8. Which record type will reveal the information about Domain's Mail Server (MX)? A. A
B. MX C. NS D. SRV

9. Which one of the following is the most framework used for information gathering detection?
A. Maltego
B. Whois Application
C. Domain Dossier tool
D. Recong-ng
popular Web Reconnaissance

purpose as well as network

10. Which tool can be used to view web server information? A. Netstat
B. Netcraft
C. Nslookup
D. Wireshark

11. To extract information regarding domain name registration, which of the following is the most appropriate?
A. Whois Lookup
B. DNS Lookup
C. Maltego
D. Recong-ng

Chapter 3: Scanning Networks

Technology Brief

After the footprinting phase, you may have enough information about the target. The scanning network phase requires some of this information to proceed further. Network Scanning is a method of obtaining network information about hosts, ports, etc., and running services by scanning the networks and its ports. The main Objective of Network Scanning is:

- To identify live hosts on a network
- To identify open and closed ports
- To identify Operating System information
- To identify services running on a network
- To identify processes running on a network
- To identify the presence of security devices like firewalls
- To identify system architecture
- To identify running services
- To identify vulnerabilities

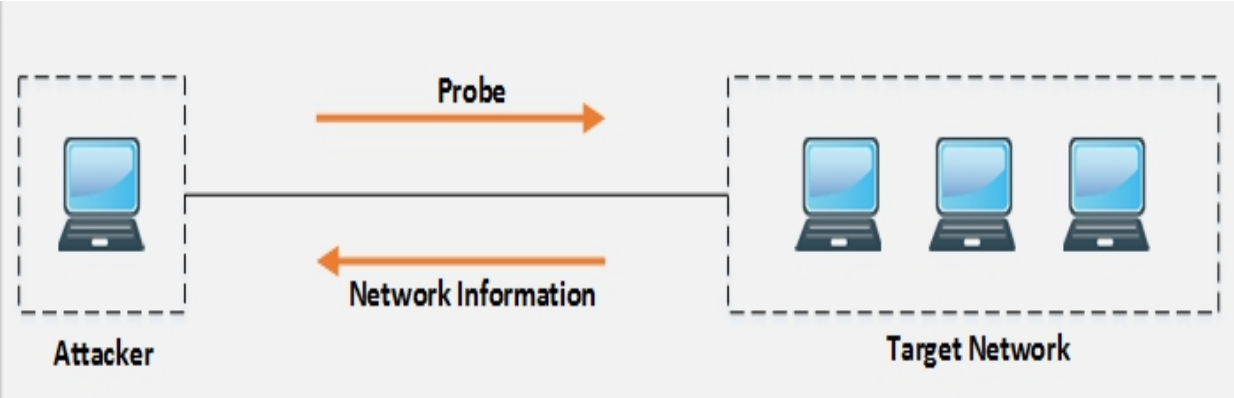


Figure 3-01: Scanning Network

An Overview of Network Scanning

The Scanning Network phase includes probing the target network to get information. When a user probes another user, the received reply can reveal very useful information. In-depth identification of networks, 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 the establishment of a successful connection. UDP is a simpler, connectionless internet protocol. Multiple messages are sent as packets in chunks using UDP. Unlike 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. The following diagram shows the TCP header:

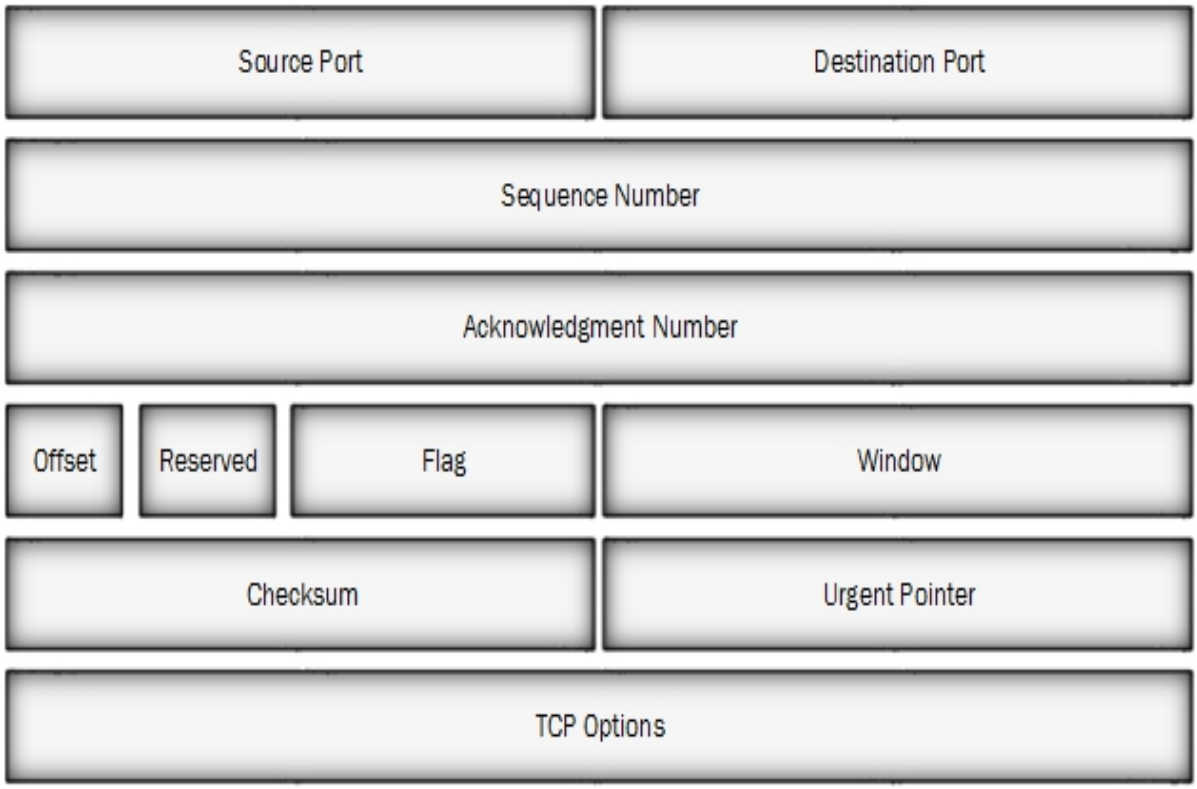


Figure 3-02: TCP Header

The flag field in the TCP header contains 9 bits. This includes the following 6 TCP flags:

Flag	Use
SYN	Initiates a connection between two hosts to facilitate communication
ACK	Acknowledges the receipt of a packet
URG	Indicates that the data contained in the packet is urgent and should be processed immediately
PSH	Instructs the sending system to send all buffered data immediately
FIN	Informs the remote system when communication ends. In essence, this gracefully closes a connection
RST	Resets a connection

Table 3-01: TCP Flags

There is a three-way handshake in establishing a TCP connection between hosts. This handshake ensures a successful, reliable, and connection-oriented sessions between hosts. The process of establishing a TCP connection includes three steps as shown in figure 3-03.

Figure 3-03: TCP Connection Handshake

Consider that host A wants to communicate with host B. A TCP Connection is established when host A sends a syn packet to host B. Host B, upon receiving the SYN packet from host A, replies to host A with a SYN+ACK packet. Host A replies with an ACK packet when it receives the SYN+ACK packet from host B. A successful handshake results in the establishment of a TCP connection.

The U.S. Department of Defence proposed the TCP/IP model by combining the 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 exchange data with 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 it becoming garbled or losing data. Layers in the TCP/IP model perform similar functions with similar specifications to the OSI model. The only difference is that they combine the top three layers into a single Application Layer .

Note: During session establishment of a TCP Connection, the client sends SYN packets to the server. The server sends a SYN-ACK packet back to the client and the client sends an ACK packet to the server. This 3 packet handshake is called a 3-way handshake.

Creating Custom Packets Using TCP Flags

Colasoft Packet Builder software is used for creating customized network packets. These customized network packets can penetrate the network for attacks. Customization can also be used to create

fragmented packets. You can download the software from www.colasoft.com.

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 the "Add" button. Select the packet type from the drop-down list. Available options are:

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

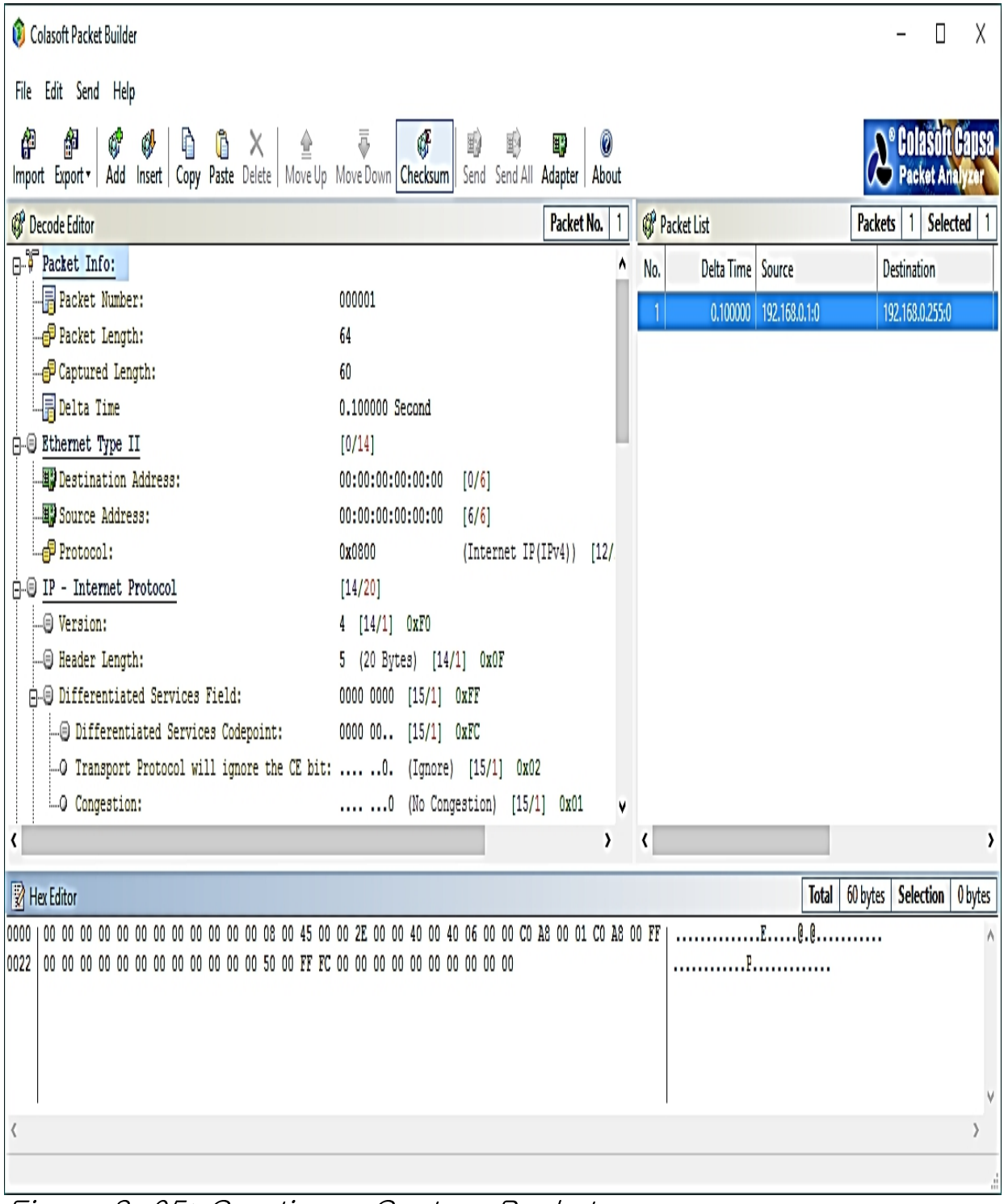


Figure 3-05: Creating a Custom Packet

After selecting the packet type, you can customize the packet. Now select the Network Adapter and send it toward the destination.

Scanning Methodology

The Scanning Methodology includes the following steps:

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

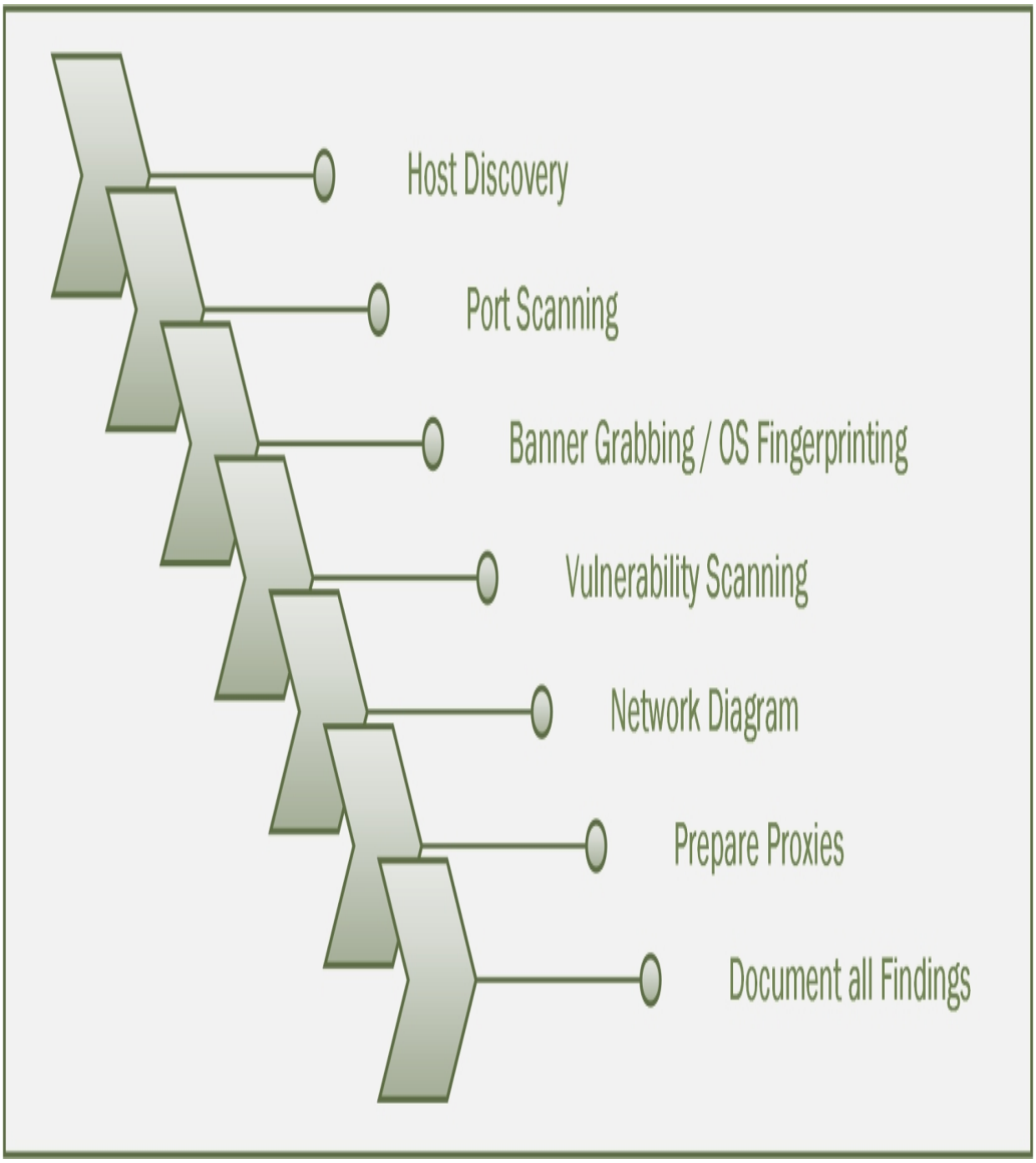


Figure 3-06: Scanning Pentesting

Checking for Live Systems

Initially, you must know about the hosts that live in the targeted network. The process of finding live hosts in a network is carried out by ICMP packets. The target replies to ICMP echo packets with an ICMP echo reply. This response verifies that the host is live.

Figure 3-07: ICMP Echo Request & Reply Packets

The above figure shows that the host with IP address 192. 168.0.2/24 is trying to identify whether the host 192. 168.0. 1/24 is live by sending the ICMP echo packets to the destination IP address 192. 168.0. 1.

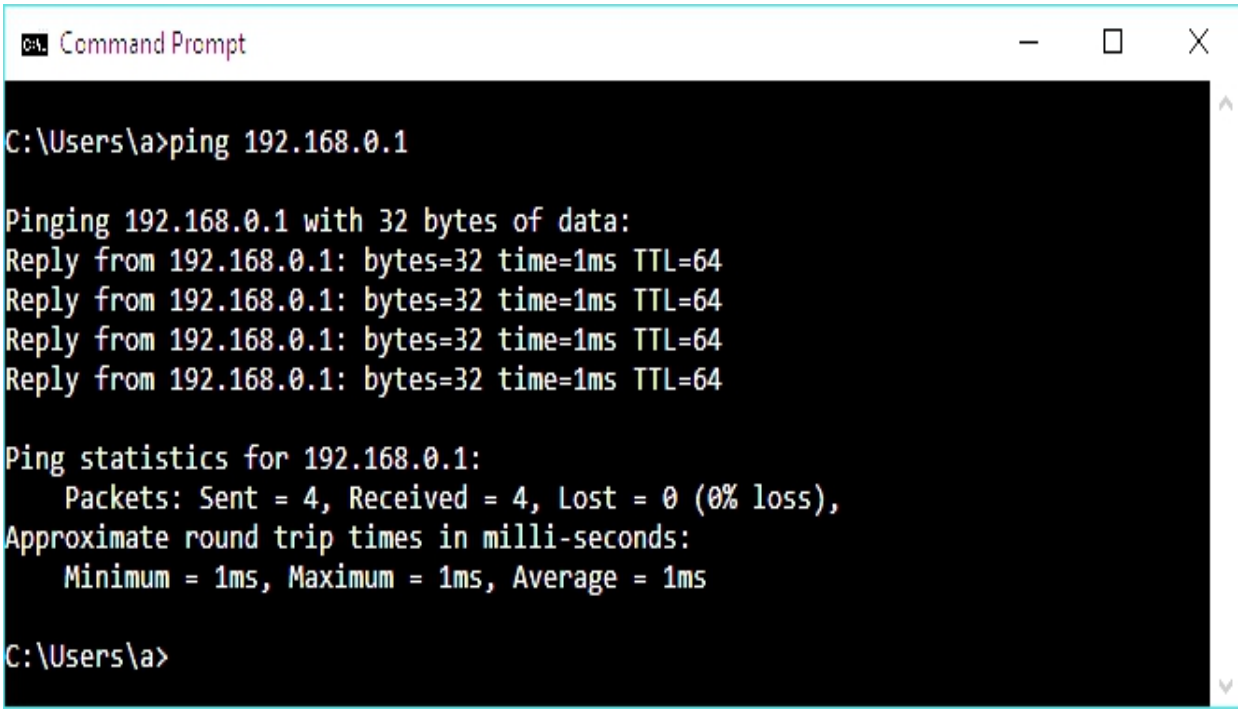


Figure 3-08: ICMP Echo Reply Packets

If the destination host successfully responds to the ICMP echo packets, the host is live. The following response of ICMP echo packets is observed when a destination host is down.

