Assessing the Network with Common Security Tools (3e)

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

Student:	Email:
Mani Sai Voore	mvoore@cbu.edu

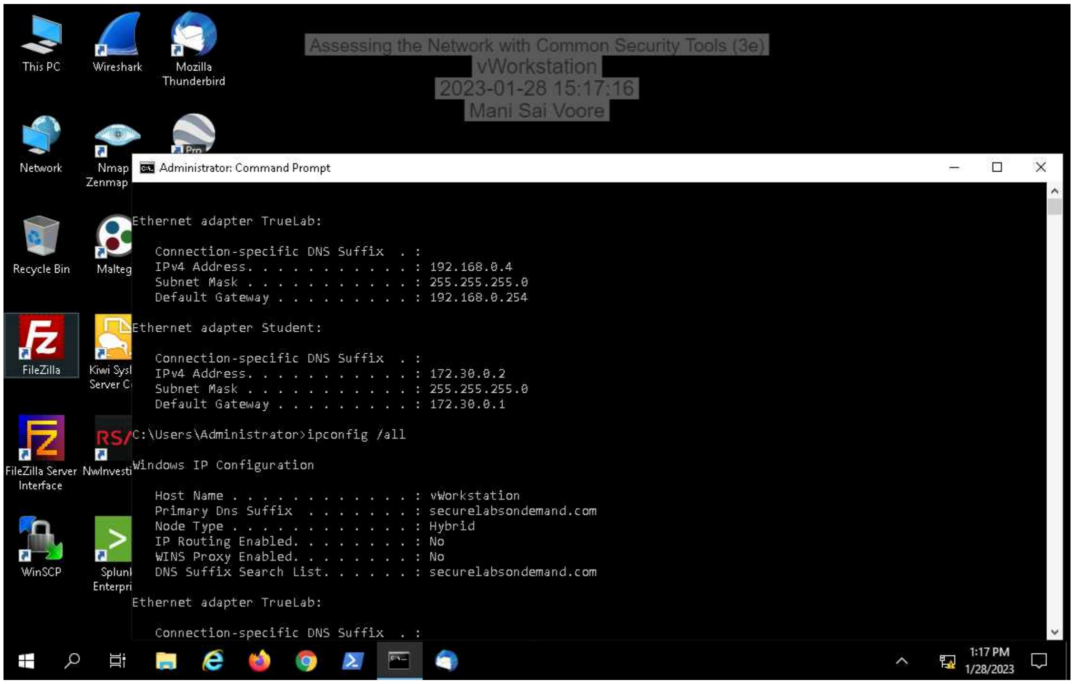
Time on Task:	Progress:
7 hours, 52 minutes	100%

Report Generated: Sunday, January 29, 2023 at 12:09 AM

Section 1: Hands-On Demonstration

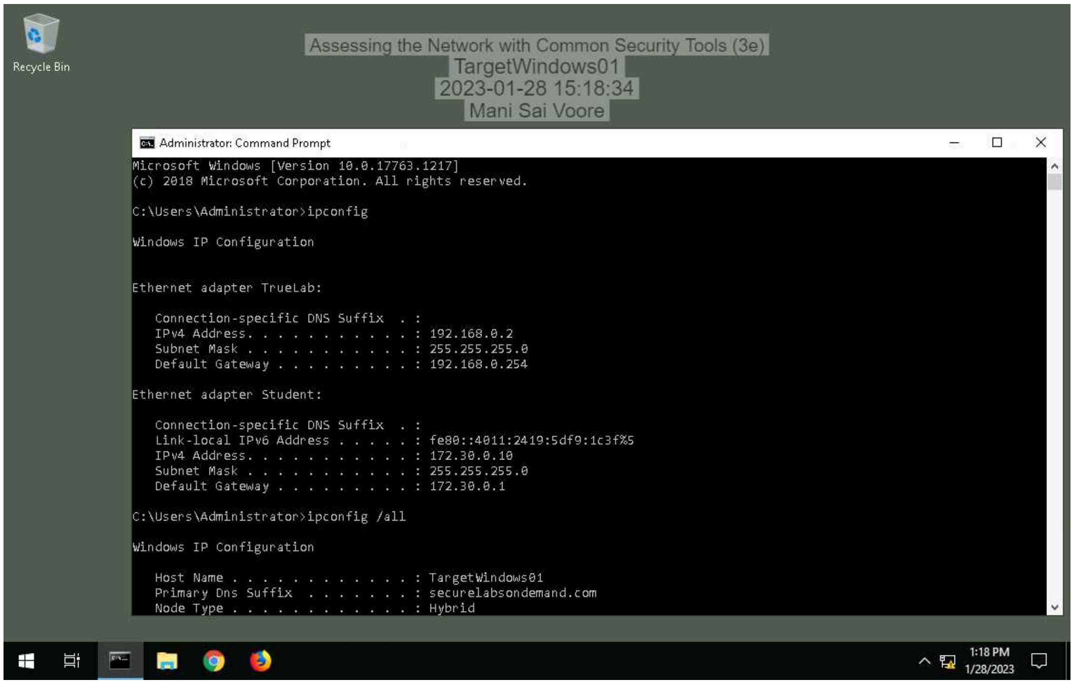
Part 1: Explore the Local Area Network

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



```
Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.254

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.30.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : vWorkstation
   Primary Dns Suffix  . . . . . . . : securelabsondemand.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : securelabsondemand.com

Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
```

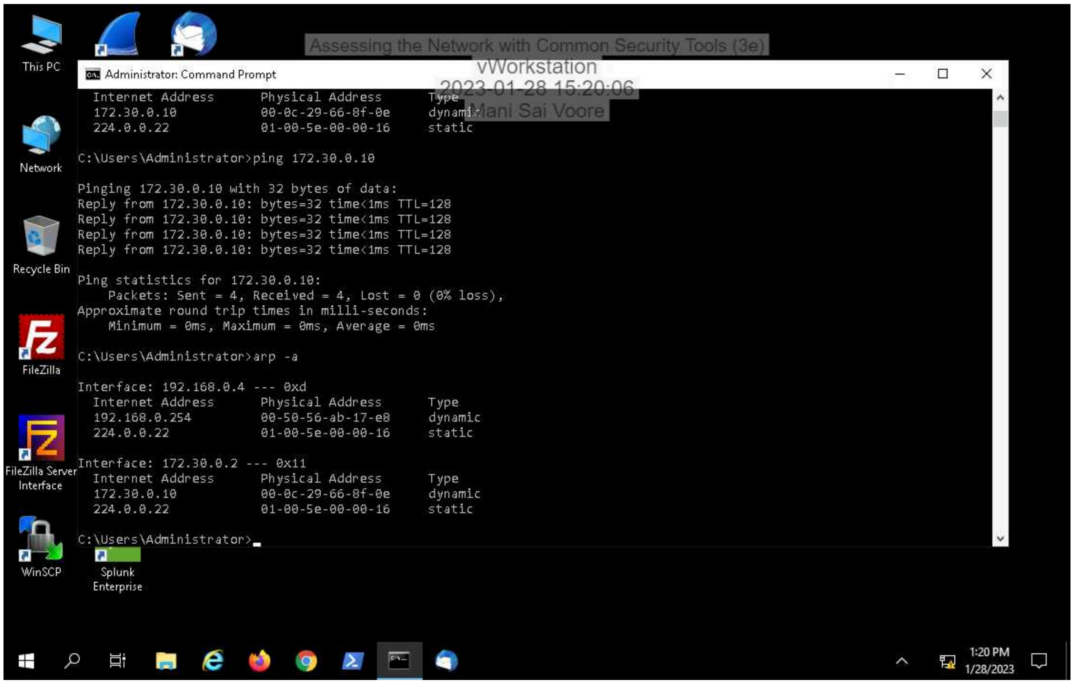
7. **Make a screen capture** showing the **ipconfig results for the Student adapter on TargetWindows01**.



