Student:	Email:
Vidhi Kadakia	jinsukrishna108@gmail.com

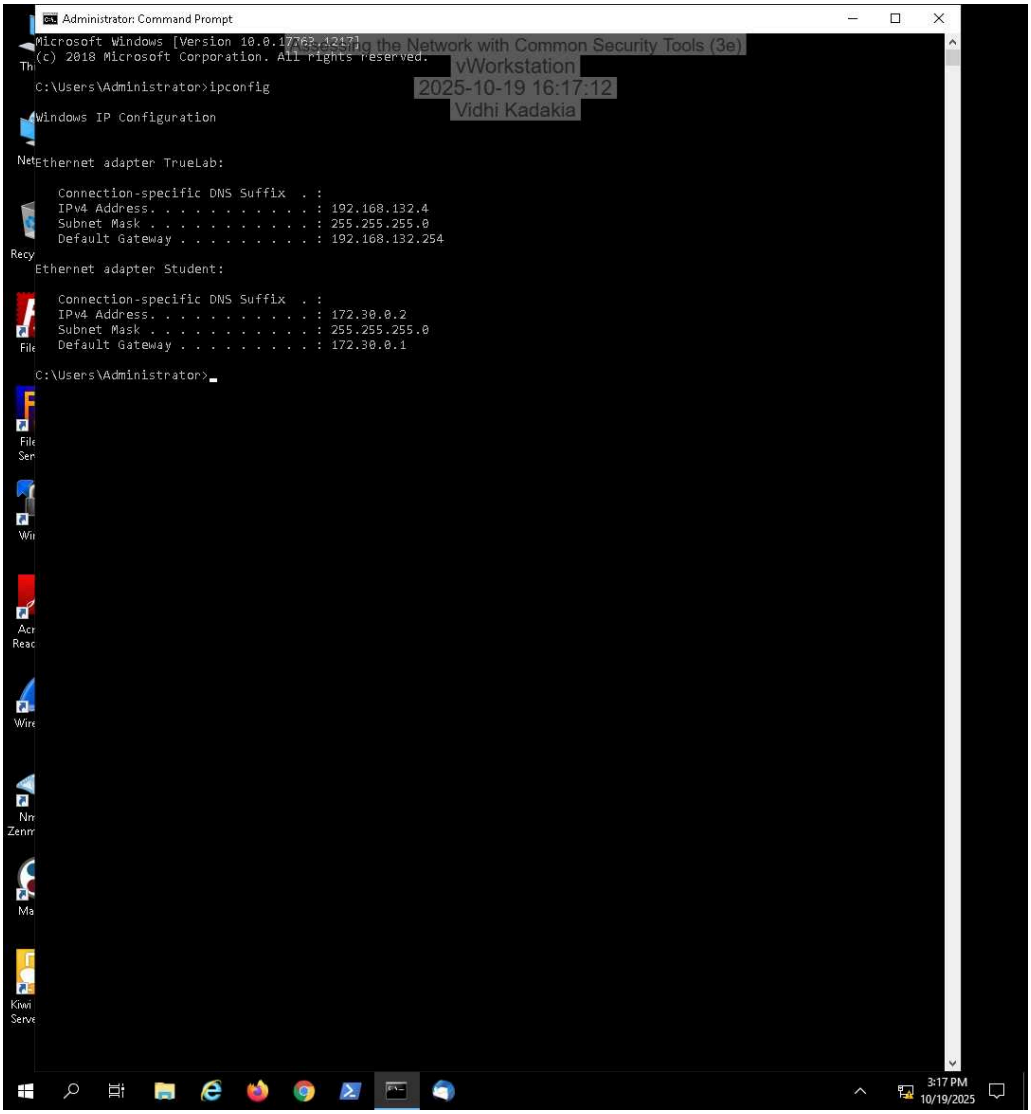
Time on Task:	Progress:
4 hours, 3 minutes	100%

