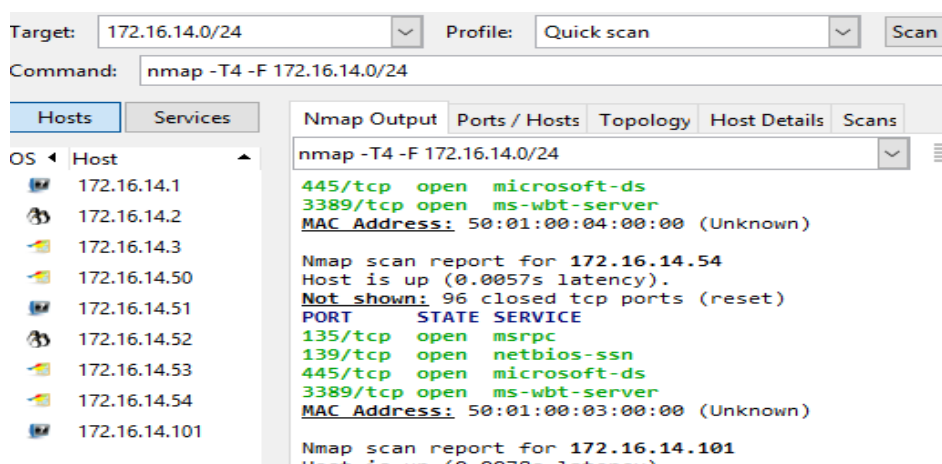


Network Administration Project
Date: July 3rd, 2030

1. Following end point devices are connected to the network 172.16.14.0/24

- a. Windows1 at 172.16.14.50
- b. Windows2 at 172.16.14.54
- c. KaliOpenVas, Linux machine at 172.16.14.51
- d. Linux machine at 172.16.14.52
- e. Windows Server at 172.16.14.53

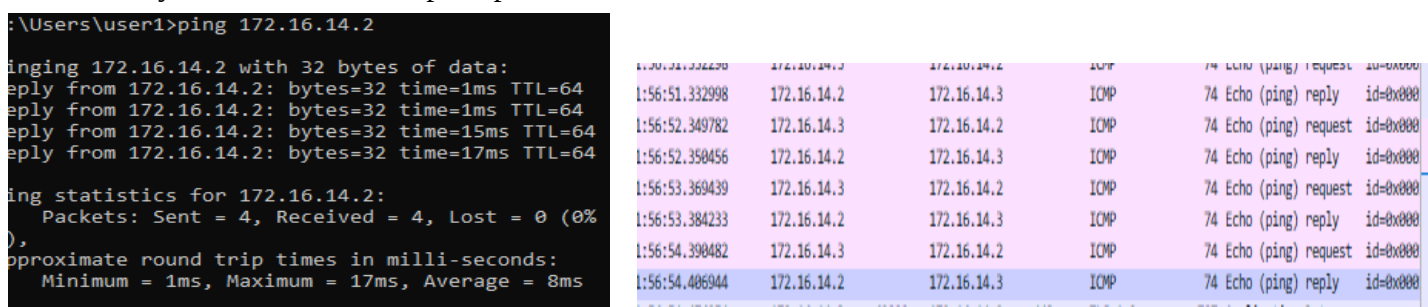
A quick scan of the network 172.16.14.0/24 with Zen map reveals additional information as follows:



- a. Network Gateway at 172.16.14.1
- b. EVE server at 172.16.14.2
- c. Jump Host (launch for EVE) at 172.16.14.3
- d. Unidentified IP not part of the network at 172.16.14.101

