Assessing the Network with Common Security Tools (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 01

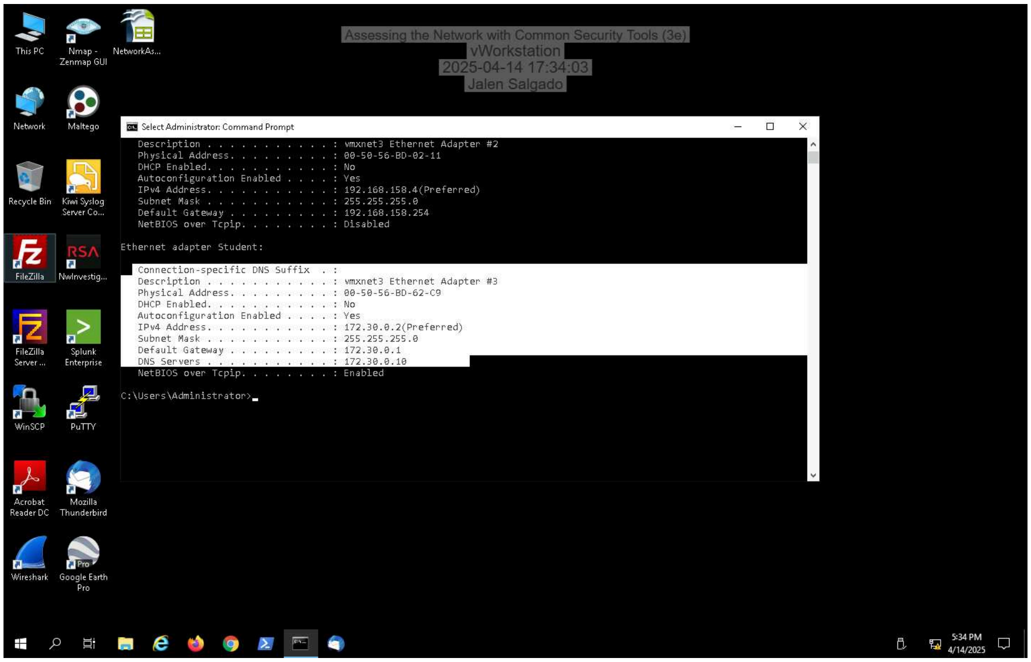
Student: Jalen Salgado	Email: jsalgado1915@gmail.com
Time on Task: 2 hours, 29 minutes	Progress: 72%

Report Generated: Saturday, July 26, 2025 at 2:10 PM

Section 1: Hands-On Demonstration

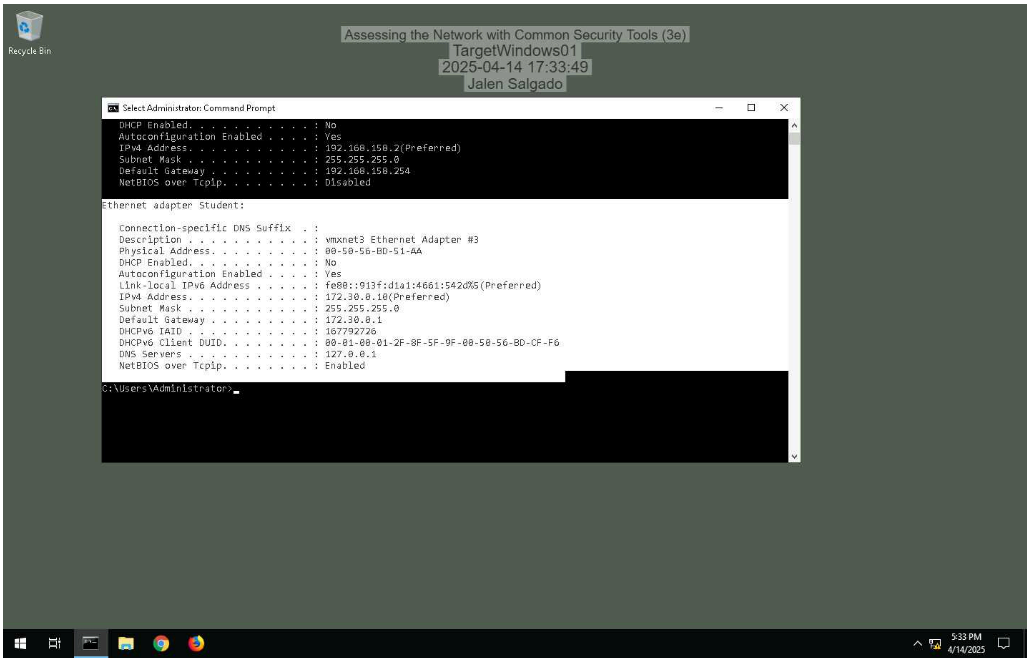
Part 1: Explore the Local Area Network

4. **Make a screen capture** showing the **ipconfig results for the Student adapter on the vWorkstation**.