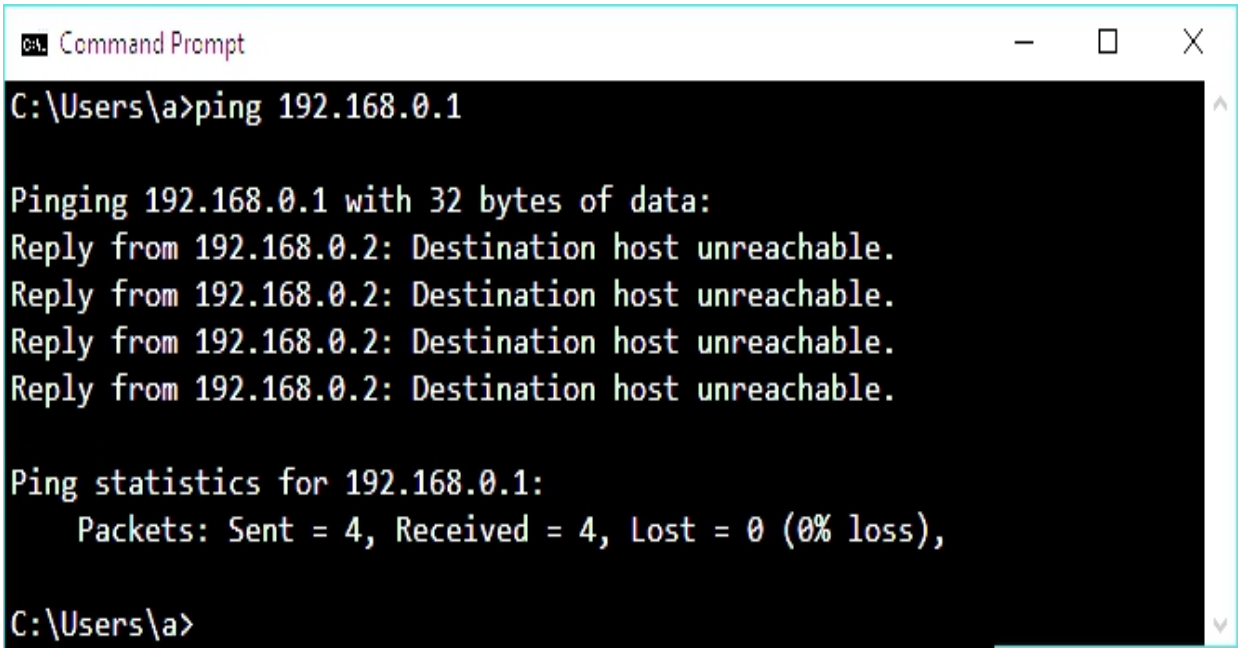


Figure 3-09: ICMP Echo Reply Packets

ICMP Scanning

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

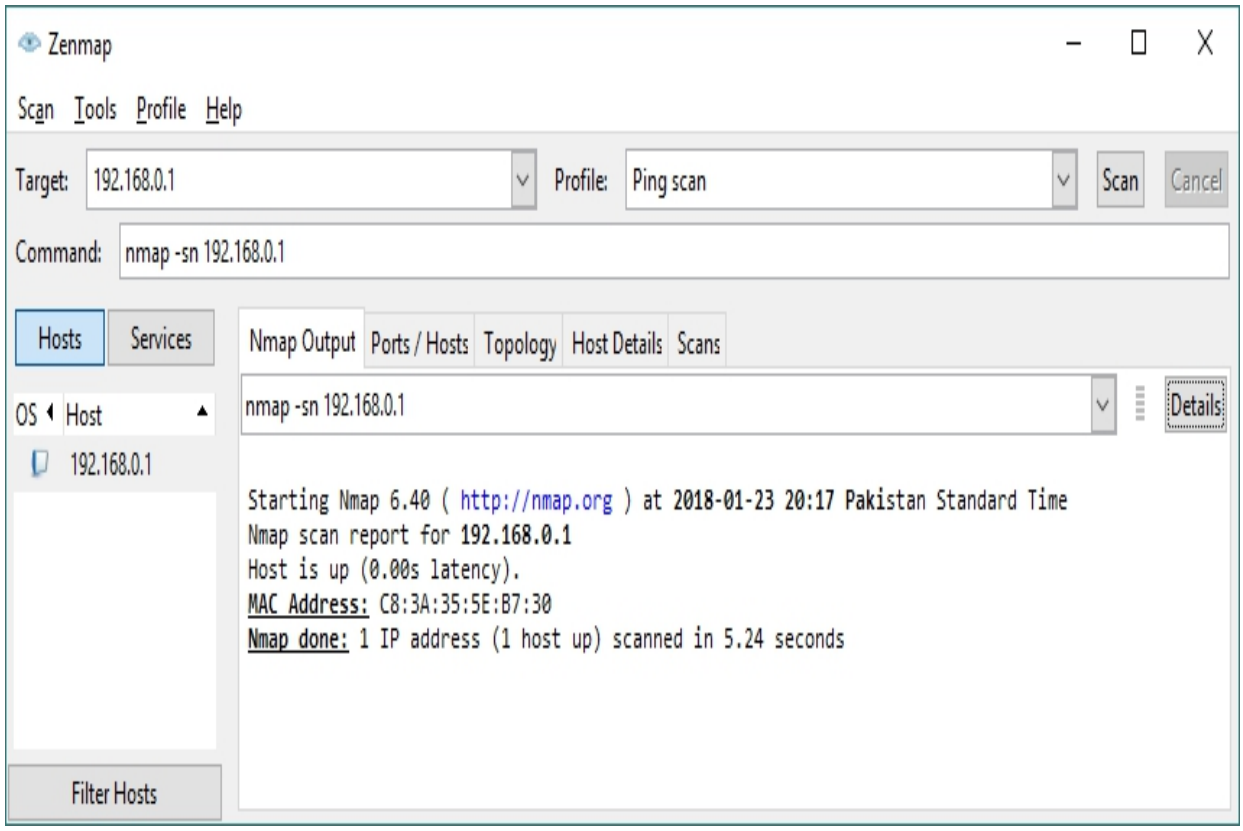


Figure 3-10: ICMP Scanning

Ping Sweep

Ping Sweep determines live hosts on a large scale. Ping Sweep is a method of sending ICMP echo request packets to a range of IP addresses, instead of sending requests one by one, 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.

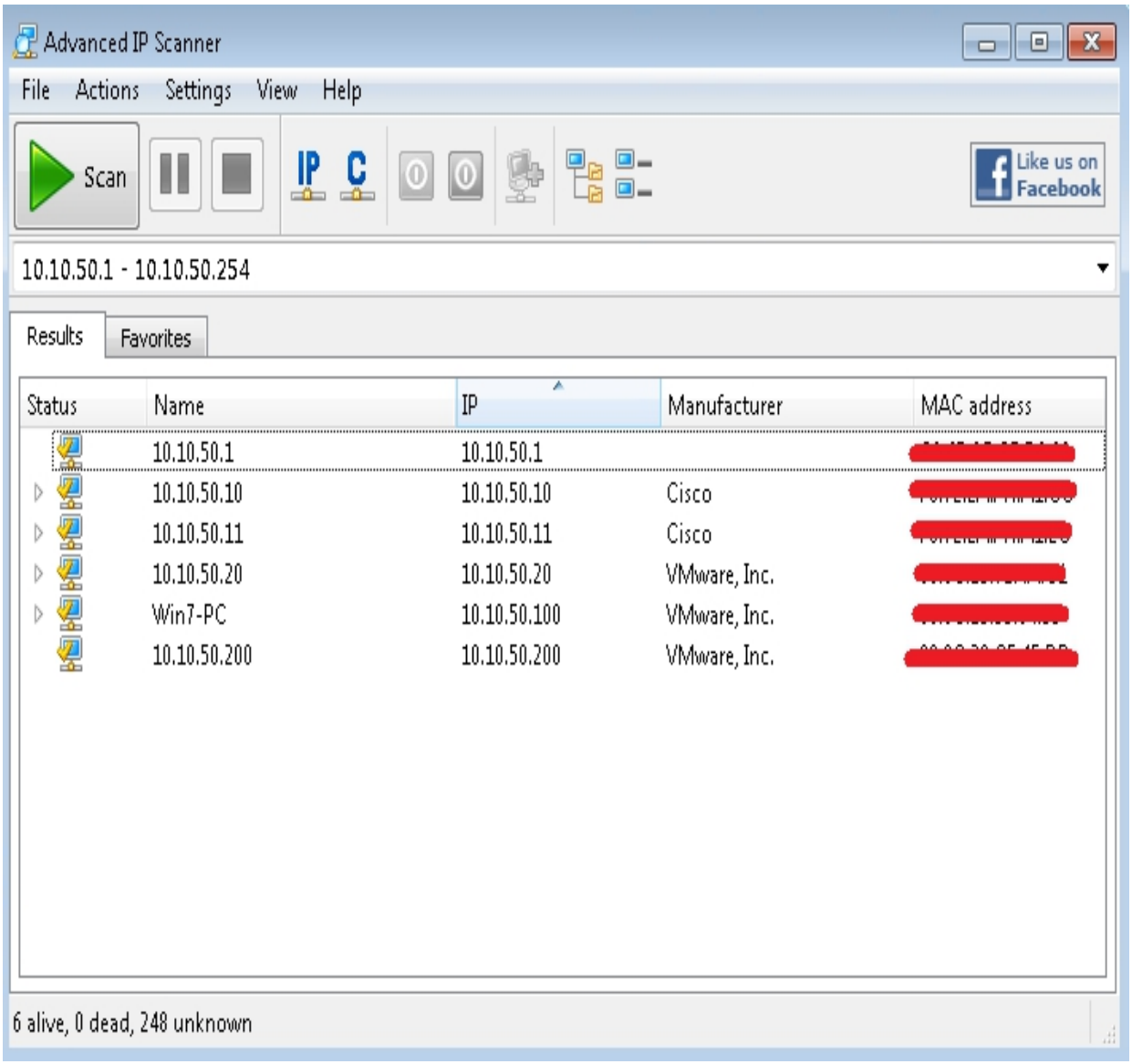


Figure 3-11: Ping Sweep

Check for Open Ports

SSDP Scanning

Simple Service Discovery Protocol (SSDP) is a protocol used for discovering network services without the assistance of server-based configuration like Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and static network host configuration. SSDP can discover Plug and 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 the 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 ping sweep, Nmap also offers a quick scan. Enter the following command for a quick scan:

nmap -sP -PE -PA< *port numbers* > < *starting IP/ending IP* >
For example:
nmap -sP -PE -PA 2 1,23,80,3389 < 192. 168.0. 1-50>

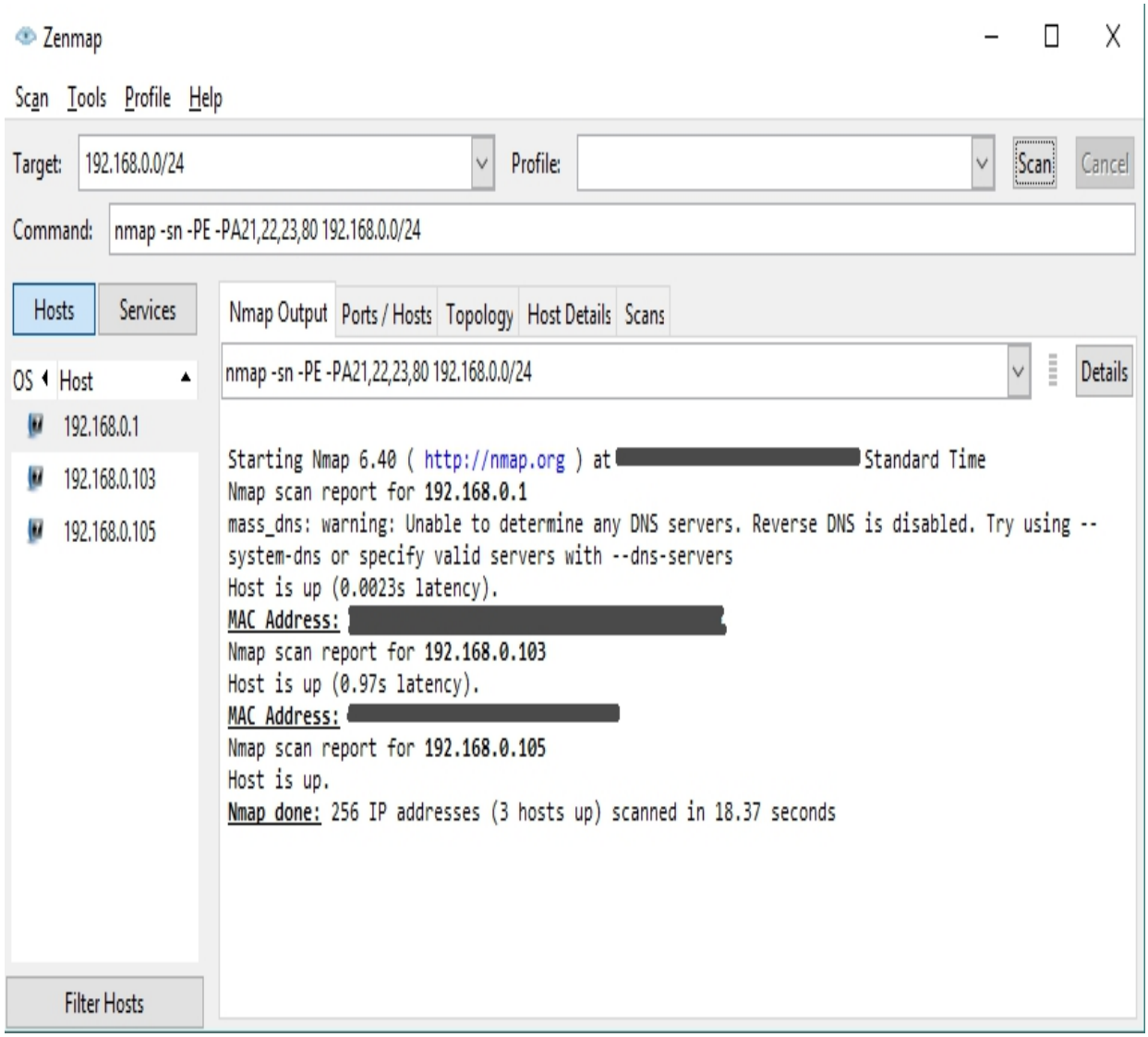


Figure 3-12: Nmap

Nmap, in a nutshell, offers host discovery, port discovery, service discovery, version information of an Operating System, hardware address (MAC) information, service version detection, vulnerabilities, and exploit detection using the Nmap Scripting Engine (NSE).

Note: Nmap Scripting engine is the most powerful engine for network discovery, version detection, vulnerability detection, and backdoor detection.

Lab 3- 1: Hping Commands

Case Study: The Nmap utility for Windows-based operating systems is called Zenmap. We will be using the Zenmap application to perform Nmap with its different options. We will be using a Windows 7 PC for scanning the network.

Procedure:
By ping scanning the network 10. 10.50.0/24, the result lists the machines that respond to the ping.
Command: nmap -sP 10. 10.50.0/24

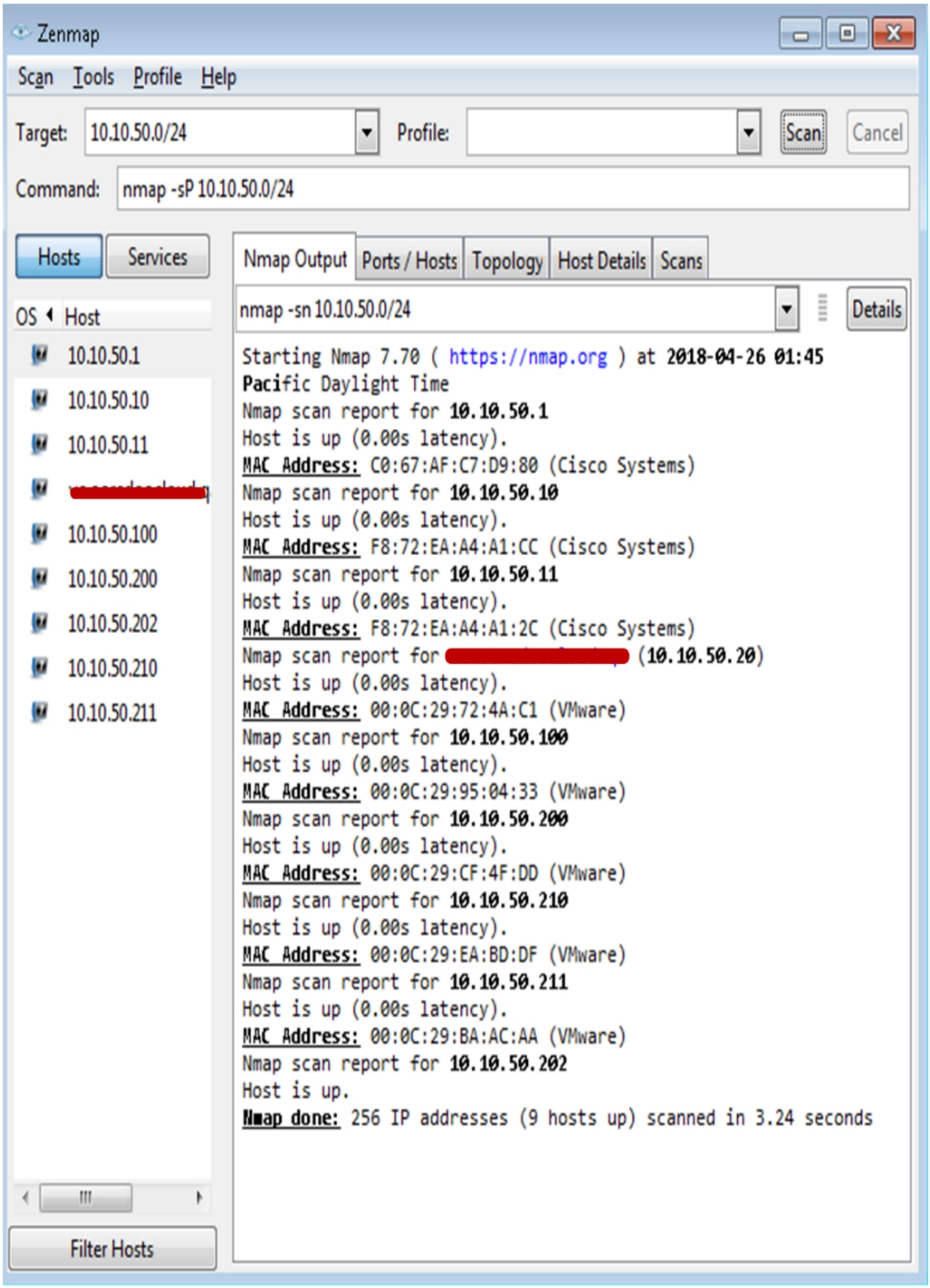

Zenmap
Scan Tools Profile Help
Target: 10.10.50.0/24
Profile:
Scan
Cancel
Command: nmap -sP 10.10.50.0/24
Hosts
Services
OS Host
10.10.50.1
10.10.50.10
10.10.50.11
10.10.50.100
10.10.50.200
10.10.50.202
10.10.50.210
10.10.50.211
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sn 10.10.50.0/24
Details
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, scan for Operating System details of target host 10. 10.50.2 10. We can scan for all hosts using the command nmap -O 10. 10.50 .*

Command: nmap -O 10. 10.50.2 10

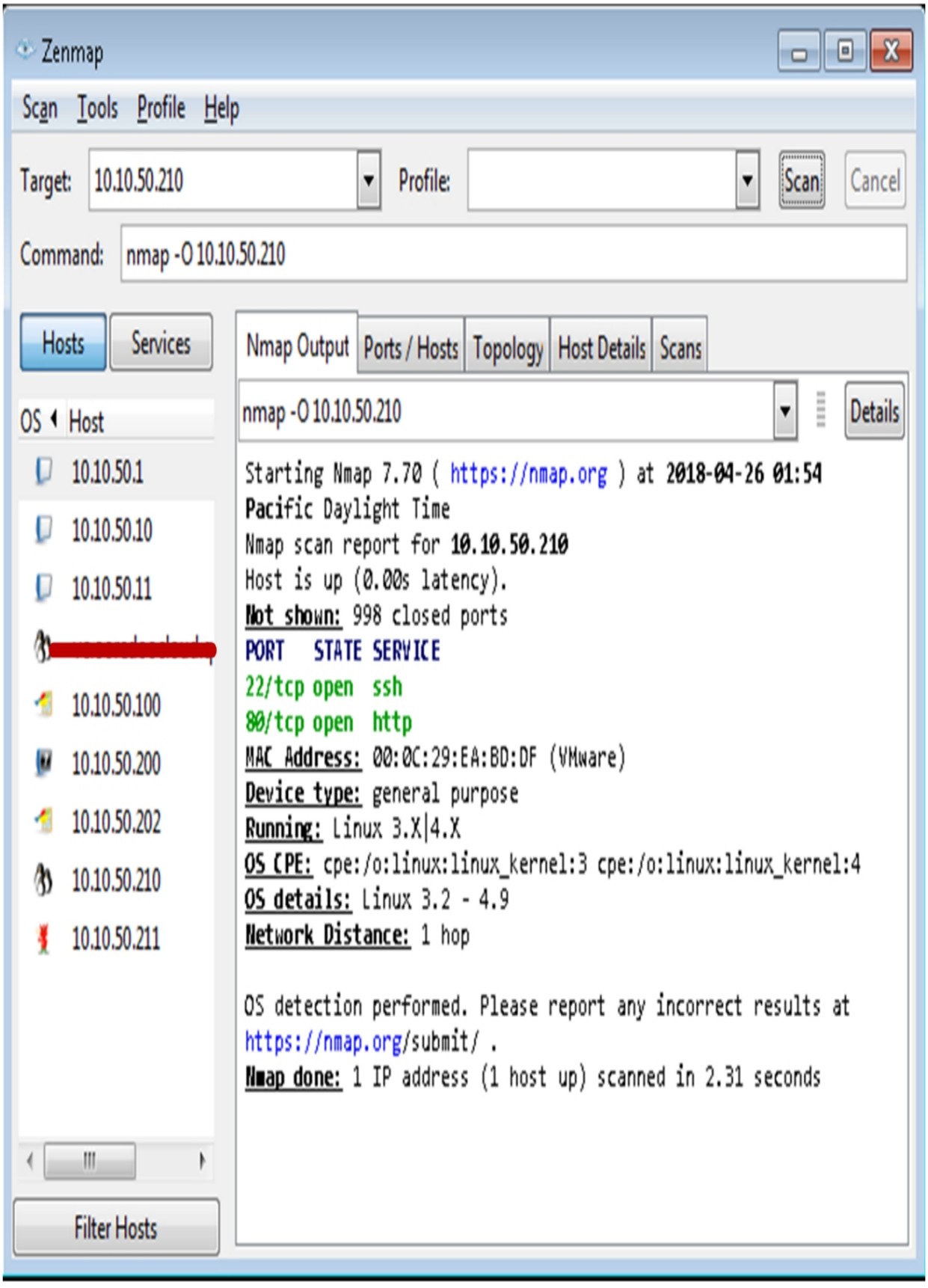

Zenmap
Scan Tools Profile Help
Target: 10.10.50.210
Profile:
Scan
Cancel
Command: nmap -O 10.10.50.210
Hosts
Services
OS Host
10.10.50.1
10.10.50.10
10.10.50.11
10.10.50.100
10.10.50.200
10.10.50.202
10.10.50.210
10.10.50.211
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -O 10.10.50.210
Details
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. It then displays the target reply as the ping command displays the ICMP echo reply packet from the targeted host. Hping can also handle fragmentation, arbitrary packets' body and size, and file transfer. It supports TCP, UDP, ICMP, and RAW-IP protocols. By 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 and others

