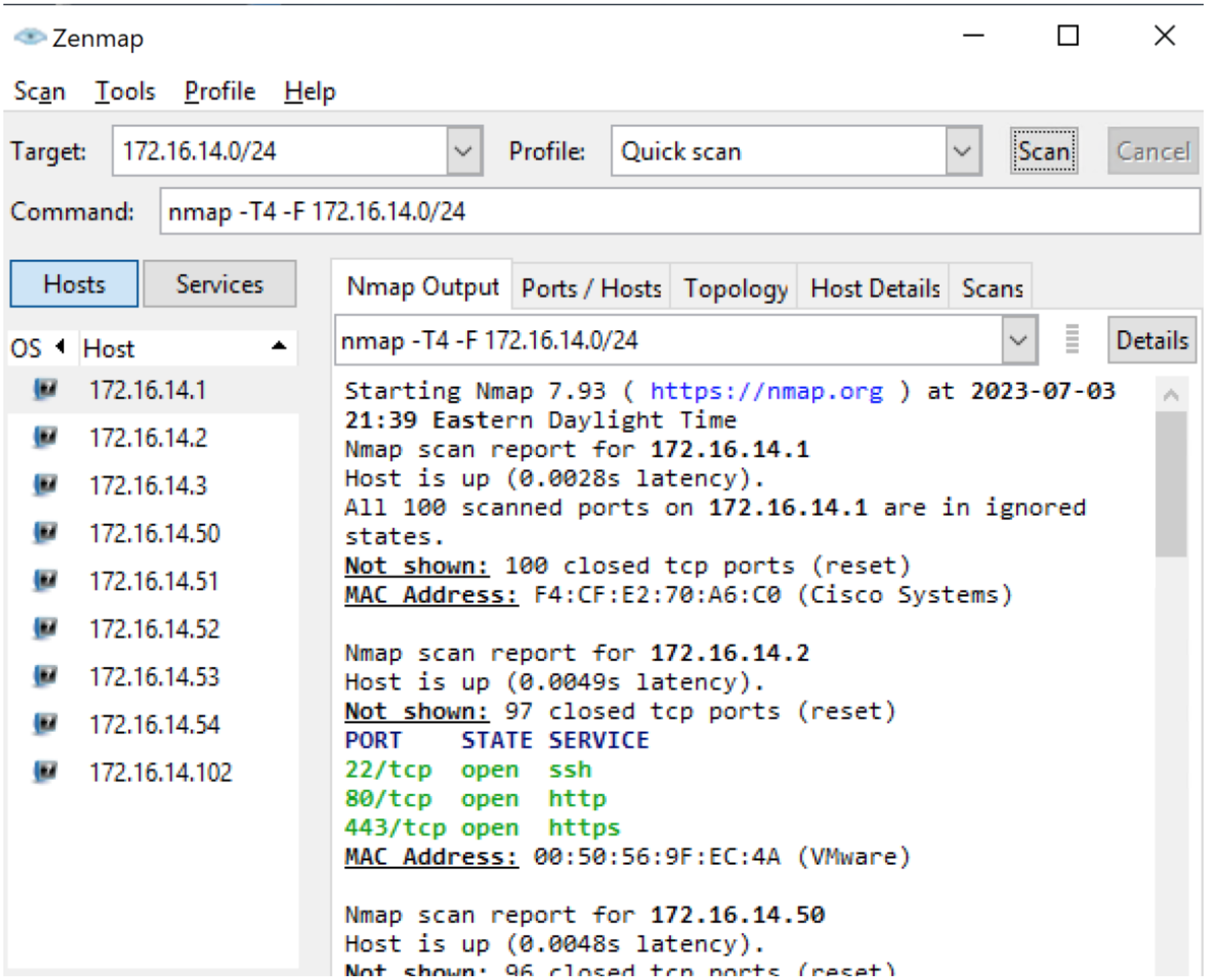
172.16.14.0 /24 Network

I ran a Zenmap scan on the network and managed to find 8 devices which I have listed below along with some more details on each. I also ran a Ping to each machine on the network to verify that a connection was valid for communication between devices.
You will find screen captures of each command I used below.

Zenmap quick scan of Network (172.16.14.0/24) using command nmap -T4 -F 172.16.14.0/24 which I used to find the 8 devices attached to the network



Target: 172.16.14.0/24
Profile: Quick scan
Command: nmap -T4 -F 172.16.14.0/24

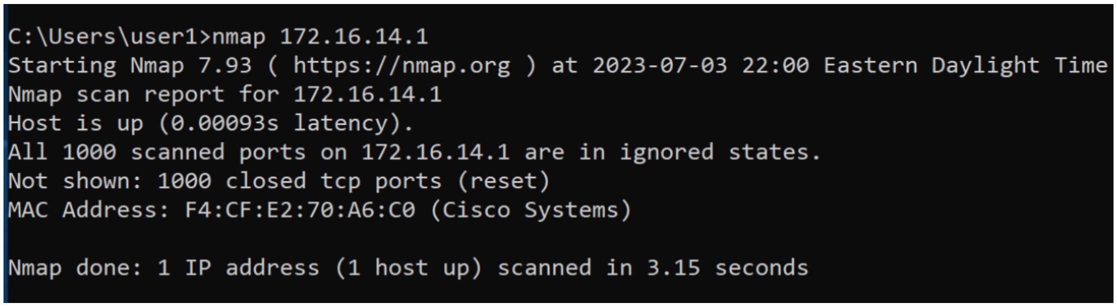
```
172.16.14.1
172.16.14.2
172.16.14.3
172.16.14.50
172.16.14.51
172.16.14.52
172.16.14.53
172.16.14.54
172.16.14.102
```

```
nmap -T4 -F 172.16.14.0/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03
21:39 Eastern Daylight Time
Nmap scan report for 172.16.14.1
Host is up (0.0028s latency).
All 100 scanned ports on 172.16.14.1 are in ignored
states.
Not shown: 100 closed tcp ports (reset)
MAC Address: F4:CF:E2:70:A6:C0 (Cisco Systems)

Nmap scan report for 172.16.14.2
Host is up (0.0049s latency).
Not shown: 97 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:50:56:9F:EC:4A (VMware)

Nmap scan report for 172.16.14.50
Host is up (0.0048s latency).
Not shown: 96 closed tcp ports (reset)
```

