

Student:	Email:
Brayden Mitchell	brayden.m.mitchell@gmail.com

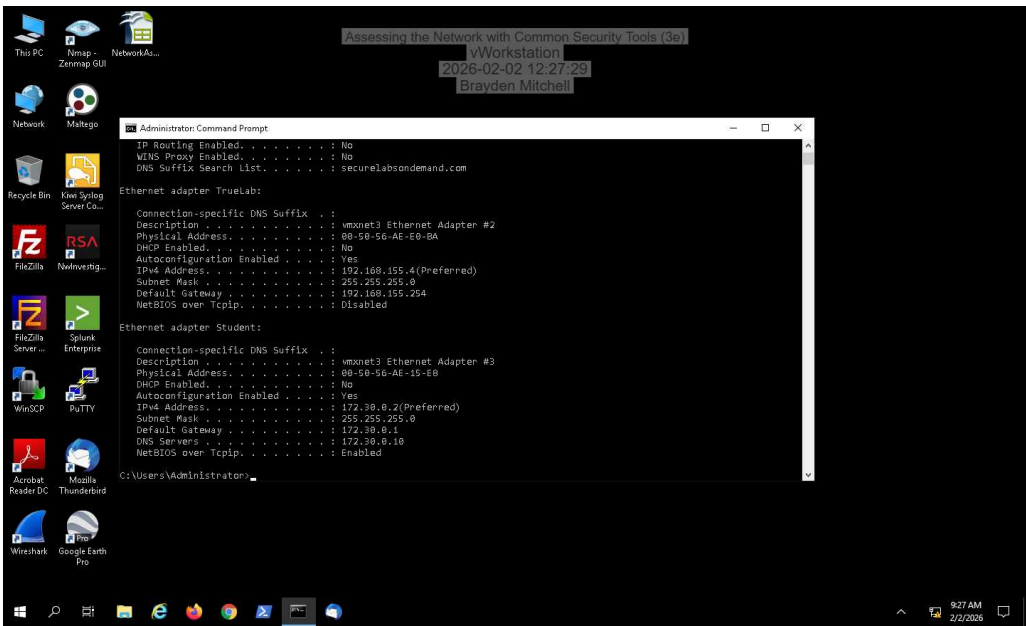
Time on Task:	Progress:
1 hour, 52 minutes	100%

Report Generated: Monday, February 2, 2026 at 2:15 PM

Section 1: Hands-On Demonstration

Part 1: Explore the Local Area Network

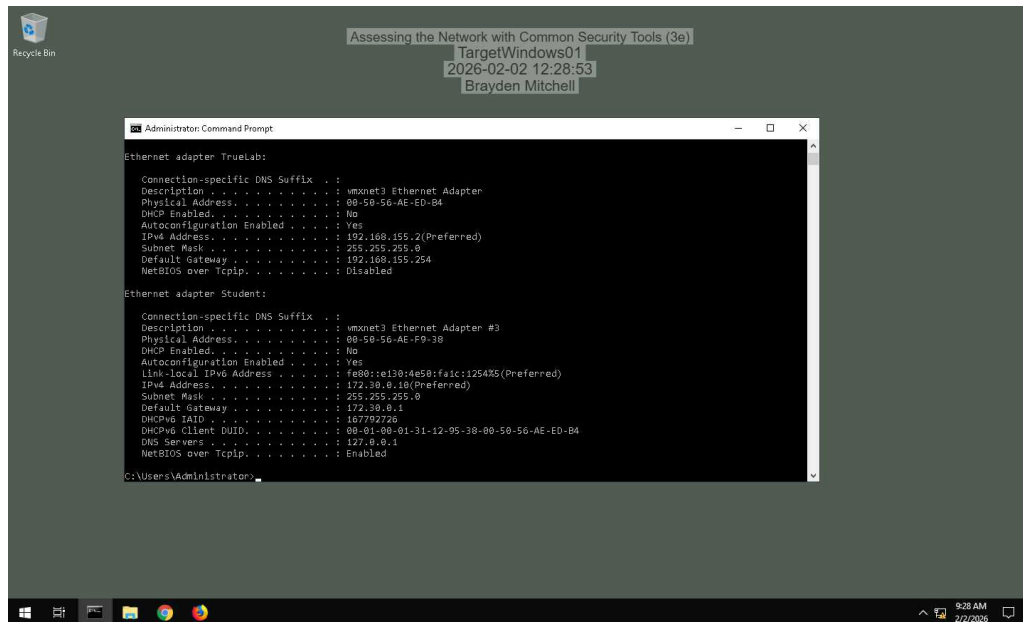
4. Make a screen capture showing the ipconfig results for the Student adapter on the vWorkstation.