Report Generated: Saturday, October 25, 2025 at 6:51 PM

Section 1: Hands-On Demonstration

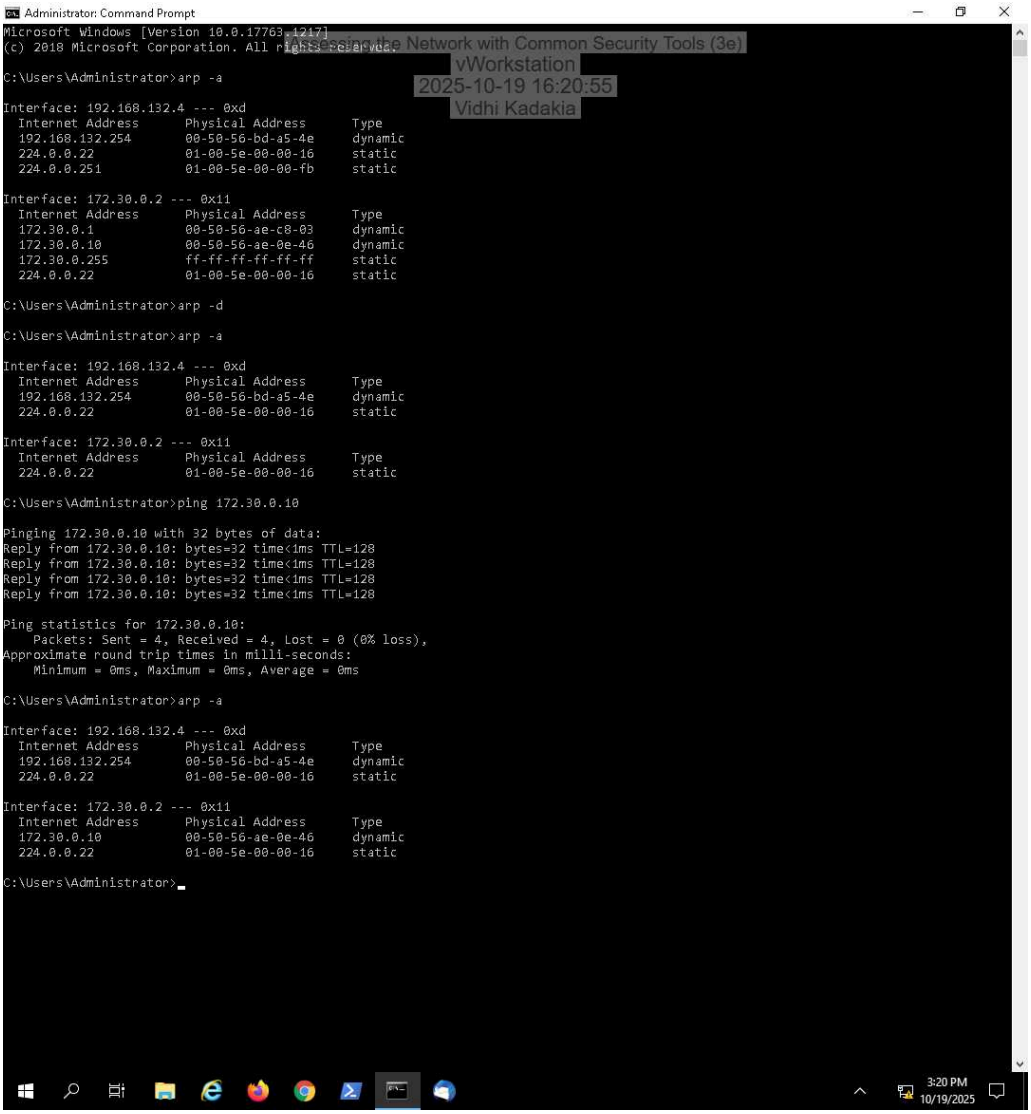
Part 1: Explore the Local Area Network

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

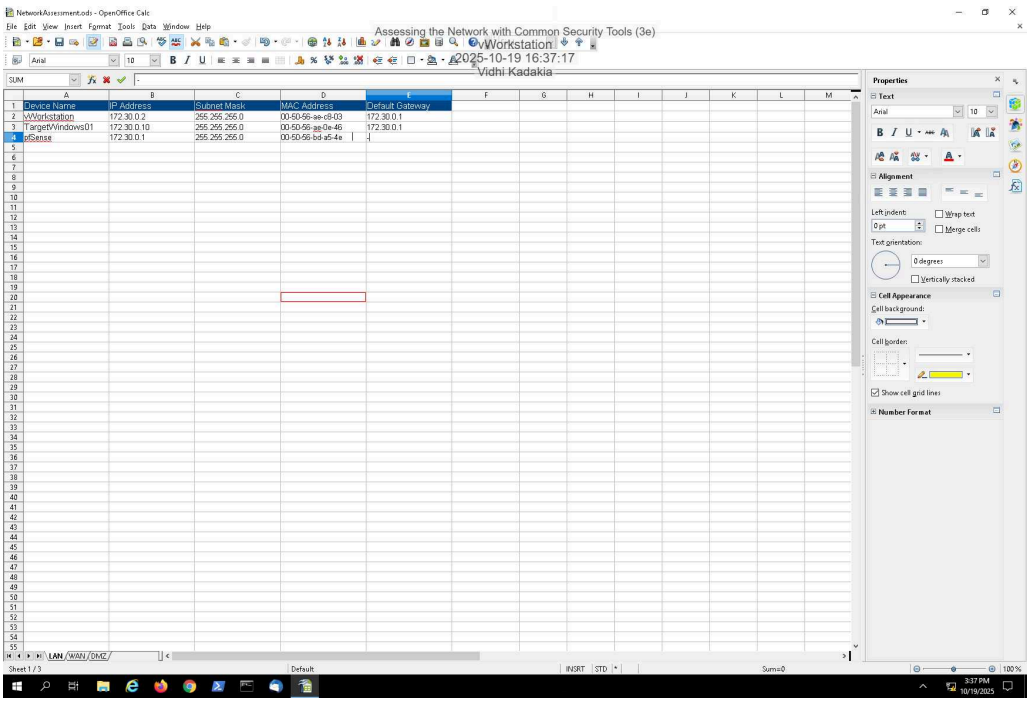


7. **Make a screen capture** showing the **ipconfig results for the Student adapter on TargetWindows01**.