172.16.14.1

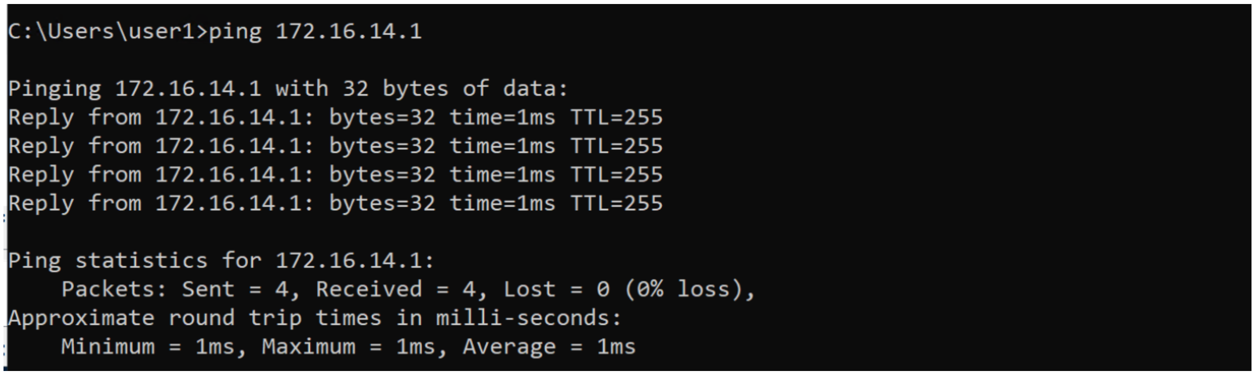
- Cisco Router (Gateway)
- MAC address: F4:CF:E2:70:A6:C0 (Cisco Systems)
- No open ports found

Nmap scan of 172.16.14.1 in Command Prompt to find more information of the device belonging to the IP address



```
C:\Users\user1>nmap 172.16.14.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:00 Eastern Daylight Time
Nmap scan report for 172.16.14.1
Host is up (0.00093s latency).
All 1000 scanned ports on 172.16.14.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: F4:CF:E2:70:A6:C0 (Cisco Systems)

Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds
```

Ping of IP address to make sure that the network is able to be found by devices

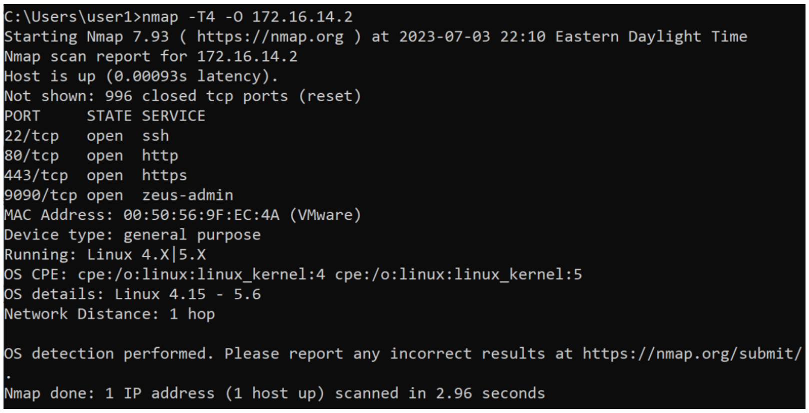


```
C:\Users\user1>ping 172.16.14.1

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),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

172.16.14.2

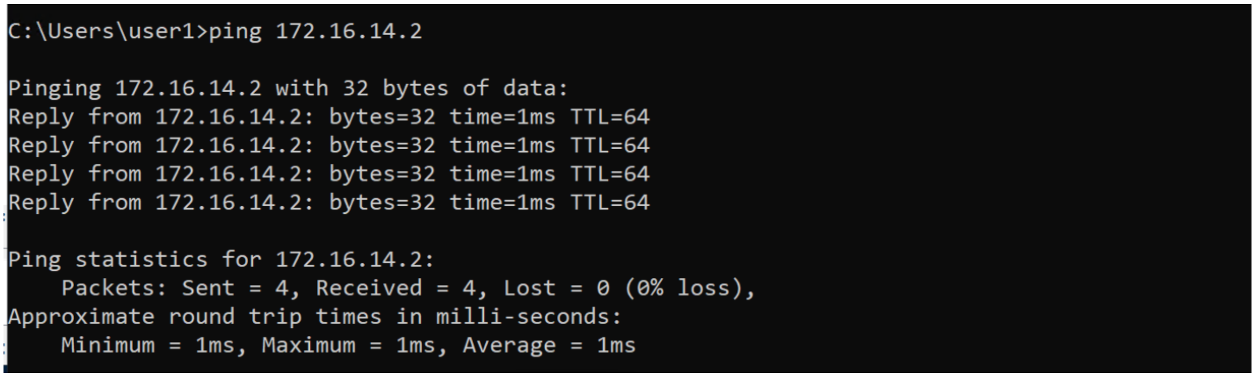
- EVE Server
- OS: Linux 4.15-5.6
- MAC address: 00:50:56:9F:EC:4A (VMware)
- Open ports
  - 22/tcp   open ssh
  - 80/tcp   open http
  - 443/tcp open https
  - 9090/tcp open zeus-admin
- Device type: general purpose

Nmap OS scan of 172.16.14.2 to find further details about the device attached to IP address



```
C:\Users\user1>nmap -T4 -O 172.16.14.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:10 Eastern Daylight Time
Nmap scan report for 172.16.14.2
Host is up (0.00093s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
9090/tcp open  zeus-admin
MAC Address: 00:50:56:9F:EC:4A (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
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 2.96 seconds
```

Ping of 172.16.14.2

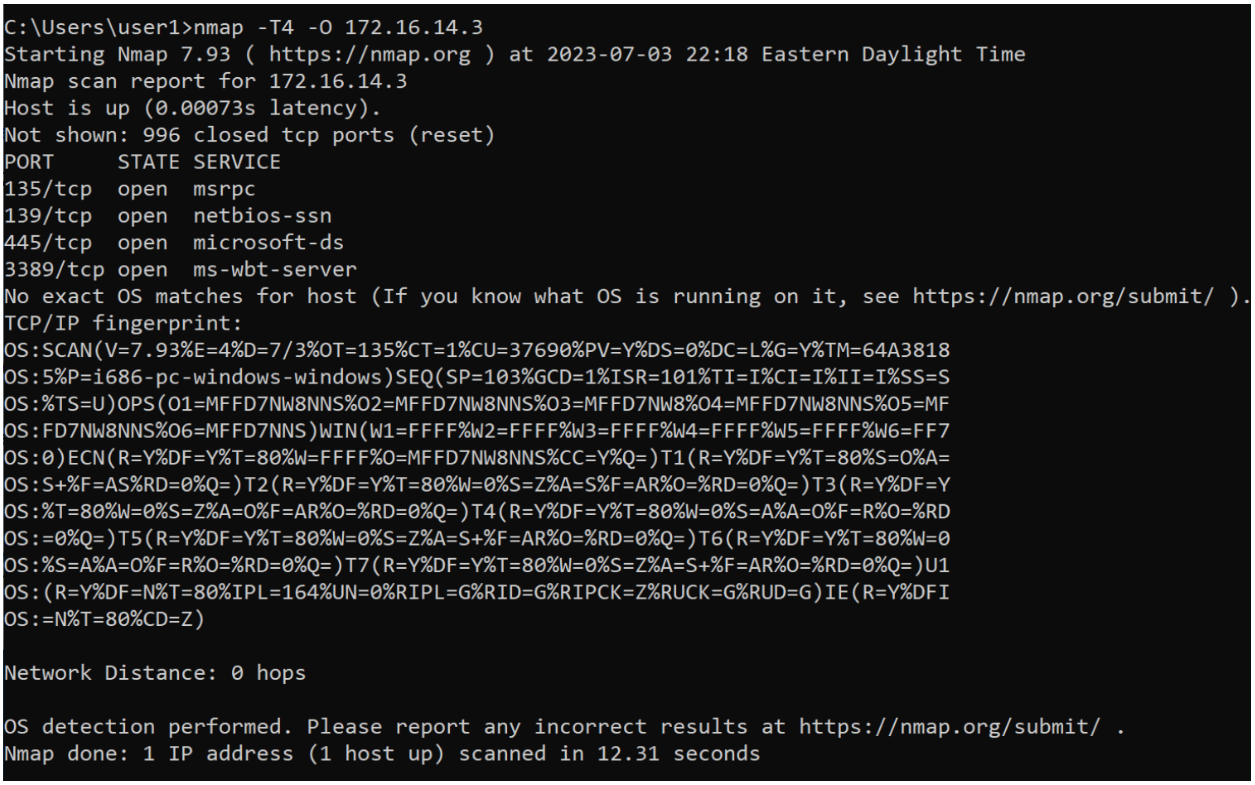


