

Dom Moore
Zenmap

Overview

The network mapping tool Nmap is an open-source utility commonly used in network discovery ("enumeration" in offensive terms) and security auditing.

Part 1: Staging Zenmap

Step 1- download Optional Zenmap GUI (all platforms): zenmap-7.91-1.noarch.rpm

Step 2- run these commands:

- apt-get update apt-get install alien
- Go to your downloads folder cd Downloads
- sudo alien "name of the downloaded package.rpm"
- sudo dpkg -i "name of a converted package.deb"

Install Zenmap

```
kali@kali: ~/Downloads

File  Actions  Edit  View  Help

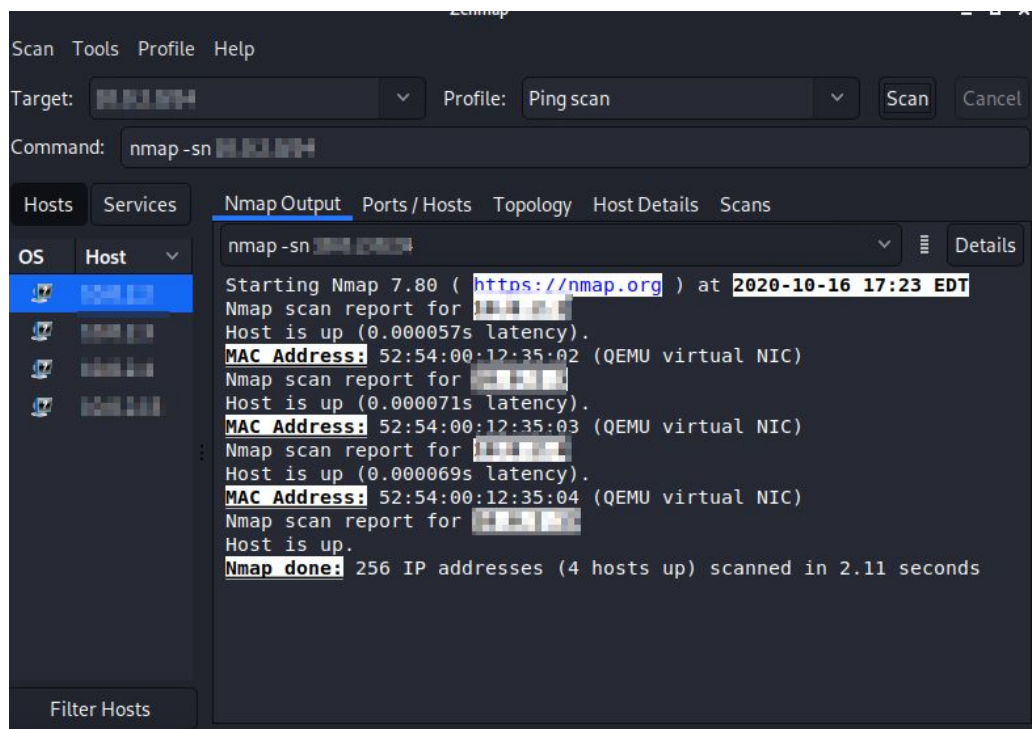
kali@kali:~/Downloads$ ls
myOp05file.txt  myOp05file.txt.gpg  test.txt  test.txt.enc  zenmap-7.91-1.noarch.rpm
kali@kali:~/Downloads$ sudo alien zenmap-7.91-1.noarch.rpm
zenmap_7.91-2_all.deb generated
kali@kali:~/Downloads$ ls
myOp05file.txt      test.txt      zenmap-7.91-1.noarch.rpm
myOp05file.txt.gpg  test.txt.enc  zenmap_7.91-2_all.deb
kali@kali:~/Downloads$ sudo dpkg -i zenmap_7.91-2_all.deb
Selecting previously unselected package zenmap.
(Reading database ... 277736 files and directories currently installed.)
Preparing to unpack zenmap_7.91-2_all.deb ...
Unpacking zenmap (7.91-2) ...
Setting up zenmap (7.91-2) ...
Processing triggers for kali-menu (2020.3.2) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for mime-support (3.64) ...
Processing triggers for man-db (2.9.3-2) ...
kali@kali:~/Downloads$
```

Part 2: Network Scanning with Zenmap

For each of the scans requested below:

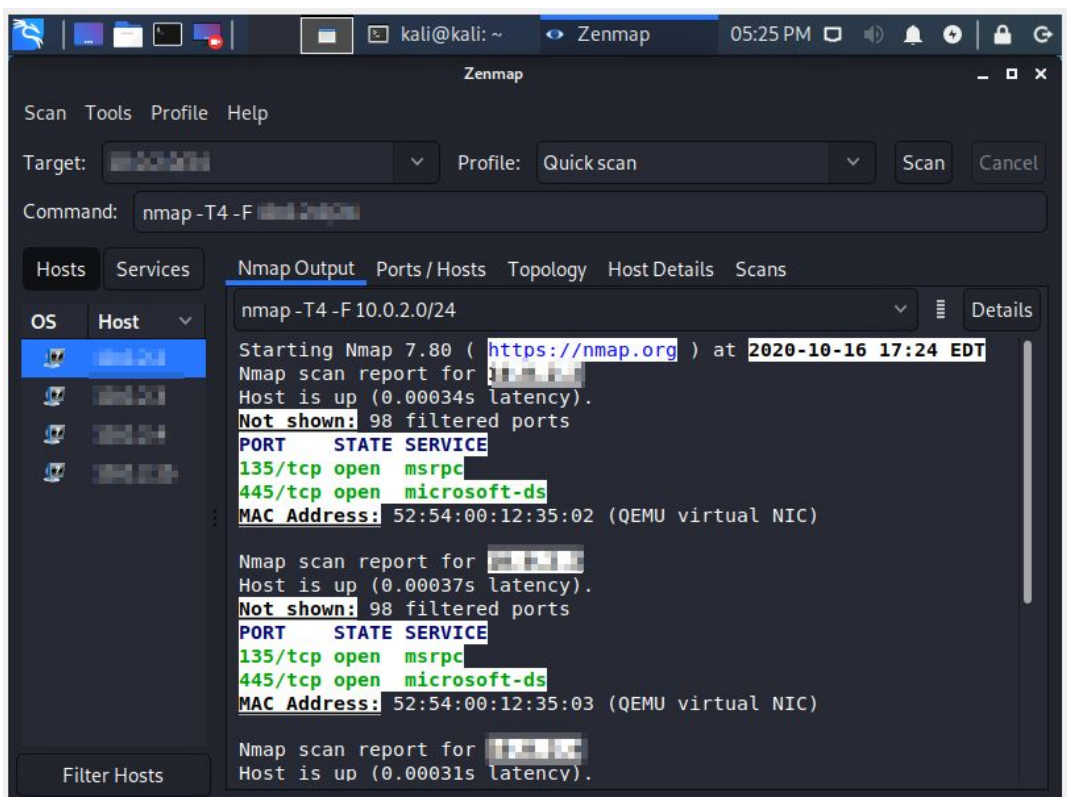
- Ping scan: **Command: nmap -sn**
 - What does this scan do in technical terms?
 - This command executes a ping scan on the target IP only but does not perform a port scan.
 - Was the scan correct?
 - The scan performed did execute as expected; it detected the four devices within the network and determined if the network was up or down.
 - Why/why not?
 - Yes, it identified that there are four devices it provided validation of those VM, it also shows that it scanned the other IP addresses within the range.

Ping scan



- Quick scan: **nmap -T4 -F**
 - What does this scan do in technical terms?
 - Scans the top 100 most common TCP ports
 - Was the scan correct?
 - Yes
 - Why/why not?
 - The Quick scan displays that there are 98 ports that are not shown, and displays the two TCP that it was able to pick up within the network.

Quick scan

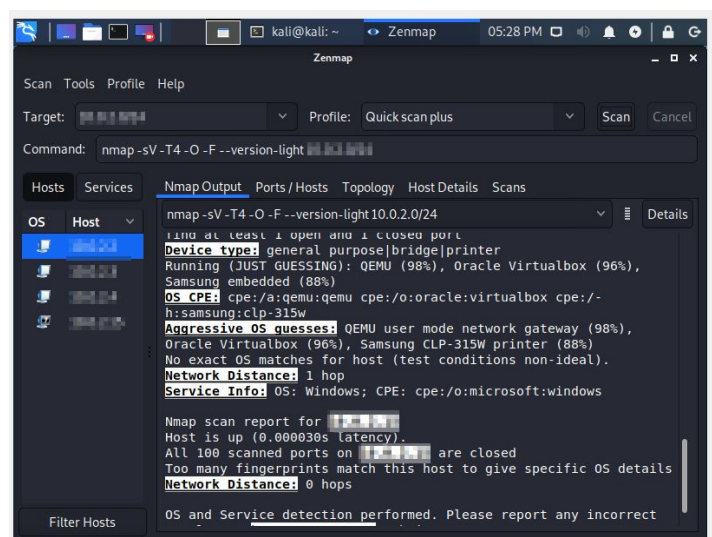
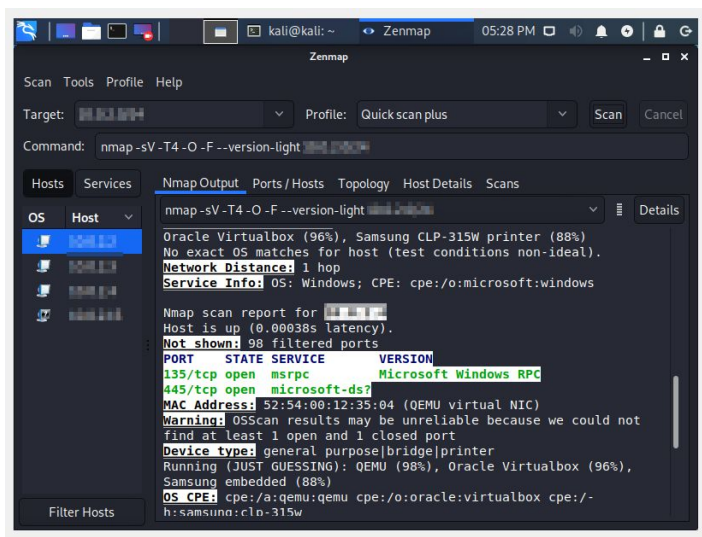


Port 143: Internet Msg Access Protocol is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection

Port 445: TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer and Leaving port 445 open leaves Windows machines vulnerable to a number of trojans and worms.