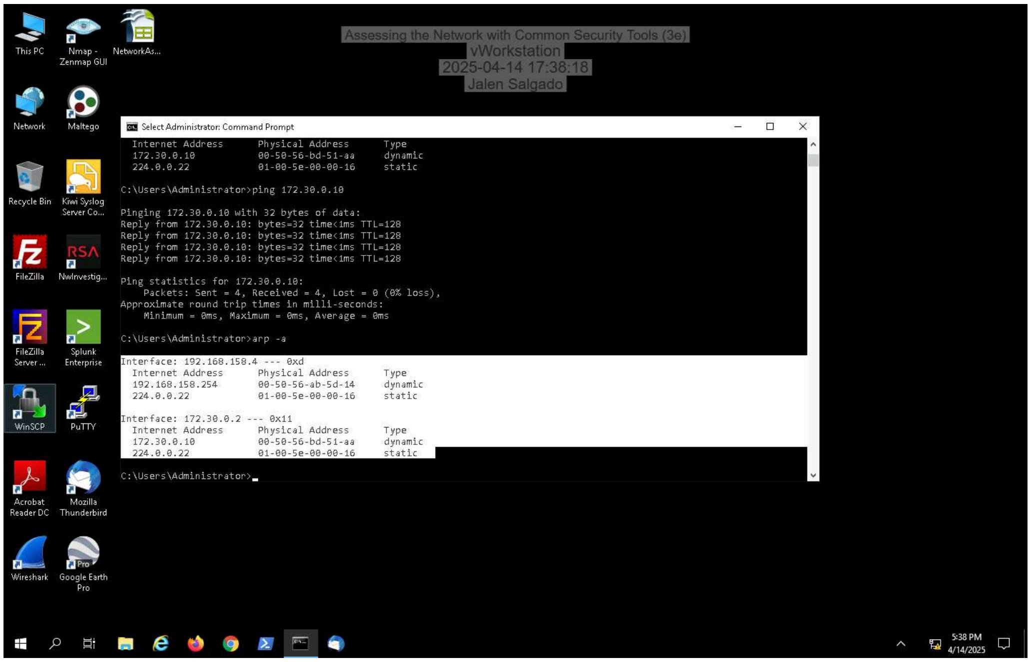
```
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-50-56-BD-02-11
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.158.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.158.254
   NetBIOS over Tcpip. . . . . . . . : Disabled

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-50-56-BD-62-C9
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.30.0.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1
   DNS Servers . . . . . . . . . . . : 172.30.0.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>_
```

7. **Make a screen capture** showing the **ipconfig results for the Student adapter on TargetWindows01**.


Recycle Bin
Assessing the Network with Common Security Tools (3e)
TargetWindows01
2025-04-14 17:33:49
Jalen Salgado
Select Administrator: Command Prompt
5:33 PM
4/14/2025