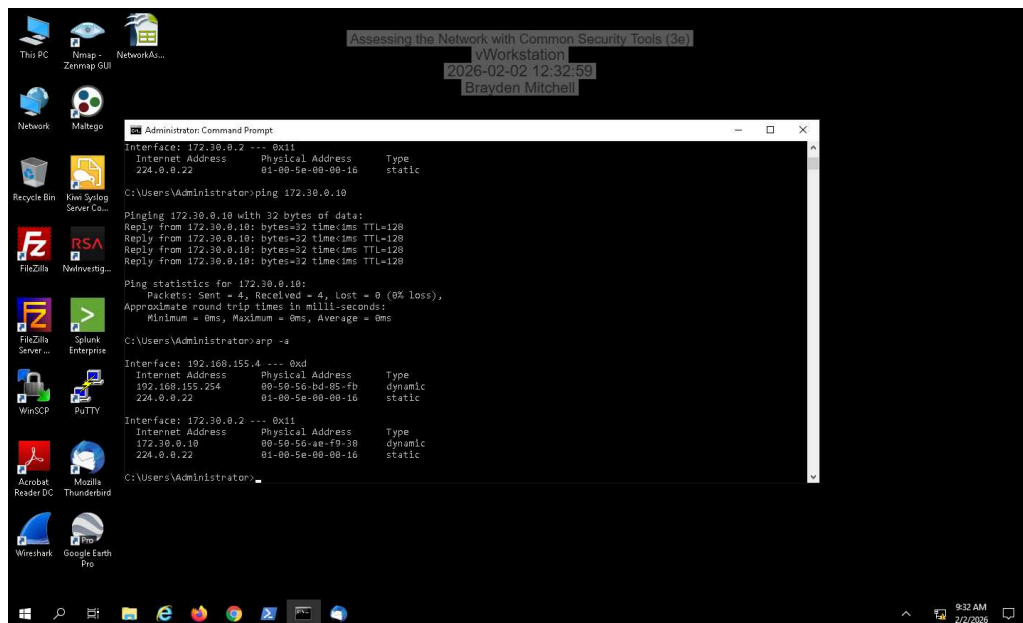
Assessing the Network with Common Security Tools (3e)

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

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



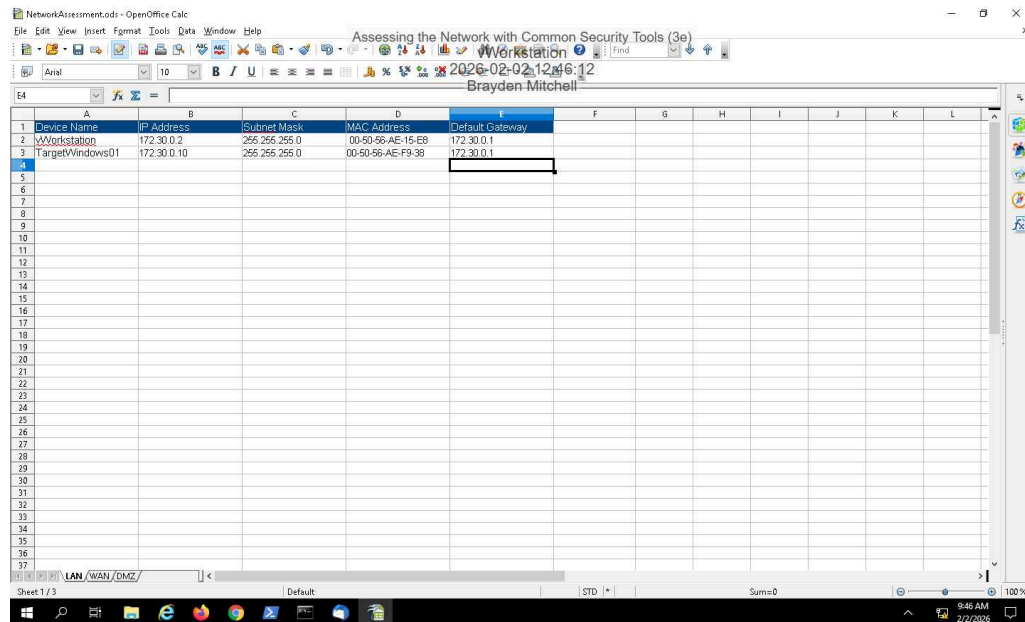
15. Make a screen capture showing the updated ARP cache on the vWorkstation.