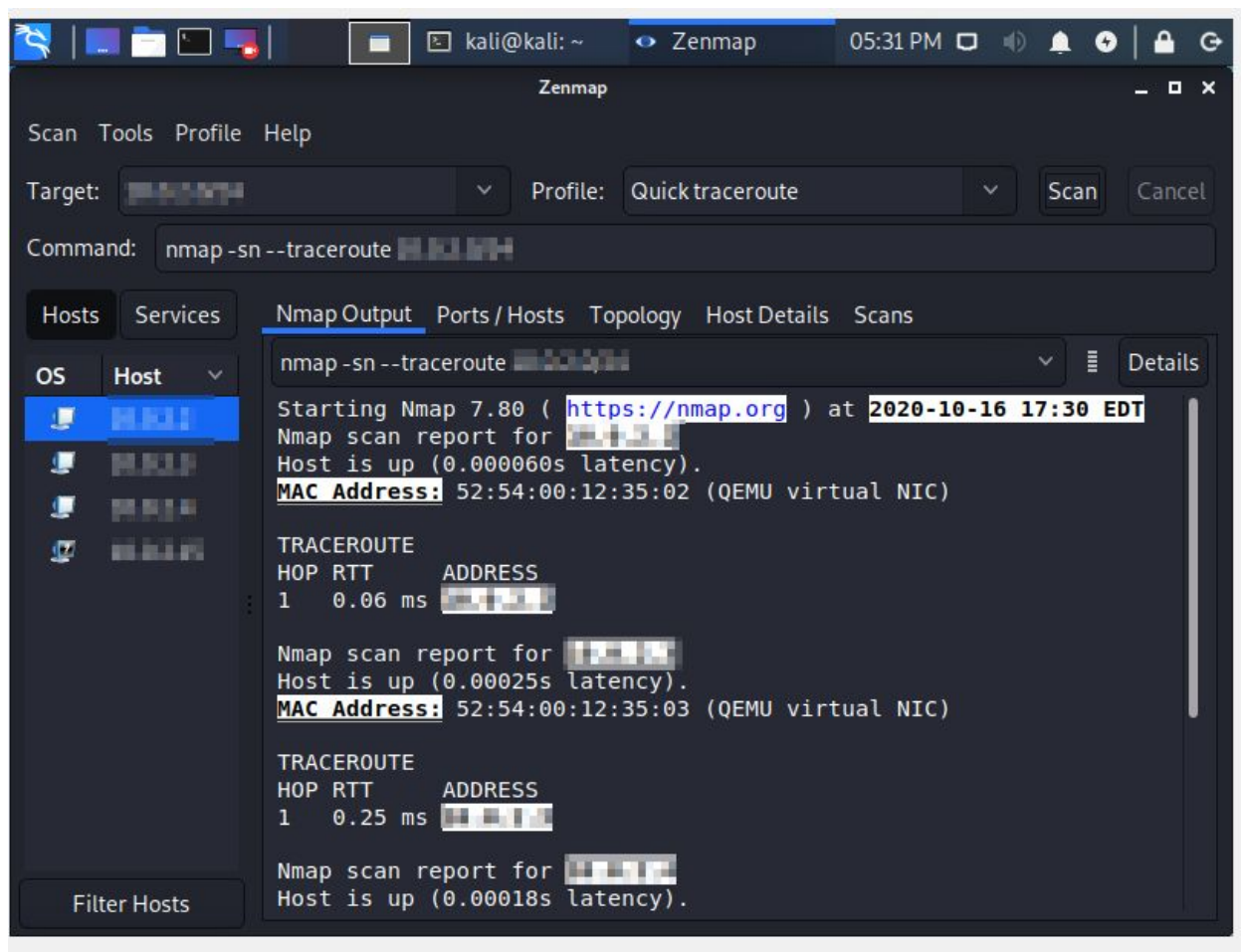
- Quick scan plus: **Nmap -sV -T4 -O -F --version-light**
 - What does this scan do in technical terms?
 - The plus version of the QS is that it adds the os information to the results.
 - Was the scan correct?
 - Yes
 - Why/why not?
 - This scan performed the scans on the 100 ports included that os as well more details about the system such as the origin of the VM's