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

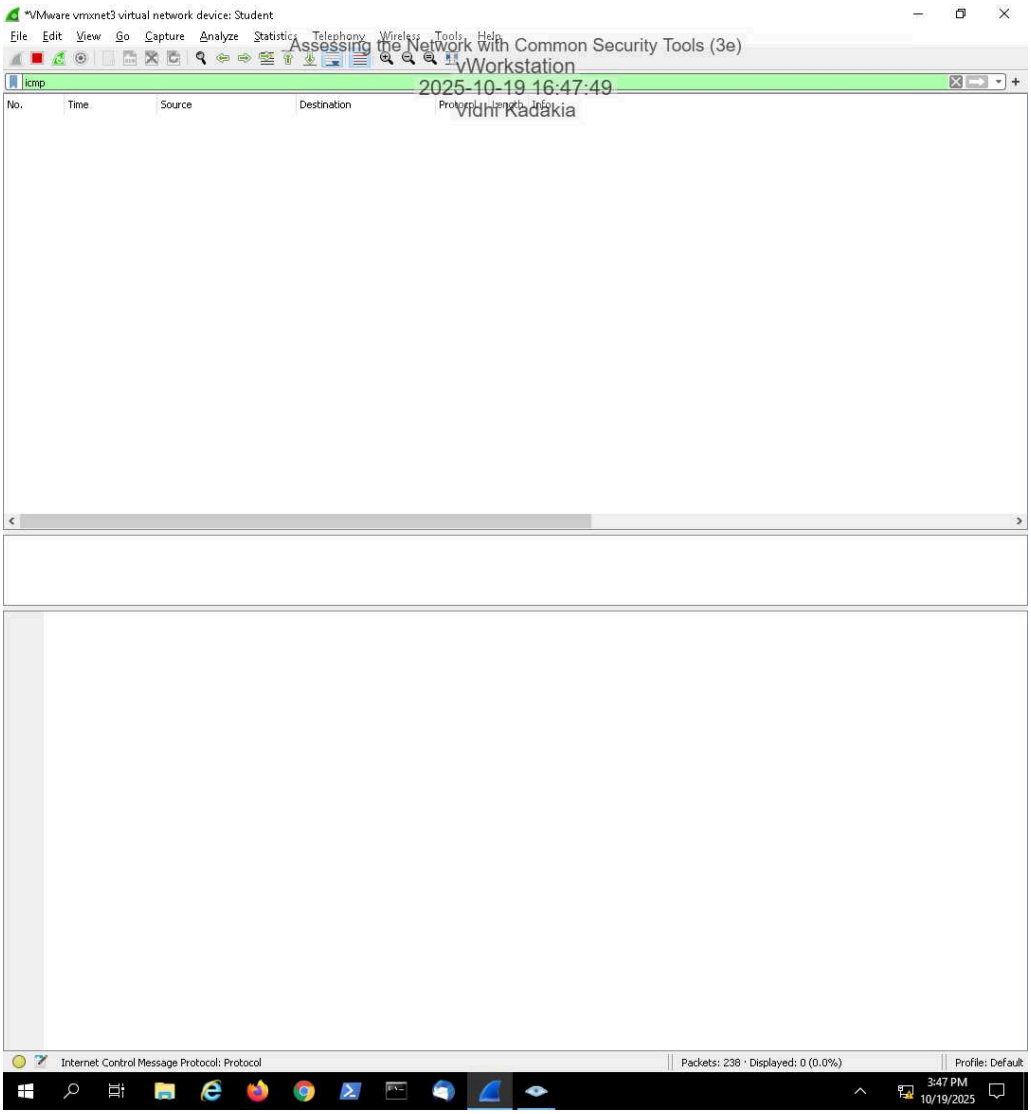

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1217]
(c) 2018 Microsoft Corporation. All rights reserved.
Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-10-19 16:20:55
Vidhi Kadakia
C:\Users\Administrator>arp -a
Interface: 192.168.132.4 --- 0xd
Internet Address Physical Address Type
192.168.132.254 00-50-56-bd-a5-4e dynamic
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
Interface: 172.30.0.2 --- 0x11
Internet Address Physical Address Type
172.30.0.1 00-50-56-ae-c8-03 dynamic
172.30.0.10 00-50-56-ae-0e-46 dynamic
172.30.0.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
C:\Users\Administrator>arp -d
C:\Users\Administrator>arp -a
Interface: 192.168.132.4 --- 0xd
Internet Address Physical Address Type
192.168.132.254 00-50-56-bd-a5-4e dynamic
224.0.0.22 01-00-5e-00-00-16 static
Interface: 172.30.0.2 --- 0x11
Internet Address Physical Address Type
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: 192.168.132.4 --- 0xd
Internet Address Physical Address Type
192.168.132.254 00-50-56-bd-a5-4e 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-ae-0e-46 dynamic
224.0.0.22 01-00-5e-00-00-16 static
C:\Users\Administrator>
3:20 PM
10/19/2025