Assessing the Network with Common Security Tools (3e)

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

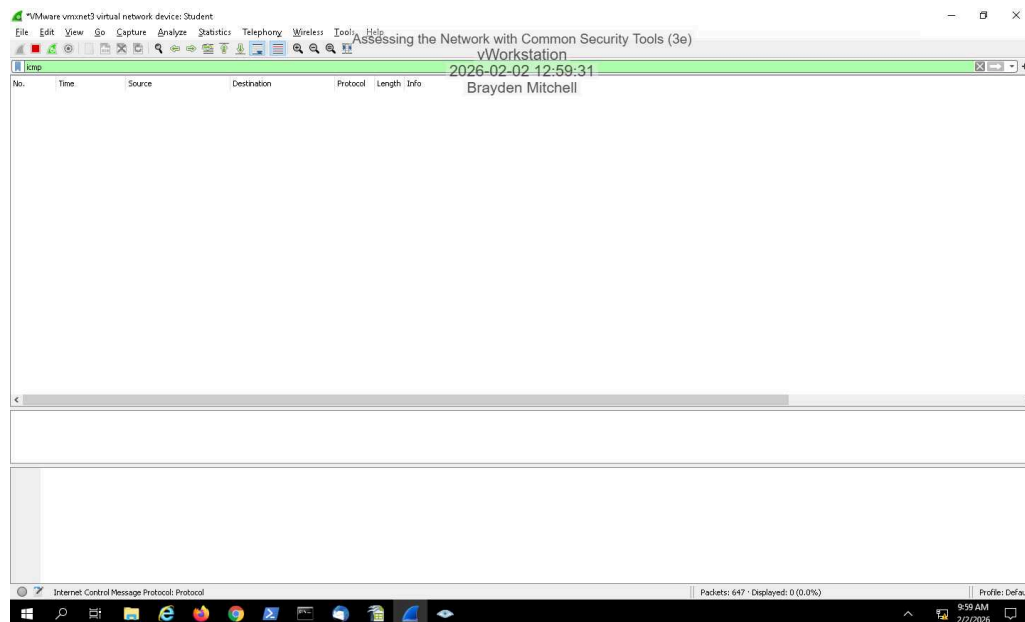
19. Make a screen capture showing the **completed LAN tab** of the Network Assessment spreadsheet.



Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
vWorkstation	172.30.0.2	255.255.255.0	00:50:56:AE:15:E8	172.30.0.1
TargetVWindows01	172.30.0.10	255.255.255.0	00:50:56:AE:F9:38	172.30.0.1

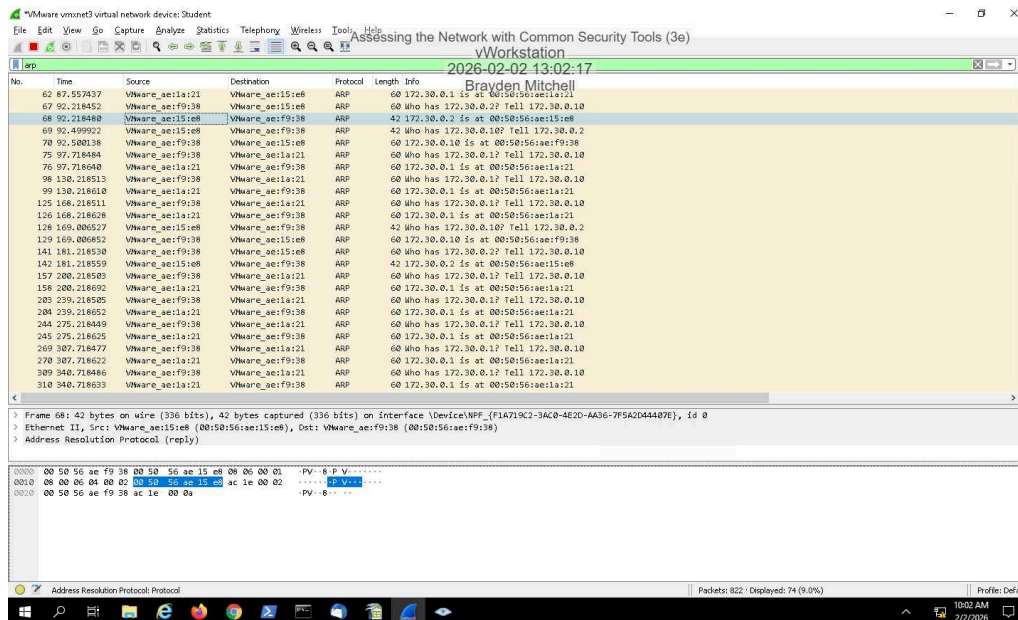
Part 2: Analyze Network Traffic

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



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.30.0.2	172.30.0.1	ICMP	64	Echo (ping) 64 bytes of data