Quick scan plus



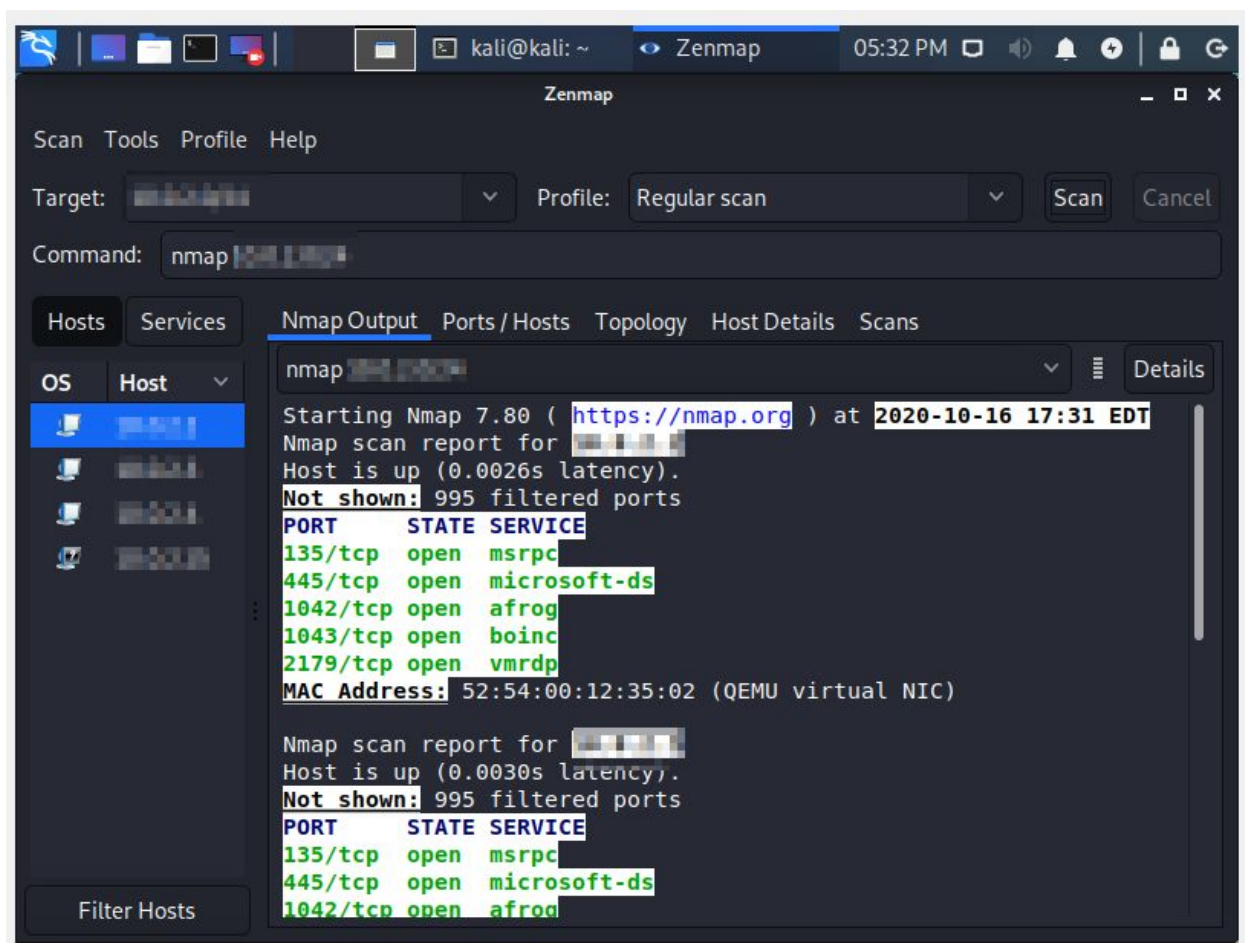
- Quick traceroute: **nmap -sn --traceroute**
 - What does this scan do in technical terms?
 - This command scans for all routers and host within the network by sending ICMP packages to all devices on the network
 - Was the scan correct?
 - Yes
 - Why/why not?
 - This command identifies the devices on the network and defines the number of hops identified as the path was determined.

Traceroute



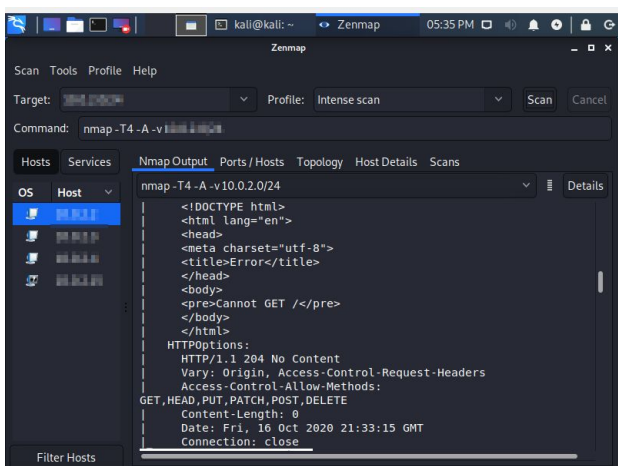
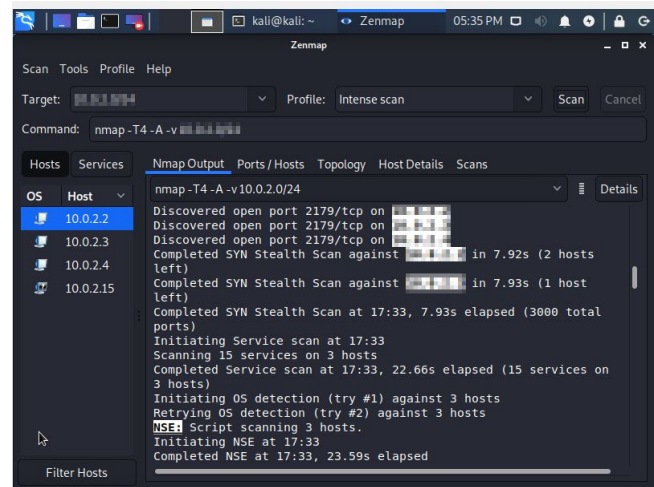
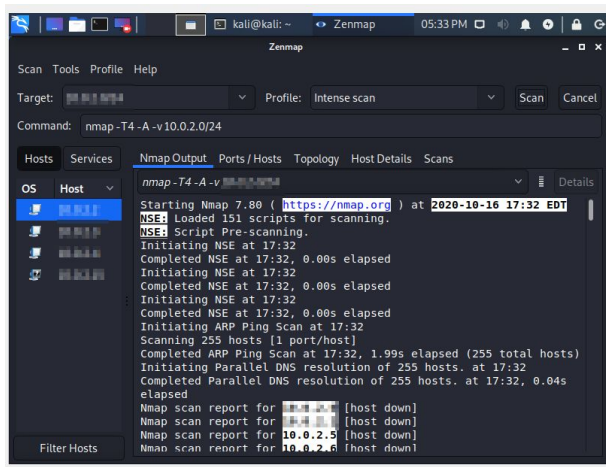
- Regular scan: **nmap**
 - What does this scan do in technical terms?
 - This means it will issue a TCP SYN scan for the most common 1000 TCP ports, using ping request
 - Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP)
 - synchronize, SYN is a TCP packet sent to another computer requesting that a connection be established between them
 - Was the scan correct?
 - Yes
 - Why/why not?
 - This command executed as expected; it displays the ping attempts and displays the TCP ports that were discovered within the scan as well as the mac address associated with the target.