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

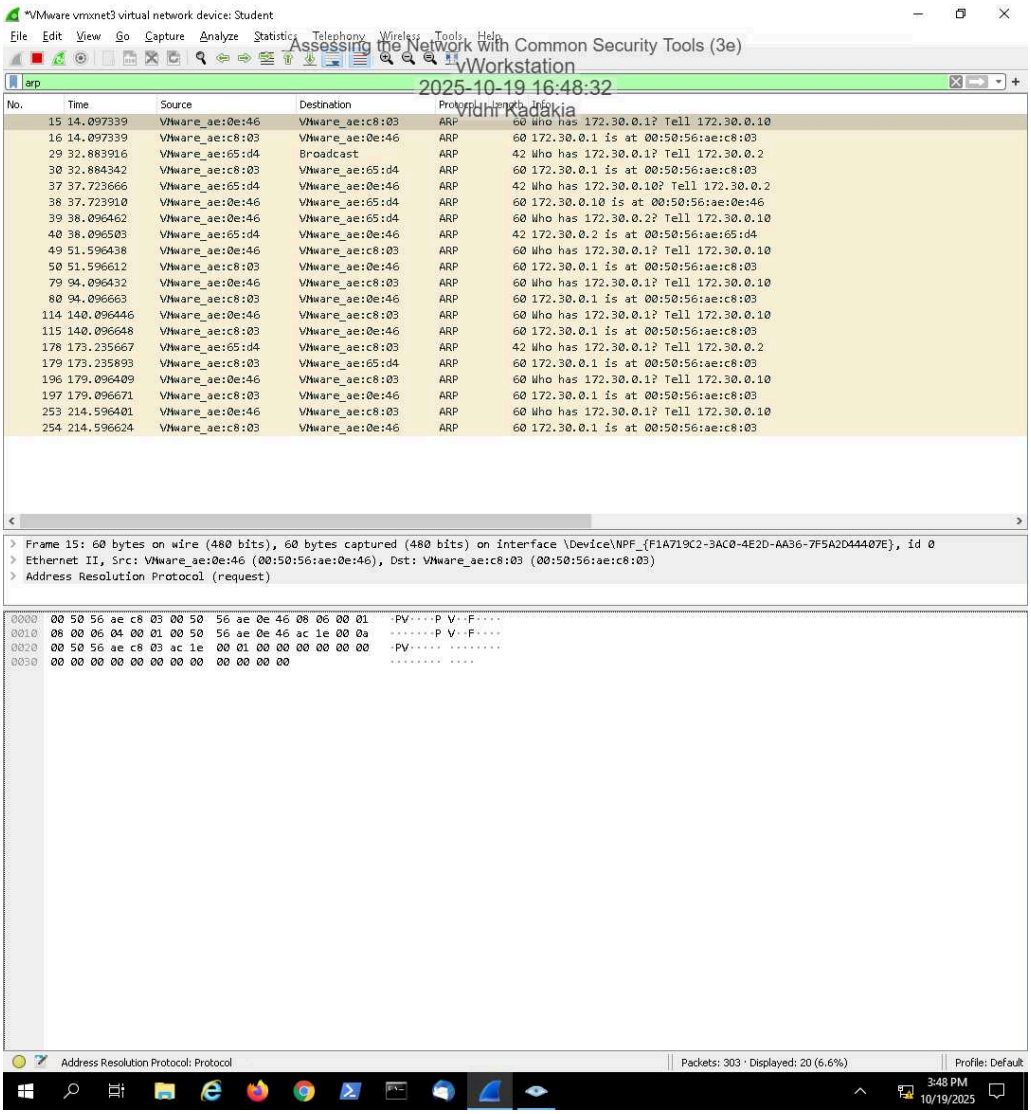


Part 2: Analyze Network Traffic

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



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



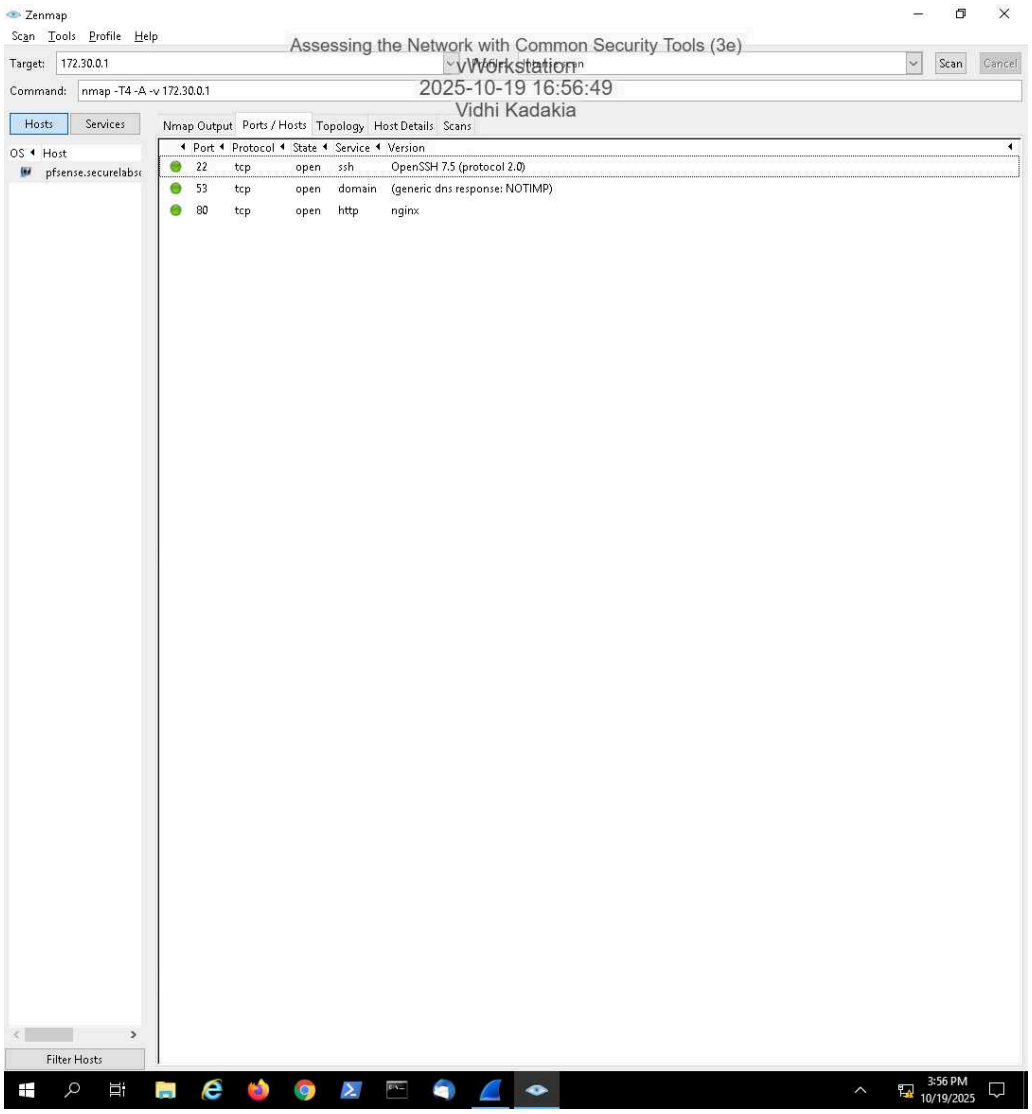
18. **Compare** the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

The Ping Scan mainly used ARP requests because ICMP traffic was blocked by the firewall. The Regular Scan, however, sent additional ARP and TCP packets to discover open ports and active hosts. This created more overall traffic and provided richer scan results.