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



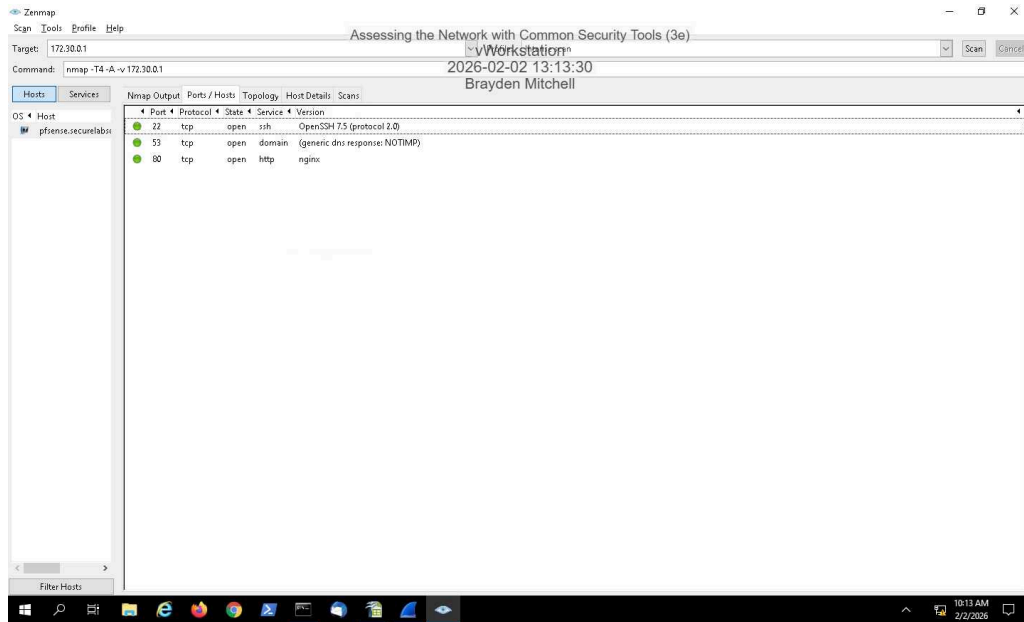
18. Compare the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

There continued to be no results for ICMP for the regular scan. There was more ARP traffic for the regular scan command to the ping scan.

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

The intense scan shows results under ICMP traffic, unlike the regular and ping scans. There is also even more ARP traffic than there was with the regular scan and the ping scan

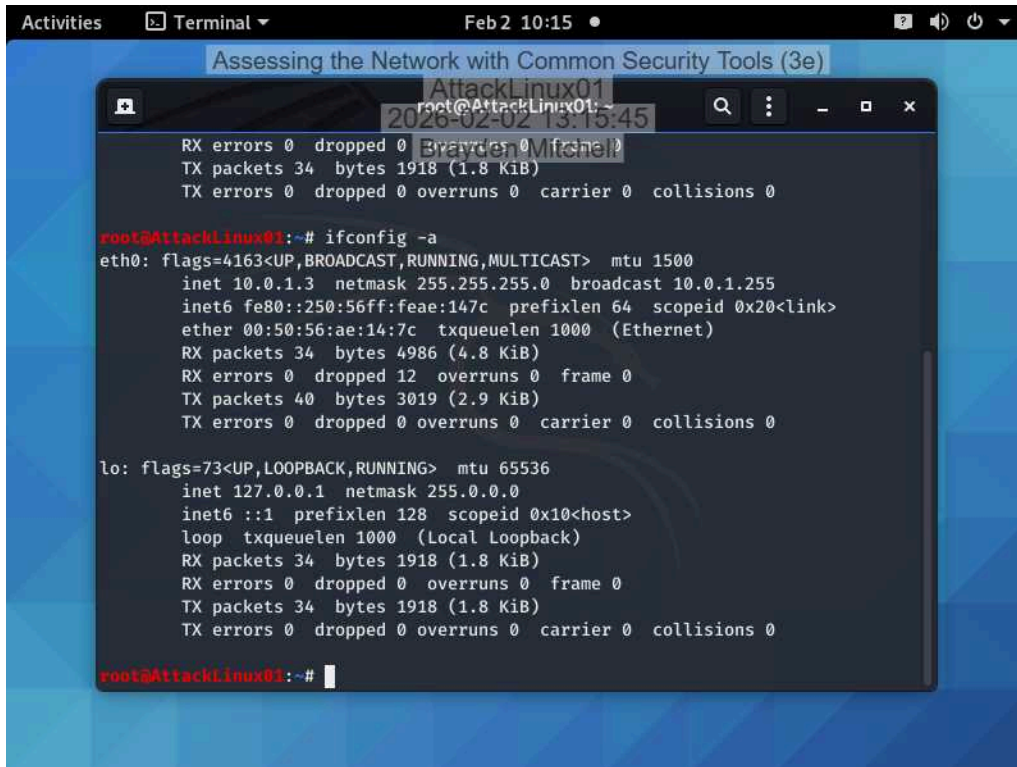
28. **Make a screen capture showing the contents of the Ports/Hosts tab.**