```
C:\Users\user1>ping 172.16.14.2

Pinging 172.16.14.2 with 32 bytes of data:
Reply from 172.16.14.2: bytes=32 time=1ms TTL=64
Reply from 172.16.14.2: bytes=32 time=1ms TTL=64
Reply from 172.16.14.2: bytes=32 time=1ms TTL=64
Reply from 172.16.14.2: bytes=32 time=1ms TTL=64

Ping statistics for 172.16.14.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

172.16.14.3

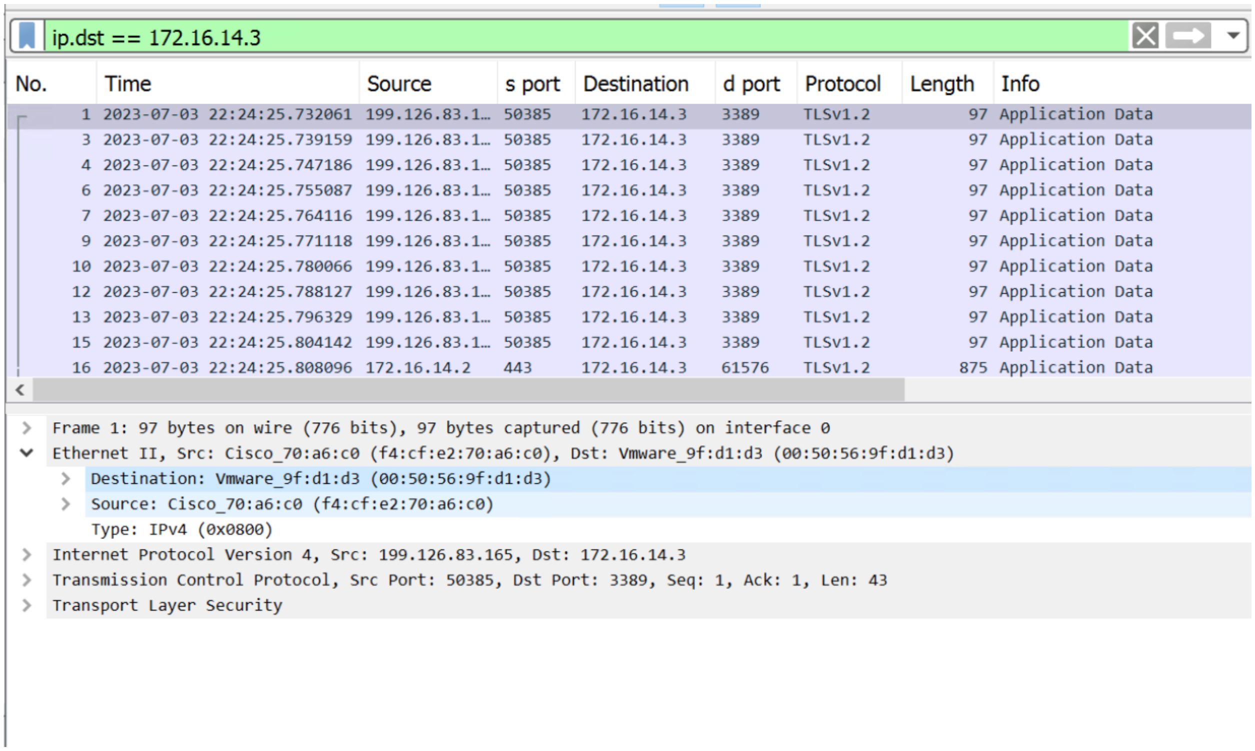
- JumpHost
- OS: Microsoft Windows 10 1809
- MAC address: 00:50:56:9F: D1: D3 (VMware)
- Open ports
  - 135/tcp open msrpc
  - 139/tcp open netbios-ssn
  - 445/tcp open microsoft-ds
  - 3389/tcp open ms-wbt-server

Nmap OS scan of 172.16.14.3 to find details about device attached to IP address



```
C:\Users\user1>nmap -T4 -O 172.16.14.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:18 Eastern Daylight Time
Nmap scan report for 172.16.14.3
Host is up (0.00073s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=7/3%OT=135%CT=1%CU=37690%PV=Y%DS=0%DC=L%G=Y%TM=64A3818
OS:5%P=i686-pc-windows-windows)SEQ(SP=103%GCD=1%ISR=101%TI=I%CI=I%II=I%SS=S
OS:%TS=U)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=MF
OS:FD7NW8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF7
OS:0)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=
OS:S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y
OS:%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0
OS:%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.31 seconds
```

Wireshark which I used to find the MAC address for 172.16.14.3 after it was not found in the Nmap OS scan