Figure 3-15: Hping3

Lab 3-2: Hping Commands

Case Study: Using Hping commands on Kali Linux, we will be 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**

Figure 3-16: Sending a Customized Packet Using the Hping3

Command

To create SYN, scan against different ports:

root@kali:~# hping3 8 1-600-S 10. 10.50.202

Figure 3-17: Sending a Customized Packet Using the Hping3 Command

To create a packet with FIN, URG, and PSH, flag sets: root@kali:~# hping3-F -P -U 10. 10.50.202

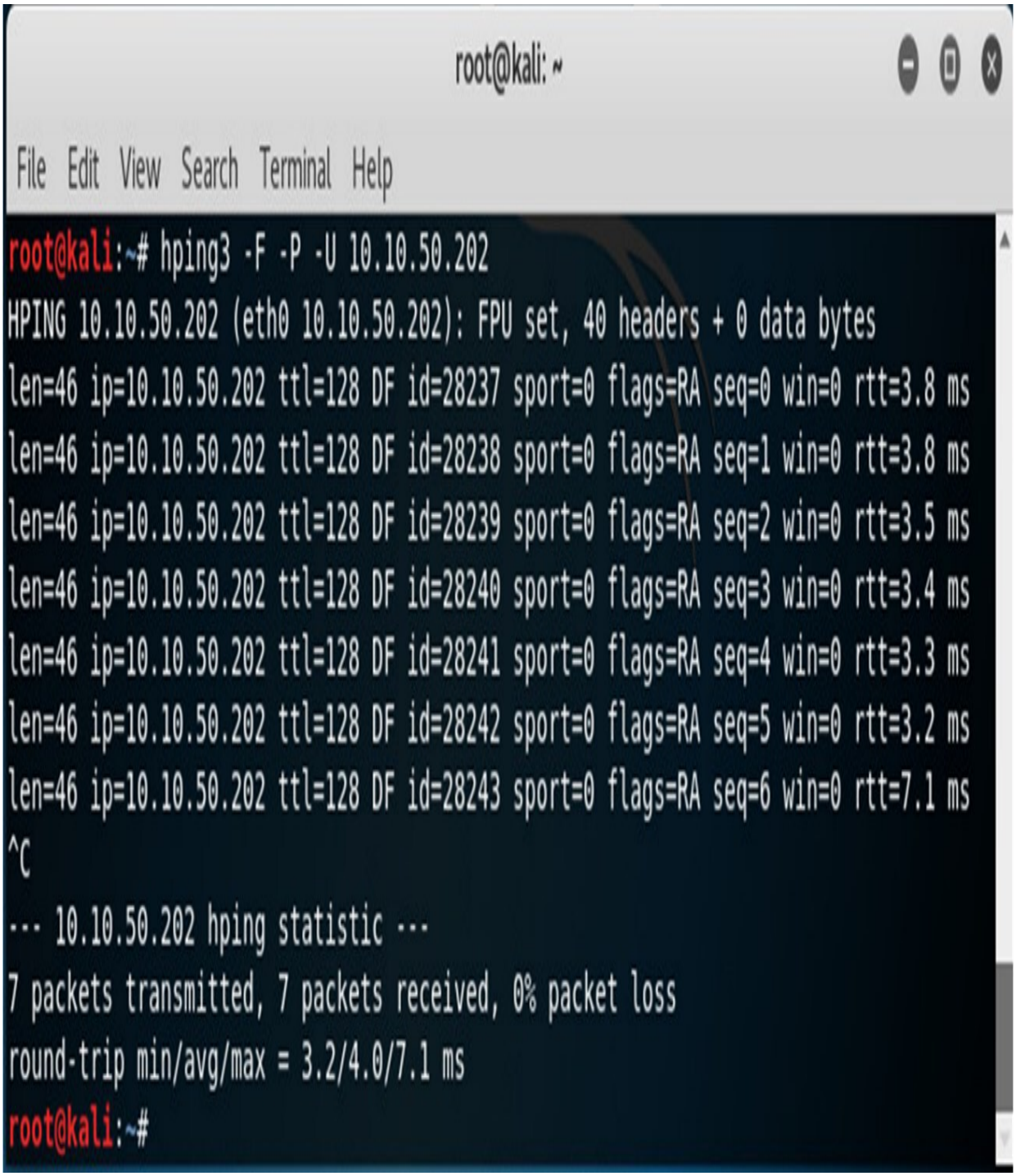


Figure 3-18: Sending a Customized Packet Using the Hping3 Command

The following are some options used with the Hping command:

-h --help
-v --version

-c --count
-I --interface

--flood
-V --verbose
-0 --rawip
- 1 --icmp Show Help

Show Version
Packet Count
Interface Name
Send packets as fast as possible. Don't show replies.

Verbose Mode
RAW IP Mode
ICMP Mode
-2 --udp
-8 --scan
-9 --listen

--rand-dest
--rand-source

-s --baseport
-p --destport
-Q --seqnum
-F --fin
-S --syn
-P --push
-A --ack
-U --urg

--TCP-timestamp UDP Mode
Scan Mode

Listen Mode
Random Destination Address Mode Random Source Address Mode
Base Source Port (default random)

[+][+]<port> Destination Port(default 0) ctrl+z inc/dec Show only TCP sequence number
Set FIN Flag
Set SYN Flag
Set PUSH Flag
Set ACK Flag
Set URG Flag
Enable the TCP timestamp option to guess the HZ/uptime

Table 3-02: Hping3 Command Options

Scanning Techniques

Scanning techniques include UDP and TCP scanning. The following figure shows the classification of scanning techniques:

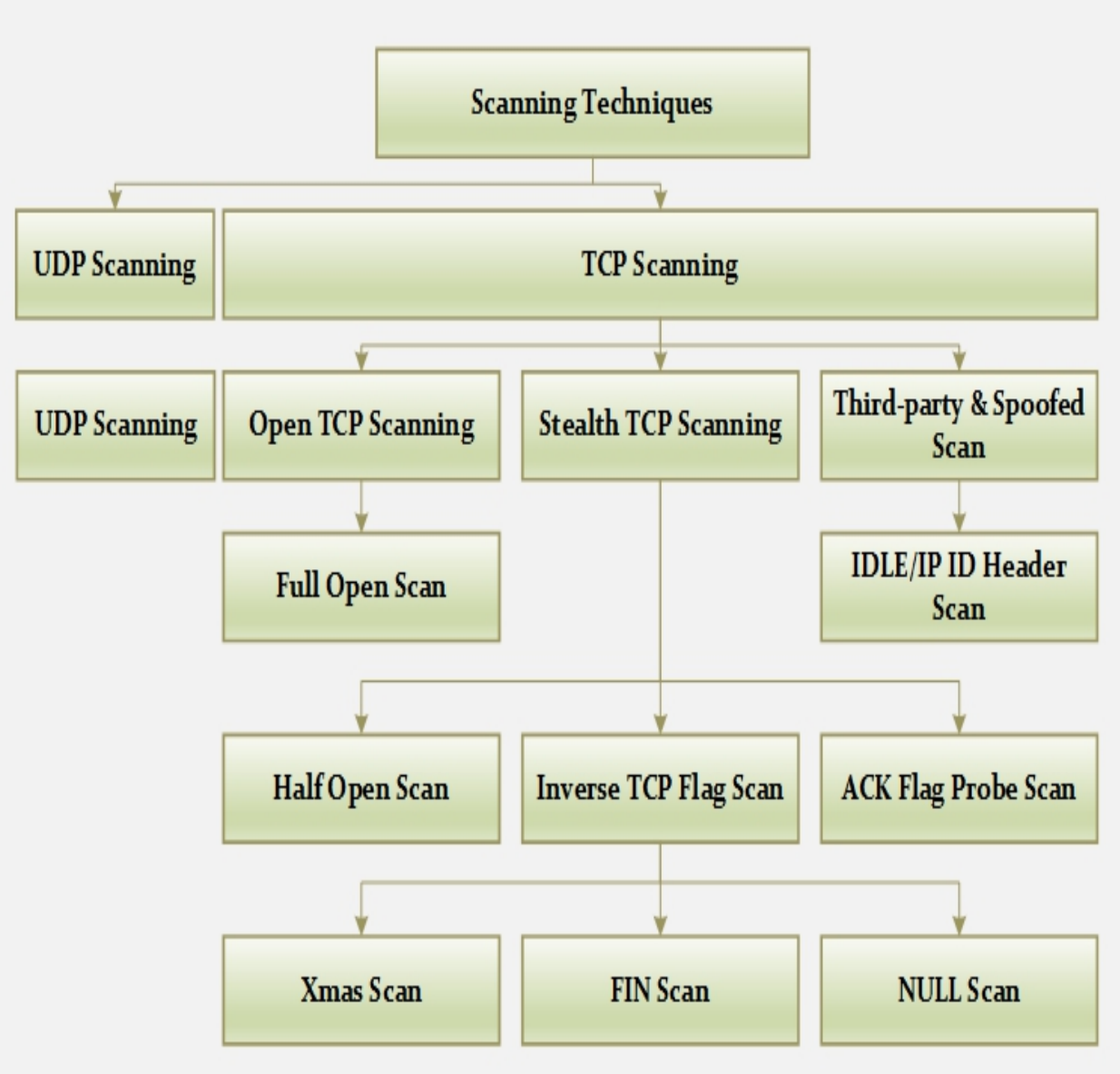


Figure 3-19: Scanning Techniques

TCP Connect / Full Open Scan

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

If a closed port is encountered while using Full Open Scanning, the RST response is sent to the incoming request to terminate the attempt. To

perform a Full Open Scan, you must use the -sT option for Connect Scan.

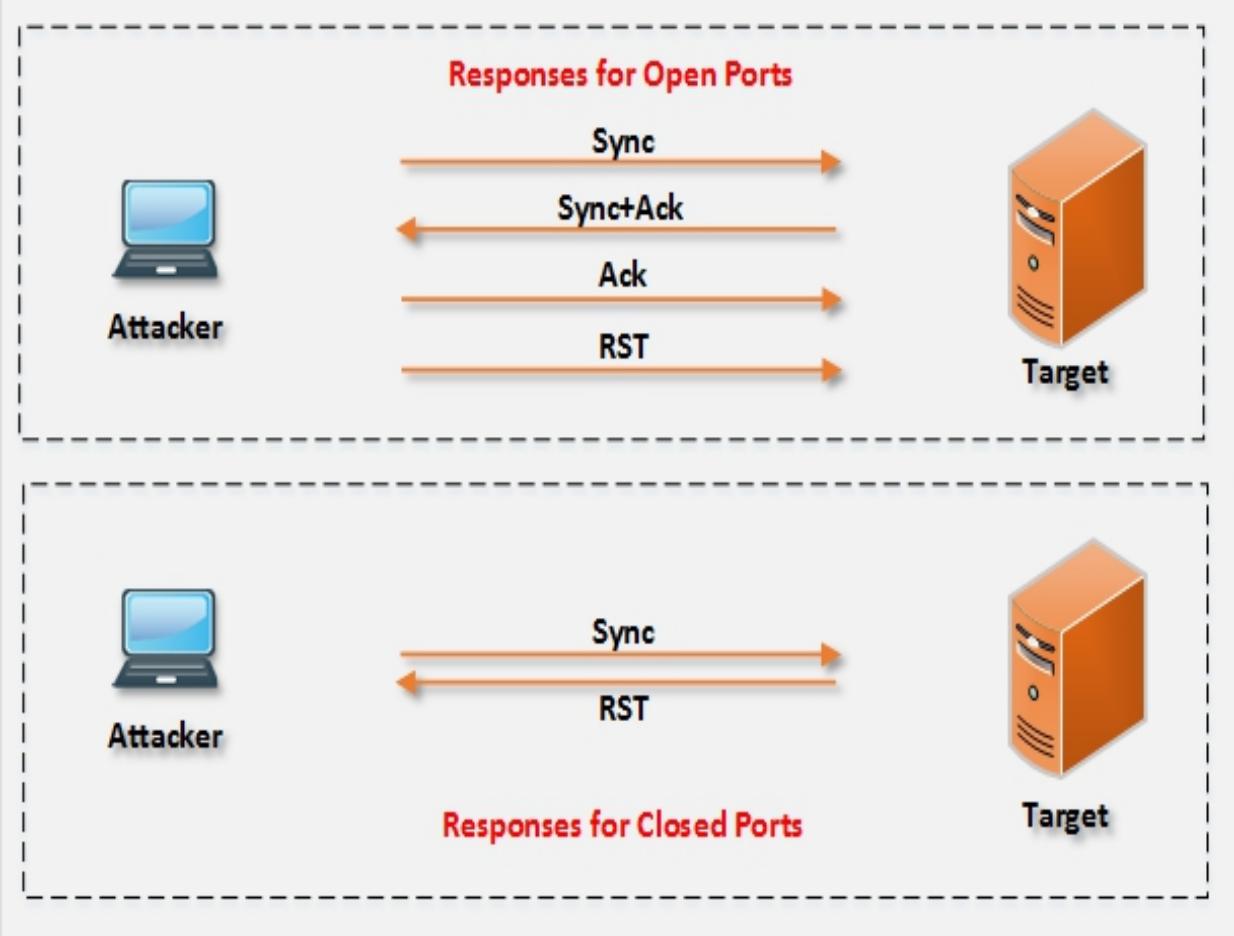


Figure 3-20: TCP Connection Responses

Type the command to execute Full Open Scan:
nmap -sT < *ip address or range* >

For example, observe the output shown in the figure below. The Zenmap tool is used to perform a Full Open Scan.

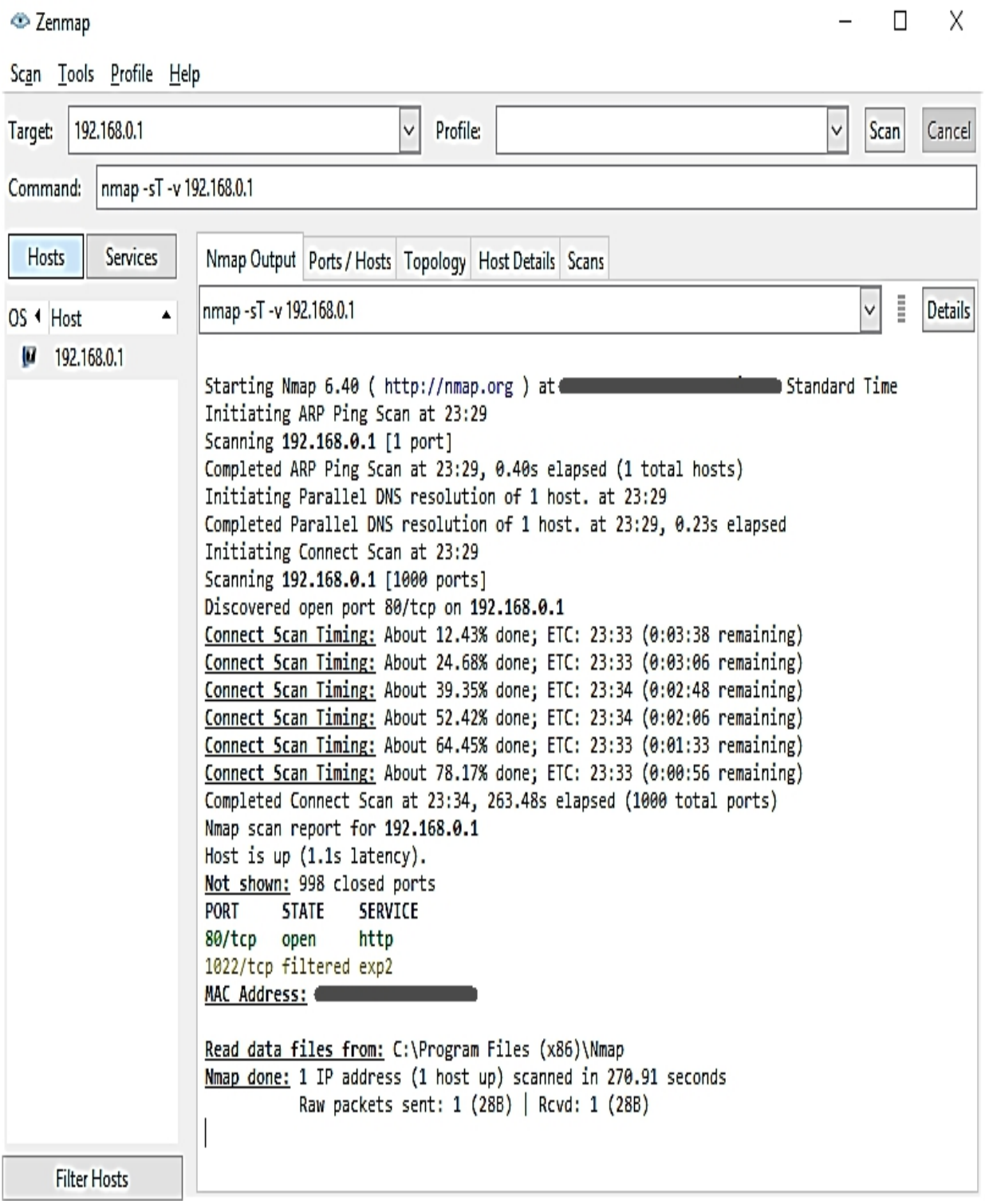


Figure 3-21: Full Open Scan

Stealth Scan (Half-Open Scan)

Stealth Scan is also known as Half-Open Scan. To understand the Half-Open Scan processes, consider the scenario of two hosts: host A and host B. Host A is the initiator of the TCP connection handshake. Host A sends the SYN packet to initiate the handshake. The receiving host (host B) replies with the SYN+ACK packet. Instead of acknowledging host B with an ACK packet, host A responds with RST.