Section 2: Applied Learning

Part 1: Explore the Wide Area Network

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



```
Activities Terminal Feb 2 10:15
Assessing the Network with Common Security Tools (3e)
AttackLinux01
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:feae:147c prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ae:14:7c txqueuelen 1000 (Ethernet)
    RX packets 34 bytes 4986 (4.8 KiB)
    RX errors 0 dropped 12 overruns 0 frame 0
    TX packets 40 bytes 3019 (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:~#
```

10.0.1.3 255.255.255.0 00:50:56:ae:14:7c

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

```
Administrator: Command Prompt
Ethernet adapter TrueLab:
    Connection-specific DNS Suffix . : 
    IP Address . . . . . : 192.168.155.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.155.254

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

Ethernet adapter Student:
    Connection-specific DNS Suffix . : 
    Description . . . . . : vmnet3 Ethernet Adapter #3
    Physical Address. . . . . : 80-50-56-AE-00-7B
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::4d2:c1bf:8dc:8bde%11(Preferred)
    IPv4 Address. . . . . : 10.0.1.2(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.1.1
    DHCPv6 IAID . . . . . : 469702614
    DHCPv6 Client DUID. . . . . : 00-01-00-01-31-12-05-10-00-50-56-AE-00-7B
    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 . . . . . : vmnet3 Ethernet Adapter #2
    Physical Address. . . . . : 80-50-56-AE-00-59
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.155.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.155.254
    NetBIOS over Tcpip. . . . . : Disabled

C:\Users\Administrator>
```

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

```
Administrator: Command Prompt
224.0.0.251 01-00-5e-00-00-7b static
224.0.0.252 01-00-5e-00-00-7c static

Interface: 192.168.155.1 --- 0xb
Internet Address Physical Address Type
192.168.155.254 00-50-56-bd-85-7b dynamic
192.168.253.254 00-50-56-bd-85-7b dynamic
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-7b static
255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Users\Administrator>arp -d

C:\Users\Administrator>arp -a

Interface: 10.0.1.2 --- 0xb
Internet Address Physical Address Type
224.0.0.22 01-00-5e-00-00-16 static

Interface: 192.168.155.1 --- 0xb
Internet Address Physical Address Type
192.168.155.254 00-50-56-bd-85-7b 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 = 1ms, 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-ae-0a-f9 dynamic
224.0.0.22 01-00-5e-00-00-16 static

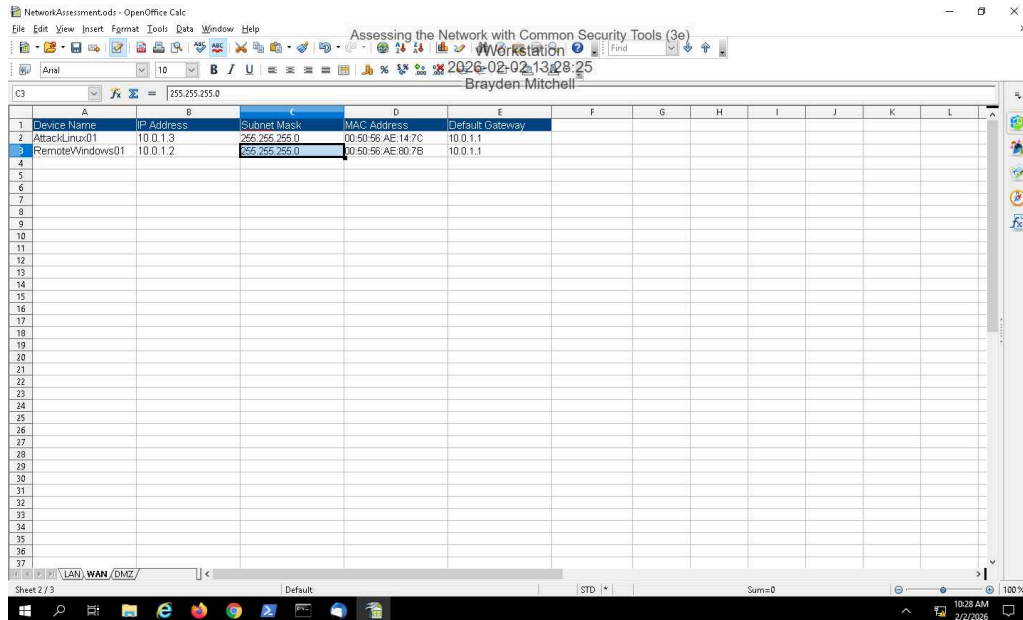
Interface: 192.168.155.1 --- 0xb
Internet Address Physical Address Type
192.168.155.254 00-50-56-bd-85-7b dynamic
224.0.0.22 01-00-5e-00-00-16 static

C:\Users\Administrator>
```