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

The Intense Scan created much heavier traffic than the Ping Scan, including TCP, UDP, DNS, and HTTP packets. It performed service and OS detection instead of just ARP host discovery. This deeper probing reveals more network details but would trigger alerts on a secure network.

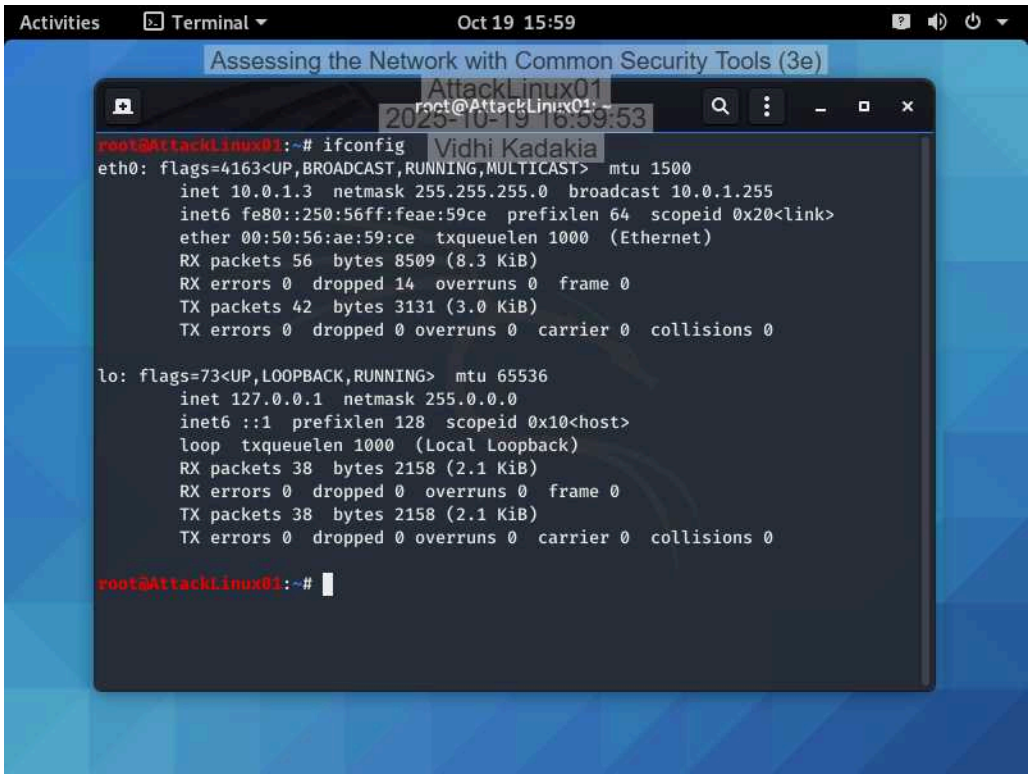
28. **Make a screen capture** showing the **contents of the Ports/Hosts tab**.