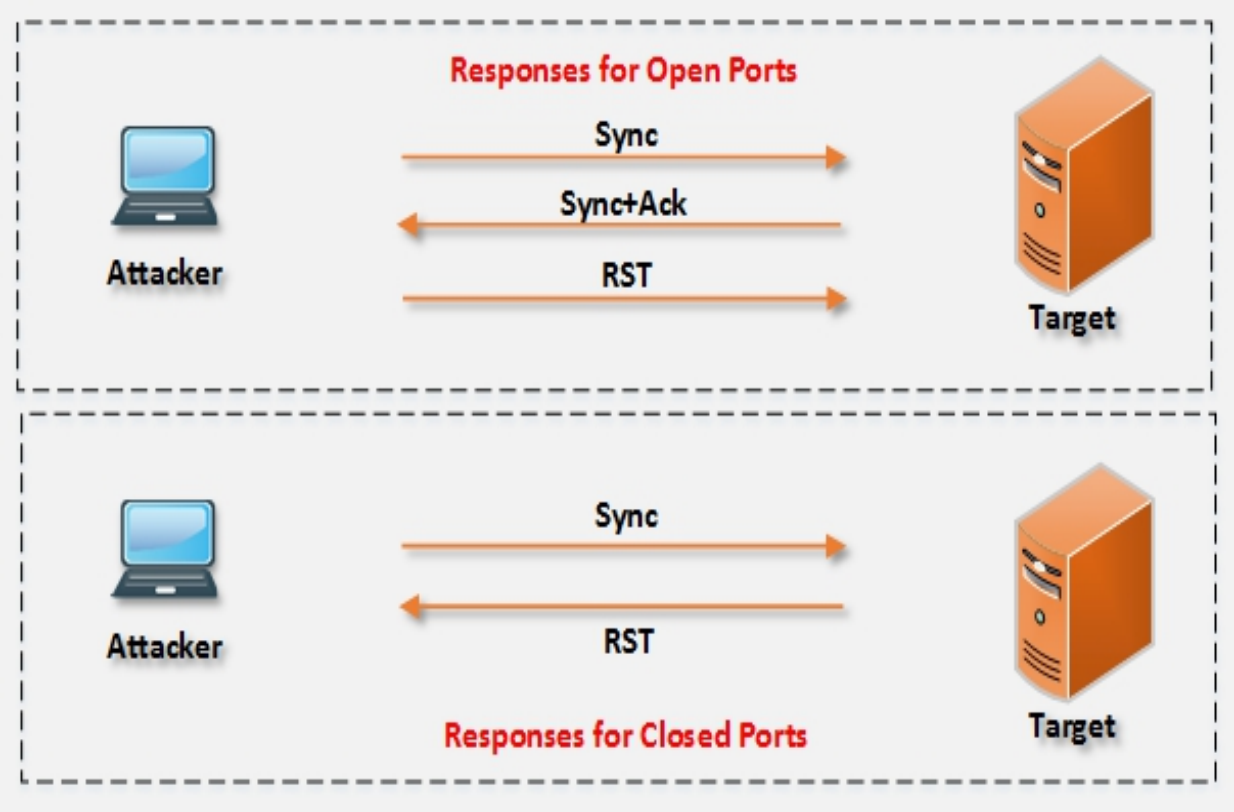


Figure 3-22: Half-Open Scan

To perform this type of scan in Nmap, use the following syntax:
nmap -sS < *ip address or range* >
Observe the result in figure 3-23:

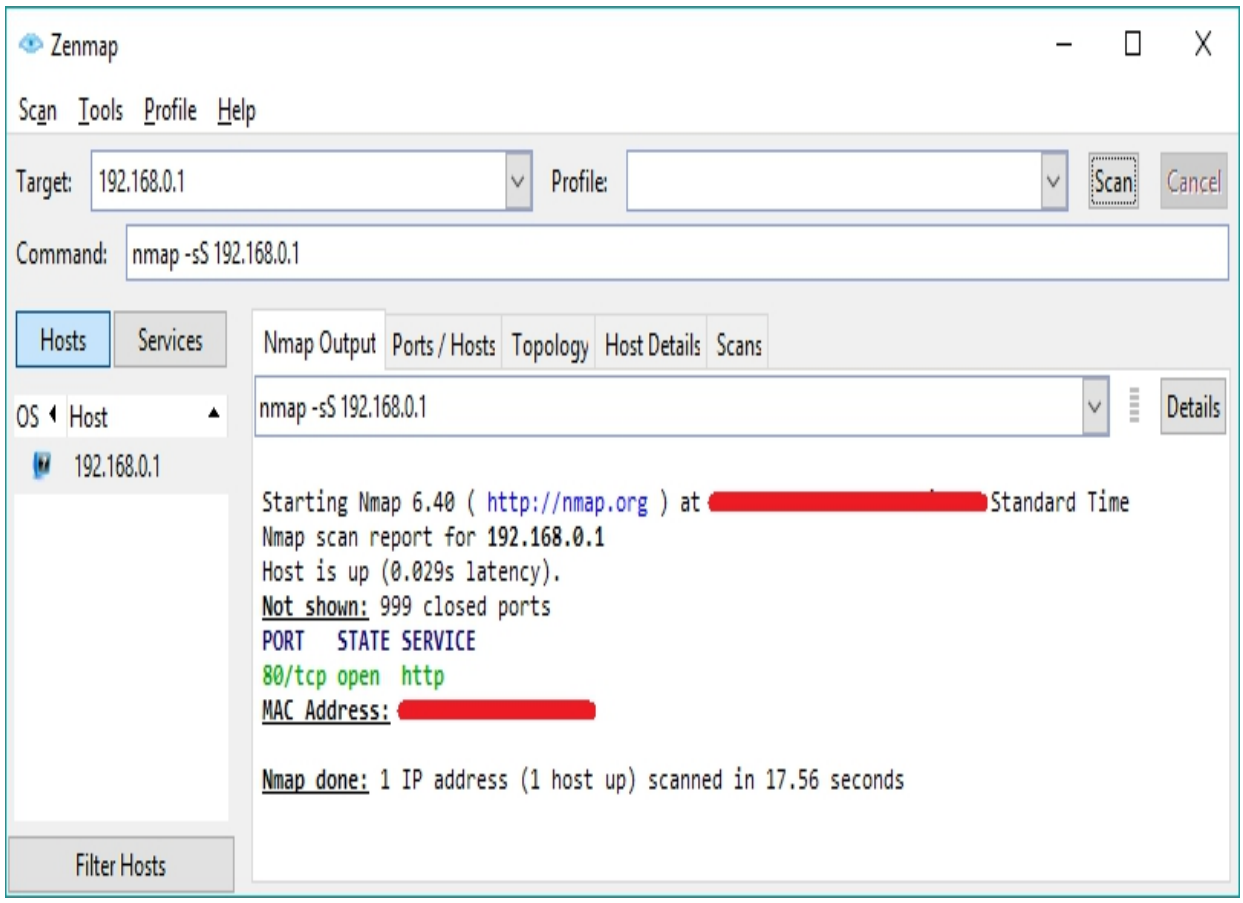


Figure 3-23: Half-Open Scan

Inverse TCP Flag Scanning

Inverse TCP Flag Scanning is a scanning process in which a sender either sends a TCP probe with TCP flags, i.e., FIN, URG, and PSH, or without flags. Probes with TCP flags are known as XMAS Scanning. If a flag set is not present, it is called Null Scanning.

Xmas Scan

Xmas Scan is a type of scan that contains multiple flags. A packet is sent to the target along with URG, PSH, and FIN; a packet having all flags creates an abnormal situation for the receiver. The receiving system has to make a decision when this condition occurs. The closed port responds with a single RST packet. If the port is open, some systems respond as an open port, but the modern system ignores or drops these requests because the combination of these flags is false. FIN Scan works only with Operating Systems with RFC793 based

TCP/IP implementation. FIN Scan does not work with any current version of Windows, i.e., Windows XP, Windows Vista, and so forth.

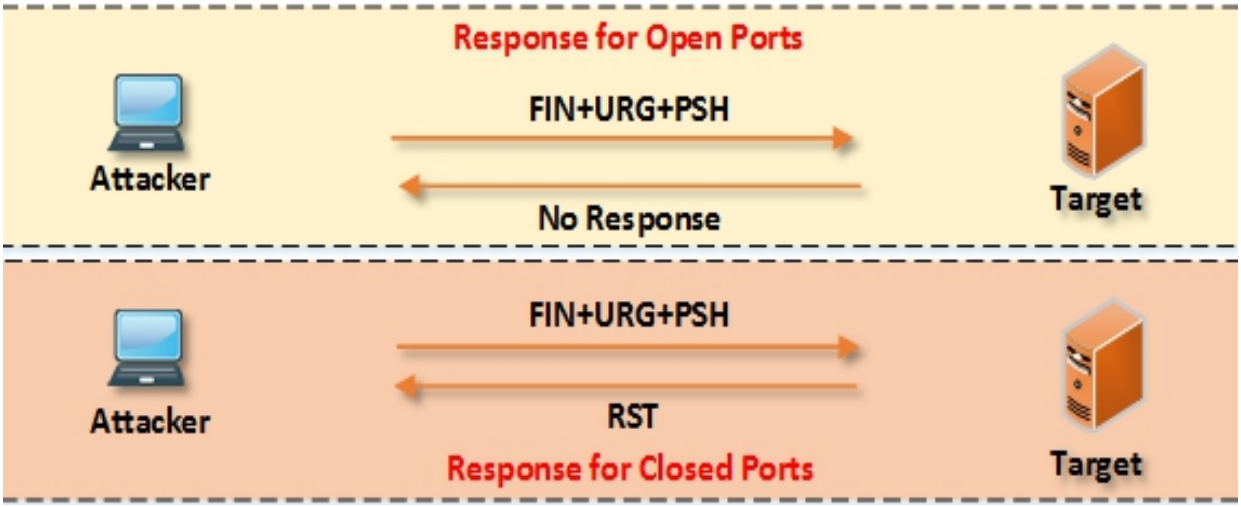


Figure 3-24: Xmas Scan

To perform this type of scan, use the following syntax:

nmap -sX -v < *ip address or range* >

Lab 3-3: Xmas Scanning

Case Study: Using Xmas Scanning on Kali Linux, we are pinging a Windows Server 20 16 host with firewall enabled and disabled state to observe the responses. Procedure:

Open Windows Server 20 16 and verify whether the firewall is enabled.

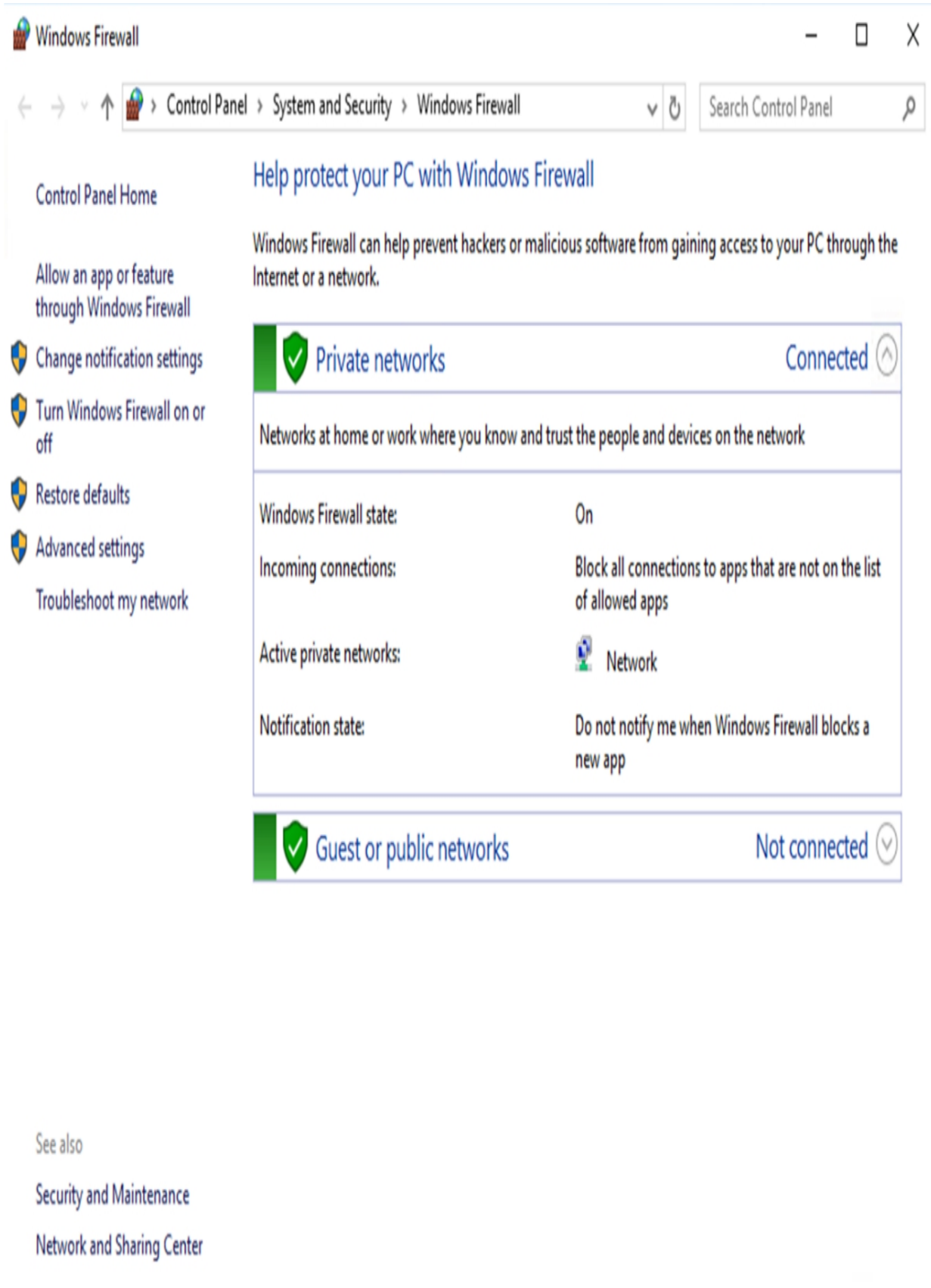

Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC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

Figure 3-25: Windows Firewall Settings

Open a terminal on your Kali Linux and enter the command as shown in the figure below:

Figure 3-26 Xmas Scanning

Observe the output shown in figure 3-26; all scanned ports are **Open** and **Filtered** . This means that the firewall is enabled. A firewall basically did not respond to these packets. Hence, it is assumed that scanned

ports are open and filtered.
Now, go back to Windows Server 20 16 and disable the firewall.

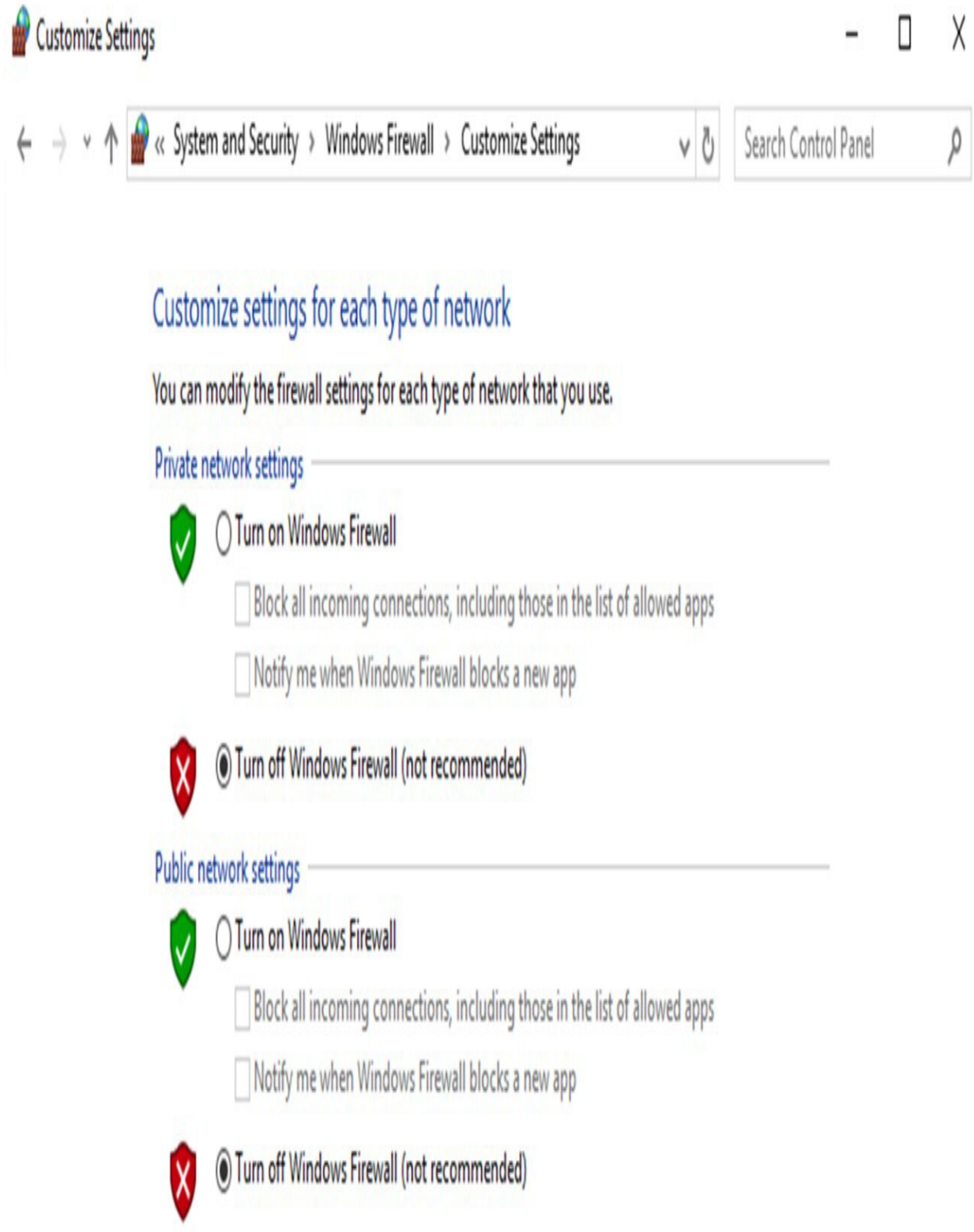


Figure 3-27: Disabling the Firewall

Now again, run the scan.

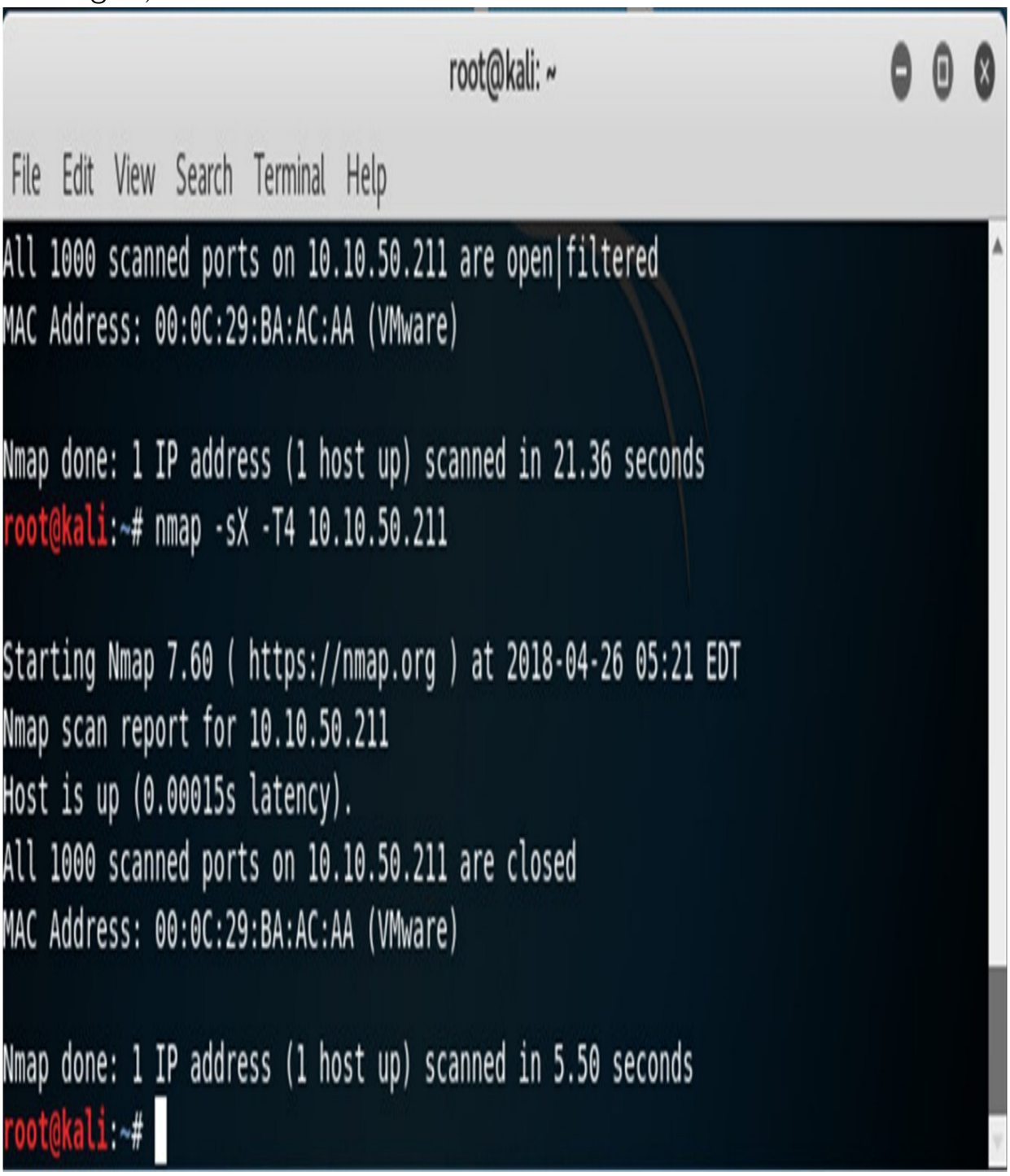


Figure 3-28: Xmas Scanning

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

FIN Scan

FIN Scan is the process of sending the packet that only has the FIN flag set. These packets have the tendency to pass through several firewalls. When FIN Scan packets are 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 following syntax:
nmap -SF < *ip address or range* >

NULL Scan

NULL Scan is the process of sending a packet without any flag set. Responses are similar to FIN and XMAS Scan. During a Null Scan, if a packet is sent to an open port, there is no response. If a packet is sent to a closed port, it responds with an RST packet. It is comparatively easy to be detected while performing this scan as there is logically no reason to send a TCP packet without any flag.