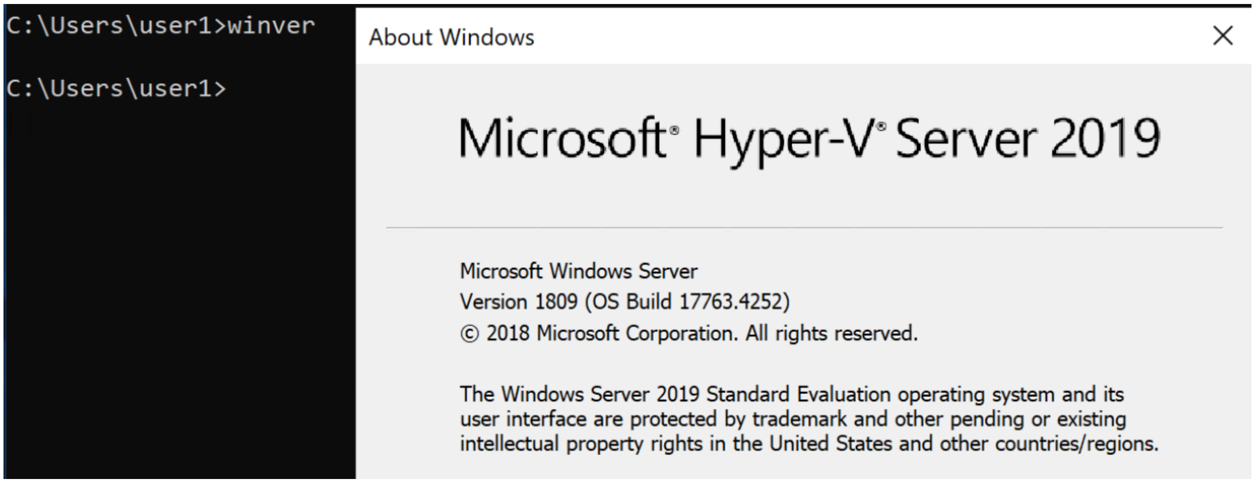


```
ip.dst == 172.16.14.3
```

```
No.  Time                        Source           s port  Destination   d port  Protocol  Length  Info
   1 2023-07-03 22:24:25.732061  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
   3 2023-07-03 22:24:25.739159  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
   4 2023-07-03 22:24:25.747186  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
   6 2023-07-03 22:24:25.755087  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
   7 2023-07-03 22:24:25.764116  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
   9 2023-07-03 22:24:25.771118  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
  10 2023-07-03 22:24:25.780066  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
  12 2023-07-03 22:24:25.788127  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
  13 2023-07-03 22:24:25.796329  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
  15 2023-07-03 22:24:25.804142  199.126.83.1…    50385   172.16.14.3   3389    TLSv1.2       97  Application Data
  16 2023-07-03 22:24:25.808096  172.16.14.2      443     172.16.14.3   61576   TLSv1.2      875  Application Data
```

```
> Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
v Ethernet II, Src: Cisco_70:a6:c0 (f4:cf:e2:70:a6:c0), Dst: Vmware_9f:d1:d3 (00:50:56:9f:d1:d3)
    > Destination: Vmware_9f:d1:d3 (00:50:56:9f:d1:d3)
    > Source: Cisco_70:a6:c0 (f4:cf:e2:70:a6:c0)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 199.126.83.165, Dst: 172.16.14.3
> Transmission Control Protocol, Src Port: 50385, Dst Port: 3389, Seq: 1, Ack: 1, Len: 43
> Transport Layer Security
```

Command Prompt and result showing that I used the winver command to find the specific OS version belonging to the JumpHost server



```
C:\Users\user1>winver

C:\Users\user1>
```

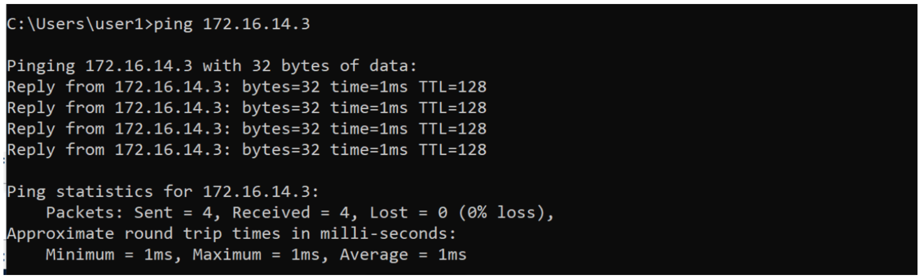
About Windows

Microsoft® Hyper-V® Server 2019

Microsoft Windows Server
Version 1809 (OS Build 17763.4252)
© 2018 Microsoft Corporation. All rights reserved.

The Windows Server 2019 Standard Evaluation operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

Ping of 172.16.14.3

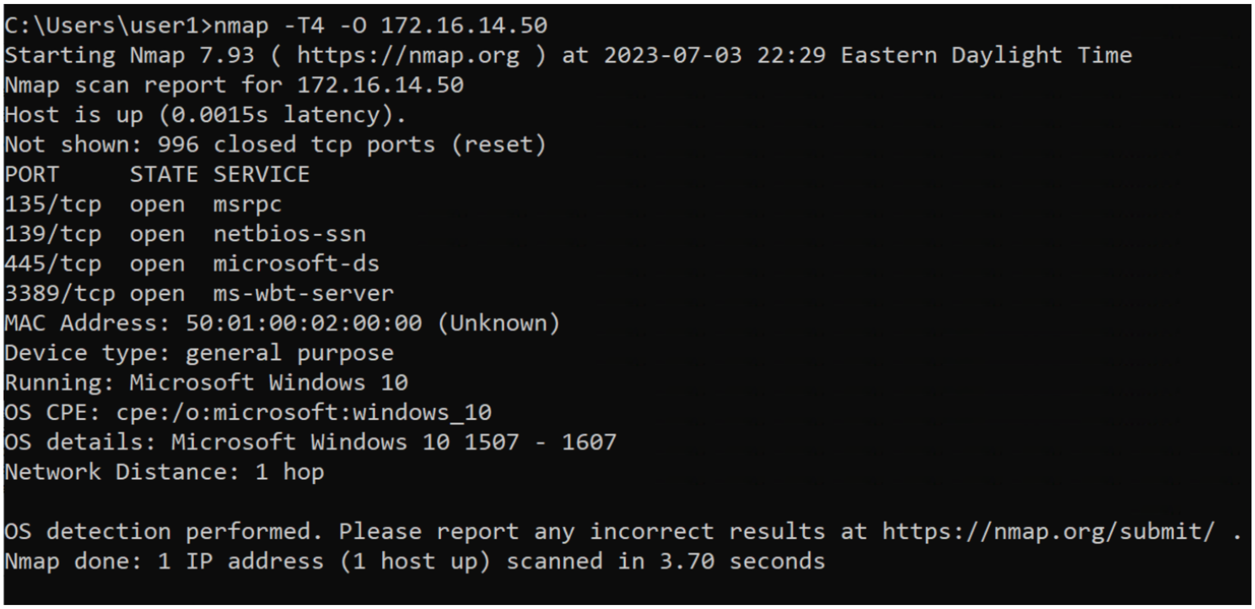


```
C:\Users\user1>ping 172.16.14.3

Pinging 172.16.14.3 with 32 bytes of data:
Reply from 172.16.14.3: bytes=32 time=1ms TTL=128
Reply from 172.16.14.3: bytes=32 time=1ms TTL=128
Reply from 172.16.14.3: bytes=32 time=1ms TTL=128
Reply from 172.16.14.3: bytes=32 time=1ms TTL=128

Ping statistics for 172.16.14.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

172.16.14.50

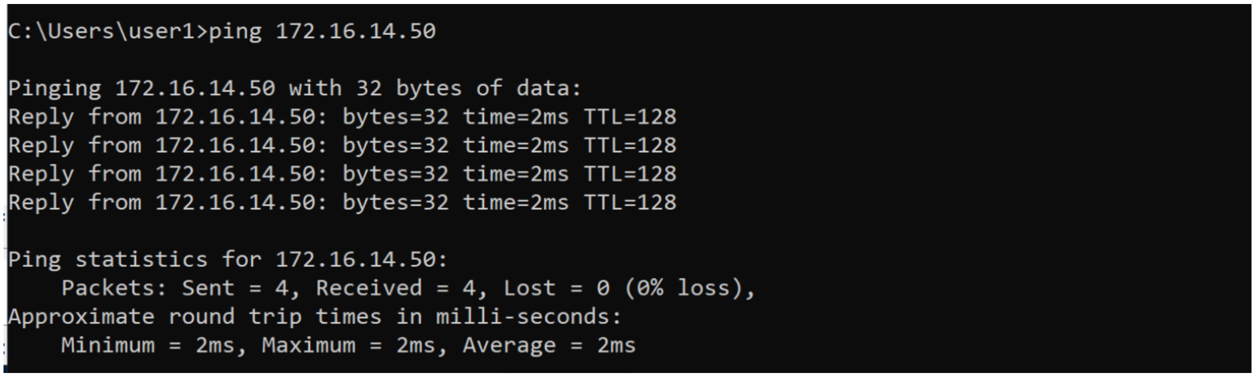
- Windows 1
- OS: Microsoft Windows 10 1507-1607
- MAC address: 50:01:00:02:00:00 (Unknown)
- Open ports
  - 135/tcp open msrpc
  - 139/tcp open netbios-ssn
  - 445/tcp open microsoft-ds
  - 3389/tcp open ms-wbt-server
- Device type: general purpose
- Network distance: 1 hop

Nmap OS scan of 172.16.14.50 to find more details about device