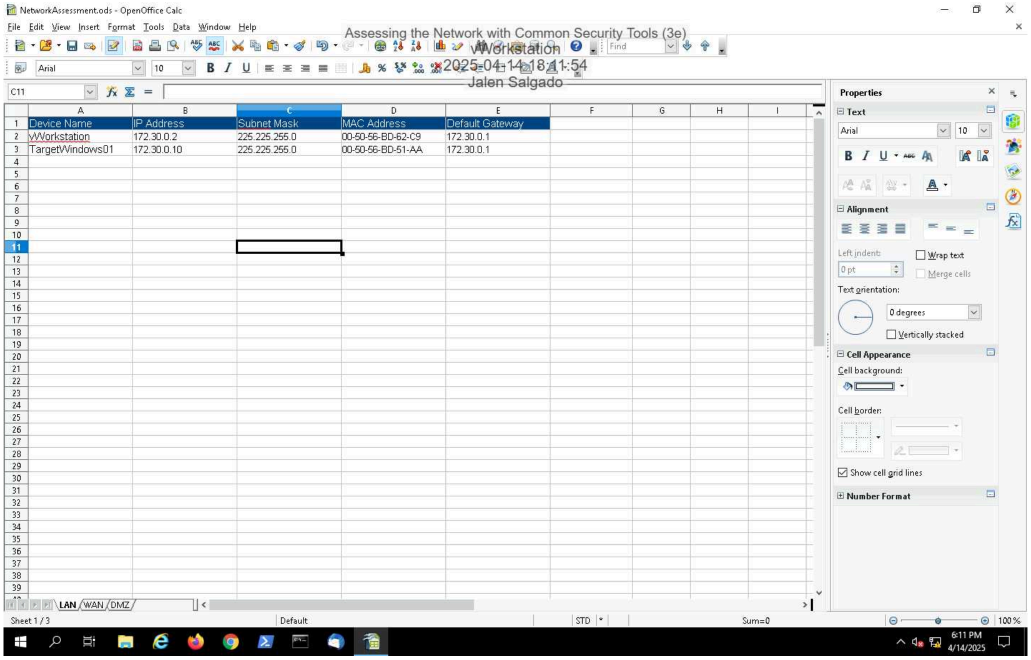
```
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.158.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.158.254
   NetBIOS over Tcpip. . . . . . . . : Disabled

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-50-56-BD-51-AA
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::913f:d1a1:4661:542d%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.30.0.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1
   DHCPv6 IAID . . . . . . . . . . . : 167792726
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-8F-5F-9F-00-50-56-BD-CF-F6
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>_
```

15. **Make a screen capture** showing the **updated ARP cache on the vWorkstation**.



```
  Internet Address      Physical Address      Type
  172.30.0.10           00-50-56-bd-51-aa     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>ping 172.30.0.10

Pinging 172.30.0.10 with 32 bytes of data:
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 172.30.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>arp -a

Interface: 192.168.158.4 --- 0xd
  Internet Address      Physical Address      Type
  192.168.158.254       00-50-56-ab-5d-14     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 172.30.0.2 --- 0x11
  Internet Address      Physical Address      Type
  172.30.0.10           00-50-56-bd-51-aa     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>_
```

19. **Make a screen capture** showing the **completed LAN tab of the Network Assessment spreadsheet**.



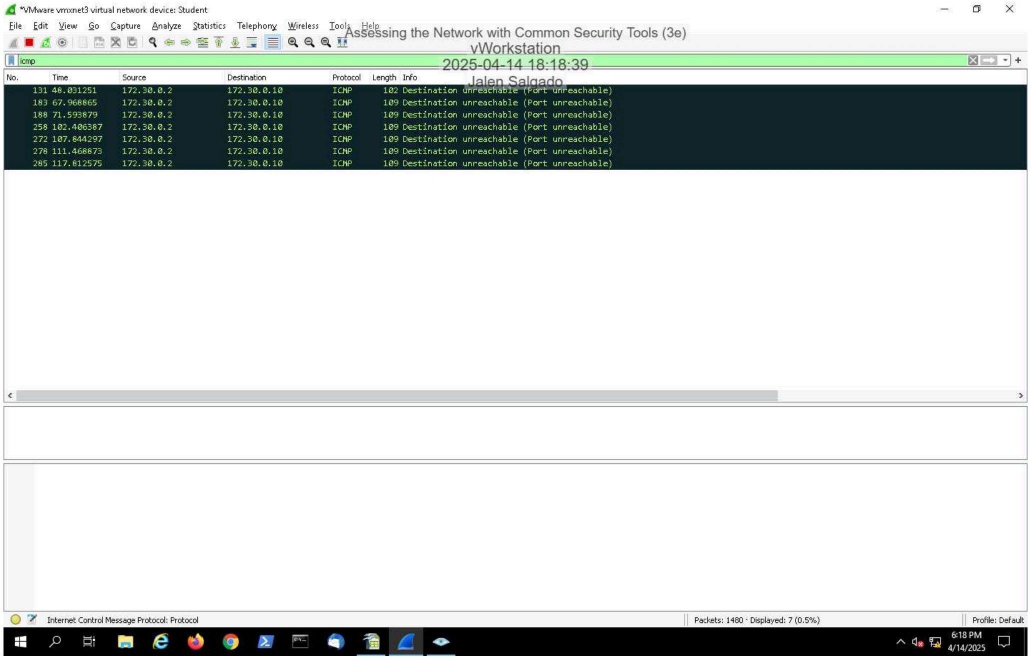
NetworkAssessment.ods - OpenOffice Calc

Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-04-14 18:11:54
Jalen Salgado

	A	B	C	D	E
1	Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
2	vWorkstation	172.30.0.2	225.225.255.0	00-50-56-BD-62-C9	172.30.0.1
3	TargetWindows01	172.30.0.10	225.225.255.0	00-50-56-BD-51-AA	172.30.0.1

Part 2: Analyze Network Traffic

9. **Make a screen capture** showing the **ICMP filtered results in Wireshark**.