To perform this type of scan, use the following syntax:
nmap -sN < *ip address or range* >

ACK Flag Probe Scanning

The ACK flag Scanning technique sends a TCP packet with ACK flag set toward the target. The sender examines the header information because even when the ACK packet has made its way toward the target, it replies with an RST packet in both cases, either when the port is open or closed. After analyzing the header information such as TTL and WINDOW fields of the RST packet, the attacker verifies whether the port is open or closed.

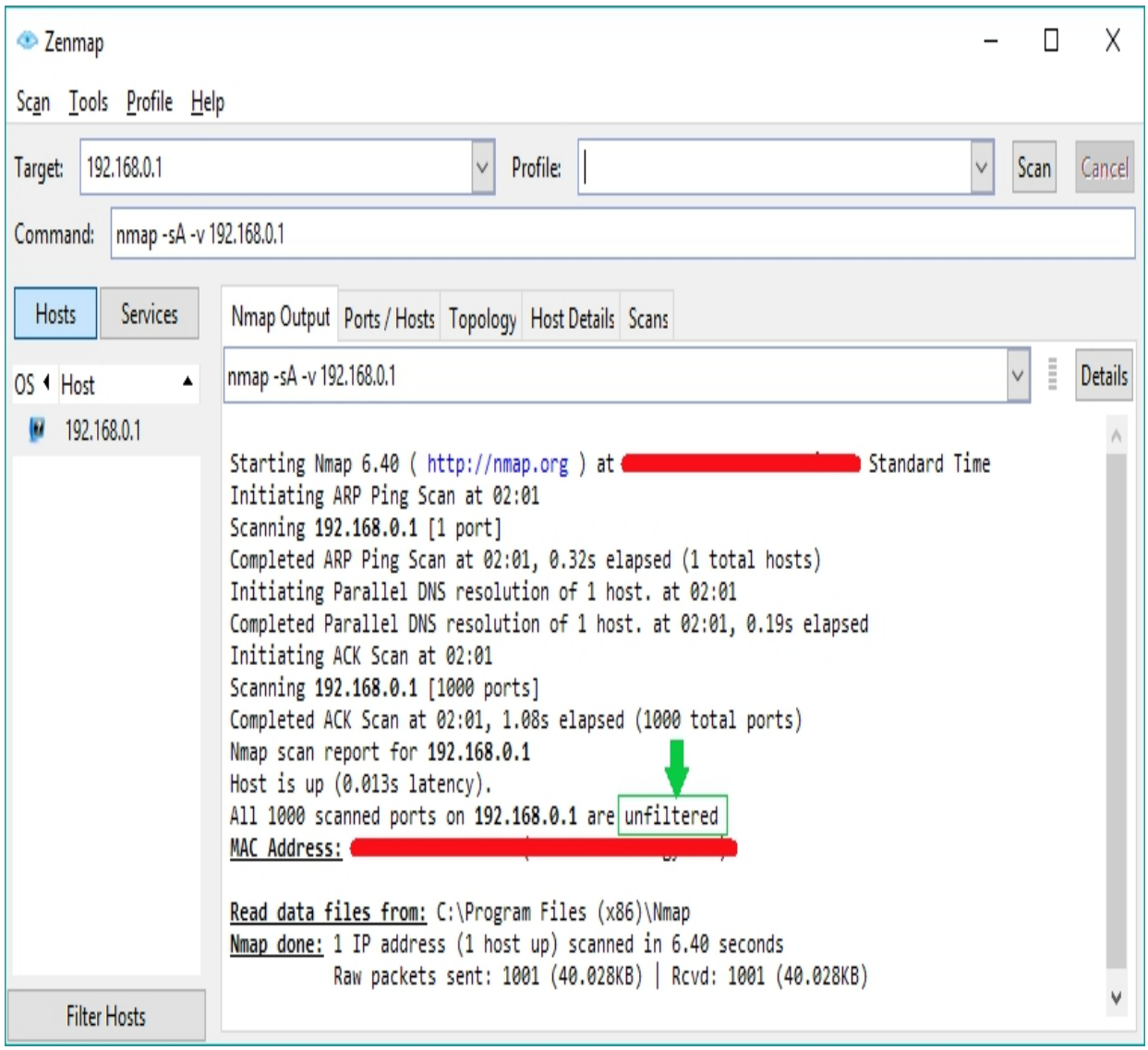


Figure 3-29: Ack Flag Probe Scanning

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

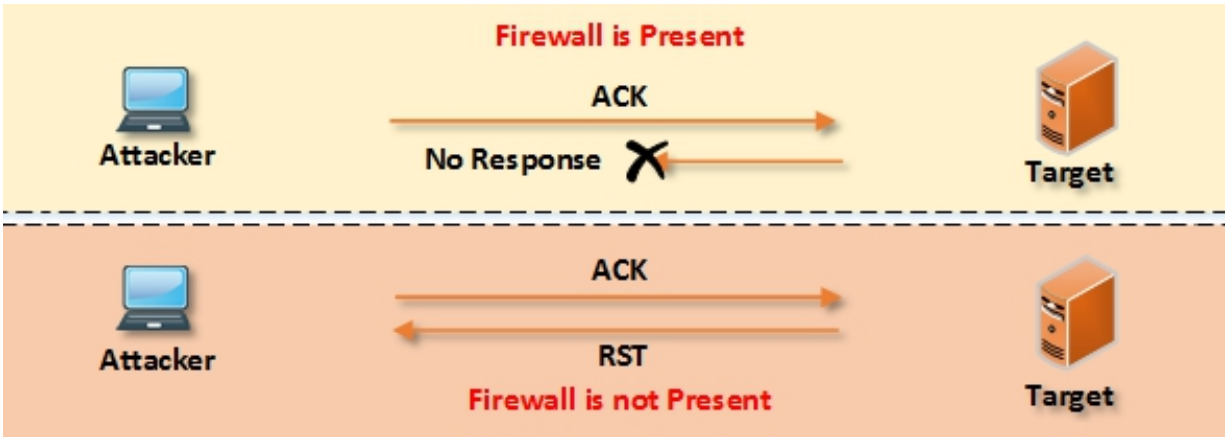


Figure 3-30: Ack Flag Probe Scanning Response

IDLE/IPID Header Scan

IDLE/IPID Header Scan is a unique and effective technique for identifying the target host's port status. This scan is capable of remaining low profile. Idle scanning describes the attacker's hidden ability. The attacker hides her/his identity by bouncing packets

from the Zombie's system. If the target investigates the threat, it traces the Zombie rather than the attacker.

Before understanding the steps required for the IDLE/IPID Scan, you must keep the following important points in mind:
• To determine an open port, send SYN packet to the port
• Target machine responds with the SYN+ACK packet if the port is open • Target Machine responds with the RST packet if the port is closed • The unsolicited SYN+ACK packet is either ignored or responded to with RST • Every IP packet has a Fragment Identification Number (IPID) • OS increments IPID for each packet

Step: 0 1 • Send SYN+ACK packet to Zombie to get its IPID Number

• Zombie is not waiting for SYN+ACK, hence responds with RST packet. Its reply discloses the IPID
• Extract IPID from Packet

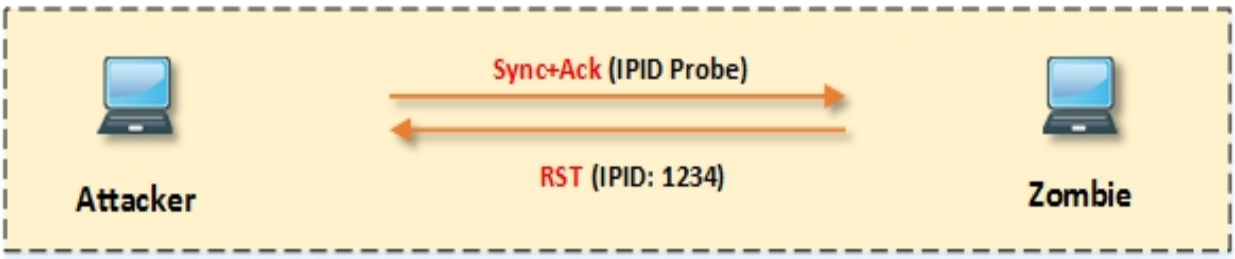


Figure 3-31: Idle Scanning

Step: 02

• Send SYN packet to the target with spoofed IP address of Zombie
• IP port is open; target replies with SYN+ACK to Zombie and Zombie replies back to target with RST packet

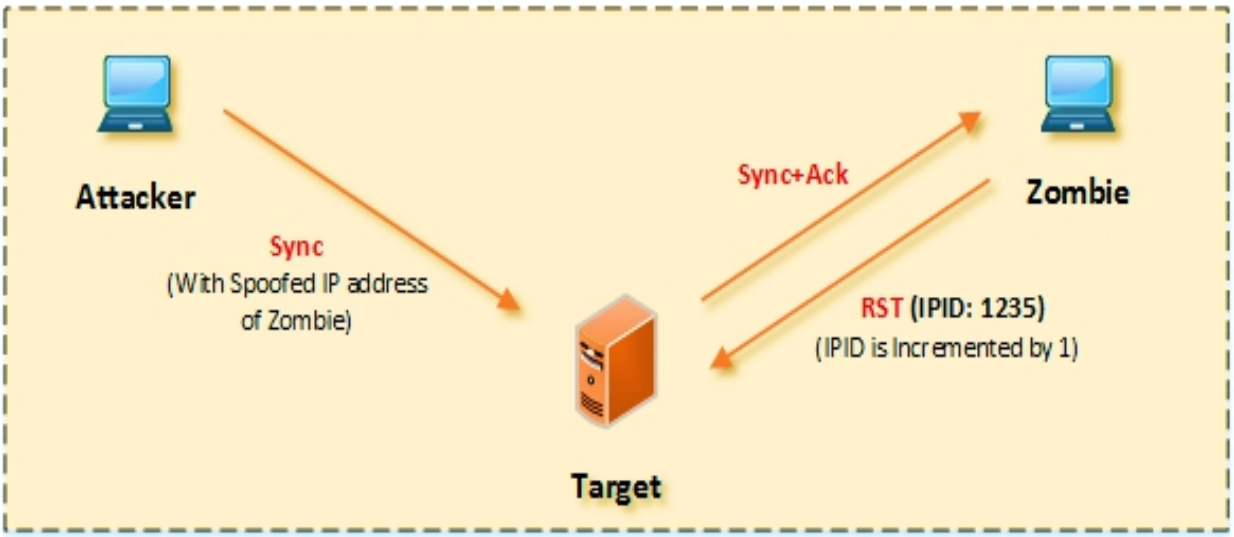


Figure 3-32: Idle Scanning

• If the port is closed, target replies with RST to Zombie and Zombie does not reply back to the target. IPID of Zombie is not incremented

Figure 3-33: Step#02 Idle Scanning

Step: 03

• Send SYN+ACK packet to Zombie again, to receive and compare its IPID Numbers to the IPID extracted in step 0 1 (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

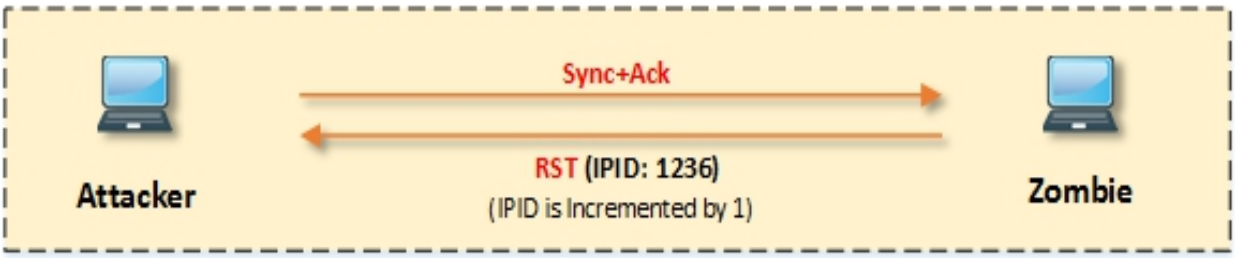


Figure 3-34: Idle Scanning

- Port is closed if IPID is incremented by 1 *UDP Scanning*

Like TCP-based scanning techniques, there are also UDP scanning methods. Keep in mind that UDP is a connectionless protocol. UDP does not have flags. UDP packets work with ports; no connection orientation is required. No response will be received if the targeted port is open; however, if the port is closed, the response message will be received stating "Port unreachable". Most of the malicious programs, Trojans, and spywares use UDP ports to access the target.

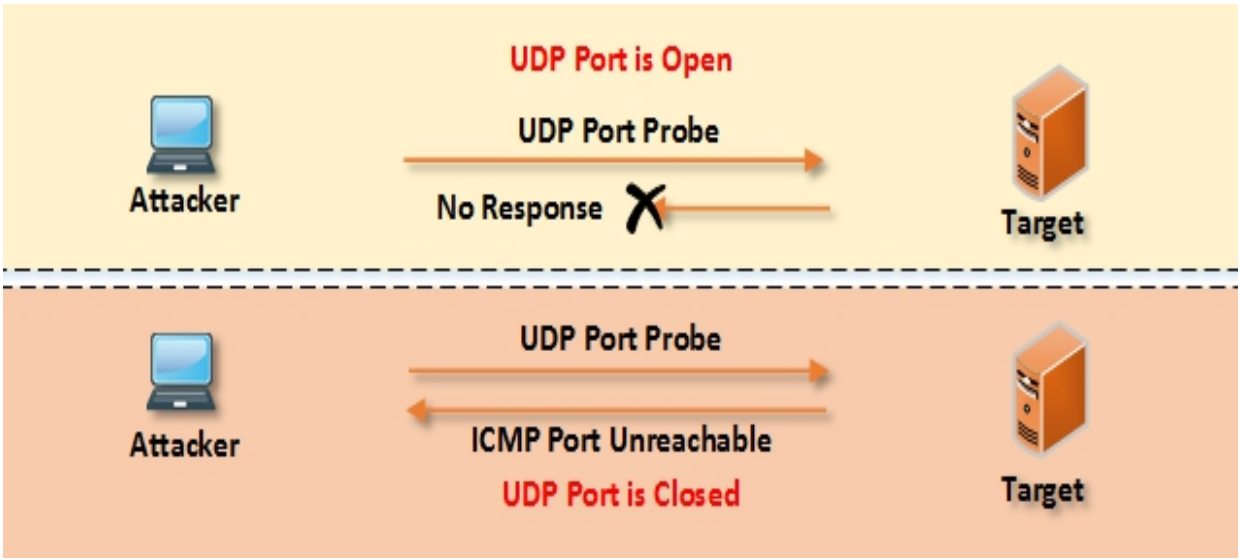


Figure 3-35: UDP Scanning Response

To perform this type of scan in Nmap, use the following syntax: nmap -sU -v < *ip address or range* > Observe the result in the following figure:

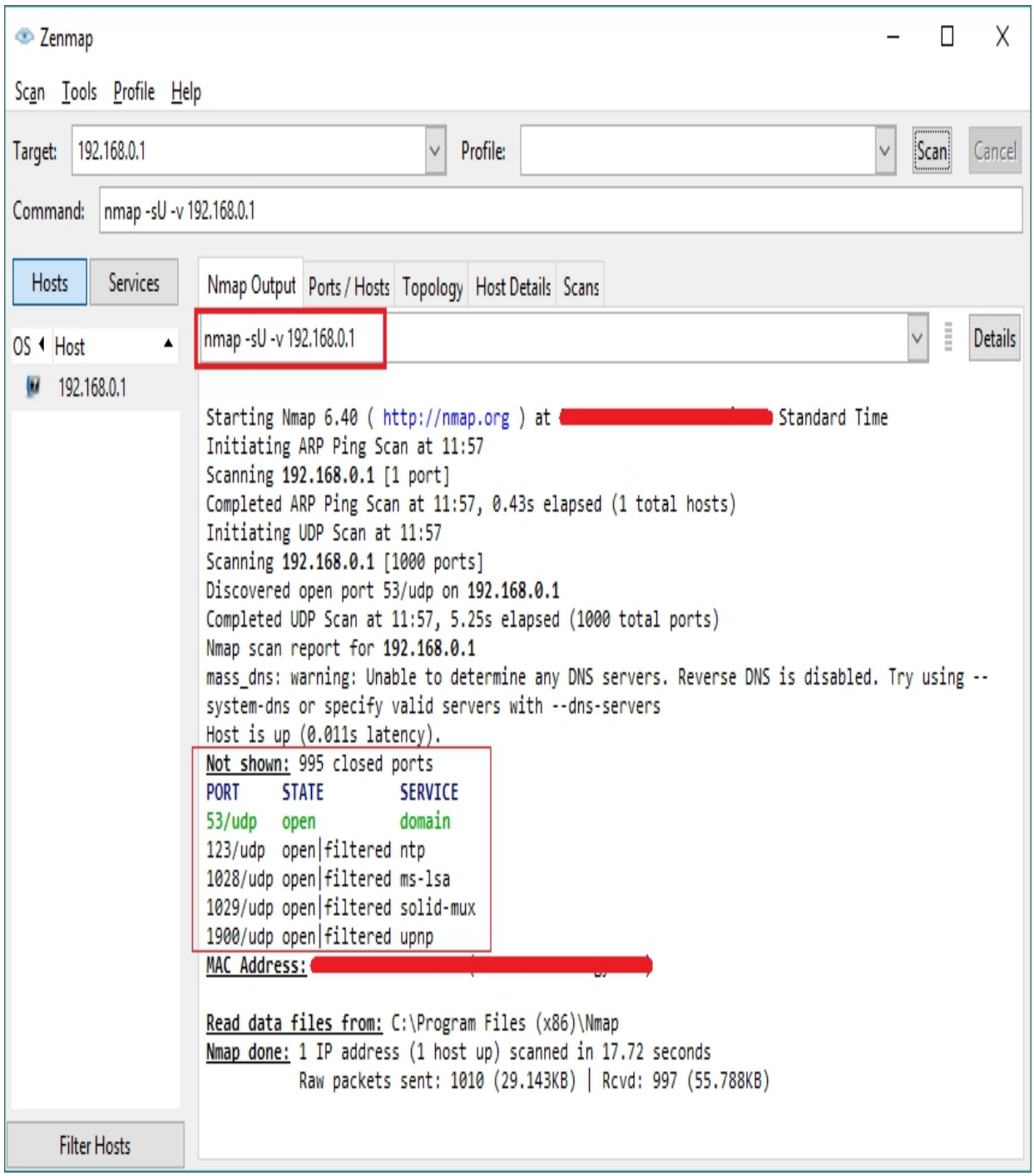


Figure 3-36: UDP Port Scanning

Scanning Tool

NetScan Tools Pro is an application that collects information, performs network troubleshooting, monitoring, discovery, and diagnostics using its integrated tools designed for the Windows-based Operating System,

which offers a focused examination of IPv4, IPv6, domain names, email, and URL using automatic and manual options.