```
C:\Users\user1>nmap -T4 -O 172.16.14.50
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:29 Eastern Daylight Time
Nmap scan report for 172.16.14.50
Host is up (0.0015s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 50:01:00:02:00:00 (Unknown)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 3.70 seconds
```

Ping of 172.16.14.50

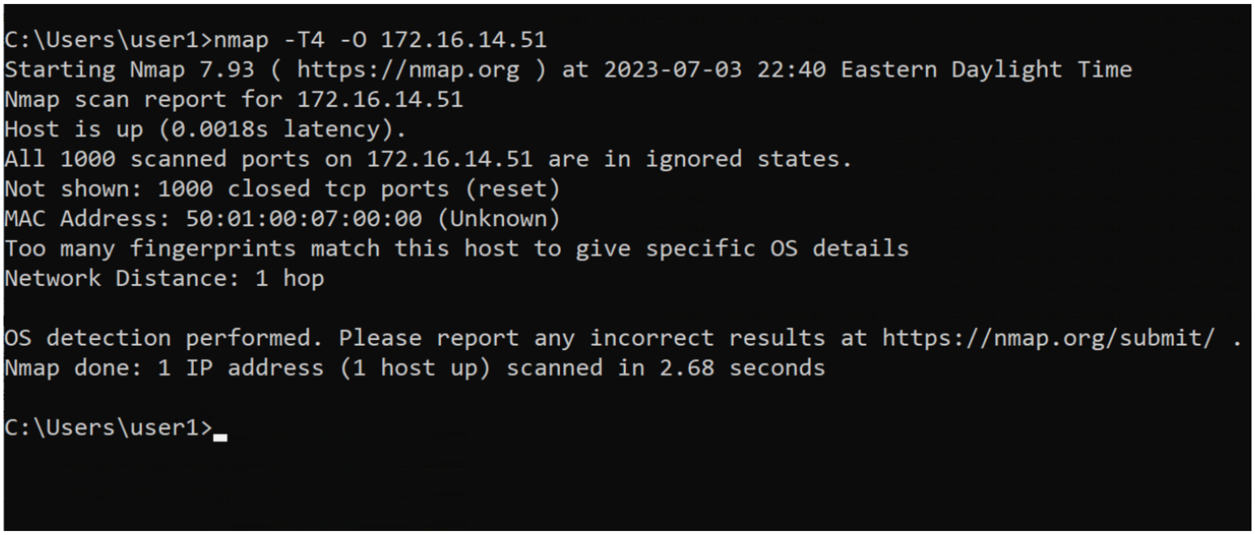


```
C:\Users\user1>ping 172.16.14.50

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=2ms 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 = 2ms, Average = 2ms
```

172.16.14.51

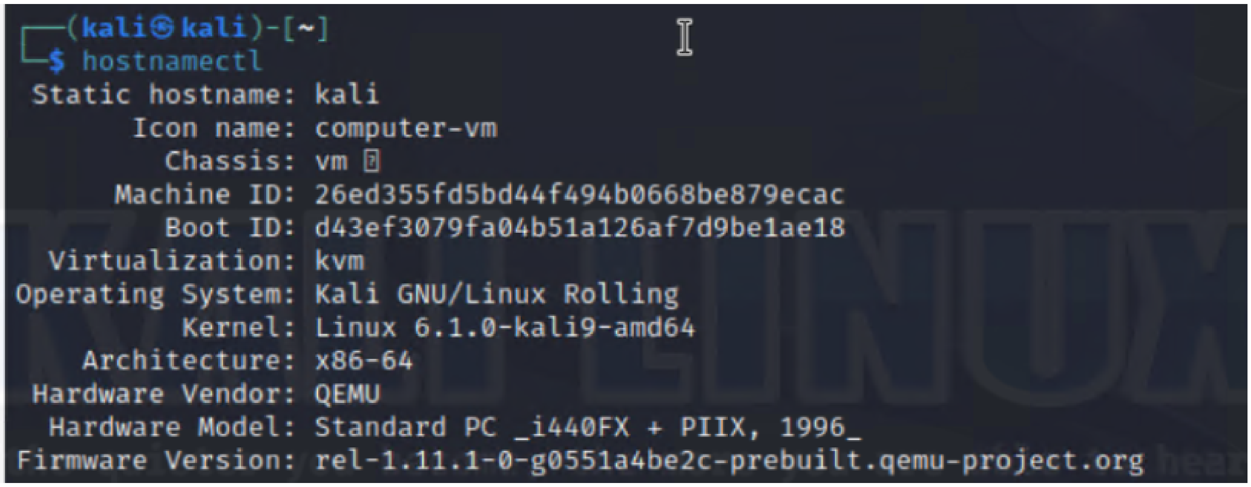
- KaliOpenVas
- OS: Kali GNU/Linux Rolling
- MAC address: 50:01:00:07:00:00 (Unknown)
- No open ports found

Nmap Scan of 172.16.14.51 to find details of device



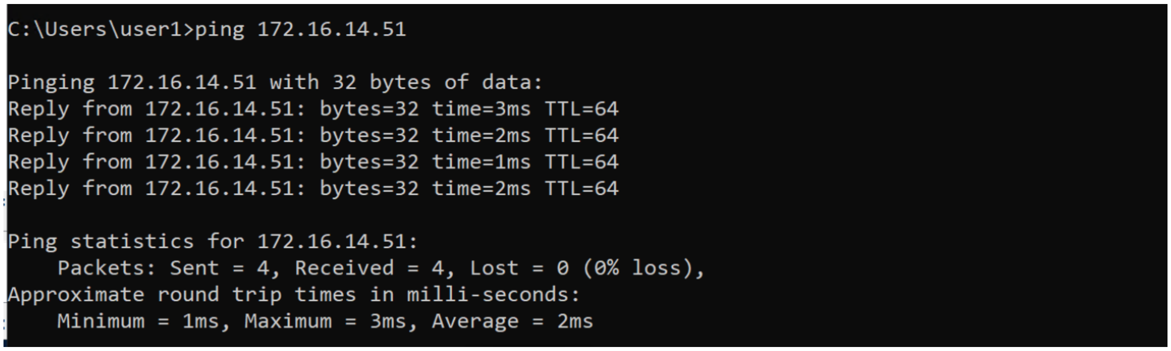
```
C:\Users\user1>nmap -T4 -O 172.16.14.51
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:40 Eastern Daylight Time
Nmap scan report for 172.16.14.51
Host is up (0.0018s latency).
All 1000 scanned ports on 172.16.14.51 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 50:01:00:07:00:00 (Unknown)
Too many fingerprints match this host to give specific OS details
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 2.68 seconds