Regular scan



- Intense scan: **nmap -T4 -A -v**
 - What does this scan do in technical terms?
 - This command uses a t4 modifier for a fast scan of TCP ports with attempts to determine os and version os host.
 - Was the scan correct?
 - Yes
 - Why/why not?
 - This executed as expected returning both hosts that were running and host that was done, as well as the number of attempts to determine version and os.

Intense scan



Intense scan plus UDP: **nmap -sS -sU -T4 -A -v**

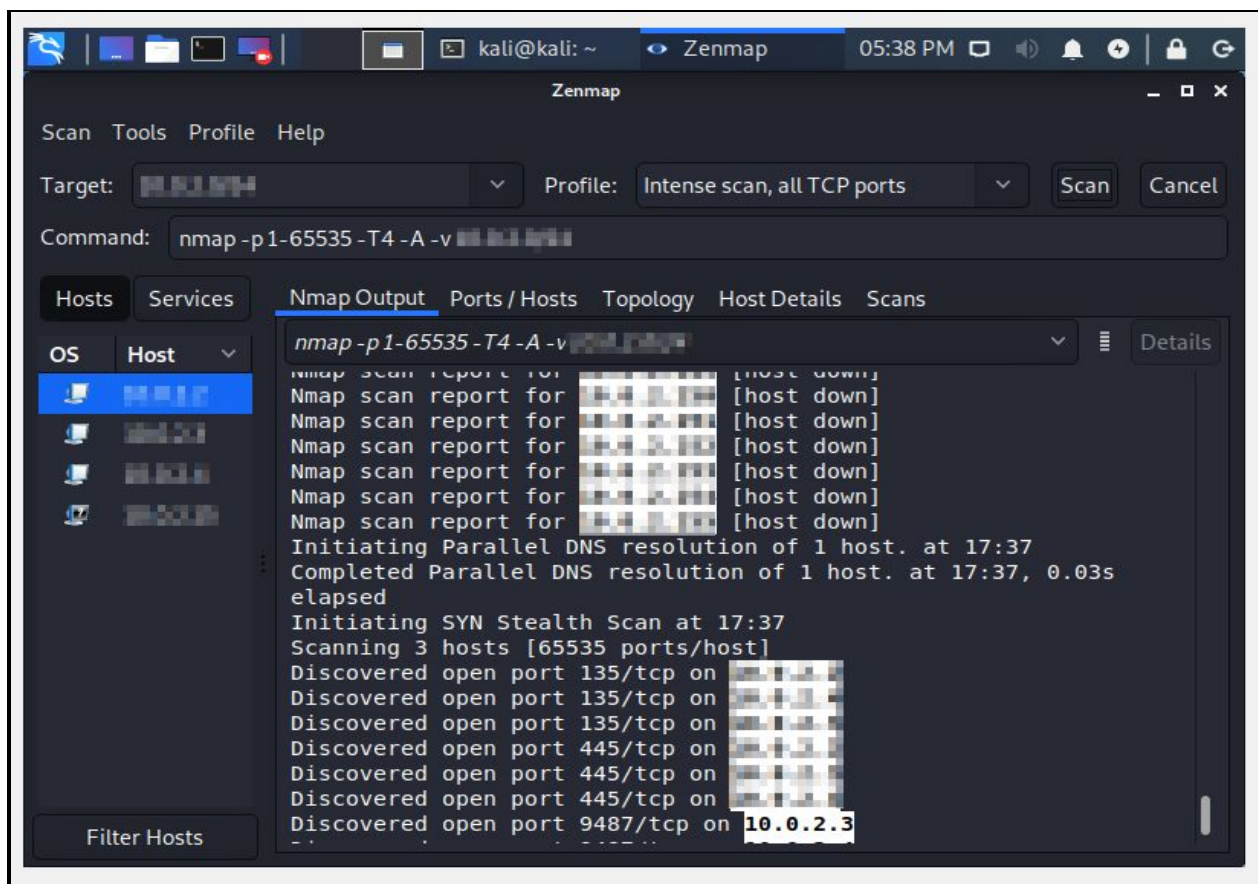
- What does this scan do in technical terms?
 - This command responds similarly to the intense scan with the added feature of UDP port scans
 - User Datagram Protocol (UDP), DP, computer applications can send messages, in this case, referred to as *datagrams*, to other hosts on an Internet Protocol
- Was the scan correct?
 - Yes
- Why/why not?
 - This executed as expected displaying both TCP and UDP attempts that the number of hosts identified.

Intense scan plus/ UDP

```
nmap -sS -sU -T4 -A -v [redacted]
Discovered open port 1043/tcp on [redacted]
Discovered open port 2179/tcp on [redacted]
Discovered open port 2179/tcp on [redacted]
Discovered open port 1043/tcp on [redacted]
Discovered open port 2179/tcp on [redacted]
Completed SYN Stealth Scan against [redacted] in 7.79s (2 hosts left)
Completed SYN Stealth Scan against [redacted] in 7.88s (1 host left)
Completed SYN Stealth Scan at 17:36, 7.88s elapsed (3000 total ports)
Initiating UDP Scan at 17:36
Scanning 3 hosts [1000 ports/host]
Increasing send delay for [redacted] from 0 to 50 due to max_successful_ryno incre
Increasing send delay for [redacted] from 0 to 50 due to max_successful_ryno incre
Increasing send delay for [redacted] from 0 to 50 due to max_successful_ryno increase to 5
```