Figure 3-37: UDP Port Scanning

Scanning Tools for Mobile

There are several basic and advanced network tools available for mobile devices on application stores. Following are some effective tools for Network Scanning.

Network Scanner

"Network Scanner" is a tool, which offers options like IP Calculator, DNS lookup, Whois tool, Traceroute, and Port Scanner.

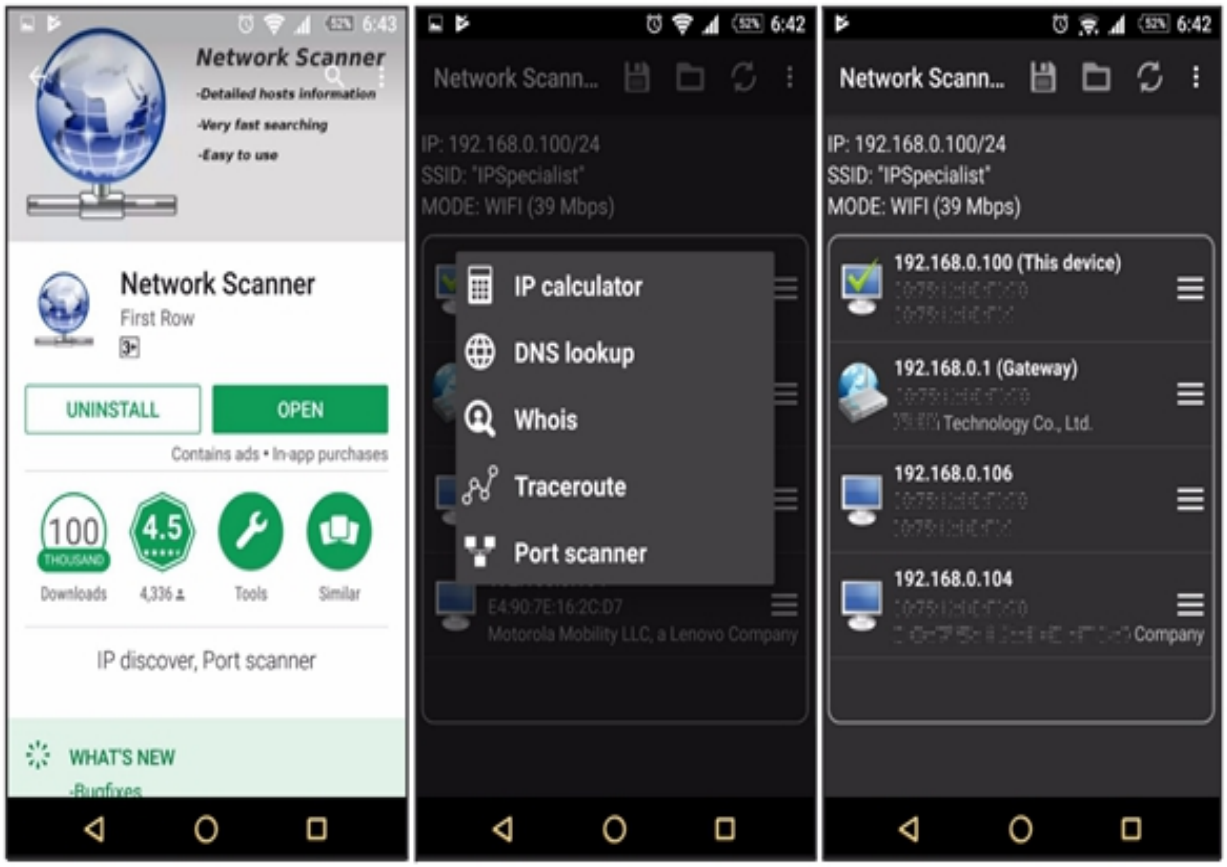
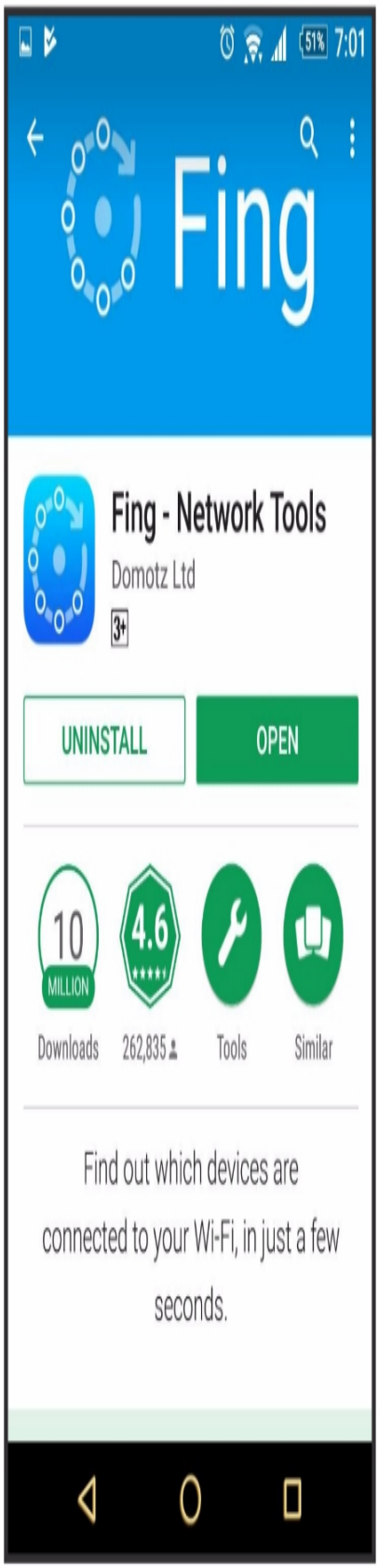
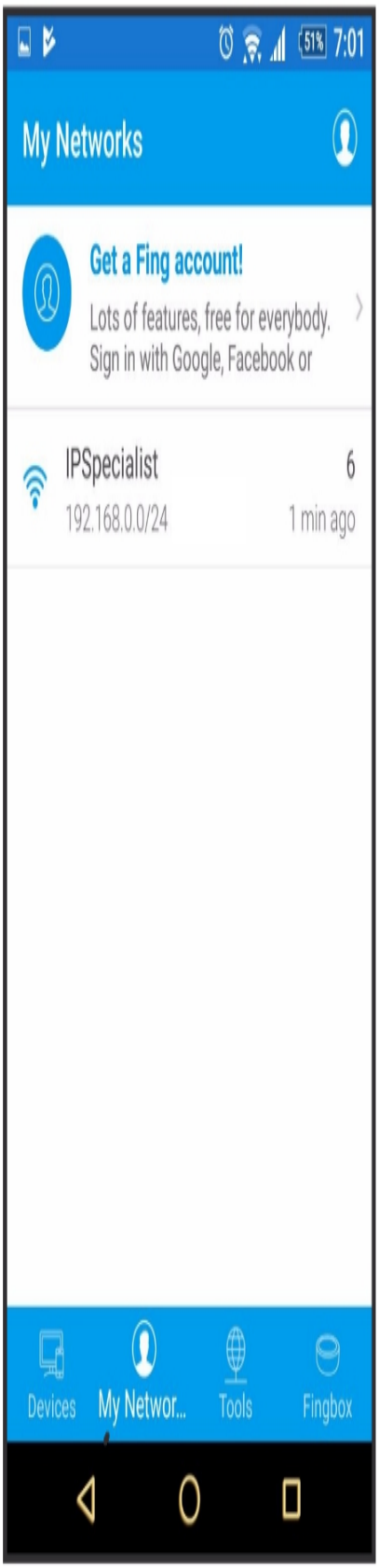


Figure 3-38: Scanning Tool for Mobile

Fing – Network Tool


7:01
Fing
Fing - Network Tools
Domotz Ltd
3+
UNINSTALL
OPEN
10
MILLION
Downloads
4.6
262,835
Tools
Similar
Find out which devices are connected to your Wi-Fi, in just a few seconds.


7:01
My Networks
Get a Fing account!
Lots of features, free for everybody. Sign in with Google, Facebook or
IPSpecialist
6
192.168.0.0/24
1 min ago
Devices
My Networ...
Tools
Fingbox


7:01
Tools
Enter IP address or domain
Scan any external device. Type above an IP address or domain, e.g. 'www.google.com'
DNS Lookup
IP Address
Hostname
Scan services
Ping
Trace route
Wake on LAN
Devices
My Networks
Tools
Fingbox

Figure 3-39: Scanning Tool for Mobile
Network Discovery Tool

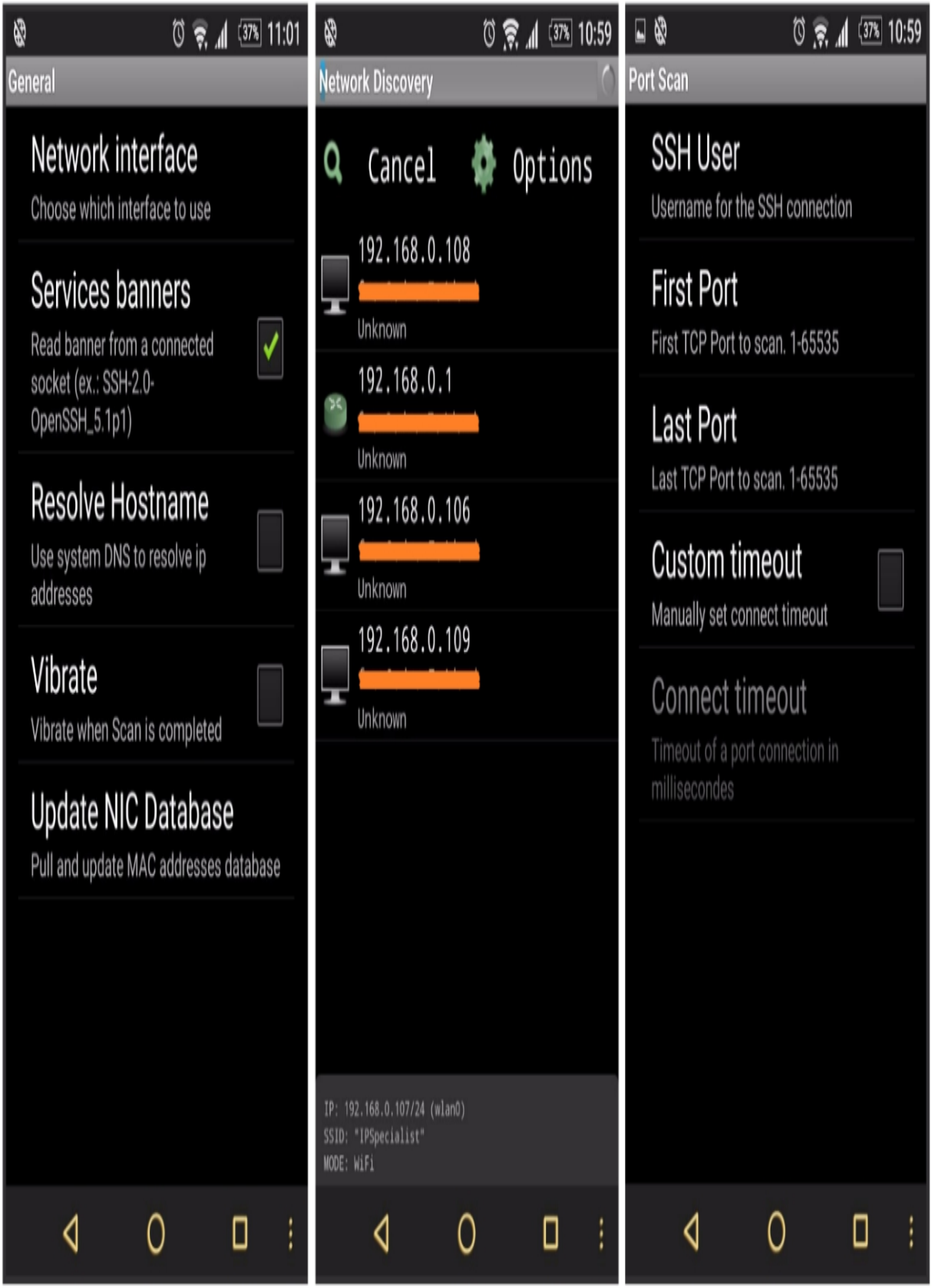
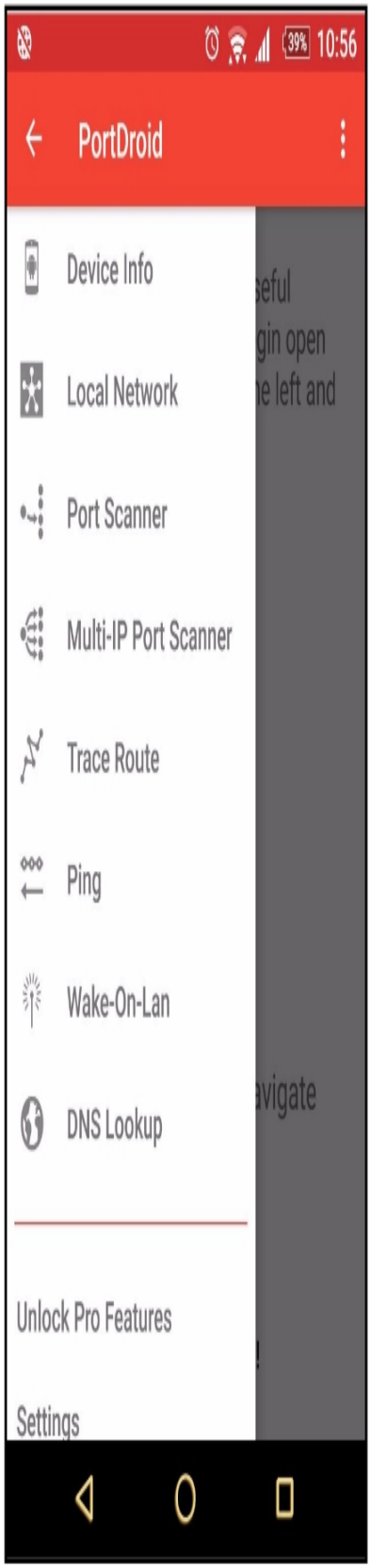

11:01
General
Network interface
Choose which interface to use
Services banners
Read banner from a connected socket (ex.: SSH-2.0-OpenSSH_5.1p1)
Resolve Hostname
Use system DNS to resolve ip addresses
Vibrate
Vibrate when Scan is completed
Update NIC Database
Pull and update MAC addresses database
10:59
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
10:59
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 millisecondes

Figure 3-40: Scanning Tool for Mobile
Port Droid Tool


39% 10:56
PortDroid
Device Info
Local Network
Port Scanner
Multi-IP Port Scanner
Trace Route
Ping
Wake-On-Lan
DNS Lookup
Unlock Pro Features
Settings


36% 11:36
Local Network
192.168.0.1
SCAN
3.9ms
192.168.0.100
SCAN
21.6ms
192.168.0.108
SCAN
233.7ms
192.168.0.103
SCAN
255.1ms
192.168.0.109
SCAN
28.3ms
192.168.0.110
SCAN
9.5ms
192.168.0.107 [This device]
SCAN
0.9ms

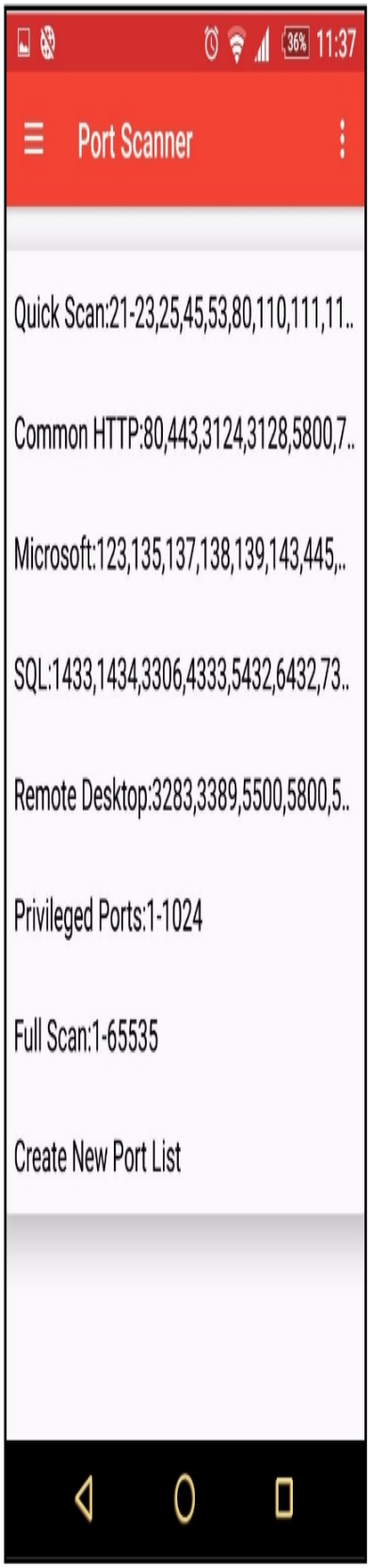

36% 11:37
Port Scanner
Quick Scan:21-23,25,45,53,80,110,111,11..
Common HTTP:80,443,3124,3128,5800,7..
Microsoft:123,135,137,138,139,143,445,..
SQL:1433,1434,3306,4333,5432,6432,73..
Remote Desktop:3283,3389,5500,5800,5..
Privileged Ports:1-1024
Full Scan:1-65535
Create New Port List

Figure 3-41: Scanning Tool for Mobile

Scanning Beyond IDS

Attackers use fragmentation to evade security devices such as Firewalls, IDS, and IPS. The basic technique that is most commonly and popularly used is splitting the payload into smaller packets. IDS must reassemble this incoming packet stream to inspect and detect the attack. These small packets are altered to make reassembling and detection more complex for packet reassembly. 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. They 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 an Operating System running on a target machine. By gathering information about the Operating System being run, an attacker can determine the vulnerabilities and possible bugs that the OS 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 determines which services are running on the target machine. Typically, Telnet is used to retrieve banner information. A banner is a message presented by the networking device when a user is accessing it. For example, "*unauthorized access to this device is prohibited, and violators will be prosecuted to the full extent of the law".* Configuring this banner with sensitive information can help attackers to get necessary information.

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's detection capability allows it to send TCP and UDP packets and observe the response from the targeted host. A detailed assessment of this response brings some clues regarding the nature of an Operating System, disclosing the type of OS.