C:\Users\user1>_
```

I used the command hostnamectl to find the OS for the KaliOpenVas device



```
┌──(kali㉿kali)-[~]
└─$ hostnamectl
 Static hostname: kali
       Icon name: computer-vm
         Chassis: vm □
      Machine ID: 26ed355fd5bd44f494b0668be879ecac
         Boot ID: d43ef3079fa04b51a126af7d9be1ae18
  Virtualization: kvm
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 6.1.0-kali9-amd64
    Architecture: x86-64
 Hardware Vendor: QEMU
  Hardware Model: Standard PC _i440FX + PIIX, 1996_
Firmware Version: rel-1.11.1-0-g0551a4be2c-prebuilt.qemu-project.org
```

Ping of 172.16.14.51

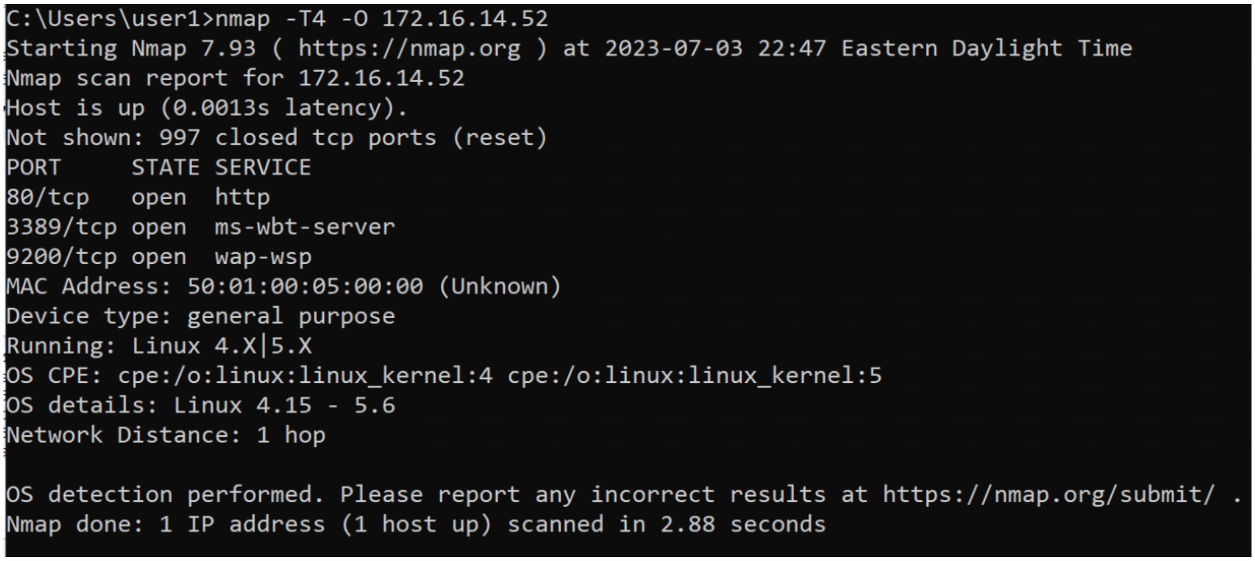


```
C:\Users\user1>ping 172.16.14.51

Pinging 172.16.14.51 with 32 bytes of data:
Reply from 172.16.14.51: bytes=32 time=3ms TTL=64
Reply from 172.16.14.51: bytes=32 time=2ms TTL=64
Reply from 172.16.14.51: bytes=32 time=1ms 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 = 1ms, Maximum = 3ms, Average = 2ms
```

172.16.14.52

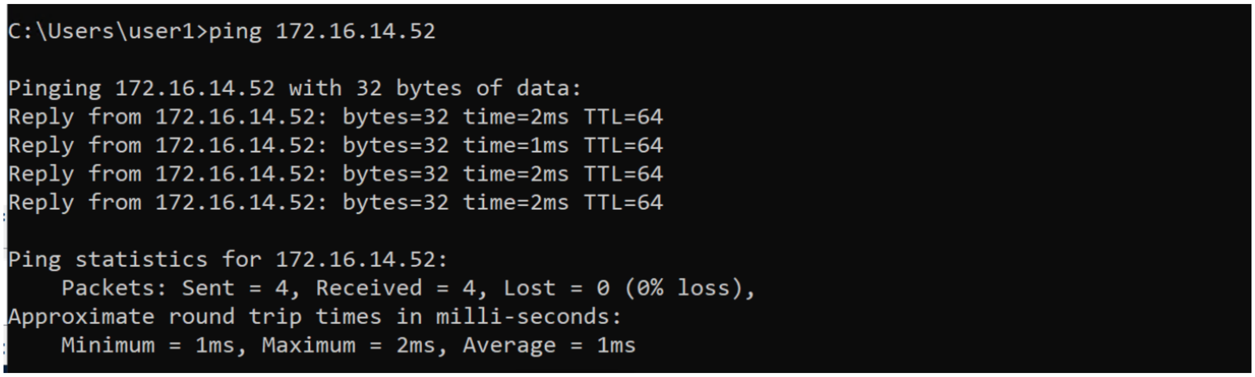
- Linux
- OS: Ubuntu 20.04.6 LTS
- MAC address: 50:01:00:05:00:00 (Unknown)
- Open ports
  - 80/tcp   open http
  - 3389/tcp open ms-wbt-server
  - 9200/tcp open wap-wsp
- Device type: general purpose

Nmap OS scan of 172.16.14.52 to find details of Linux device



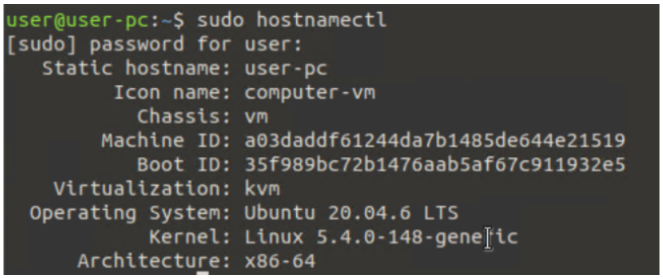
```
C:\Users\user1>nmap -T4 -O 172.16.14.52
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:47 Eastern Daylight Time
Nmap scan report for 172.16.14.52
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
9200/tcp open  wap-wsp
MAC Address: 50:01:00:05:00:00 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
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 2.88 seconds
```

Ping of 172.16.14.52



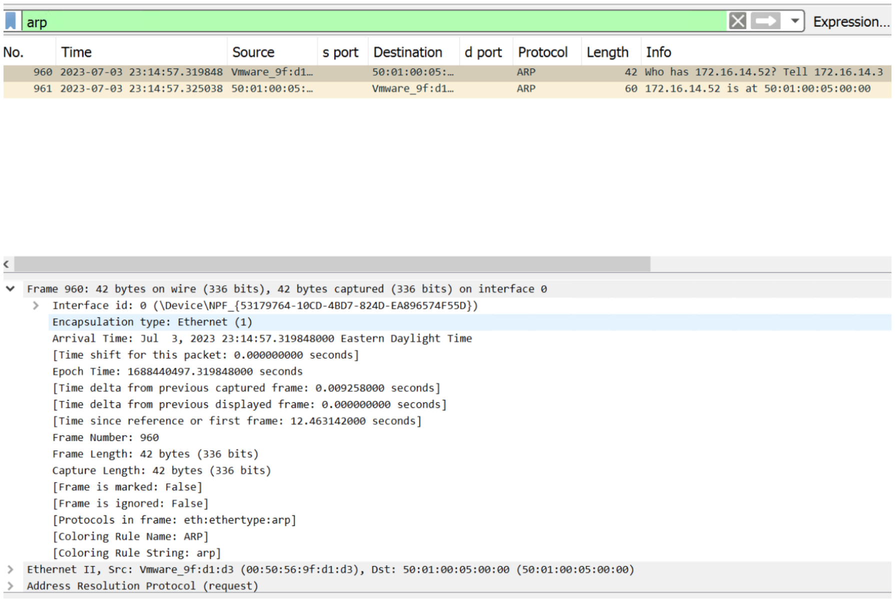
```
C:\Users\user1>ping 172.16.14.52