*VMware vmxnet3 virtual network device: Student

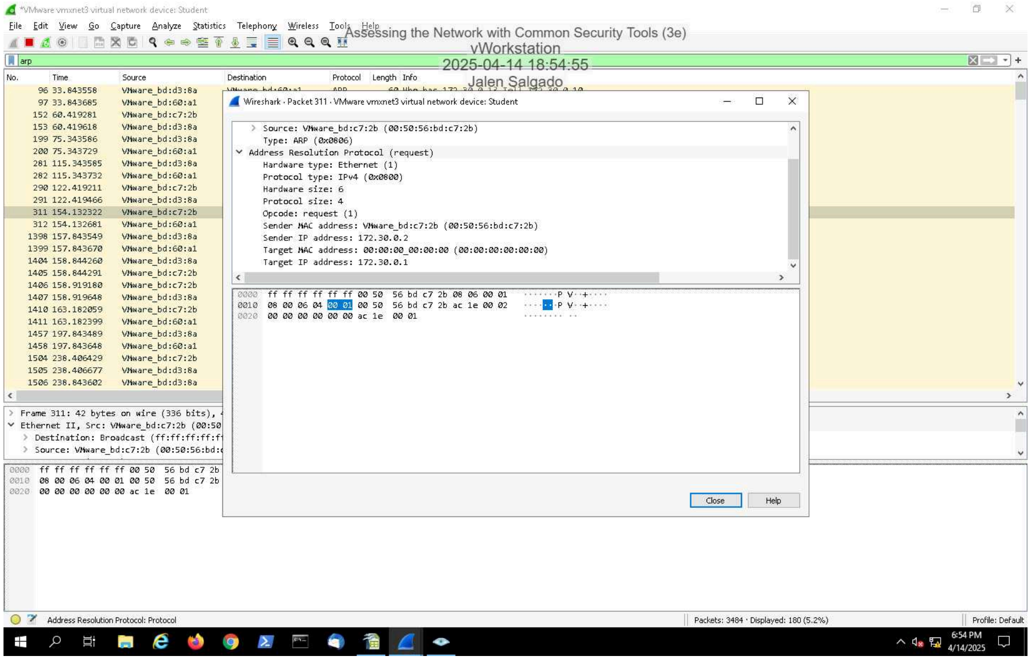
Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-04-14 18:18:39
Jalen Salgado

icmp

```
No.  Time        Source      Destination  Protocol  Length Info
 131 48.031251   172.30.0.2  172.30.0.10  ICMP      102 Destination unreachable (Port unreachable)
 183 67.968865   172.30.0.2  172.30.0.10  ICMP      109 Destination unreachable (Port unreachable)
 188 71.593879   172.30.0.2  172.30.0.10  ICMP      109 Destination unreachable (Port unreachable)
 258 102.406387  172.30.0.2  172.30.0.10  ICMP      109 Destination unreachable (Port unreachable)
 272 107.844297  172.30.0.2  172.30.0.10  ICMP      109 Destination unreachable (Port unreachable)
 278 111.468873  172.30.0.2  172.30.0.10  ICMP      109 Destination unreachable (Port unreachable)
 285 117.812575  172.30.0.2  172.30.0.10  ICMP      109 Destination unreachable (Port unreachable)
```

Internet Control Message Protocol: Protocol
Packets: 1480 · Displayed: 7 (0.5%)
Profile: Default

12. **Make a screen capture** showing the **ARP filtered results in Wireshark**.


*VMware vmxnet3 virtual network device: Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-04-14 18:54:55
Jalen Salgado
Wireshark · Packet 311 · VMware vmxnet3 virtual network device: Student
Close
Help
6:54 PM
4/14/2025