To perform OS detection with Nmap, use the following syntax:
nmap -O < *ip address* >

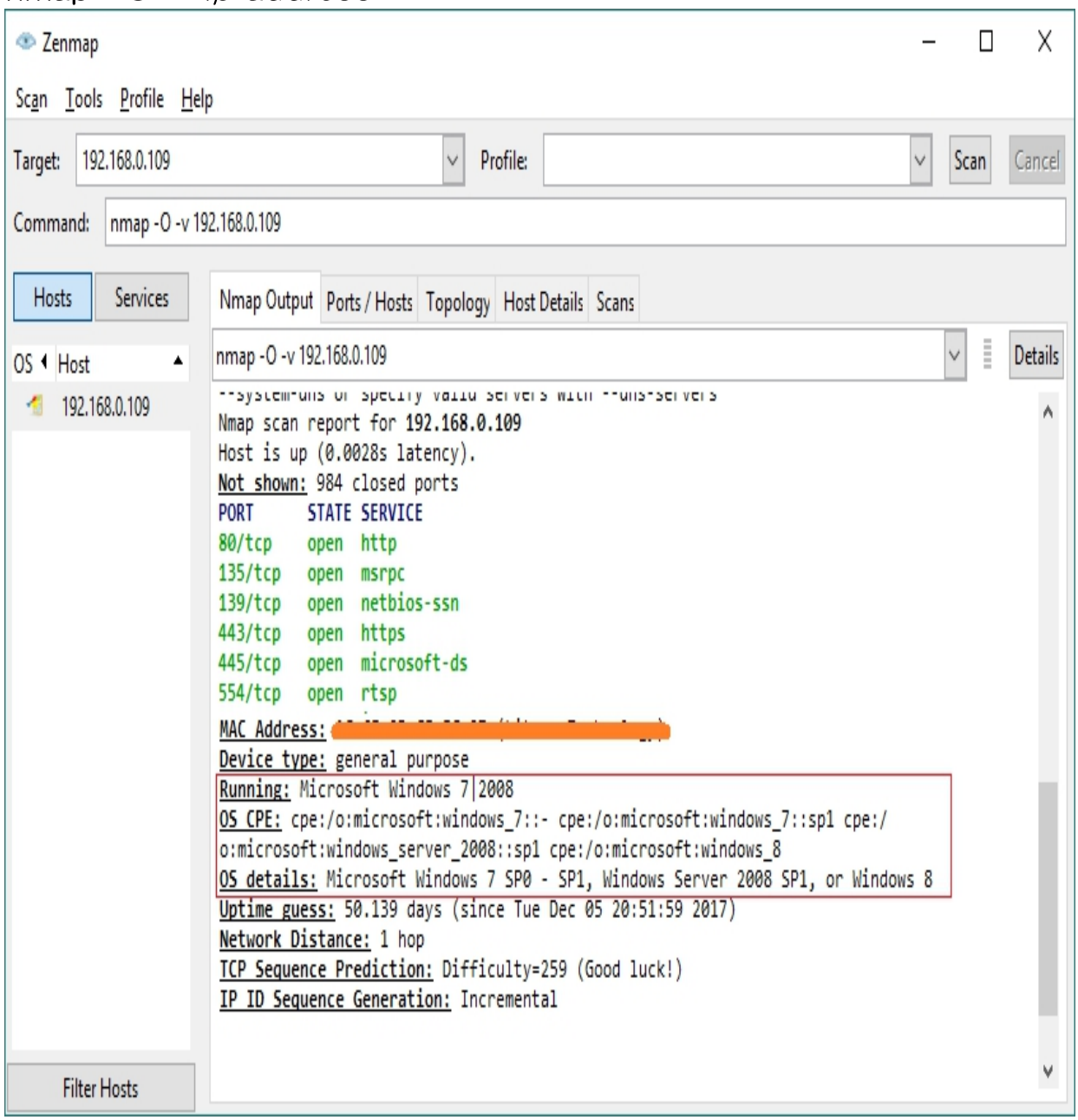


Figure 3-42: OS Fingerprinting

Passive OS Fingerprinting or Banner Grabbing

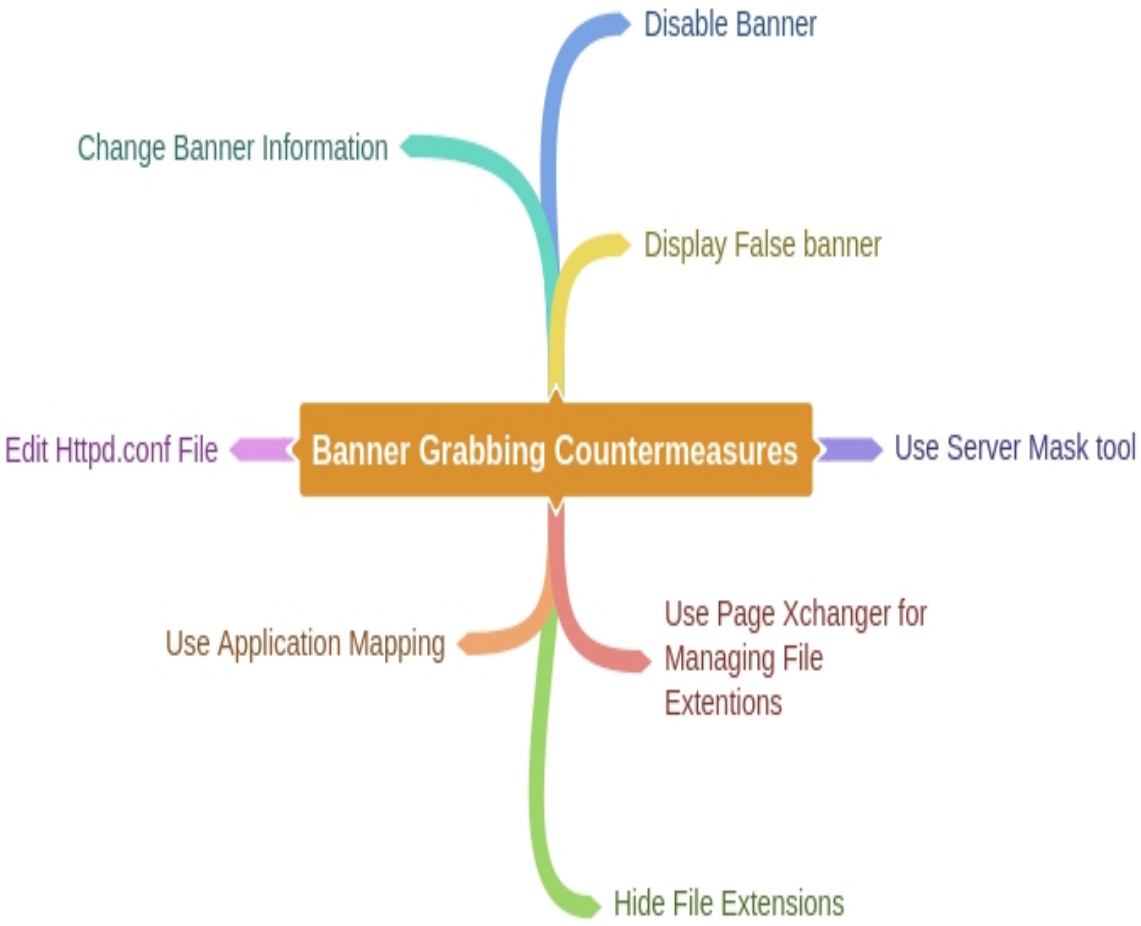
Passive OS Fingerprinting requires detailed assessment of traffic. You can perform passive banner grabbing by analyzing network traffic along with a special inspection of Time to Live (TTL) value and Window Size. TTL value and Window Size are inspected from a header of the TCP packet while observing 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 8 192
Cisco Router (iOS 12.4) 255 4 128
Table 3-03: Passive OS Fingerprinting Values

Banner Grabbing Tools

There are many tools available for banner grabbing. Some of them are as follows: ■ 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 a network diagram is designed, it defines a logical and physical path leading to the appropriate target within a network. A network diagram visually explains the network environment and provides an even clearer picture of that network. Network Mappers are the network mapping tools that use scanning and other network tools and techniques to draw a picture of a network. What is important

to consider is that these tools generate traffic that can reveal the presence of an attacker or pentester on the network.

Network Discovery Tool

OpManager is an advanced network monitoring tool that offers fault management support over WAN links, Router, Switch, VoIP, and servers. It can also carry out performance management. Network View is an advanced network discovery tool. It can perform discovery of routes, TCP/IP nodes using DNS, ports, and other network protocols. Some popular tools are listed below:

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

Drawing Network Diagrams

Solar Wind Network Topology Mapper can discover a network and create a comprehensive network topology diagram. It also offers additional features like editing nodes manually, exporting diagrams to Visio, multi-level network discovery, etc. Mapped topology can display node name, IP address, hostname, system name, machine type, vendor, system location, and other information.

Lab 3-4: Creating a Network Topology Map Creating a Network Topology Map

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

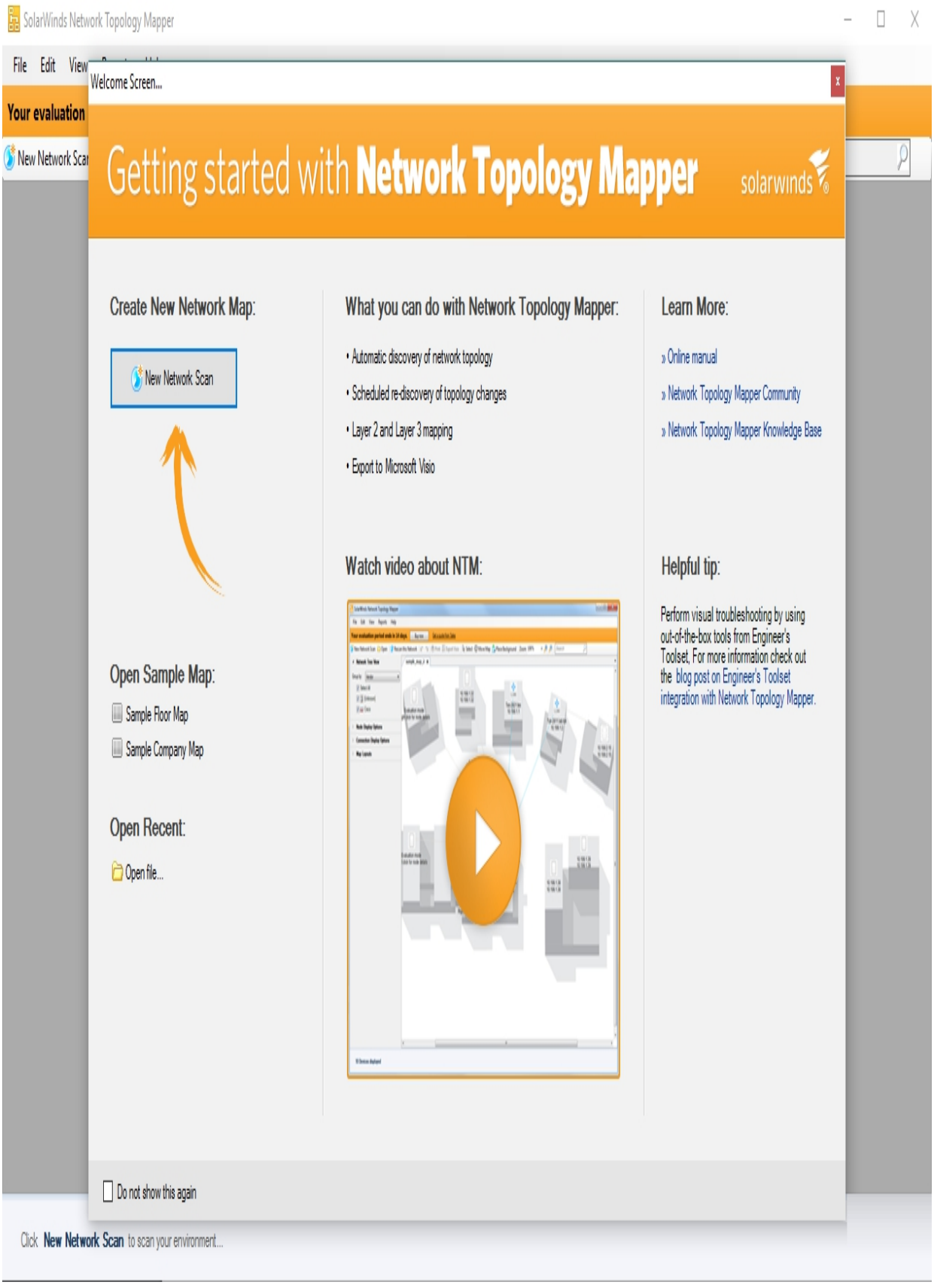

SolarWinds Network Topology Mapper
File Edit View
Your evaluation
New Network Scan
Welcome Screen...
Getting started with Network Topology Mapper
solarwinds
Create New Network Map:
New Network Scan
Open Sample Map:
Sample Floor Map
Sample Company Map
Open Recent:
Open file...
What you can do with Network Topology Mapper:
• Automatic discovery of network topology
• Scheduled re-discovery of topology changes
• Layer 2 and Layer 3 mapping
• Export to Microsoft Visio
Watch video about NTM:
Learn More:
» Online manual
» Network Topology Mapper Community
» Network Topology Mapper Knowledge Base
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.
Do not show this again
Click New Network Scan to scan your environment...

Figure 3-43: Network Topology Mapper Tool

Provide network information, configure discovery settings, and provide any credentials required.

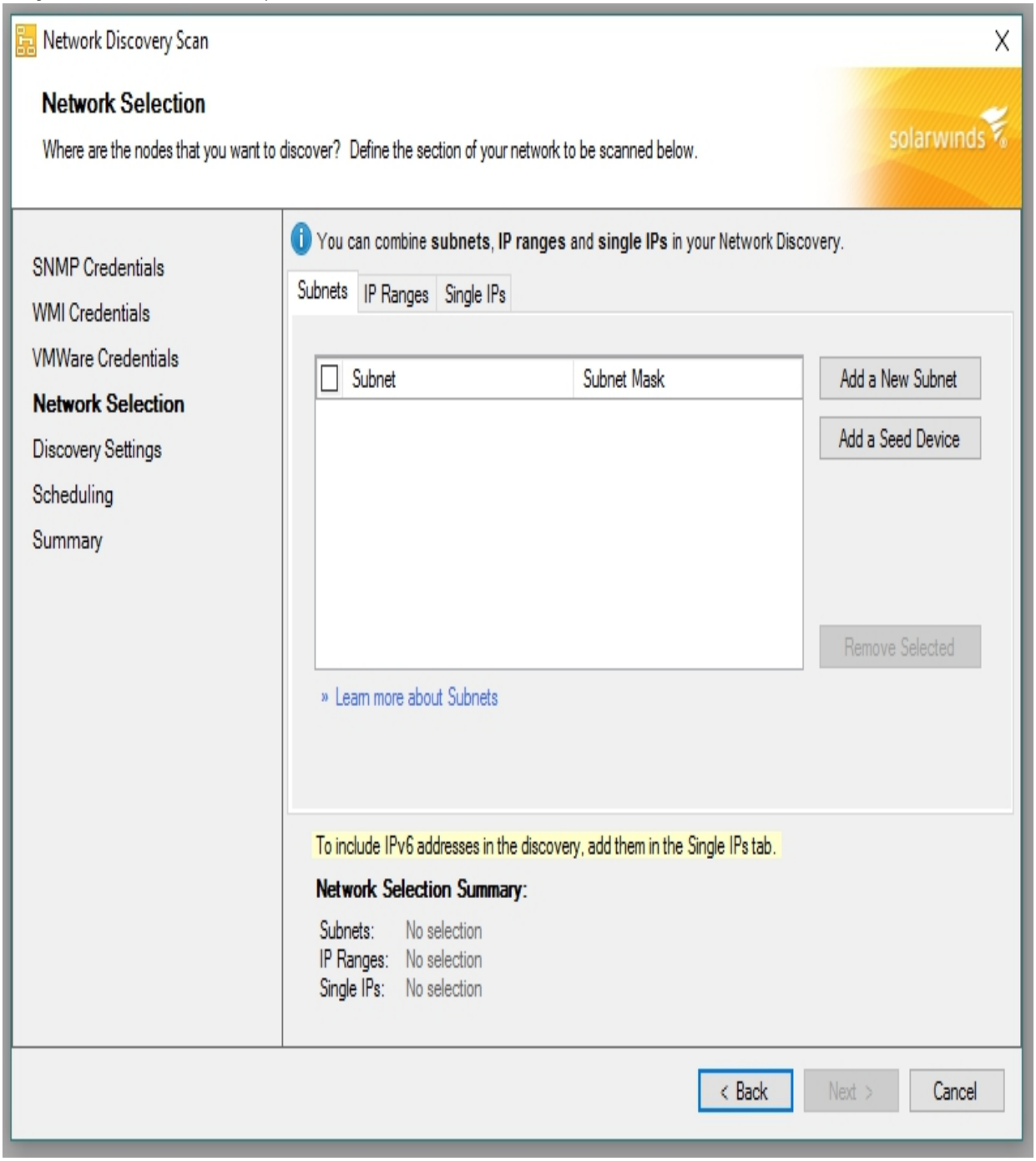


Figure 3-44: Configuring Scan

Once you have configured all settings, start the scan.