Section 2: Applied Learning

Part 1: Explore the Wide Area Network

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

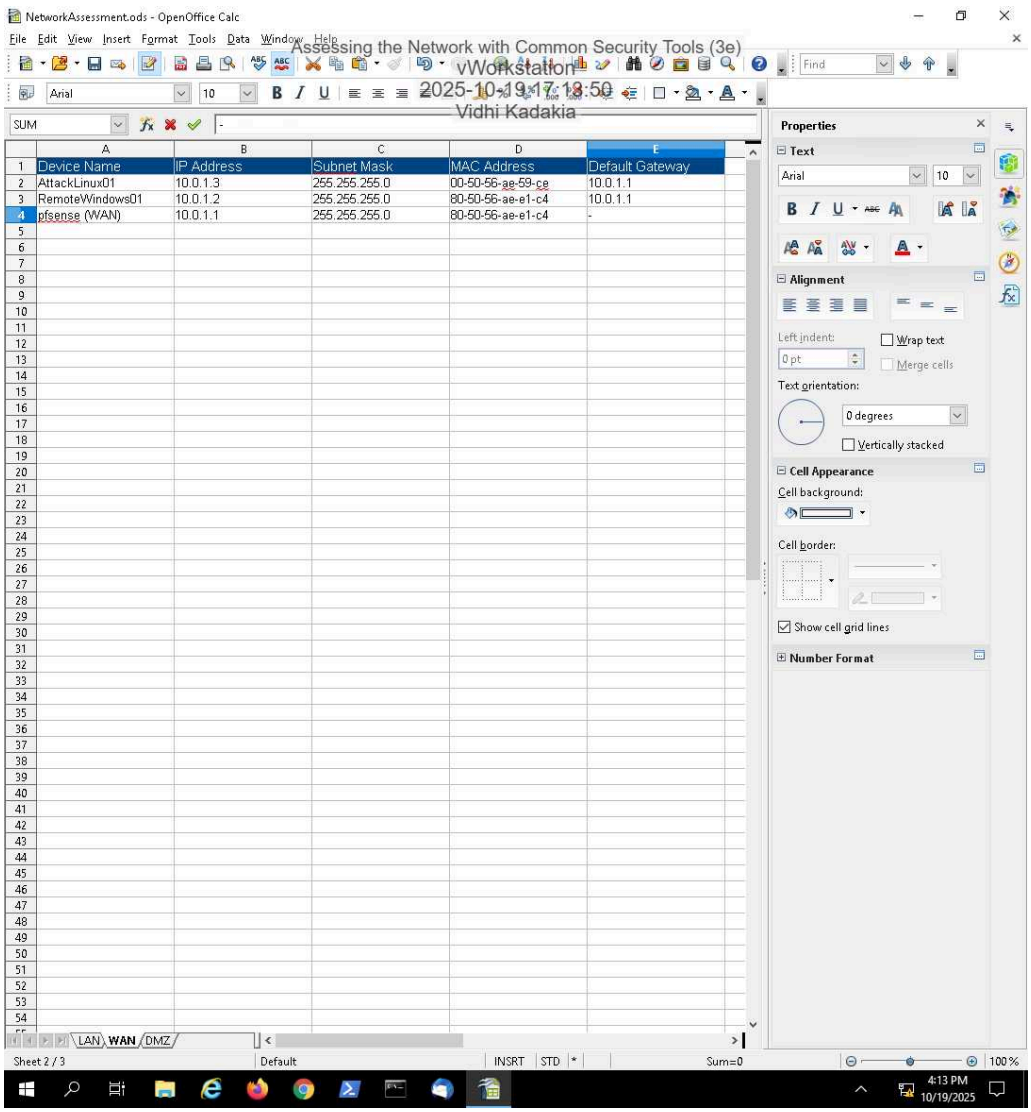


12. **Make a screen capture** showing the **ipconfig results on RemoteWindows01**.