Assessing the Network with Common Security Tools (3e)
TargetWindows01
2023-01-28 15:18:34
Mani Sai Voore

```
Microsoft Windows [Version 10.0.17763.1217]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.254

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4011:2419:5df9:1c3f%5
   IPv4 Address. . . . . . . . . . . : 172.30.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : TargetWindows01
   Primary Dns Suffix  . . . . . . . : securelabsondemand.com
   Node Type . . . . . . . . . . . . : Hybrid
```

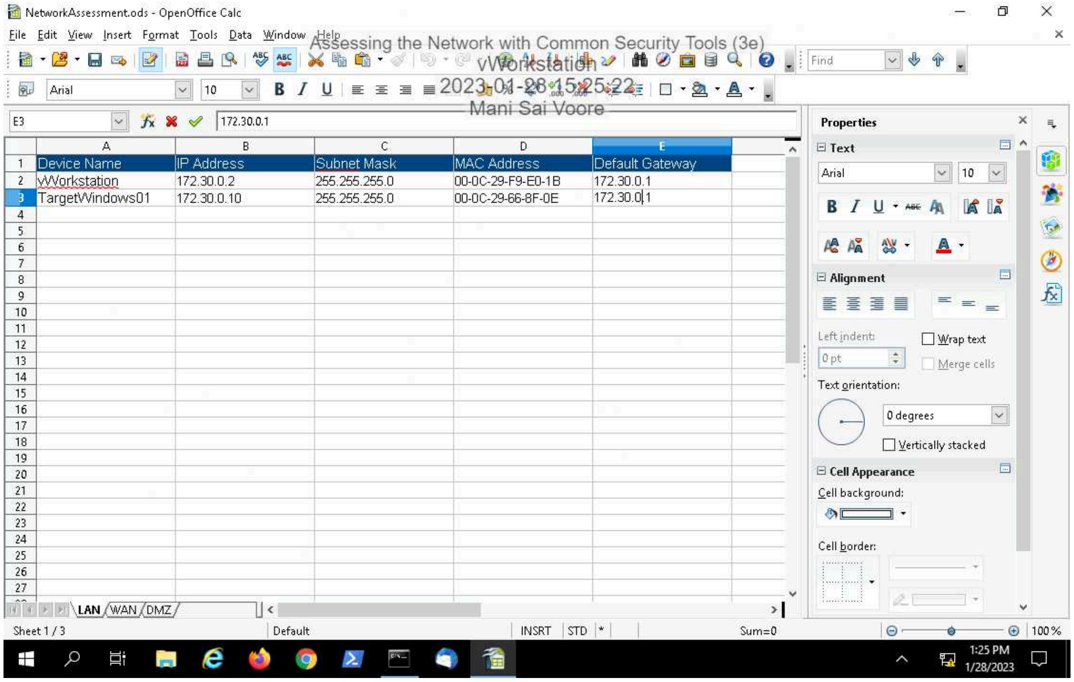
15. **Make a screen capture** showing the **updated ARP cache on the vWorkstation**.



Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-01-28 15:20:06
Mani Sai Voore

```
  Internet Address      Physical Address      Type
  172.30.0.10           00-0c-29-66-8f-0e     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: 192.168.0.4 --- 0xd
  Internet Address      Physical Address      Type
  192.168.0.254         00-50-56-ab-17-e8     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           00-0c-29-66-8f-0e     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

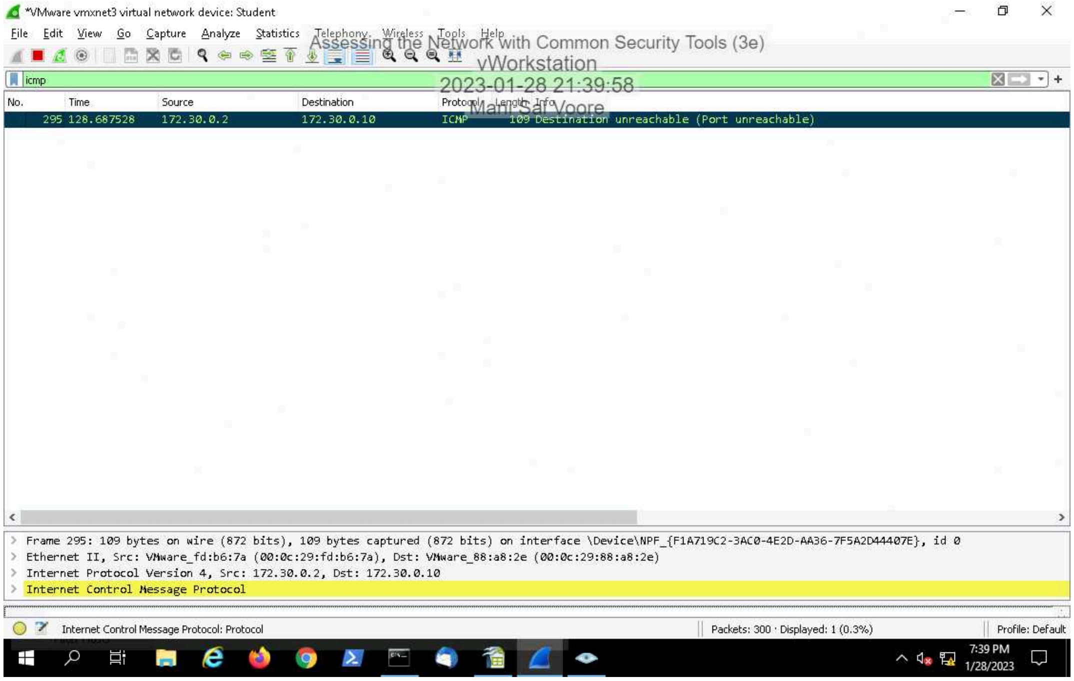
Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-01-28 15:25:22
Mani Sai Voore

E3 172.30.0.1

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
vWorkstation	172.30.0.2	255.255.255.0	00-0C-29-F9-E0-1B	172.30.0.1
TargetWindows01	172.30.0.10	255.255.255.0	00-0C-29-66-8F-0E	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
2023-01-28 21:39:58
Mani Sai Voore

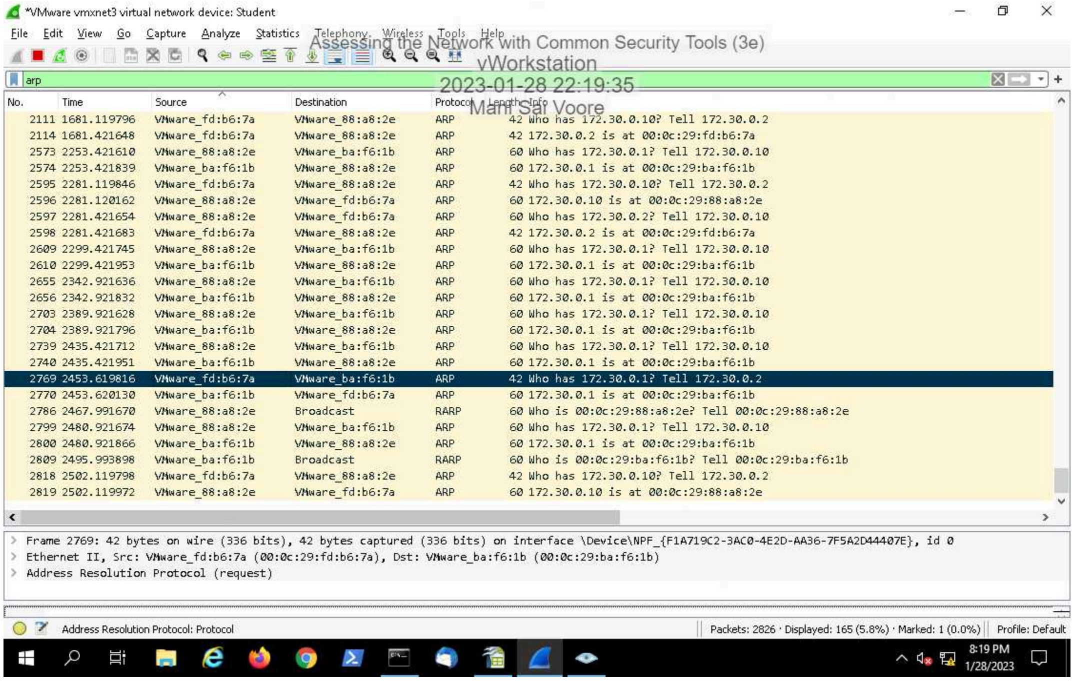
Filter: icmp