arp

```
No.   Time        Source
  96  33.843558   VMware_bd:d3:8a
  97  33.843685   VMware_bd:60:a1
 152  60.419281   VMware_bd:c7:2b
 153  60.419618   VMware_bd:d3:8a
 199  75.343586   VMware_bd:d3:8a
 200  75.343729   VMware_bd:60:a1
 281  115.343585  VMware_bd:d3:8a
 282  115.343732  VMware_bd:60:a1
 290  122.419211  VMware_bd:c7:2b
 291  122.419466  VMware_bd:d3:8a
 311  154.132322  VMware_bd:c7:2b
 312  154.132681  VMware_bd:60:a1
1398  157.843549  VMware_bd:d3:8a
1399  157.843670  VMware_bd:60:a1
1404  158.844260  VMware_bd:d3:8a
1405  158.844291  VMware_bd:c7:2b
1406  158.919180  VMware_bd:c7:2b
1407  158.919648  VMware_bd:d3:8a
1410  163.182059  VMware_bd:c7:2b
1411  163.182399  VMware_bd:60:a1
1457  197.843489  VMware_bd:d3:8a
1458  197.843648  VMware_bd:60:a1
1504  238.406429  VMware_bd:c7:2b
1505  238.406677  VMware_bd:d3:8a
1506  238.843602  VMware_bd:d3:8a
```

```
  > Source: VMware_bd:c7:2b (00:50:56:bd:c7:2b)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: VMware_bd:c7:2b (00:50:56:bd:c7:2b)
    Sender IP address: 172.30.0.2
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.30.0.1
```

```
0000  ff ff ff ff ff ff 00 50  56 bd c7 2b 08 06 00 01   ······P V··+····
0010  08 00 06 04 00 01 00 50  56 bd c7 2b ac 1e 00 02   ······P V··+····
0020  00 00 00 00 00 00 ac 1e  00 01                     ········ ··
```

```
> Frame 311: 42 bytes on wire (336 bits), 4
v Ethernet II, Src: VMware_bd:c7:2b (00:50
  > Destination: Broadcast (ff:ff:ff:ff:ff
  > Source: VMware_bd:c7:2b (00:50:56:bd:c
```

```
0000  ff ff ff ff ff ff 00 50  56 bd c7 2b
0010  08 00 06 04 00 01 00 50  56 bd c7 2b
0020  00 00 00 00 00 00 ac 1e  00 01
```

Address Resolution Protocol: Protocol | Packets: 3484 · Displayed: 180 (5.2%) | Profile: Default

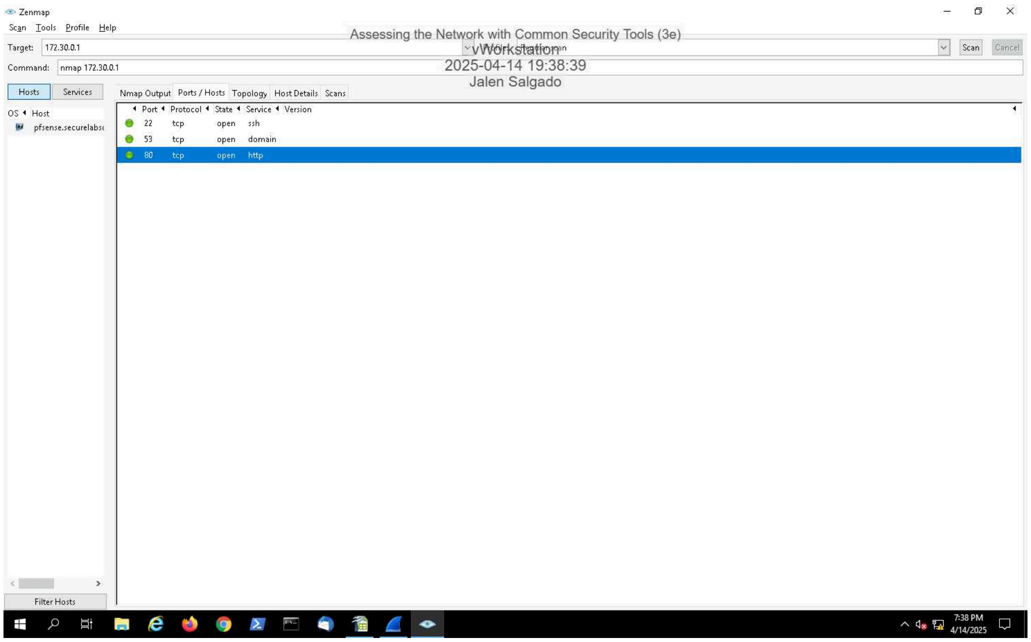
18. **Compare** the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

1 ARP reply and request from the target IP 1 ICMP Echo replyping scan was dozens of ARP requests with some replies and 70+ ECHO requests with a few replies

24. **Compare** the Intense scan results with the results from the Ping scan.