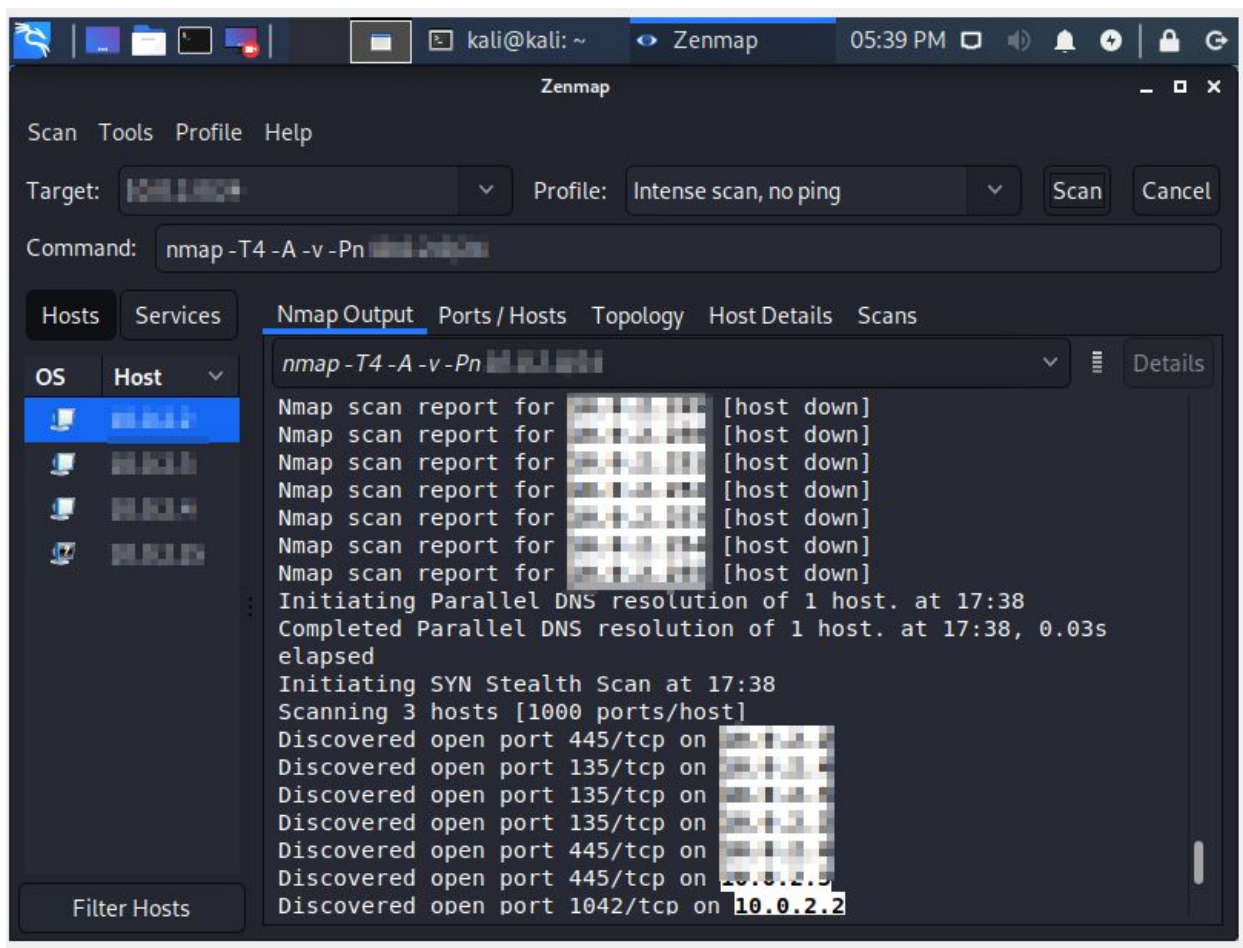

- Intense scan, all TCP ports: **nmap -p 1-65535 -T4 -A -v**
 - What does this scan do in technical terms?
 - Scans a list of 1000 most common protocols between 1 -65535 including all TCP ports
 - Was the scan correct?
 - Yes
 - Why/why not?
 - This command executes as expected showing all 65535 attempts focusing on TCP open and closed ports.

Intense scan / Tcp



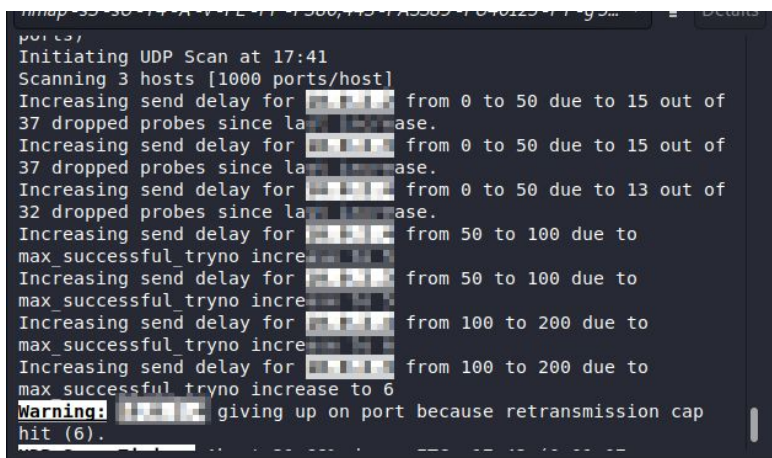
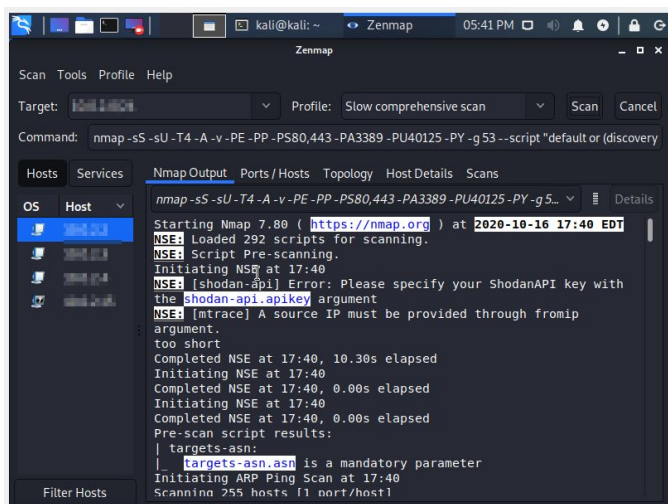
- Intense scan, no ping: **-T4 -A -v -Pn**
 - What does this scan do in technical terms?
 - This performs the same functions as the intense scan with the expectation that the target is up, and does not send ICMP packets
 - Was the scan correct?
 - Yes
 - Why/why not?
 - Command worked as expected not displaying any ICMP request