Pinging 172.16.14.52 with 32 bytes of data:
Reply from 172.16.14.52: bytes=32 time=2ms TTL=64
Reply from 172.16.14.52: bytes=32 time=1ms TTL=64
Reply from 172.16.14.52: bytes=32 time=2ms TTL=64
Reply from 172.16.14.52: bytes=32 time=2ms TTL=64

Ping statistics for 172.16.14.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Capture of hostnamectl command that I used to find the OS of the Linux system



```
user@user-pc:~$ sudo hostnamectl
[sudo] password for user:
   Static hostname: user-pc
         Icon name: computer-vm
           Chassis: vm
        Machine ID: a03daddf61244da7b1485de644e21519
           Boot ID: 35f989bc72b1476aab5af67c911932e5
    Virtualization: kvm
  Operating System: Ubuntu 20.04.6 LTS
            Kernel: Linux 5.4.0-148-generic
      Architecture: x86-64
```

Wireshark capture during the ping of 172.16.14.52 showing an ARP result



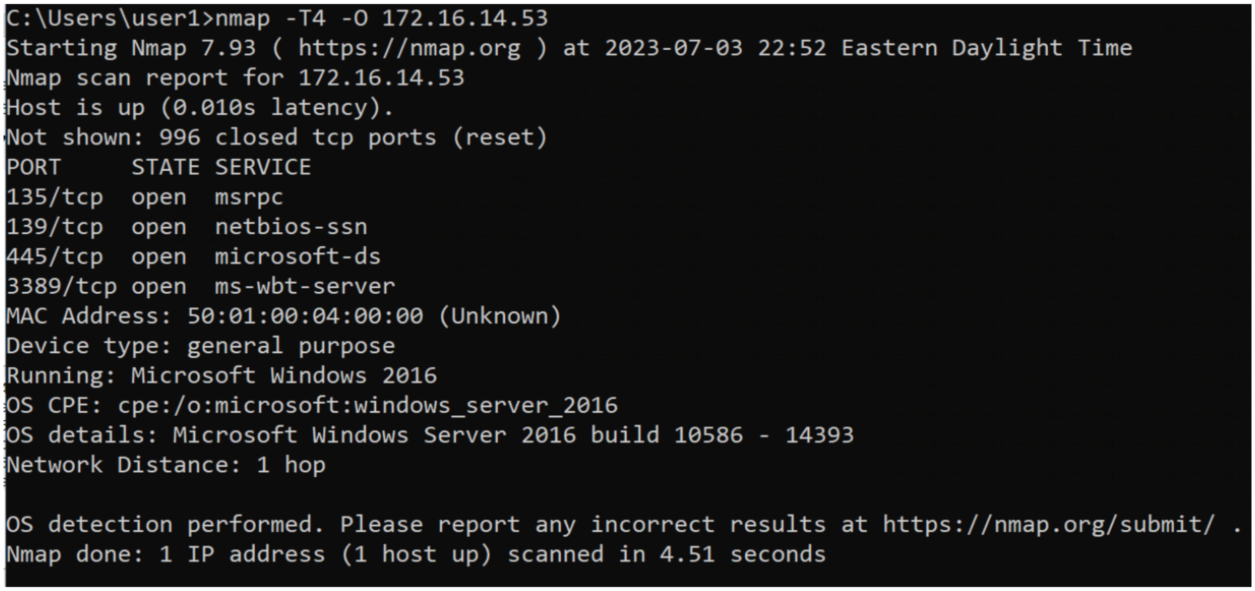
No.	Time	Source	s port	Destination	d port	Protocol	Length	Info
960	2023-07-03 23:14:57.319848	Vmware_9f:d1…		50:01:00:05:…		ARP	42	Who has 172.16.14.52? Tell 172.16.14.3
961	2023-07-03 23:14:57.325038	50:01:00:05:…		Vmware_9f:d1…		ARP	60	172.16.14.52 is at 50:01:00:05:00:00

```
Frame 960: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
  Interface id: 0 (\Device\NPF_{53179764-10CD-4BD7-824D-EA896574F55D})
  Encapsulation type: Ethernet (1)
  Arrival Time: Jul  3, 2023 23:14:57.319848000 Eastern Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1688440497.319848000 seconds
  [Time delta from previous captured frame: 0.009258000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 12.463142000 seconds]
  Frame Number: 960
  Frame Length: 42 bytes (336 bits)
  Capture Length: 42 bytes (336 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:arp]
  [Coloring Rule Name: ARP]
  [Coloring Rule String: arp]
Ethernet II, Src: Vmware_9f:d1:d3 (00:50:56:9f:d1:d3), Dst: 50:01:00:05:00:00 (50:01:00:05:00:00)
Address Resolution Protocol (request)
```