```
No.   Time        Source       Destination  Protocol Length Info
  295 128.687528  172.30.0.2   172.30.0.10  ICMP        109 Destination unreachable (Port unreachable)
```

```
> Frame 295: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface \Device\NPF_{F1A719C2-3AC0-4E2D-AA36-7F5A2D44407E}, id 0
> Ethernet II, Src: VMware_fd:b6:7a (00:0c:29:fd:b6:7a), Dst: VMware_88:a8:2e (00:0c:29:88:a8:2e)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.10
> Internet Control Message Protocol
```

Internet Control Message Protocol: Protocol | Packets: 300 · Displayed: 1 (0.3%) | 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
arp

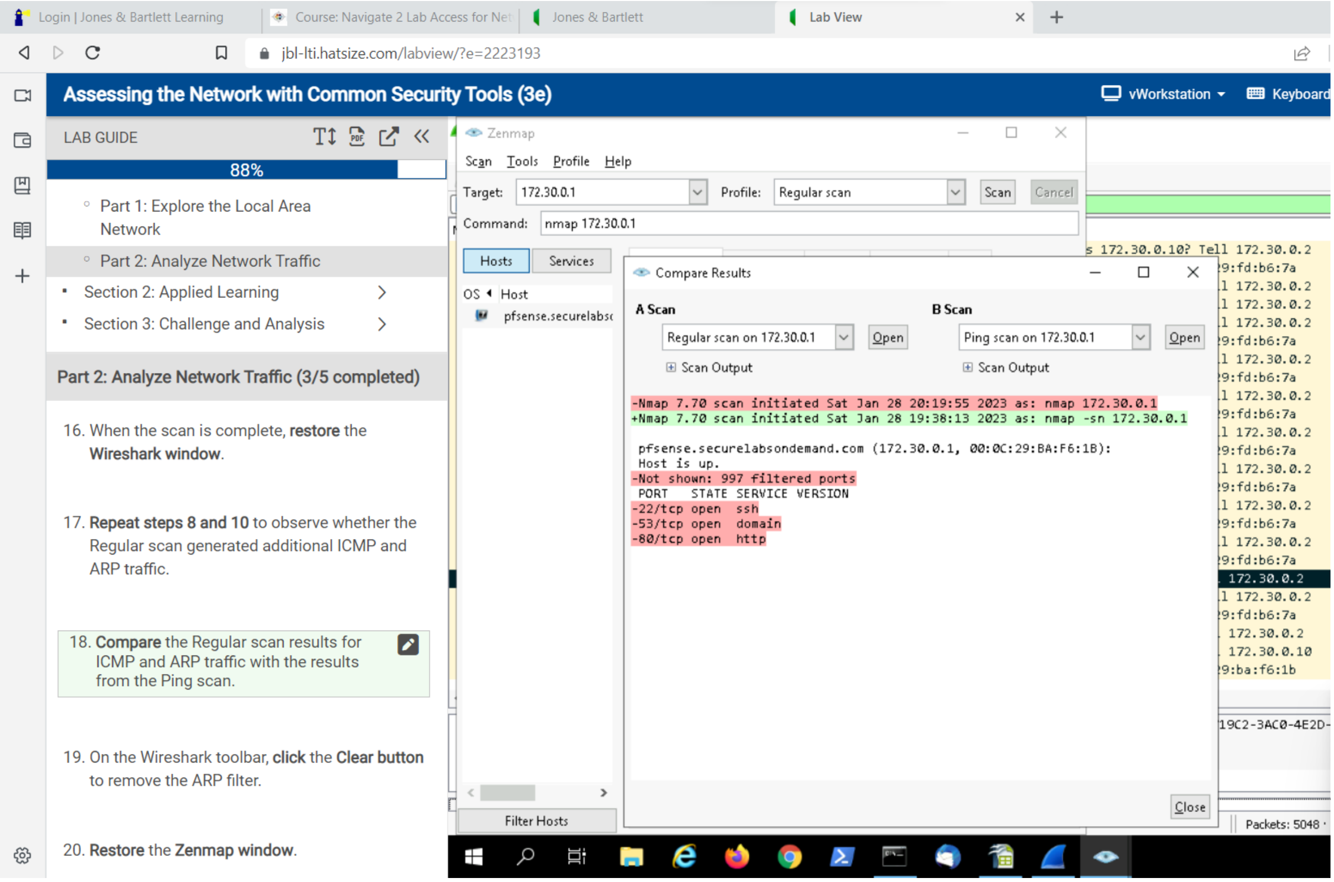
Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-01-28 22:19:35
Mani Sai Voore