The intense scan generated 1 ARP request and 1 ARP reply from the target IP, along with 1 ICMP Echo Reply.
The ping scan resulted in dozens of ARP requests across the subnet with some ARP replies, and over 70 ICMP Echo Requests with a few Echo Replies.

28. **Make a screen capture** showing the **contents of the Ports/Hosts tab**.



Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-04-14 19:38:39
Jalen Salgado

Target: 172.30.0.1

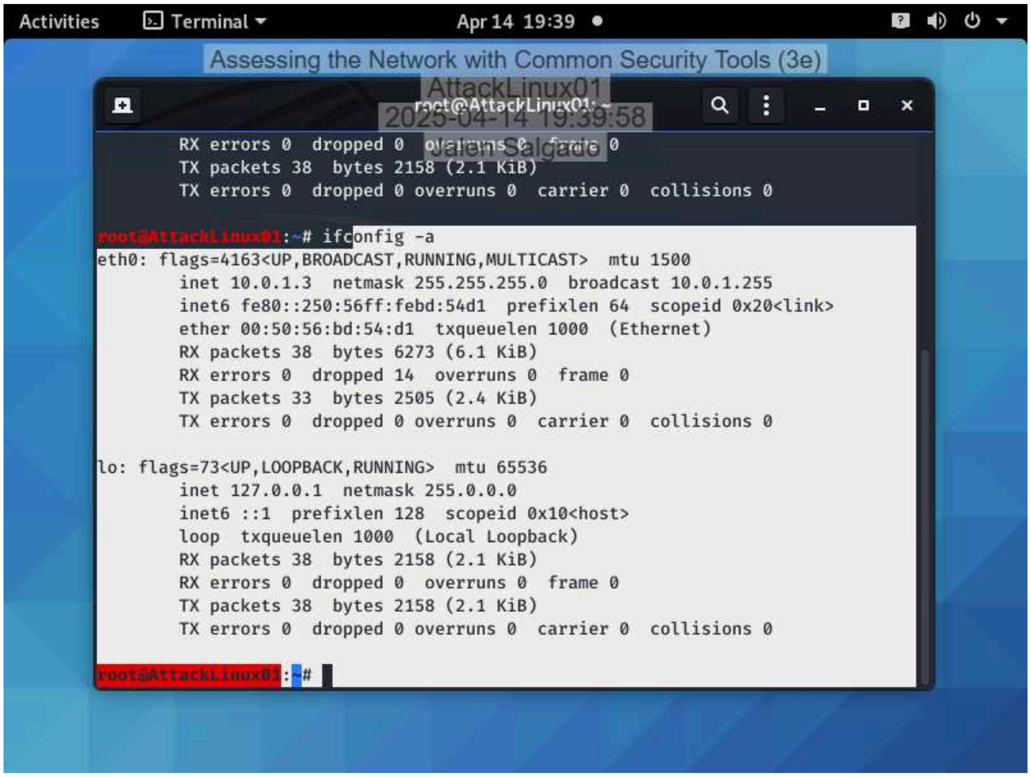
Command: nmap 172.30.0.1

```
Port  Protocol  State  Service  Version
22    tcp       open   ssh
53    tcp       open   domain
80    tcp       open   http
```