Intense scan / no ping



- Slow comprehensive scan: **-sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53**
 - What does this scan do in technical terms?
 - This command scans for TCP, UDP, and SCTP and puts a lot of effort to identify the host within the network trying to identify OS and host and could be time-intensive, taking over an hour to complete
 - Was the scan correct?
 - Yes
 - Why/why not?
 - Yes, this performed a very thorough scan taking over an hour and many attempts to identify host ports connected with each port.

Slow comprehensive



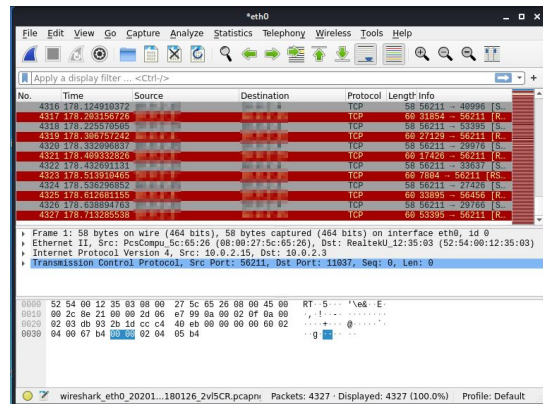
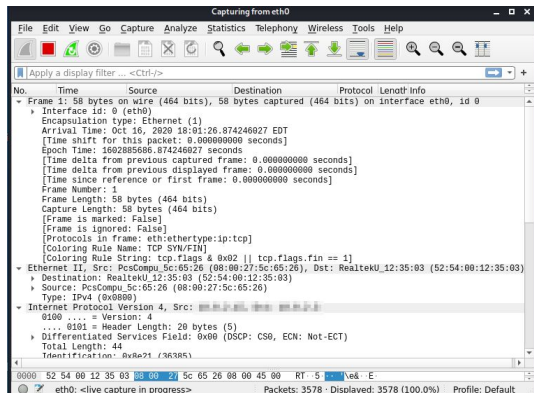
Part 3: Sniffing ICMP Packets with Wireshark

Step 1- Launch Wireshark from Kali Linux (it's part of Kali).

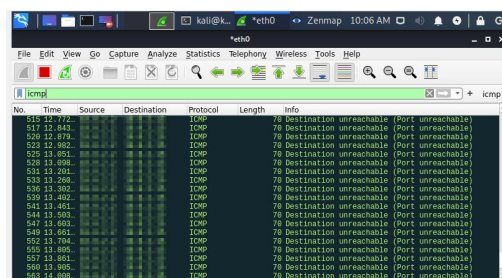
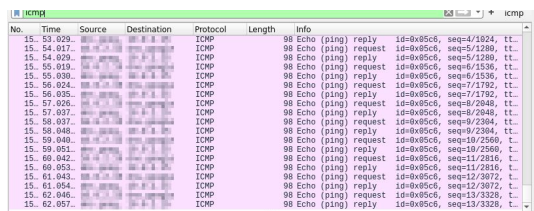
Step 2- Begin sniffing.

Step 3 - Filter the view to ICMP packets only

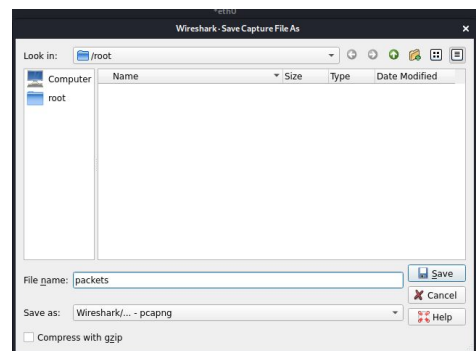
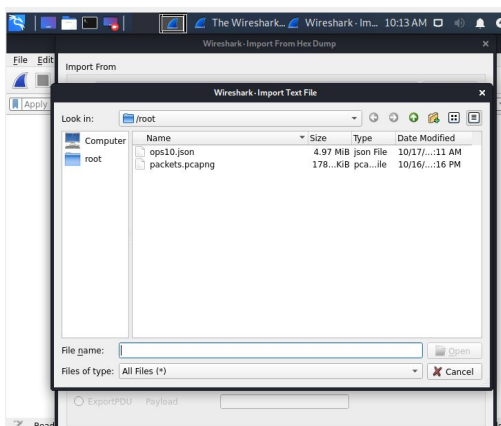
Wireshark



Icmp



File



Part 4: Reporting

Compile your findings in an organized fashion.