```
No.   Time         Source             Destination        Protocol Length Info
 2111 1681.119796  VMware_fd:b6:7a    VMware_88:a8:2e    ARP      42 Who has 172.30.0.10? Tell 172.30.0.2
 2114 1681.421648  VMware_fd:b6:7a    VMware_88:a8:2e    ARP      42 172.30.0.2 is at 00:0c:29:fd:b6:7a
 2573 2253.421610  VMware_88:a8:2e    VMware_ba:f6:1b    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
 2574 2253.421839  VMware_ba:f6:1b    VMware_88:a8:2e    ARP      60 172.30.0.1 is at 00:0c:29:ba:f6:1b
 2595 2281.119846  VMware_fd:b6:7a    VMware_88:a8:2e    ARP      42 Who has 172.30.0.10? Tell 172.30.0.2
 2596 2281.120162  VMware_88:a8:2e    VMware_fd:b6:7a    ARP      60 172.30.0.10 is at 00:0c:29:88:a8:2e
 2597 2281.421654  VMware_88:a8:2e    VMware_fd:b6:7a    ARP      60 Who has 172.30.0.2? Tell 172.30.0.10
 2598 2281.421683  VMware_fd:b6:7a    VMware_88:a8:2e    ARP      42 172.30.0.2 is at 00:0c:29:fd:b6:7a
 2609 2299.421745  VMware_88:a8:2e    VMware_ba:f6:1b    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
 2610 2299.421953  VMware_ba:f6:1b    VMware_88:a8:2e    ARP      60 172.30.0.1 is at 00:0c:29:ba:f6:1b
 2655 2342.921636  VMware_88:a8:2e    VMware_ba:f6:1b    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
 2656 2342.921832  VMware_ba:f6:1b    VMware_88:a8:2e    ARP      60 172.30.0.1 is at 00:0c:29:ba:f6:1b
 2703 2389.921628  VMware_88:a8:2e    VMware_ba:f6:1b    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
 2704 2389.921796  VMware_ba:f6:1b    VMware_88:a8:2e    ARP      60 172.30.0.1 is at 00:0c:29:ba:f6:1b
 2739 2435.421712  VMware_88:a8:2e    VMware_ba:f6:1b    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
 2740 2435.421951  VMware_ba:f6:1b    VMware_88:a8:2e    ARP      60 172.30.0.1 is at 00:0c:29:ba:f6:1b
 2769 2453.619816  VMware_fd:b6:7a    VMware_ba:f6:1b    ARP      42 Who has 172.30.0.1? Tell 172.30.0.2
 2770 2453.620130  VMware_ba:f6:1b    VMware_fd:b6:7a    ARP      60 172.30.0.1 is at 00:0c:29:ba:f6:1b
 2786 2467.991670  VMware_88:a8:2e    Broadcast          RARP     60 Who is 00:0c:29:88:a8:2e? Tell 00:0c:29:88:a8:2e
 2799 2480.921674  VMware_88:a8:2e    VMware_ba:f6:1b    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
 2800 2480.921866  VMware_ba:f6:1b    VMware_88:a8:2e    ARP      60 172.30.0.1 is at 00:0c:29:ba:f6:1b
 2809 2495.993898  VMware_ba:f6:1b    Broadcast          RARP     60 Who is 00:0c:29:ba:f6:1b? Tell 00:0c:29:ba:f6:1b
 2818 2502.119798  VMware_fd:b6:7a    VMware_88:a8:2e    ARP      42 Who has 172.30.0.10? Tell 172.30.0.2
 2819 2502.119972  VMware_88:a8:2e    VMware_fd:b6:7a    ARP      60 172.30.0.10 is at 00:0c:29:88:a8:2e
```

```
> Frame 2769: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F1A719C2-3AC0-4E2D-AA36-7F5A2D44407E}, id 0
> Ethernet II, Src: VMware_fd:b6:7a (00:0c:29:fd:b6:7a), Dst: VMware_ba:f6:1b (00:0c:29:ba:f6:1b)
> Address Resolution Protocol (request)
```

Address Resolution Protocol: Protocol | Packets: 2826 · Displayed: 165 (5.8%) · Marked: 1 (0.0%) | Profile: Default

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


Login | Jones & Bartlett Learning
Course: Navigate 2 Lab Access for Net
Jones & Bartlett
Lab View
jbl-lti.hatsize.com/labview/?e=2223193
Assessing the Network with Common Security Tools (3e)
vWorkstation
Keyboard
LAB GUIDE
88%
Part 1: Explore the Local Area Network
Part 2: Analyze Network Traffic
Section 2: Applied Learning
Section 3: Challenge and Analysis
Zenmap
Scan Tools Profile Help
Scan
Cancel
Hosts
Services
OS Host
pfsense.securelabsc
Filter Hosts
Compare Results
A Scan
B Scan
Open
Scan Output
Close
Packets: 5048

Part 2: Analyze Network Traffic (3/5 completed)

16. When the scan is complete, **restore** the **Wireshark window**.

17. **Repeat steps 8 and 10** to observe whether the Regular scan generated additional ICMP and ARP traffic.

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

19. On the Wireshark toolbar, **click** the **Clear button** to remove the ARP filter.

20. **Restore** the **Zenmap window**.

Target: 172.30.0.1 Profile: Regular scan

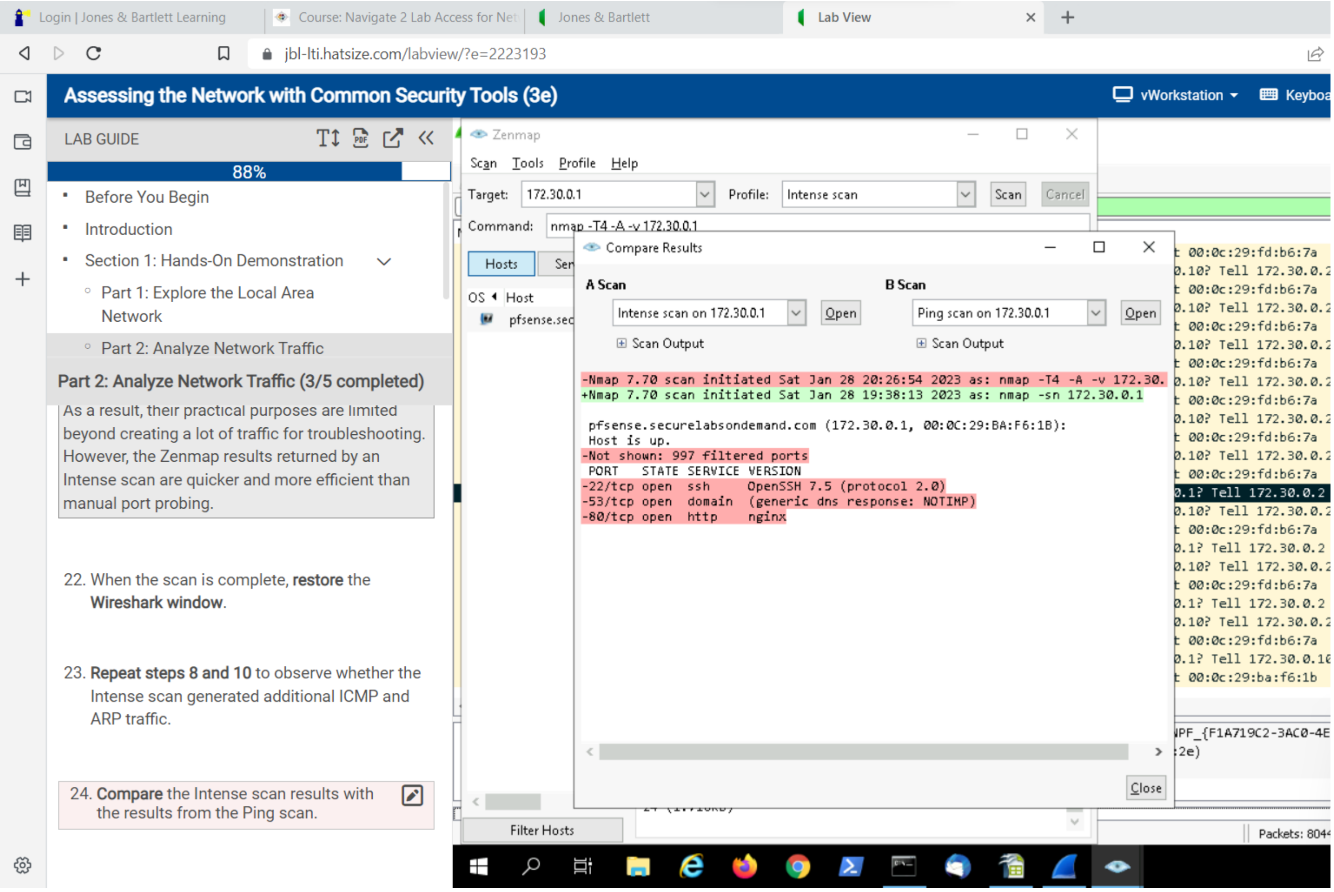
Command: nmap 172.30.0.1

A Scan: Regular scan on 172.30.0.1

B Scan: Ping scan on 172.30.0.1