Section 2: Applied Learning

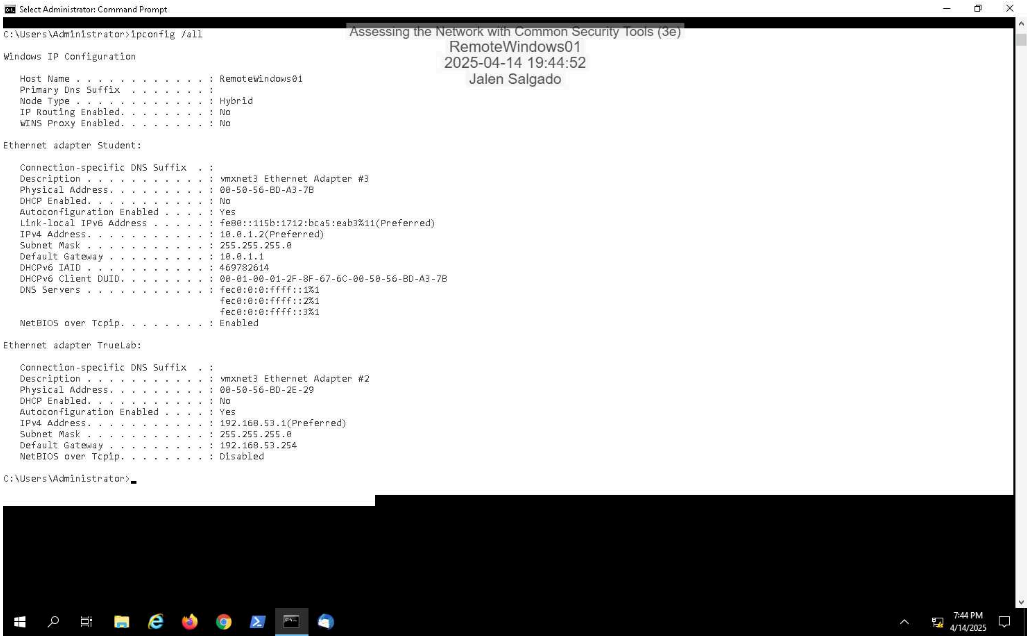
Part 1: Explore the Wide Area Network

6. **Make a screen capture** showing the **ifconfig results on AttackLinux01**.



```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38  bytes 2158 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@AttackLinux01:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.3  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::250:56ff:febd:54d1  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:bd:54:d1  txqueuelen 1000  (Ethernet)
        RX packets 38  bytes 6273 (6.1 KiB)
        RX errors 0  dropped 14  overruns 0  frame 0
        TX packets 33  bytes 2505 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 38  bytes 2158 (2.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38  bytes 2158 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@AttackLinux01:~# 
```

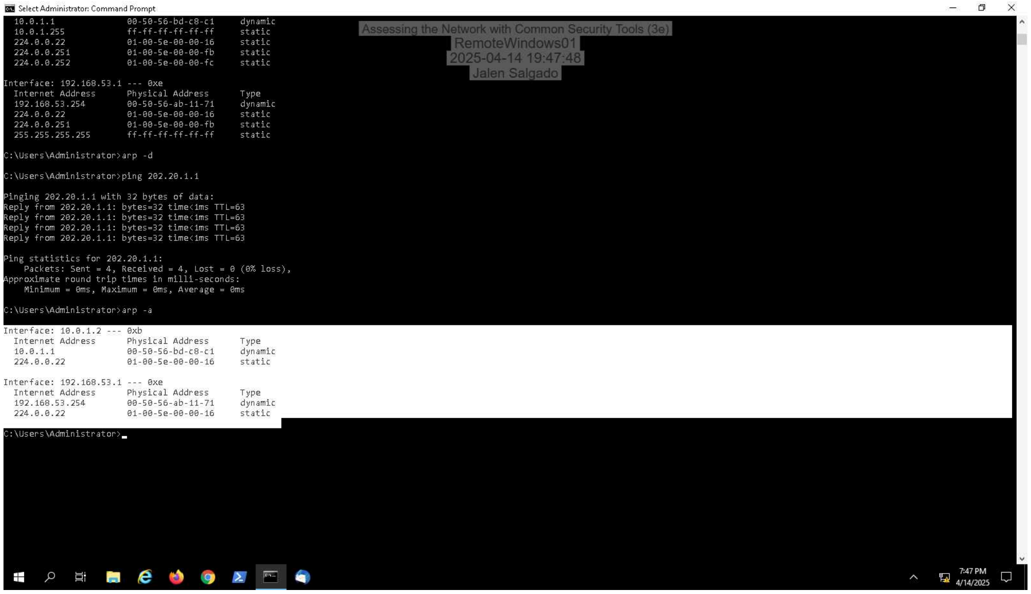
12. **Make a screen capture** showing the **ipconfig results on RemoteWindows01**.



Assessing the Network with Common Security Tools (3e)
RemoteWindows01
2025-04-14 19:44:52
Jalen Salgado

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : RemoteWindows01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-50-56-BD-A3-7B
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::115b:1712:bca5:eab3%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.1.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1
   DHCPv6 IAID . . . . . . . . . . . : 469782614
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-8F-67-6C-00-50-56-BD-A3-7B
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-50-56-BD-2E-29
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.53.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.53.254
   NetBIOS over Tcpip. . . . . . . . : Disabled