3. When using Wireshark and command prompt on Jump host each machine is pinged, following results are obtained:

- a. EVE server at 172.16.14.2 and Jumpshot at 172.16.14.3 are shown to respond to the ping. Ping is a connection less ICMP protocol. Screen shot below shows the time, source, destination and the protocol used. Source port and destination port are not shown because ICMP exist on the network layer and has no concept of ports.



```
C:\Users\user1>ping 172.16.14.1

Pinging 172.16.14.1 with 32 bytes of data:
Reply from 172.16.14.1: bytes=32 time=1ms TTL=255
Reply from 172.16.14.1: bytes=32 time=1ms TTL=255
Reply from 172.16.14.1: bytes=32 time=1ms TTL=255
Reply from 172.16.14.1: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

172.16.14.1	ICMP	74 Echo (ping) request	id=0x0001, seq=50/12800, ttl=128 (reply in 174)
172.16.14.3	ICMP	74 Echo (ping) reply	id=0x0001, seq=50/12800, ttl=255 (request in 173)
172.16.14.1	ICMP	74 Echo (ping) request	id=0x0001, seq=51/13056, ttl=128 (reply in 195)
172.16.14.3	ICMP	74 Echo (ping) reply	id=0x0001, seq=51/13056, ttl=255 (request in 194)
172.16.14.1	ICMP	74 Echo (ping) request	id=0x0001, seq=52/13312, ttl=128 (reply in 207)
172.16.14.3	ICMP	74 Echo (ping) reply	id=0x0001, seq=52/13312, ttl=255 (request in 206)
172.16.14.1	ICMP	74 Echo (ping) request	id=0x0001, seq=53/13568, ttl=128 (reply in 224)
172.16.14.3	ICMP	74 Echo (ping) reply	id=0x0001, seq=53/13568, ttl=255 (request in 223)

b. Similar results are seen when Gateway router is pinged at 172.16.14.1. Both the router and Jumpshot respond to the ping.

```
C:\Users\user1>ping 172.16.14.50

Pinging 172.16.14.50 with 32 bytes of data:
Reply from 172.16.14.50: bytes=32 time=2ms TTL=128
Reply from 172.16.14.50: bytes=32 time=3ms TTL=128
Reply from 172.16.14.50: bytes=32 time=2ms TTL=128
Reply from 172.16.14.50: bytes=32 time=2ms TTL=128

Ping statistics for 172.16.14.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

177	2023-07-04 15:15:43.394862	172.16.14.3	172.16.14.50	ICMP	74 Echo (ping) request
178	2023-07-04 15:15:43.396445	172.16.14.50	172.16.14.3	ICMP	74 Echo (ping) reply
201	2023-07-04 15:15:44.418322	172.16.14.3	172.16.14.50	ICMP	74 Echo (ping) request
202	2023-07-04 15:15:44.420299	172.16.14.50	172.16.14.3	ICMP	74 Echo (ping) reply
215	2023-07-04 15:15:45.4443077	172.16.14.3	172.16.14.50	ICMP	74 Echo (ping) request
216	2023-07-04 15:15:45.444555	172.16.14.50	172.16.14.3	ICMP	74 Echo (ping) reply
280	2023-07-04 15:15:46.467481	172.16.14.3	172.16.14.50	ICMP	74 Echo (ping) request
283	2023-07-04 15:15:46.468945	172.16.14.50	172.16.14.3	ICMP	74 Echo (ping) reply

c. Screenshot shown above show results when Windows 1 machine is pinged

```
C:\Users\user1>ping 172.16.14.51

Pinging 172.16.14.51 with 32 bytes of data:
Reply from 172.16.14.51: bytes=32 time=5ms TTL=64
Reply from 172.16.14.51: bytes=32 time=2ms TTL=64
Reply from 172.16.14.51: bytes=32 time=2ms TTL=64
Reply from 172.16.14.51: bytes=32 time=2ms TTL=64

Ping statistics for 172.16.14.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 2ms
```

271	2023-07-04 15:27:53.472325	172.16.14.3	172.16.14.51	ICMP	74 Echo (ping) request
273	2023-07-04 15:27:53.476361	172.16.14.51	172.16.14.3	ICMP	74 Echo (ping) reply
296	2023-07-04 15:27:54.486046	172.16.14.3	172.16.14.51	ICMP	74 Echo (ping) request
297	2023-07-04 15:27:54.487086	172.16.14.51	172.16.14.3	ICMP	74 Echo (ping) reply
313	2023-07-04 15:27:55.507993	172.16.14.3	172.16.14.51	ICMP	74 Echo (ping) request
314	2023-07-04 15:27:55.509243	172.16.14.51	172.16.14.3	ICMP	74 Echo (ping) reply
331	2023-07-04 15:27:56.525524	172.16.14.3	172.16.14.51	ICMP	74 Echo (ping) request
332	2023-07-04 15:27:56.526911	172.16.14.51	172.16.14.3	ICMP	74 Echo (ping) reply