```
-Nmap 7.70 scan initiated Sat Jan 28 20:19:55 2023 as: nmap 172.30.0.1
+Nmap 7.70 scan initiated Sat Jan 28 19:38:13 2023 as: nmap -sn 172.30.0.1

 pfsense.securelabsondemand.com (172.30.0.1, 00:0C:29:BA:F6:1B):
 Host is up.
-Not shown: 997 filtered ports
 PORT   STATE SERVICE VERSION
-22/tcp open  ssh
-53/tcp open  domain
-80/tcp open  http
```

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



Login | Jones & Bartlett Learning
Course: Navigate 2 Lab Access for Net
Jones & Bartlett
Lab View
jbl-lti.hatsize.com/labview/?e=2223193
Assessing the Network with Common Security Tools (3e)
vWorkstation
LAB GUIDE
88%
Before You Begin
Introduction
Section 1: Hands-On Demonstration
Part 1: Explore the Local Area Network
Part 2: Analyze Network Traffic
Part 2: Analyze Network Traffic (3/5 completed)
Zenmap
Scan Tools Profile Help
Compare Results
Close
Filter Hosts

As a result, their practical purposes are limited beyond creating a lot of traffic for troubleshooting. However, the Zenmap results returned by an Intense scan are quicker and more efficient than manual port probing.

22. When the scan is complete, **restore** the **Wireshark window**.

23. **Repeat steps 8 and 10** to observe whether the Intense scan generated additional ICMP and ARP traffic.

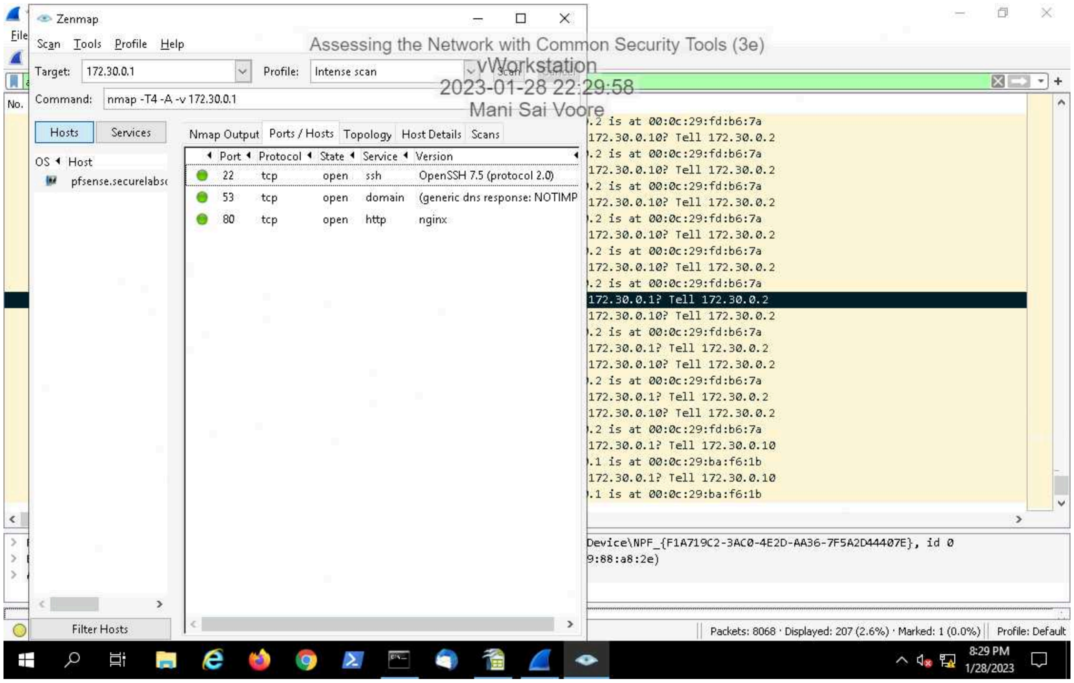
24. **Compare** the Intense scan results with the results from the Ping scan.

Target: 172.30.0.1
Profile: Intense scan
Command: nmap -T4 -A -v 172.30.0.1

A Scan: Intense scan on 172.30.0.1
B Scan: Ping scan on 172.30.0.1

```
-Nmap 7.70 scan initiated Sat Jan 28 20:26:54 2023 as: nmap -T4 -A -v 172.30.
+Nmap 7.70 scan initiated Sat Jan 28 19:38:13 2023 as: nmap -sn 172.30.0.1