172.16.14.53

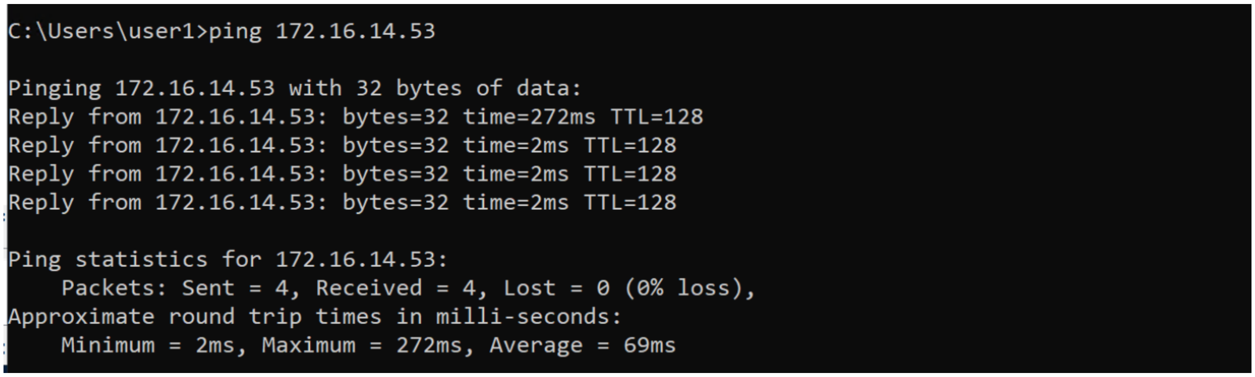
- Windows Server
- OS: Microsoft Windows 2016
- MAC address: 50:01:00:04:00:00 (Unknown)
- Open ports
  - 135/tcp open msrpc
  - 139/tcp open netbios-ssn
  - 445/tcp open microsoft-ds
  - 3389/tcp open ms-wbt-server

Nmap OS scan of 172.16.14.53 to find details of device attached to the address



```
C:\Users\user1>nmap -T4 -O 172.16.14.53
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:52 Eastern Daylight Time
Nmap scan report for 172.16.14.53
Host is up (0.010s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 50:01:00:04:00:00 (Unknown)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
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 4.51 seconds
```

Ping of 172.16.14.53

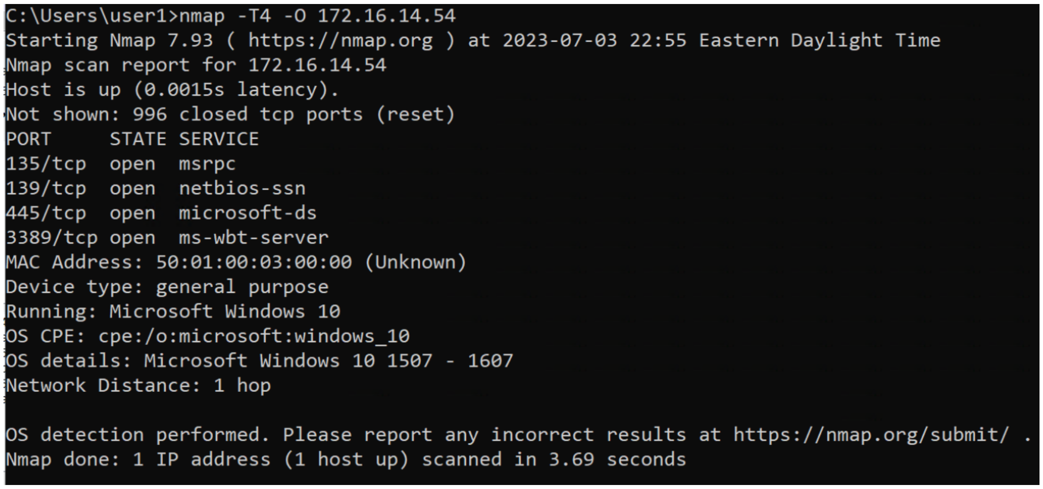


```
C:\Users\user1>ping 172.16.14.53

Pinging 172.16.14.53 with 32 bytes of data:
Reply from 172.16.14.53: bytes=32 time=272ms TTL=128
Reply from 172.16.14.53: bytes=32 time=2ms TTL=128
Reply from 172.16.14.53: bytes=32 time=2ms TTL=128
Reply from 172.16.14.53: bytes=32 time=2ms TTL=128

Ping statistics for 172.16.14.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 272ms, Average = 69ms
```

172.16.14.54

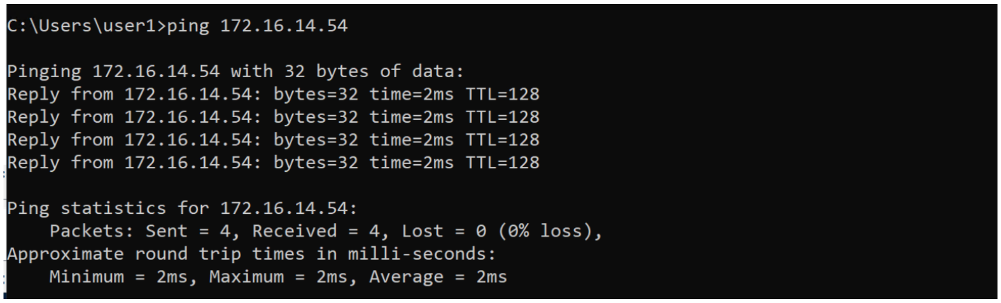
- Windows 2
- OS: Microsoft Windows 10
- MAC address: 50:01:00:03:00:00 (Unknown)
- Open ports
  - 135/tcp open msrpc
  - 139/tcp open netbios-ssn
  - 445/tcp open microsoft-ds
  - 3389/tcp open ms-wbt-server

Nmap OS scan of 172.16.14.54 to find details about corresponding device



```
C:\Users\user1>nmap -T4 -O 172.16.14.54
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:55 Eastern Daylight Time
Nmap scan report for 172.16.14.54
Host is up (0.0015s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 50:01:00:03:00:00 (Unknown)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 3.69 seconds
```

Ping of 172.16.14.54



```
C:\Users\user1>ping 172.16.14.54

Pinging 172.16.14.54 with 32 bytes of data:
Reply from 172.16.14.54: bytes=32 time=2ms TTL=128
Reply from 172.16.14.54: bytes=32 time=2ms TTL=128
Reply from 172.16.14.54: bytes=32 time=2ms TTL=128
Reply from 172.16.14.54: bytes=32 time=2ms TTL=128

Ping statistics for 172.16.14.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

References

AddressResolutionProtocol. (n.d.). Wireshark Wiki. Retrieved July 3, 2023, from https://wiki.wireshark.org/AddressResolutionProtocol

How to Check Kali Linux Version - javatpoint. (n.d.). Javatpoint. Retrieved July 3, 2023, from https://www.javatpoint.com/how-to-check-kali-linux-version

What version of Windows am I running? - Windows Client Management. (2023, April 21). Microsoft Learn. Retrieved July 3, 2023, from https://learn.microsoft.com/en-us/windows/client-management/client-tools/windows-version-search

Wireshark Labs - Jim Kurose Homepage. (n.d.). gaia. Retrieved July 3, 2023, from https://gaia.cs.umass.edu/kurose_ross/wireshark.php