C:\Users\Administrator>
```

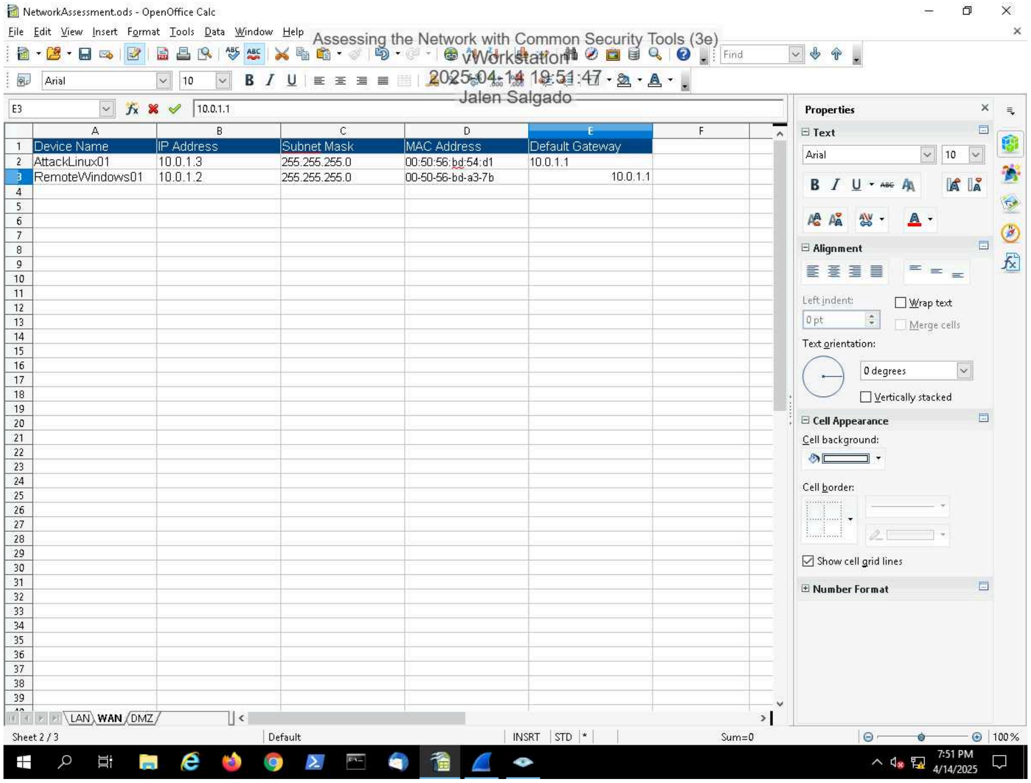
18. **Make a screen capture** showing the **updated ARP cache on RemoteWindows01**.



Assessing the Network with Common Security Tools (3e)
RemoteWindows01
2025-04-14 19:47:48
Jalen Salgado

```
  10.0.1.1              00-50-56-bd-c8-c1     dynamic
  10.0.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 192.168.53.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.53.254        00-50-56-ab-11-71     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>arp -d

C:\Users\Administrator>ping 202.20.1.1

Pinging 202.20.1.1 with 32 bytes of data:
Reply from 202.20.1.1: bytes=32 time<1ms TTL=63
Reply from 202.20.1.1: bytes=32 time<1ms TTL=63
Reply from 202.20.1.1: bytes=32 time<1ms TTL=63
Reply from 202.20.1.1: bytes=32 time<1ms TTL=63

Ping statistics for 202.20.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>arp -a

Interface: 10.0.1.2 --- 0xb
  Internet Address      Physical Address      Type
  10.0.1.1              00-50-56-bd-c8-c1     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.53.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.53.254        00-50-56-ab-11-71     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>
```

22. **Make a screen capture** showing the **completed WAN tab of the Network Assessment spreadsheet**.



NetworkAssessment.ods - OpenOffice Calc
File Edit View Insert Format Tools Data Window Help
Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-04-14 19:51:47
Jalen Salgado
E3
10.0.1.1
Properties
LAN WAN DMZ
Sheet 2 / 3
Default
Sum=0
100%
7:51 PM
4/14/2025

	A	B	C	D	E
1	Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
2	AttackLinux01	10.0.1.3	255.255.255.0	00:50:56:bd:54:d1	10.0.1.1
3	RemoteWindows01	10.0.1.2	255.255.255.0	00-50-56-bd-a3-7b	10.0.1.1

Part 2: Analyze Network Traffic

9. **Make a screen capture** showing **tcpdump echo back the captured packets**.

Incomplete

12. **Make a screen capture** showing the **attempted three-way handshake in tcpdump**.

Incomplete

17. **Make a screen capture** showing the **results of the get command**.

Incomplete

Section 3: Challenge and Analysis

Part 1: Explore the DMZ

Make a screen capture showing the **completed DMZ tab of the NetworkAssessment spreadsheet**.

Incomplete

Part 2: Perform Reconnaissance on the Firewall

Briefly summarize and analyze your findings in a technical memo to your boss.

Incomplete