Assessing the Network with Common Security Tools (3e)

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

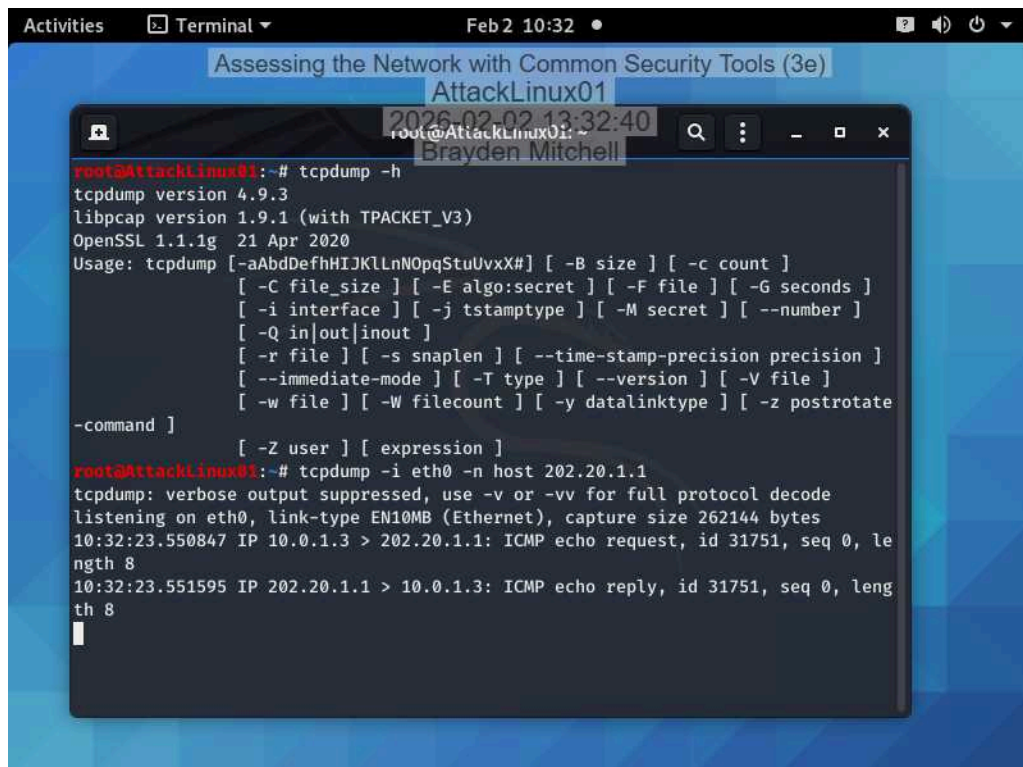
22. Make a screen capture showing the **completed WAN tab** of the Network Assessment spreadsheet.



Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
AttackLinux01	10.0.1.3	255.255.255.0	00:50:56:AE:14:7C	10.0.1.1
RemoteWindows01	10.0.1.2	255.255.255.0	00:50:56:AE:80:7B	10.0.1.1

