packets are resembled to extract the message.

IP spoofing can be detected by different techniques including Direct TTL probing technique and through IP Identification Number. In the process of sending direct TTL probes, packets are sent to the host that is suspected of sending spoofed packets and responses are observed. By comparing TTL value from the reply from the suspected host, IP spoofing can be detected. It will be a spoofed packet if TTL value is not same as in spoofed packet. However, TTL values can vary in even normal traffic and this technique identify the spoofing when the attacker is on a different subnet.

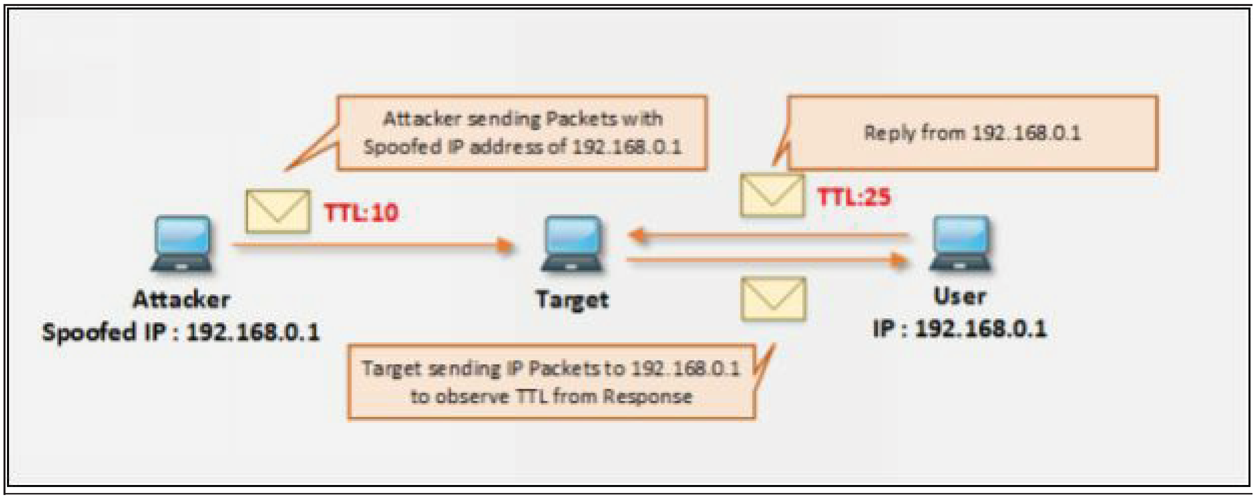

Attacker sending Packets with Spoofed IP address of 192.168.0.1
Reply from 192.168.0.1
TTL:10
TTL:25
Attacker
Spoofed IP : 192.168.0.1
Target
User
IP : 192.168.0.1
Target sending IP Packets to 192.168.0.1 to observe TTL from Response

Figure 3-51 Direct TTL Probing

Similarly, additional probes are sent to verify the IPID of the host. If IPID values are not closer, suspect traffic is spoofed. This technique can be used in case if the attacker is within a subnet.

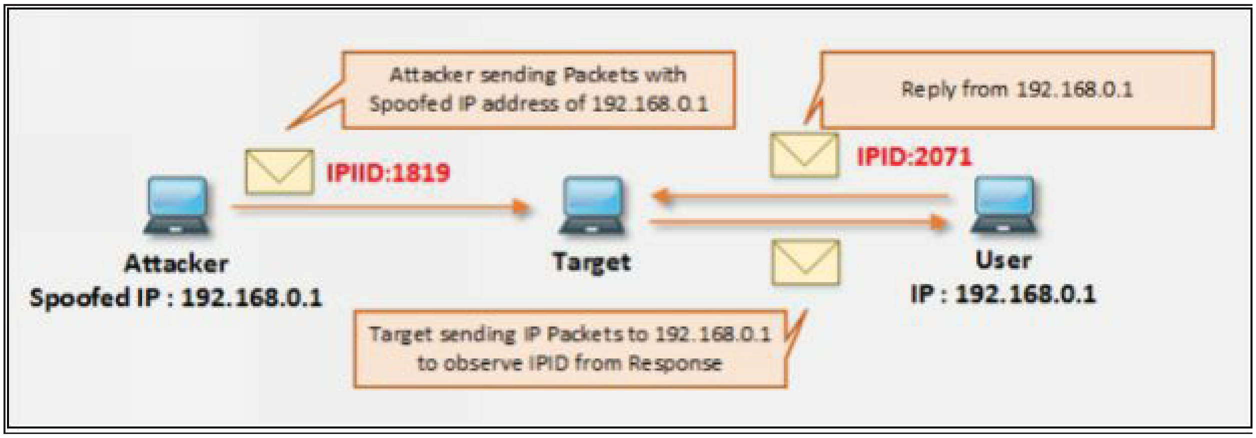

Attacker sending Packets with Spoofed IP address of 192.168.0.1
Reply from 192.168.0.1
IPIID:1819
IPID:2071
Attacker
Spoofed IP : 192.168.0.1
Target
User
IP : 192.168.0.1
Target sending IP Packets to 192.168.0.1 to observe IPID from Response

Figure 3-52 Verifying IPID Number