 pfsense.securelabsondemand.com (172.30.0.1, 00:0C:29:BA:F6:1B):
 Host is up.
-Not shown: 997 filtered ports
 PORT   STATE SERVICE VERSION
-22/tcp open  ssh     OpenSSH 7.5 (protocol 2.0)
-53/tcp open  domain  (generic dns response: NOTIMP)
-80/tcp open  http    nginx
```

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



Target: 172.30.0.1
Profile: Intense scan
Command: nmap -T4 -A -v 172.30.0.1

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 7.5 (protocol 2.0)
53	tcp	open	domain	(generic dns response: NOTIMP
80	tcp	open	http	nginx

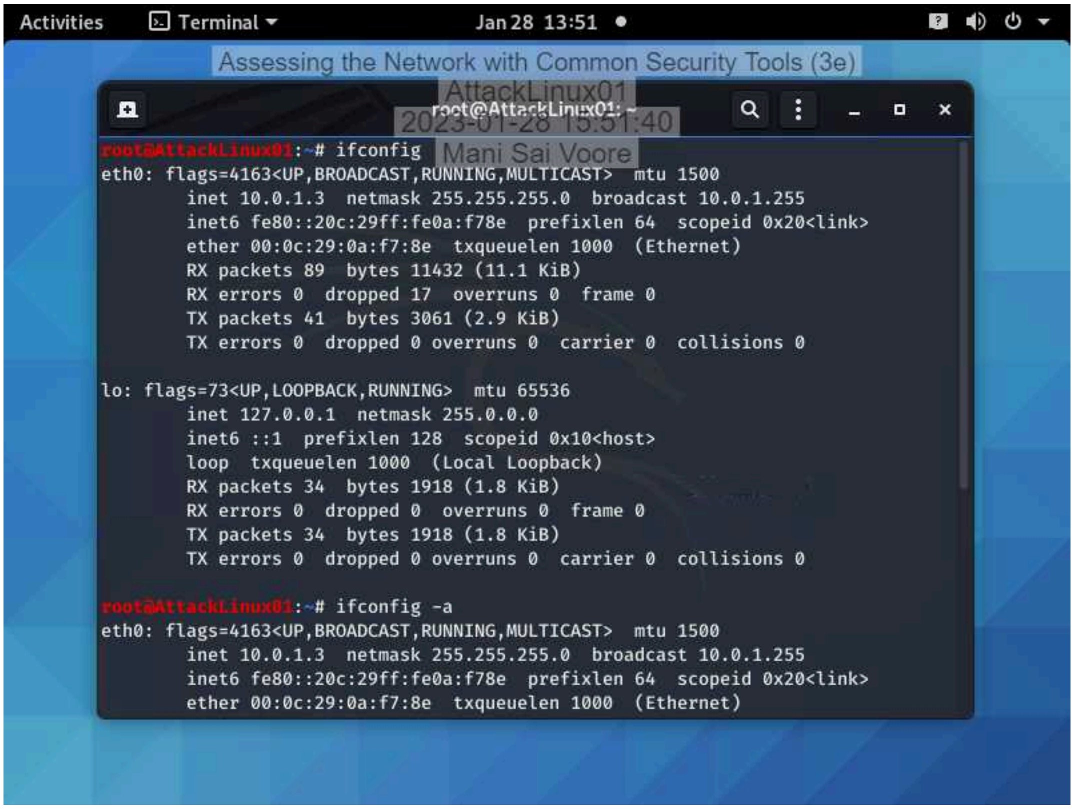
```
Device\NPF_{F1A719C2-3AC0-4E2D-AA36-7F5A2D44407E}, id 0
9:88:a8:2e)
```

Packets: 8068 · Displayed: 207 (2.6%) · Marked: 1 (0.0%) | Profile: Default

Section 2: Applied Learning

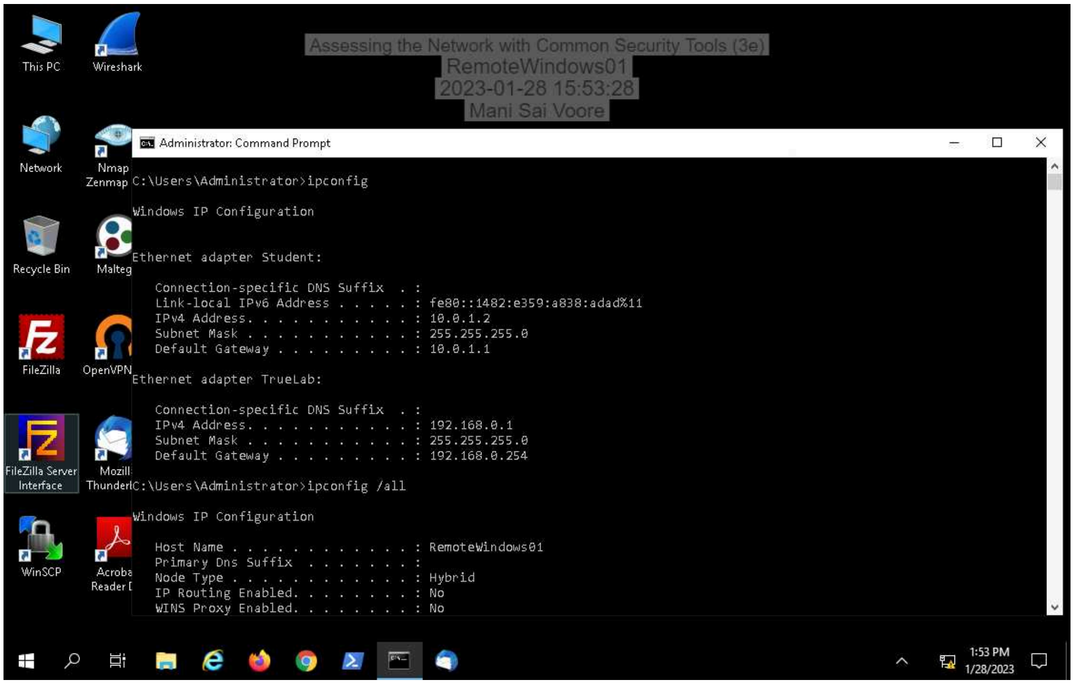
Part 1: Explore the Wide Area Network

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



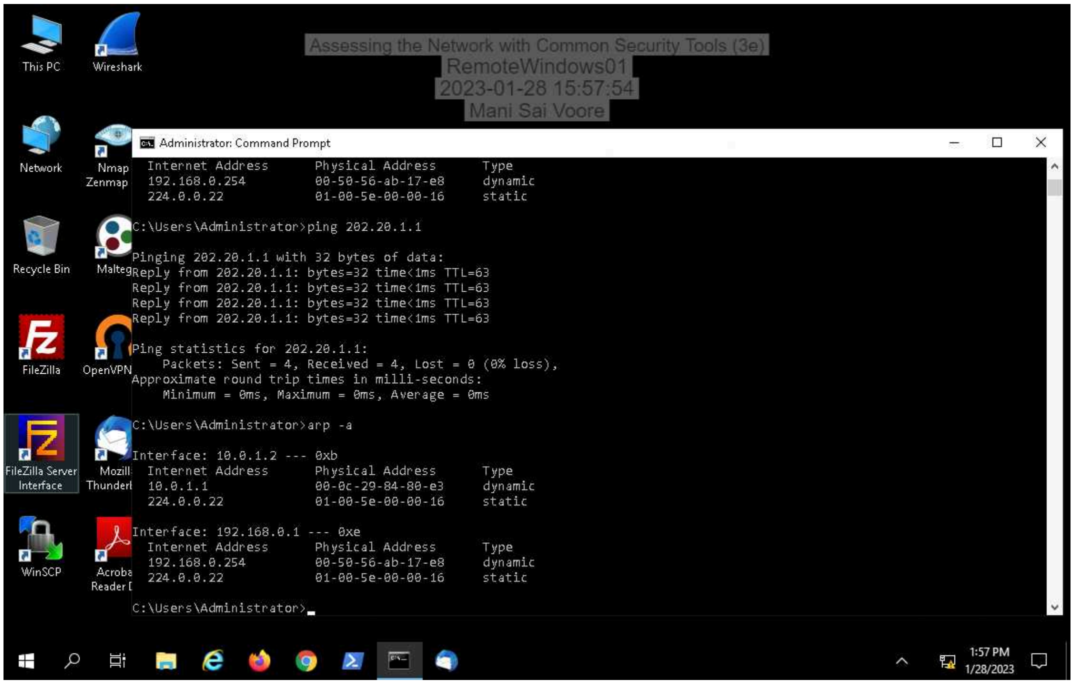
```
root@AttackLinux01:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.3  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::20c:29ff:fe0a:f78e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0a:f7:8e  txqueuelen 1000  (Ethernet)
        RX packets 89  bytes 11432 (11.1 KiB)
        RX errors 0  dropped 17  overruns 0  frame 0
        TX packets 41  bytes 3061 (2.9 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 34  bytes 1918 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 1918 (1.8 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::20c:29ff:fe0a:f78e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0a:f7:8e  txqueuelen 1000  (Ethernet)
```

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



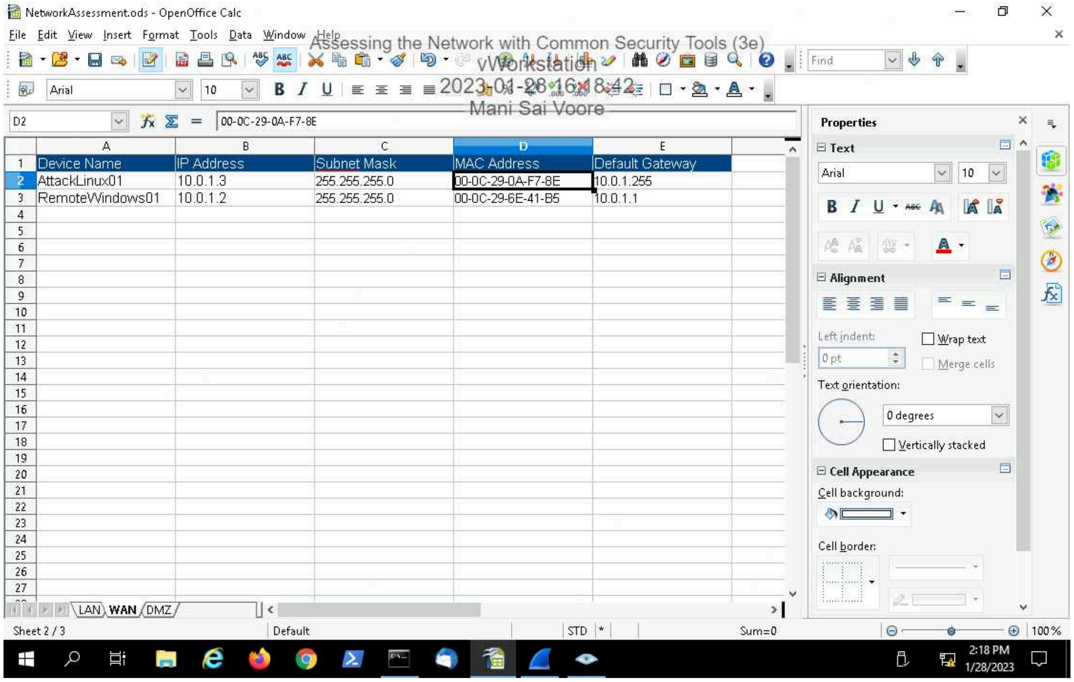
```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1482:e359:a838:adad%11
   IPv4 Address. . . . . . . . . . . : 10.0.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1
Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.254
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
```

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