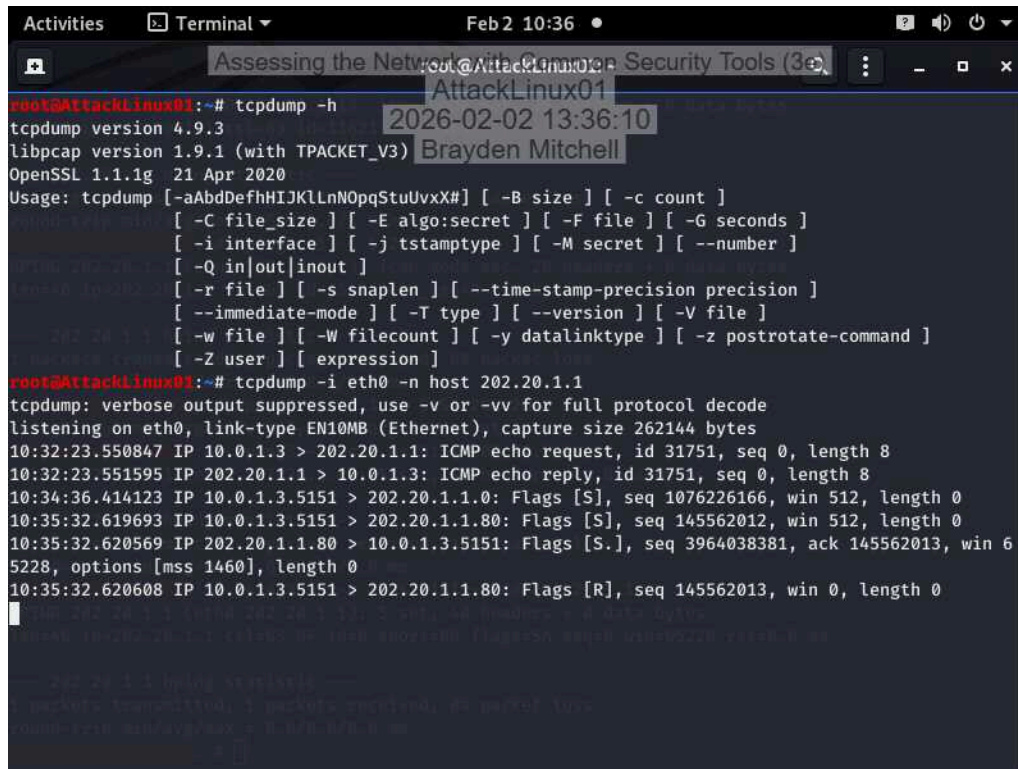
Part 2: Analyze Network Traffic

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 [-aAbDefhHIJKLlnNOpqStuUvX#] [-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
10:32:23.550847 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 31751, seq 0, length 8
10:32:23.551595 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 31751, seq 0, length 8
```

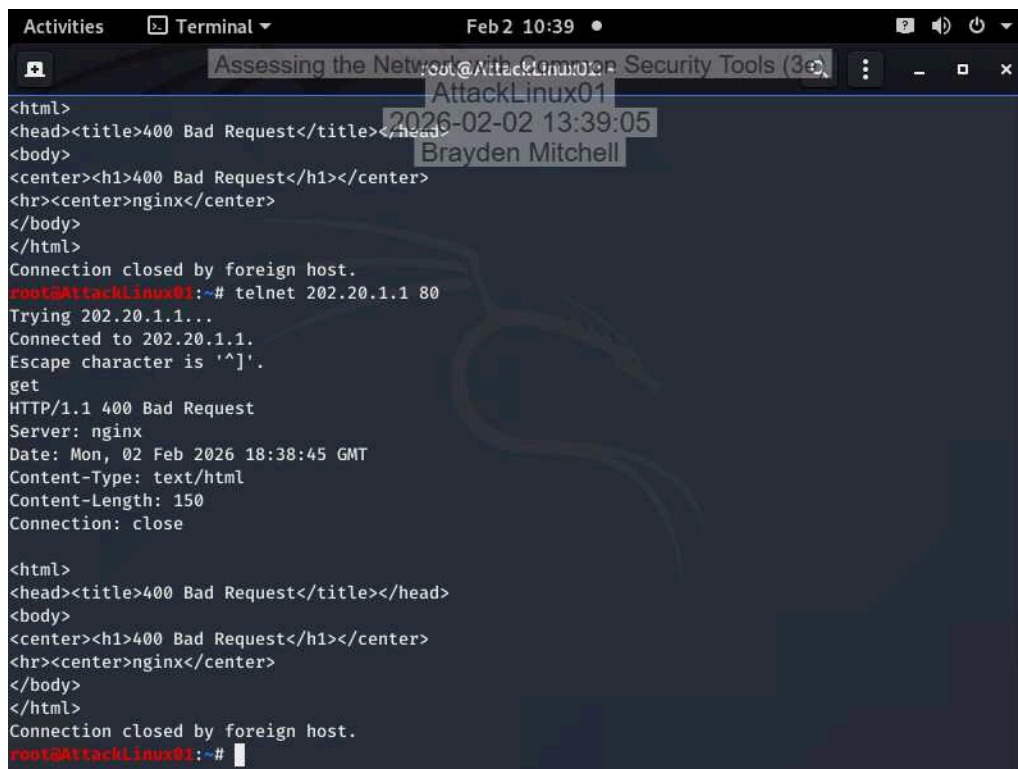

12. Make a screen capture showing the attempted three-way handshake in tcpdump.