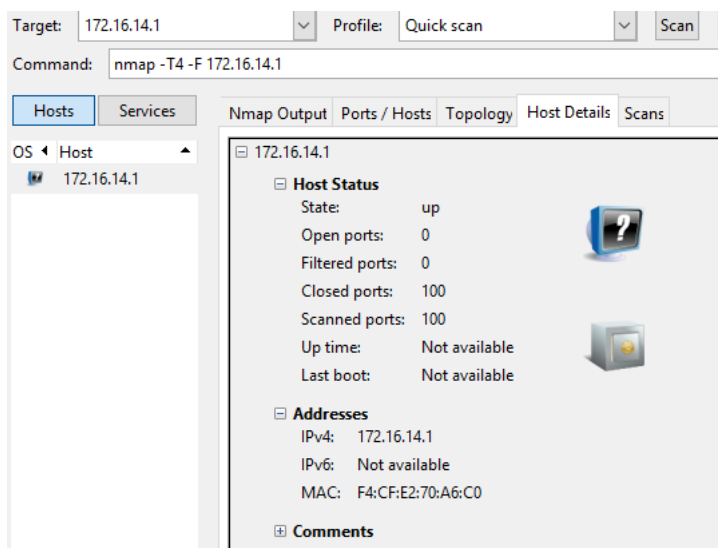
d. Screenshot above shows results obtained when Kali machine is pinged at 172.16.14.51. Similar results are seen when Windows server and Linux machine are pinged at 172.16.14.53 & 172.16.14.52 respectively.

5. Zemap of the network at 172.16.14.0/24 as shown in part 1 shows following devices on the network:

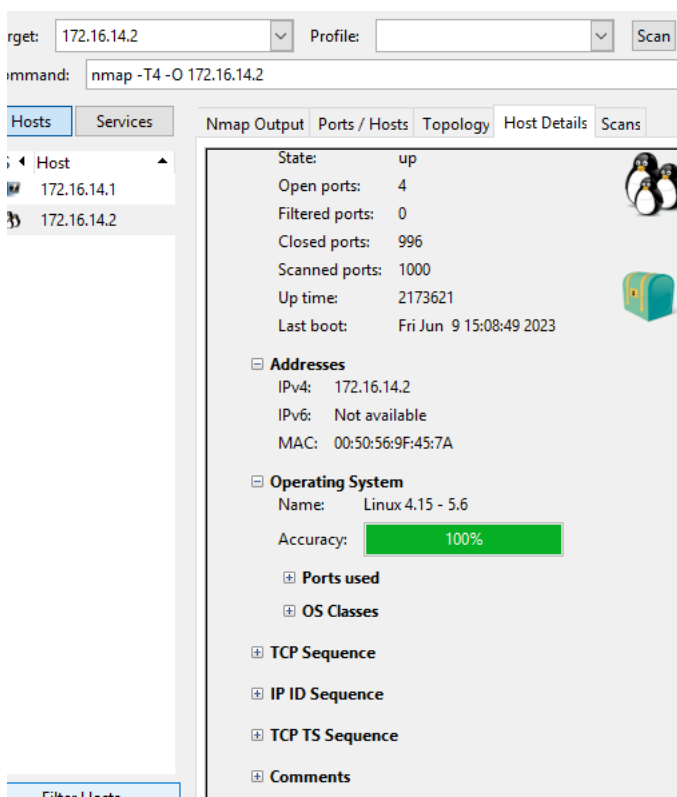
- Network Gateway at 172.16.14.1
- EVE server at 172.16.1 4.2
- Jump Host (launch for EVE) at 172.16.14.3
- Windows1 at 172.16.14.50

- e. Windows2 at 172.16.14.54
- f. KaliOpenVas, Linux machine at 172.16.14.51
- g. Linux machine at 172.16.14.52
- h. Windows Server at 172.16.14.53
- I. Unidentified IP not part of the network at 172.16.14.101

An Zenmap scan of Gateway rudder at 172.16.14.1 shows following information. Device' MAC address is shown and it has no open ports.



Scan of EVE server at 172.16.14.2 shows its running Linux 4.15-5.6 and it has four open ports.