```
  Internet Address      Physical Address      Type
  192.168.0.254         00-50-56-ab-17-e8     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

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              00-0c-29-84-80-e3     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.0.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.254         00-50-56-ab-17-e8     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**.



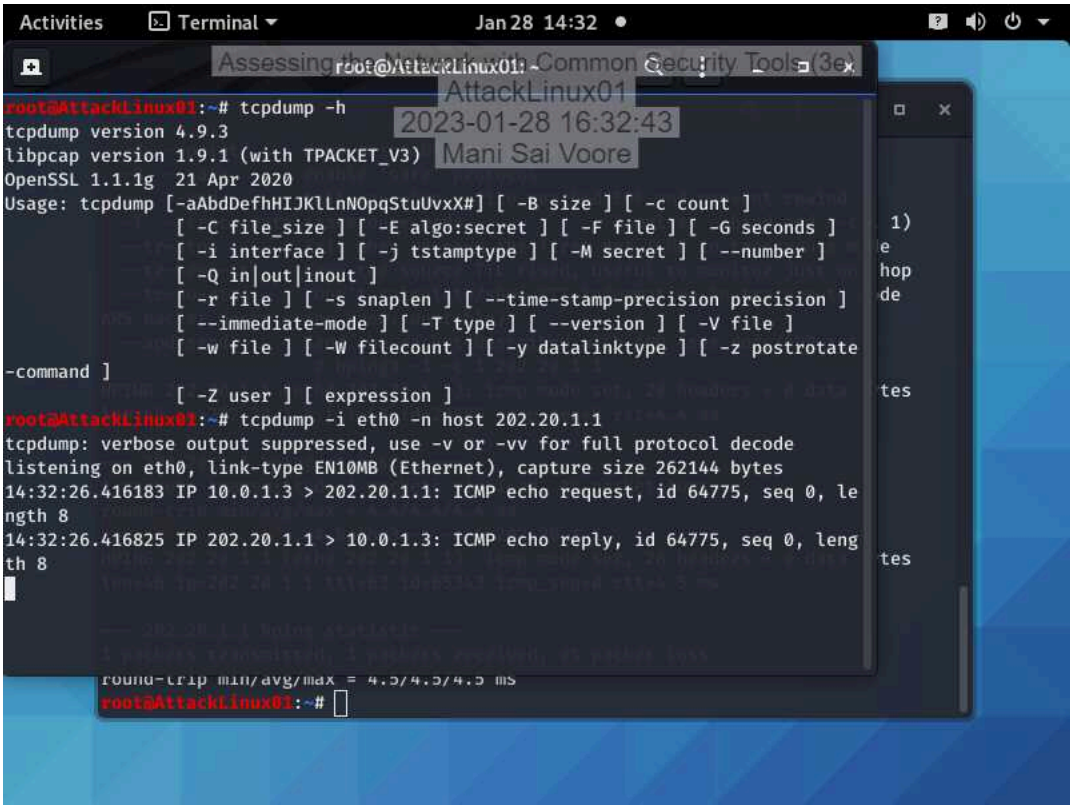
NetworkAssessment.ods - OpenOffice Calc

D2 = 00-0C-29-0A-F7-8E

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
AttackLinux01	10.0.1.3	255.255.255.0	00-0C-29-0A-F7-8E	10.0.1.255
RemoteWindows01	10.0.1.2	255.255.255.0	00-0C-29-6E-41-B5	10.0.1.1

Part 2: Analyze Network Traffic

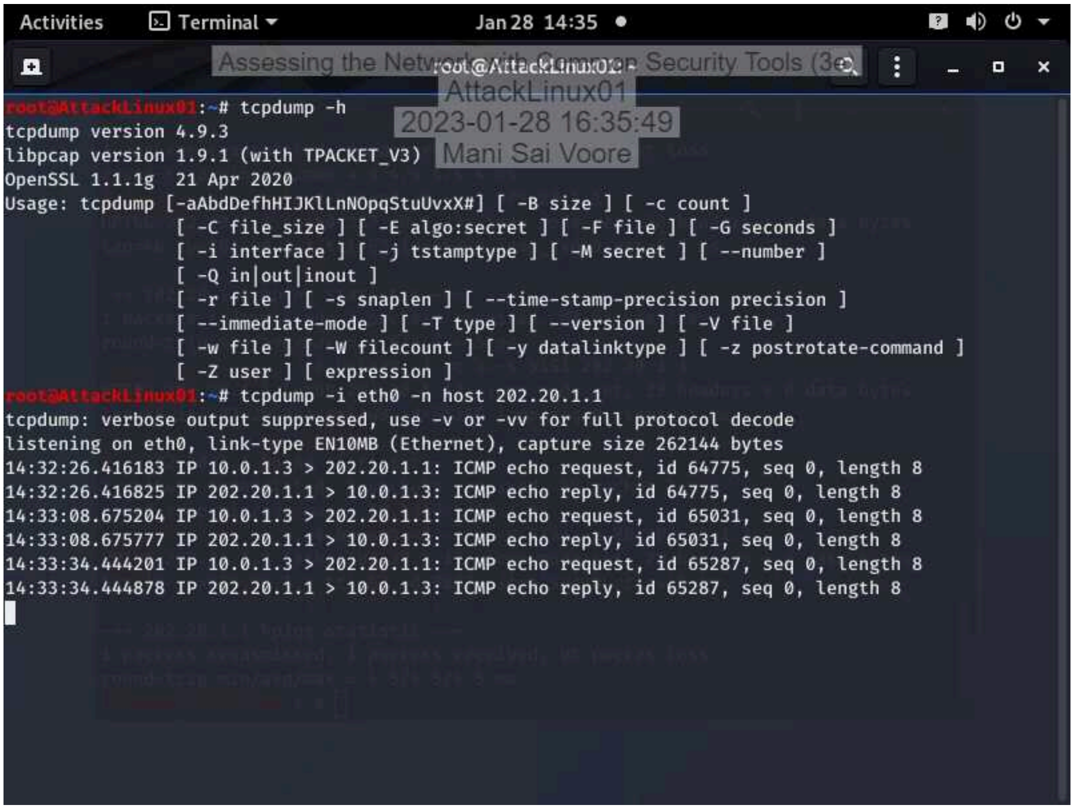
9. **Make a screen capture** showing **tcpdump echo back the captured packets**.



```
root@AttackLinux01:~# tcpdump -h
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1g  21 Apr 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate
-command ]
                [ -Z user ] [ expression ]
root@AttackLinux01:~# tcpdump -i eth0 -n host 202.20.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:32:26.416183 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 64775, seq 0, le
ngth 8
14:32:26.416825 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 64775, seq 0, leng
th 8
```