- Create a **Scans Performed** table with three columns: Scan Type, Scan Results, Actual.
 - Populate the table with your results.
- Create a **Service Enumeration** table with three columns: Server IP Address, Ports Open, and Service/Banner.
 - Populate the table with your results.
 - Indicate above the table your network range with CIDR block notation.

Scans performed table

```
File Edit Search View Document Help
/lospkkt.csv - Mousepad

No. Time Source Destination Protocol Length Info
1 0.000000000 cdns01.comcast.net DNS 76 Standard query 0x9e49 A www.facebook.com
2 0.000012500 cdns01.comcast.net DNS 76 Standard query 0x114e AAAA www.facebook.com
3 0.015477108 cdns01.comcast.net DNS 121 Standard query response 0x9e49 A www.facebook.com CNAME star-mini.c10r.facebook.com A 31.13.88.35
4 0.020216455 cdns01.comcast.net DNS 133 Standard query response 0x114e AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f118:82:fac
5 0.020927398 facebook.com TCP 74 46336 > 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3210994501 TSecr=0 WS=128
6 0.037768632 facebook.com TCP 60 443 > 46336 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7 0.037802873 facebook.com TCP 54 46336 > 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8 0.038525232 facebook.com TLSv1.3 571 Client Hello
9 0.038624032 facebook.com TCP 60 443 > 46336 [ACK] Seq=1 Ack=518 Win=65535 Len=0
10 0.061304921 facebook.com TLSv1.3 1446 Server Hello, Change Cipher Spec, Application Data
11 0.061329429 facebook.com TCP 54 46336 > 443 [ACK] Seq=518 Ack=1393 Win=64032 Len=0
12 0.062442741 facebook.com TLSv1.3 1792 Application Data, Application Data
13 0.062447102 facebook.com TCP 54 46336 > 443 [ACK] Seq=518 Ack=3131 Win=62480 Len=0
14 0.069556009 cdns01.comcast.net DNS 77 Standard query 0x7f3f A ocsf.digicert.com
15 0.069571355 cdns01.comcast.net DNS 77 Standard query 0xe732 AAAA ocsf.digicert.com
16 0.085649489 cdns01.comcast.net DNS 125 Standard query response 0x7f3f A ocsf.digicert.com CNAME cs9.wac.phicdn.net A 72.21.91.29
17 0.090517086 cdns01.comcast.net DNS 174 Standard query response 0xe732 AAAA ocsf.digicert.com CNAME cs9.wac.phicdn.net SOA ns1.edgecastcdn.net
18 0.091551471 cs9.wac.phicdn.net TCP 74 35722 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3474115693 TSecr=0 WS=128
19 0.108183453 cs9.wac.phicdn.net TCP 60 80 > 35722 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
20 0.108213715 cs9.wac.phicdn.net TCP 54 35722 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
21 0.108658385 cs9.wac.phicdn.net OCSP 425 Request
22 0.108742389 cs9.wac.phicdn.net TCP 60 80 > 35722 [ACK] Seq=1 Ack=372 Win=65535 Len=0
23 0.130631611 cs9.wac.phicdn.net OCSP 853 Response
24 0.130649063 cs9.wac.phicdn.net TCP 54 35722 > 80 [ACK] Seq=372 Ack=800 Win=63920 Len=0
25 0.133379056 facebook.com TLSv1.3 118 Change Cipher Spec, Application Data
26 0.133408831 facebook.com TCP 60 443 > 46336 [ACK] Seq=3131 Ack=582 Win=65535 Len=0
27 0.133555104 facebook.com TLSv1.3 224 Application Data
28 0.133615788 facebook.com TCP 60 443 > 46336 [ACK] Seq=3131 Ack=752 Win=65535 Len=0
29 0.148319219 facebook.com TLSv1.3 330 Application Data, Application Data, Application Data
30 0.148336019 facebook.com TCP 54 46336 > 443 [ACK] Seq=752 Ack=3407 Win=63900 Len=0
31 0.148588759 facebook.com TLSv1.3 85 Application Data
32 0.148669190 facebook.com TCP 60 443 > 46336 [ACK] Seq=3407 Ack=783 Win=65535 Len=0
33 0.229182634 facebook.com TLSv1.3 290 Application Data
34 0.229426944 facebook.com TCP 60 443 > 46336 [ACK] Seq=3407 Ack=1019 Win=65535 Len=0
35 0.243978007 facebook.com TLSv1.3 89 Application Data
36 0.243993354 facebook.com TCP 54 46336 > 443 [ACK] Seq=1019 Ack=3442 Win=63900 Len=0
37 0.417767971 facebook.com TLSv1.3 8574 Application Data, Application Data
38 0.417795577 facebook.com TCP 54 46336 > 443 [ACK] Seq=1019 Ack=11962 Win=59640 Len=0
39 0.417844353 facebook.com TCP 1278 443 > 46336 [PSH, ACK] Seq=11962 Ack=1019 Win=65535 Len=1224 [TCP segment of a reassembled PDU]
40 0.417846408 facebook.com TCP 54 46336 > 443 [ACK] Seq=1019 Ack=13186 Win=58416 Len=0
41 0.418818695 facebook.com TCP 4230 443 > 46336 [PSH, ACK] Seq=13186 Ack=1019 Win=65535 Len=4176 [TCP segment of a reassembled PDU]
42 0.418827655 facebook.com TCP 54 46336 > 443 [ACK] Seq=1019 Ack=17362 Win=62480 Len=0
```