Port	Protocol	State	Service	Version
22	tcp	open	ssh	
80	tcp	open	http	
443	tcp	open	https	
9090	tcp	open	zeus-admin	

Scan of Jumphost server shows following scan. It is shown to run Windows 10 OS with 97% accuracy, but its running Windows server OS. It shows 4 open ports.

get: 172.16.14.3

Profile:

Scan

Car

mmand: nmap -T4 -O 172.16.14.3

Hosts

Services

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

Host

172.16.14.1

172.16.14.2

172.16.14.3

Filter Hosts

172.16.14.3

Host Status

State: up

Open ports: 4

Filtered ports: 0

Closed ports: 996

Scanned ports: 1000

Up time: Not available

Last boot: Not available

Addresses

IPv4: 172.16.14.3

IPv6: Not available

MAC: Not available

Operating System

Name: Microsoft Windows 10 1809 - 1909

Accuracy: 97%

Ports used

OS Classes

TCP Sequence

IP ID Sequence

TCP TS Sequence

Port	Protocol	State	Service	Ver
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
445	tcp	open	microsoft-ds	
3389	tcp	open	ms-wbt-server	

Zenmap scan of Windows1 indicates its running Windows 10 OS and it has 4 open ports

Target: 172.16.14.50

Profile:

Scan

Car

Command: nmap -T4 -O 172.16.14.50

Hosts

Services

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

OS

Host

172.16.14.1

172.16.14.2

172.16.14.3

172.16.14.50

Filter Hosts

172.16.14.50

Host Status

State: up

Open ports: 5

Filtered ports: 0

Closed ports: 995

Scanned ports: 1000

Up time: 38388

Last boot: Tue Jul 4 08:49:52 2023

Addresses

IPv4: 172.16.14.50

IPv6: Not available

MAC: 50:01:00:02:00:00

Operating System

Name: Microsoft Windows 10 1507 - 1607

Accuracy: 100%

Ports used

OS Classes

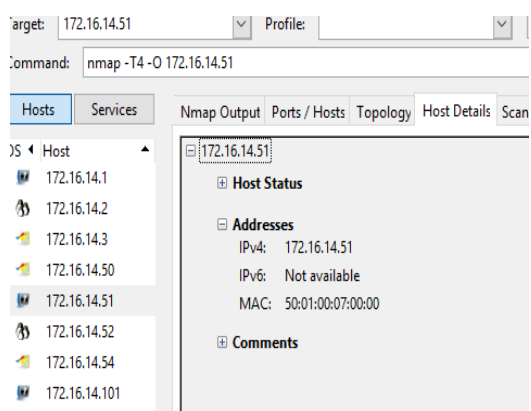
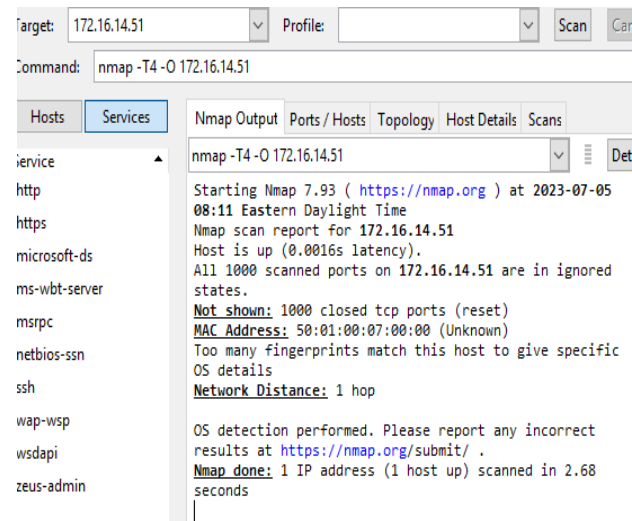
TCP Sequence

IP ID Sequence

TCP TS Sequence

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
445	tcp	open	microsoft-ds	
3389	tcp	open	ms-wbt-server	
5357	tcp	open	wsdapi	

Kali Linux machine on IP 172.16.14.51 does not show any ports. As Kali is a secure machine with no open ports, Zenmap scan does not reveal any information about OS. MAC is shown as 50:01:00:07:00:00



Zenmap scan of Linux machine shows its running Linux 5.0-5.3. MAC is 50:01:00:05:00:00. It shows 3 open ports for tcp, microsoft web server and wireless connections. ICMP and ARPs are captured with Wireshark.