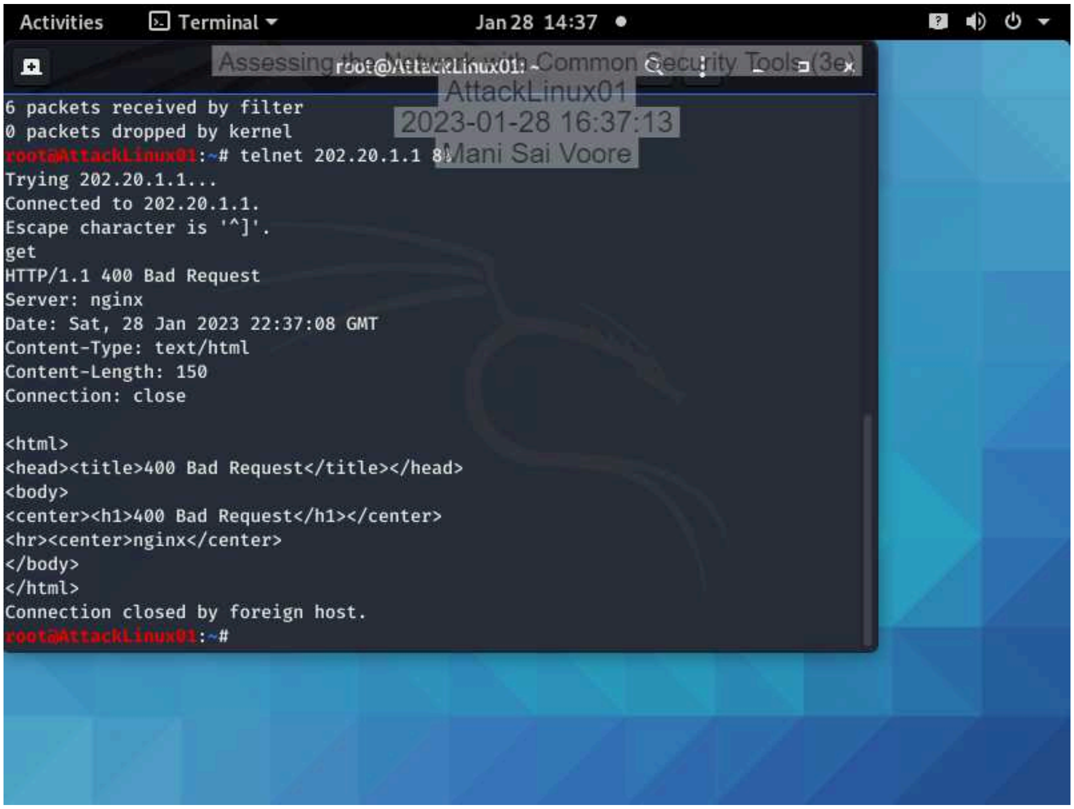
```
round-trip min/avg/max = 4.5/4.5/4.5 ms
root@AttackLinux01:~# 
```

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



```
root@AttackLinux01:~# tcpdump -h
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1g  21 Apr 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
root@AttackLinux01:~# tcpdump -i eth0 -n host 202.20.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:32:26.416183 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 64775, seq 0, length 8
14:32:26.416825 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 64775, seq 0, length 8
14:33:08.675204 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 65031, seq 0, length 8
14:33:08.675777 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 65031, seq 0, length 8
14:33:34.444201 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 65287, seq 0, length 8
14:33:34.444878 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 65287, seq 0, length 8
```

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

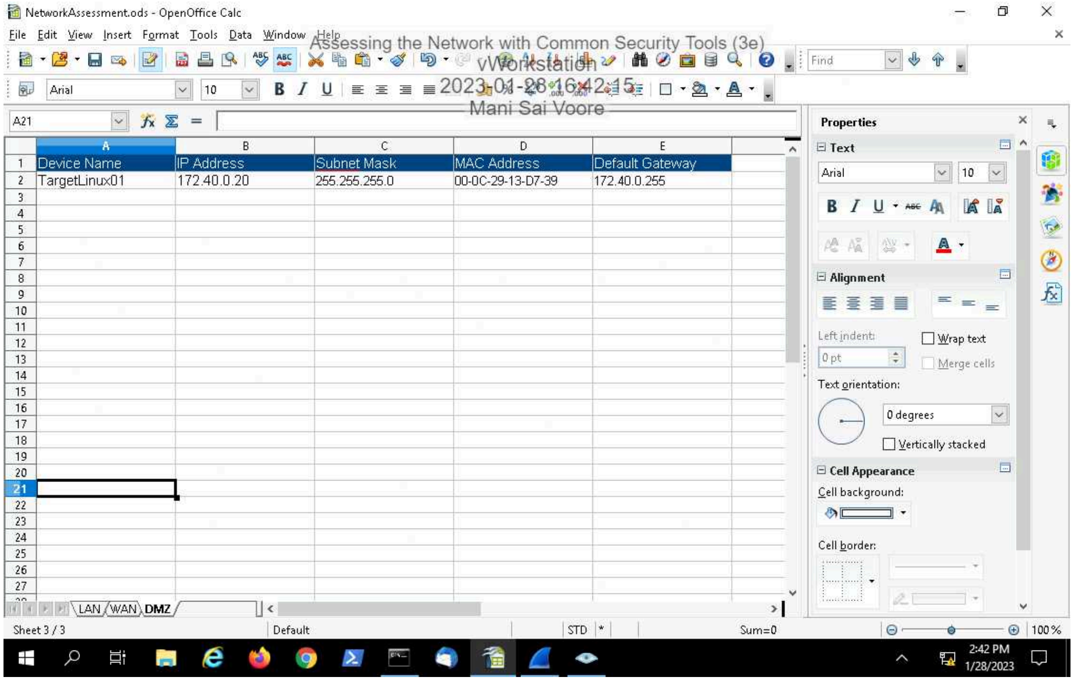


```
6 packets received by filter
0 packets dropped by kernel
root@AttackLinux01:~# telnet 202.20.1.1 80
Trying 202.20.1.1...
Connected to 202.20.1.1.
Escape character is '^]'.
get
HTTP/1.1 400 Bad Request
Server: nginx
Date: Sat, 28 Jan 2023 22:37:08 GMT
Content-Type: text/html
Content-Length: 150
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
Connection closed by foreign host.
root@AttackLinux01:~#
```

Section 3: Challenge and Analysis

Part 1: Explore the DMZ

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



NetworkAssessment.ods - OpenOffice Calc

Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-01-28 16:42:15
Mani Sai Voore

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
TargetLinux01	172.40.0.20	255.255.255.0	00-0C-29-13-D7-39	172.40.0.255

Part 2: Perform Reconnaissance on the Firewall

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

1. ICMP echo request and reply packets were received by the firewall with the identification number , sequence number 0 and 27910 length 8 in the lab for ICMP packets towards firewall.

2. In ARP packets towards the firewall, ARP packets were received for the IP address 10.0.1.3.5151 with a source port of 80 and a destination IP of 202.20.1.1, which included the flags, sequence number 1827888039, window size 512, and length 0. Apparently, an ARP packet was also received from 202.20.1.1 with a source port 80, destination IP of 10.0.1.3.5151, flags, sequence number 1018804028, ack no1827888040, and window size 165228.

3.No DNS (Domain Name System)

4. 80 and 22 ports are opened and running in the fire wall server.