```
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 [-aAbCdDeFfHIJKLlnNOpqStuUvXx#] [-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
10:32:23.550847 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 31751, seq 0, length 8
10:32:23.551595 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 31751, seq 0, length 8
10:34:36.414123 IP 10.0.1.3.5151 > 202.20.1.1.0: Flags [S], seq 1076226166, win 512, length 0
10:35:32.619693 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [S], seq 145562012, win 512, length 0
10:35:32.620569 IP 202.20.1.1.80 > 10.0.1.3.5151: Flags [S.], seq 3964038381, ack 145562013, win 65228, options [mss 1460], length 0
10:35:32.620608 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [R], seq 145562013, win 0, length 0
```

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



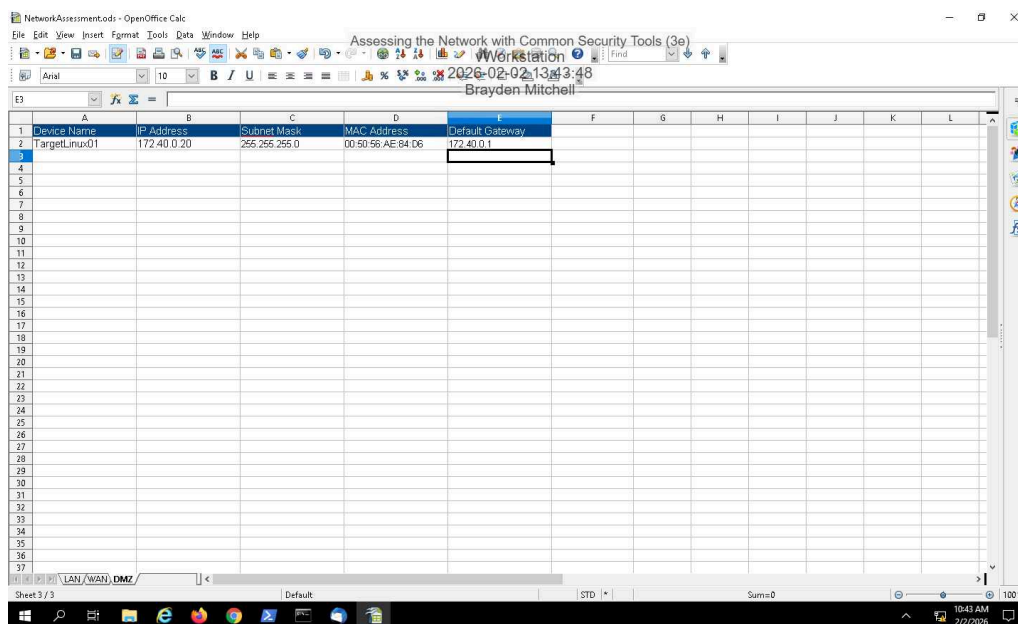
```
<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
Connection closed by foreign host.
root@AttackLinux01:~# telnet 202.20.1.1 80
Trying 202.20.1.1...
Connected to 202.20.1.1.
Escape character is '^]'.
get
HTTP/1.1 400 Bad Request
Server: nginx
Date: Mon, 02 Feb 2026 18:38:45 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.



Part 2: Perform Reconnaissance on the Firewall

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

To: Supervisor From: Brayden Mitchell Date: 2/2/26

Overview As part of the reconnaissance phase, I performed a Regular scan of the pfSense firewall's external interface (202.20.1.1) from the AttackLinux01 machine (10.0.1.3) while capturing traffic using Wireshark. The goal was to observe network-level behavior and identify exposed services.

ICMP Traffic: ICMP packets were observed during the scan. While standard Echo (ping) requests were present, the capture also revealed ICMP Timestamp requests and replies (Frame 6).

ARP Traffic: ARP traffic was captured during the scan, but it was limited to local network resolution. The logs show the scanning machine (10.0.1.3) sending ARP requests for the local gateway (10.0.1.1) rather than the target IP.

DNS Traffic: DNS packets were captured during the session, but they were not directed at the target firewall.

There were two open ports on the pfSense firewall. They are 80(http) and 22(ssh).