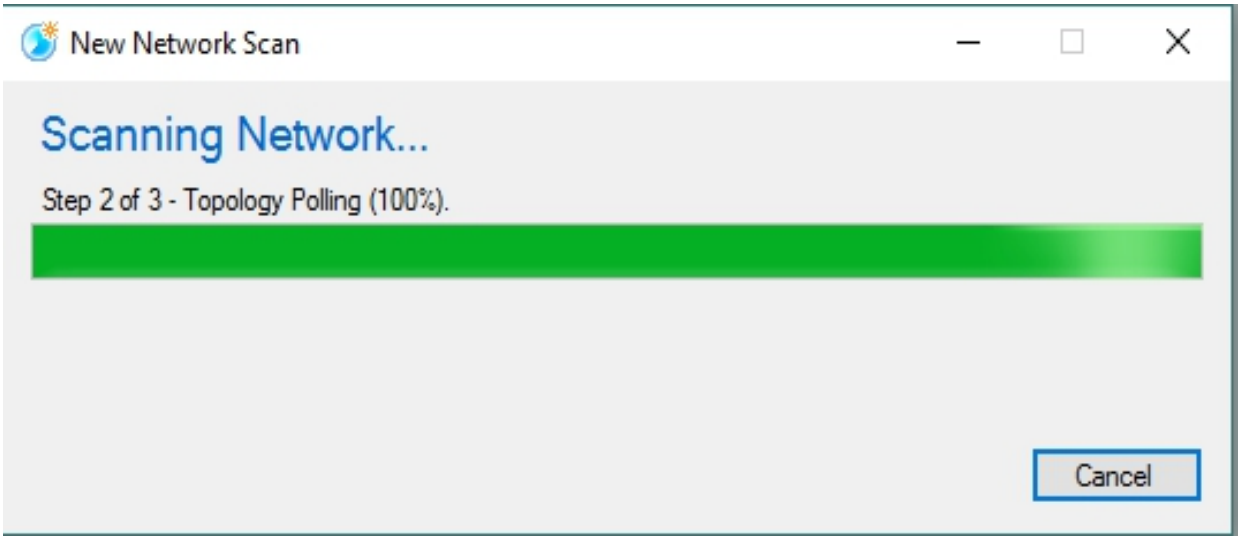


Figure 3-45: Scanning Network

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

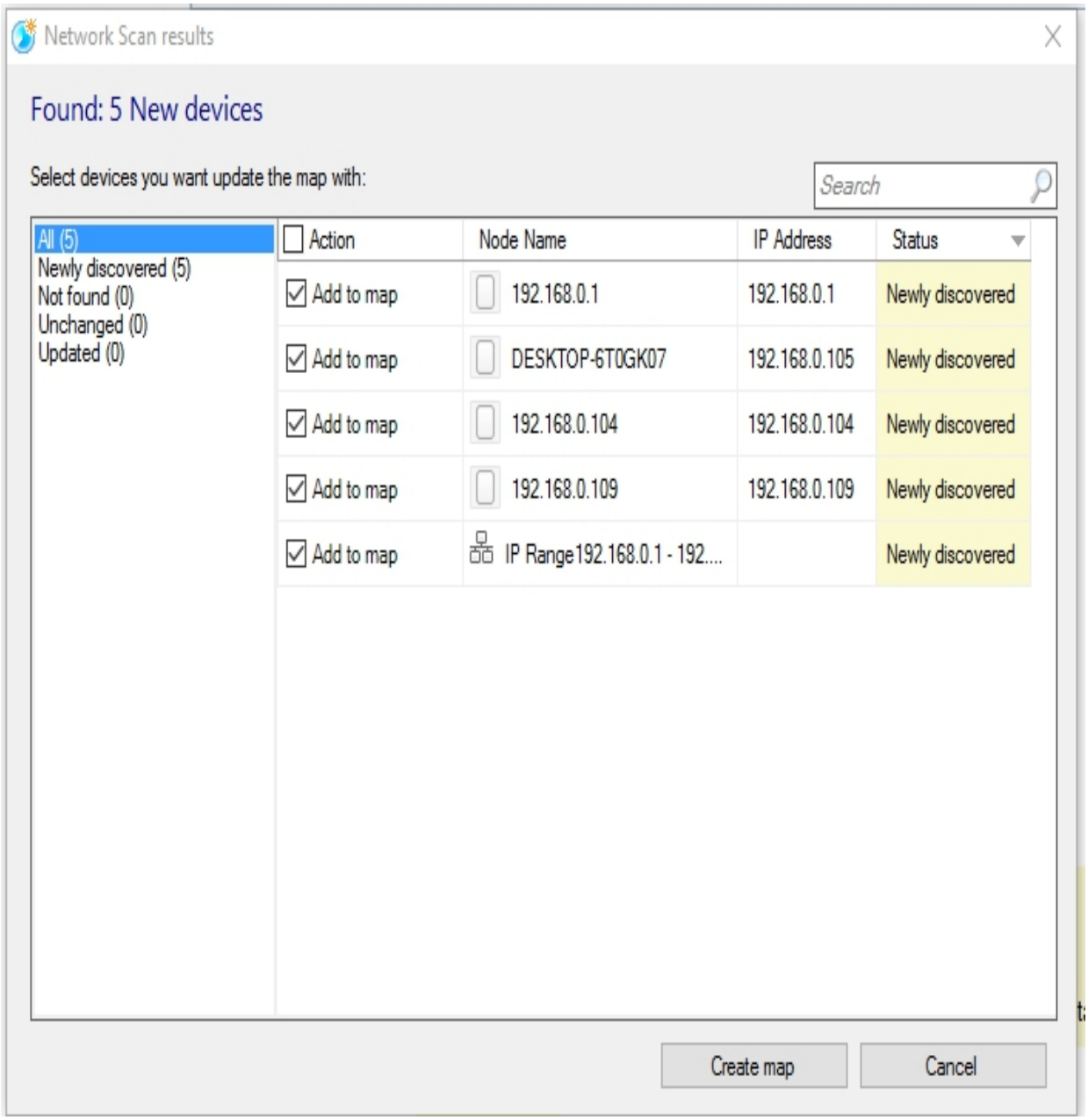


Figure 3-46: List of Discovered Devices

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

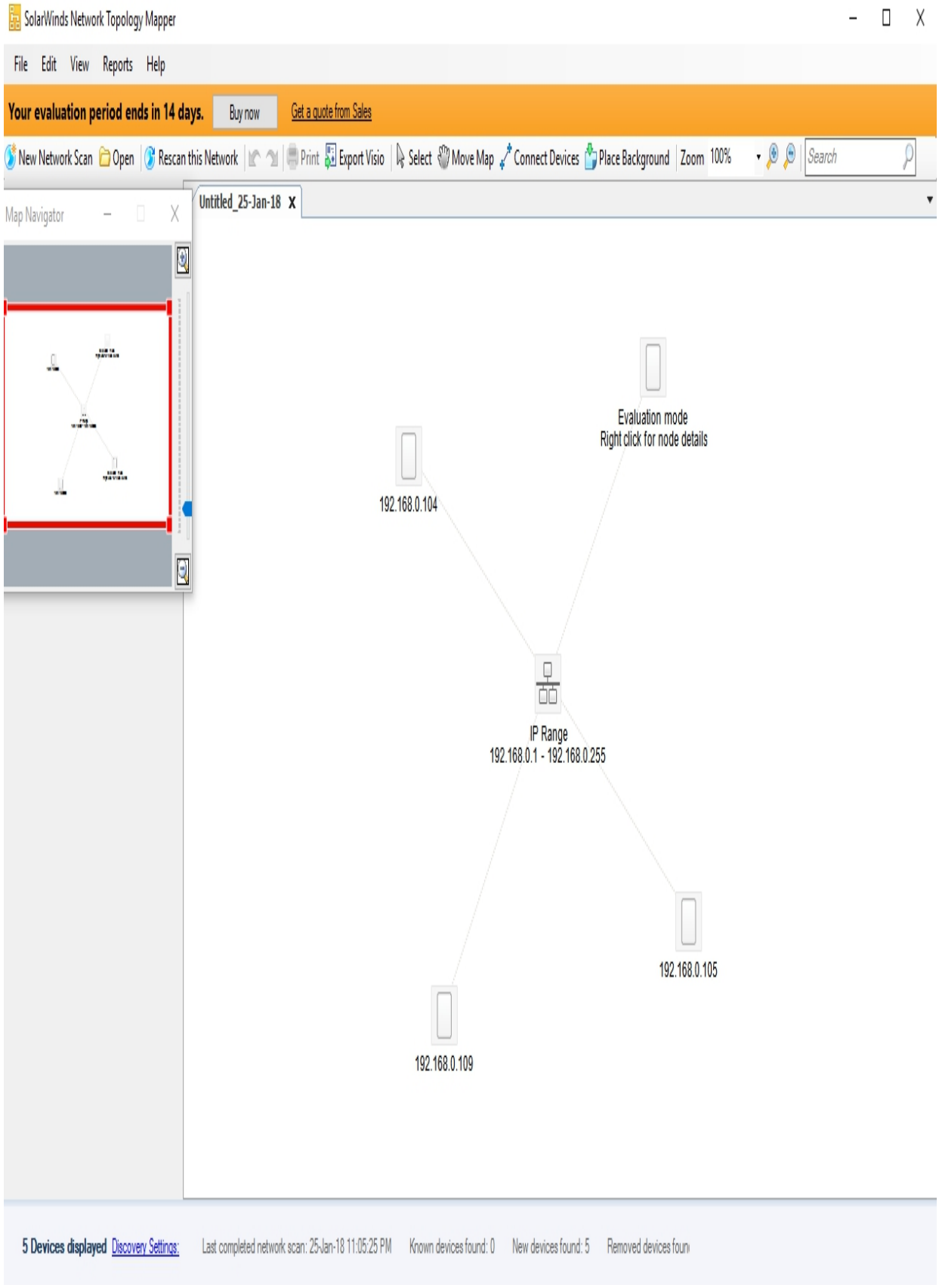

SolarWinds Network Topology Mapper
File Edit View Reports Help
Your evaluation period ends in 14 days.
Buy now
Get a quote from Sales
New Network Scan
Open
Rescan this Network
Print
Export Visio
Select
Move Map
Connect Devices
Place Background
Zoom 100%
Search
Map Navigator
Untitled_25-Jan-18
Evaluation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

Figure 3-47: Topology

Prepare Proxies

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

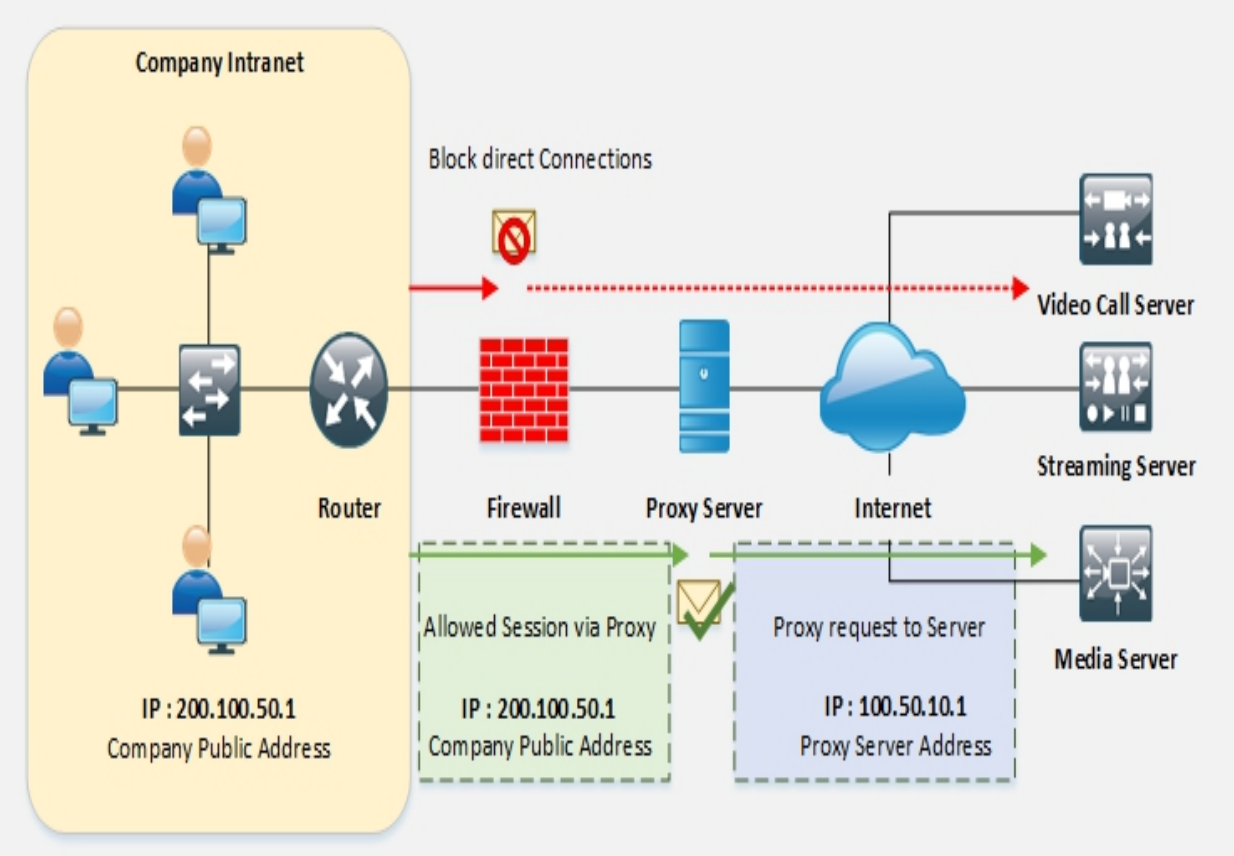


Figure 3-48: Proxy Server

Proxy Servers

Proxy Servers anonymize the web traffic to provide anonymity. When a user sends a request to access any resource to the other publically available servers, a proxy server acts as an intermediary for these requests. A user's request is forwarded to the proxy server first. The proxy server will entertain these requests in the form of a web page request, file download request, connection request to another server, etc. The most commonly used proxy server is a web proxy server.

Web proxy servers are used to provide access to the world wide web by bypassing the IP address blocking.

Uses of a 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 for using multiple proxy servers. One proxy server forwards the traffic to the next proxy server. This process is not recommended for production environments nor is it a long-term solution. However, this technique leverages your existing proxy.

Figure 3-49: Proxy Chaining

Proxy Tool

There are a number of proxy tools available, and you can also search online for a proxy server and configure it manually on your web browser. Available proxy tools include:

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

Proxy Switcher

A Proxy Switcher tool scans for the available proxy servers. You can enable any proxy server to hide your IP address. Figure 3-50 shows the search process of proxy servers performed by Proxy Switcher tool.

Figure 3-50: Proxy Switcher

Proxy Tools for Mobile

There are several proxy applications available on Google Play store and App store for Android and iOS devices respectively.

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 activities untraceable. The basic purposes of using anonymizers are to minimize risk, identify and prevent information theft, bypass restrictions and censorship, and carry out 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 via a USB or DVD. It is an Operating System that is specially designed to help you use the internet anonymously – leaving no trace behind. Tails preserves privacy and anonymity.

Anonymizers for Mobile

- Orbot
- Psiphon
- Open Door

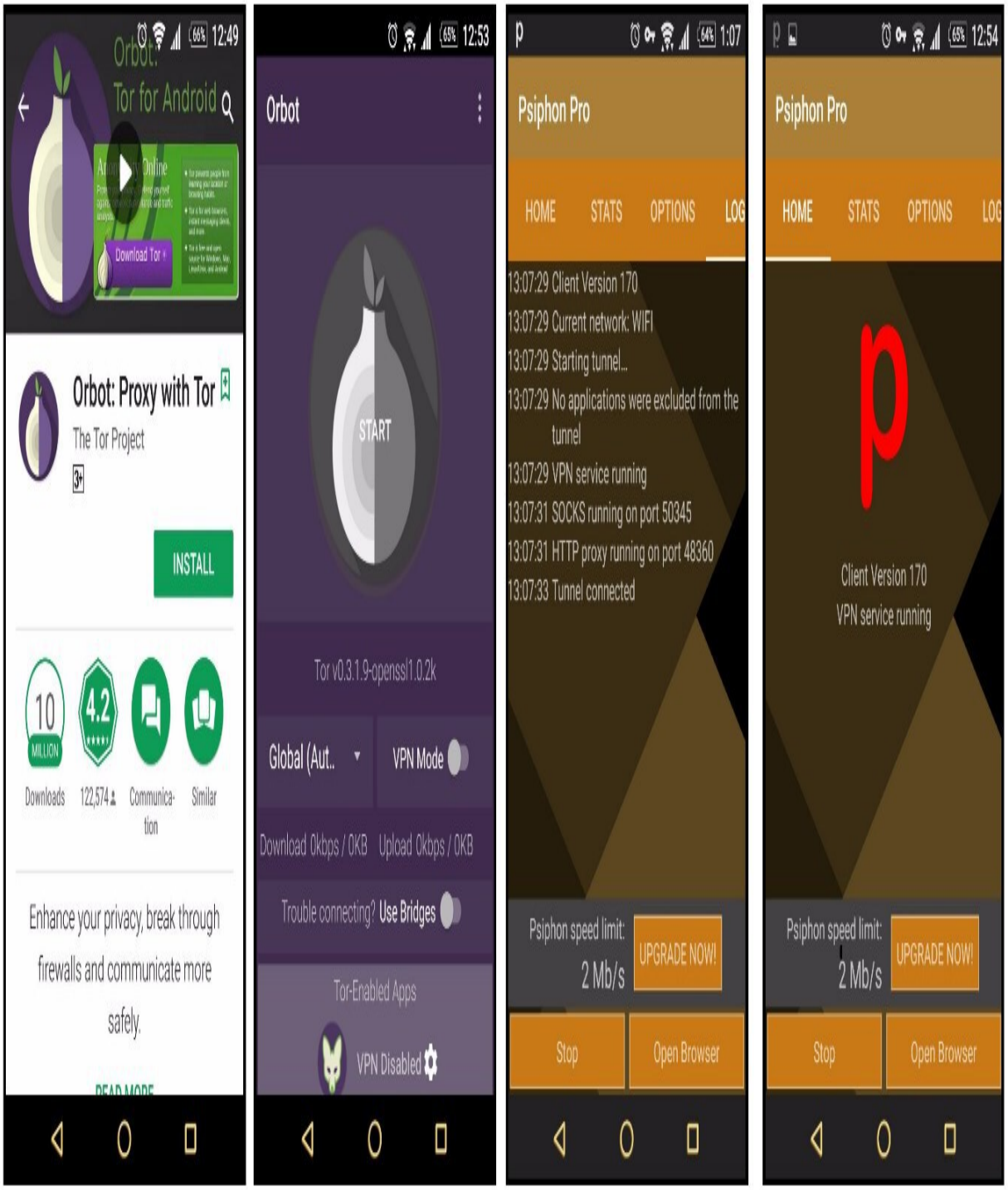


Figure 3-51: Anonymizers for Mobile

Spoofing IP Address

IP Address Spoofing is a technique that is used to gain unauthorized access to machines by spoofing an IP address. An attacker illicitly

impersonates any user machine by sending manipulated IP packets with a spoofed IP address. The spoofing process involves modification of a header with a spoofed source IP address, a checksum, and the order values. Packet-switched networking causes an out of order series of incoming packets. When these out of order packets are received at the destination, they are reassembled to extract the message.

IP spoofing can be detected by different techniques including the 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. IP spoofing can be detected by comparing TTL values from the suspected host's reply. It will be a spoofed packet if the TTL value is not the same as the one in the spoofed packet. However, TTL values can vary in even normal traffic, and this technique identifies spoofing when the attacker is on a different subnet.

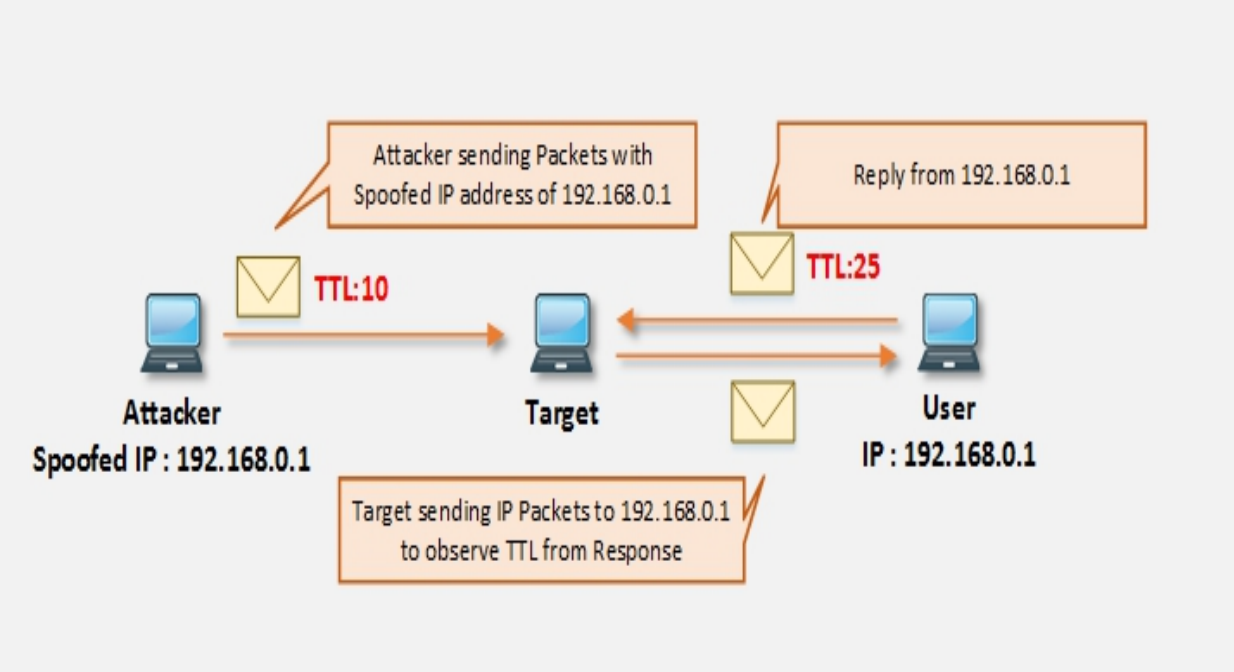


Figure 3-52: Direct TTL Probing

Similarly, additional probes are sent to verify the IPID of the host. If the IPID value is not close to the recent values, the suspected traffic is spoofed. This technique can be used if the attacker is within a subnet.

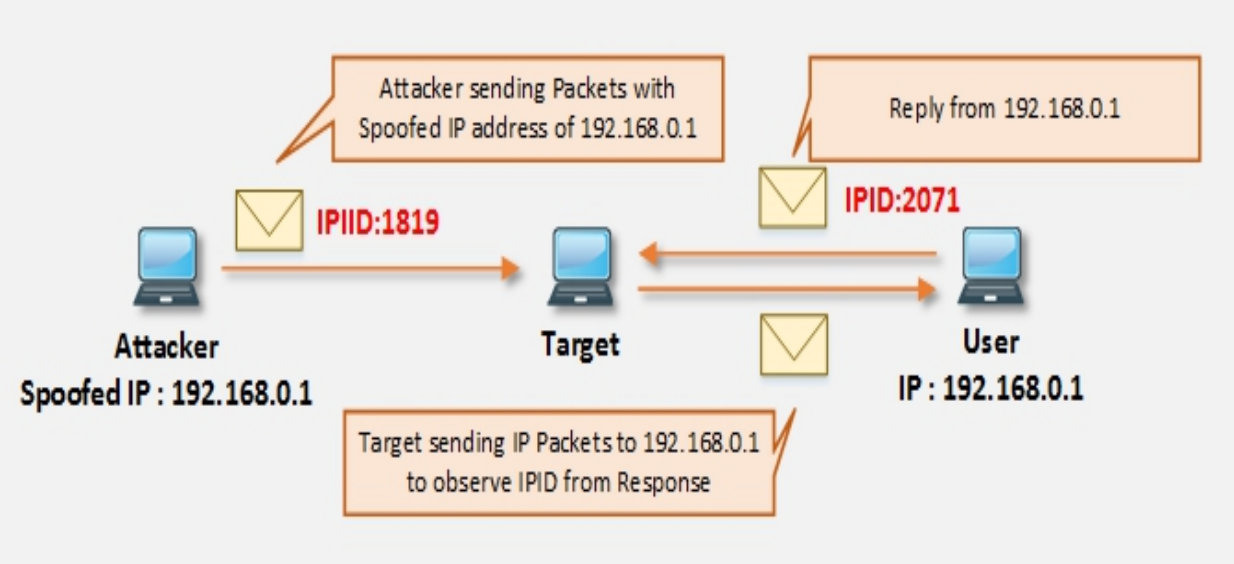


Figure 3-53: Verifying IPID Number

Practice Questions

1. Which of the following statement below is correct? A. UCP is connection oriented & TDP is Connectionless B. TCP is connection oriented & UDP is Connectionless C. TCP & UDP are both Connection oriented D. TCP & UDP are both Connectionless

2. What is three-way handshaking the process of? A. Establishment of TCP Connection
B. Establishment of UDP Connection
C. Establishment of either TCP or UDP Connection D. Does not belong to TCP or UDP

3. Which of the following tools are used for Banner Grabbing? (Choose 2) A. SCP
B. SSH
C. Telnet
D. Nmap

4. Which server anonymizes the web traffic to provide anonymity? A. Proxy Server
B. Web Server
C. Application
D. DNS Server