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

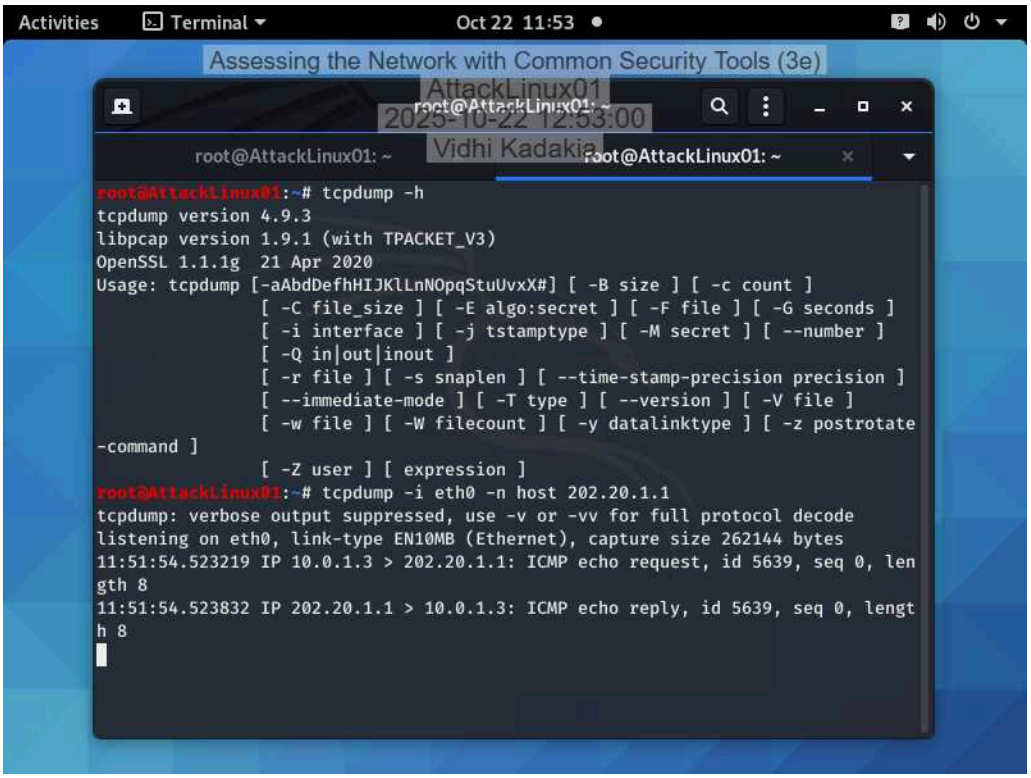

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1217]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Student:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::35a8:6b88:61e:a842%11
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. . . . . : 192.168.132.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.132.254
C:\Users\Administrator>arp -a
Interface: 10.0.1.2 --- 0xb
Internet Address Physical Address Type
10.0.1.1 00-50-56-ae-e1-c4 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: 192.168.132.1 --- 0xe
Internet Address Physical Address Type
192.168.132.254 00-50-56-bd-a5-4e dynamic
192.168.253.254 00-50-56-bd-a5-4e 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>
Assessing the Network with Common Security Tools (3e)
RemoteWindows01
2025-10-19 17:01:09
Vidhi Kadakia
4:01 PM
10/19/2025

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

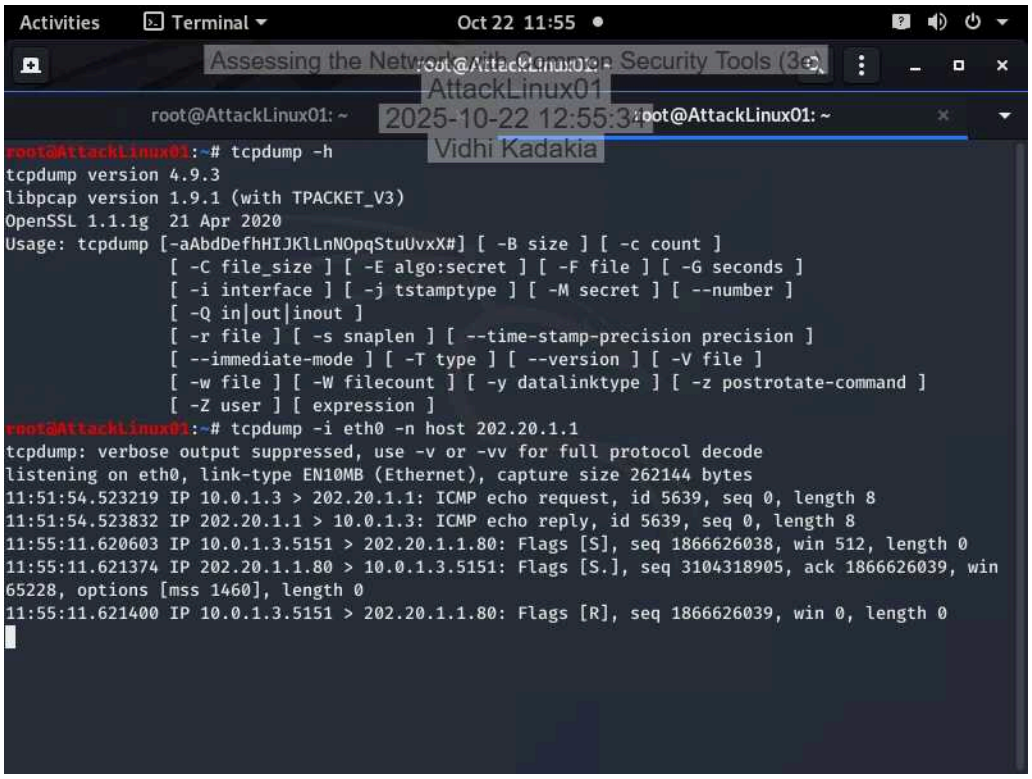


Part 2: Analyze Network Traffic

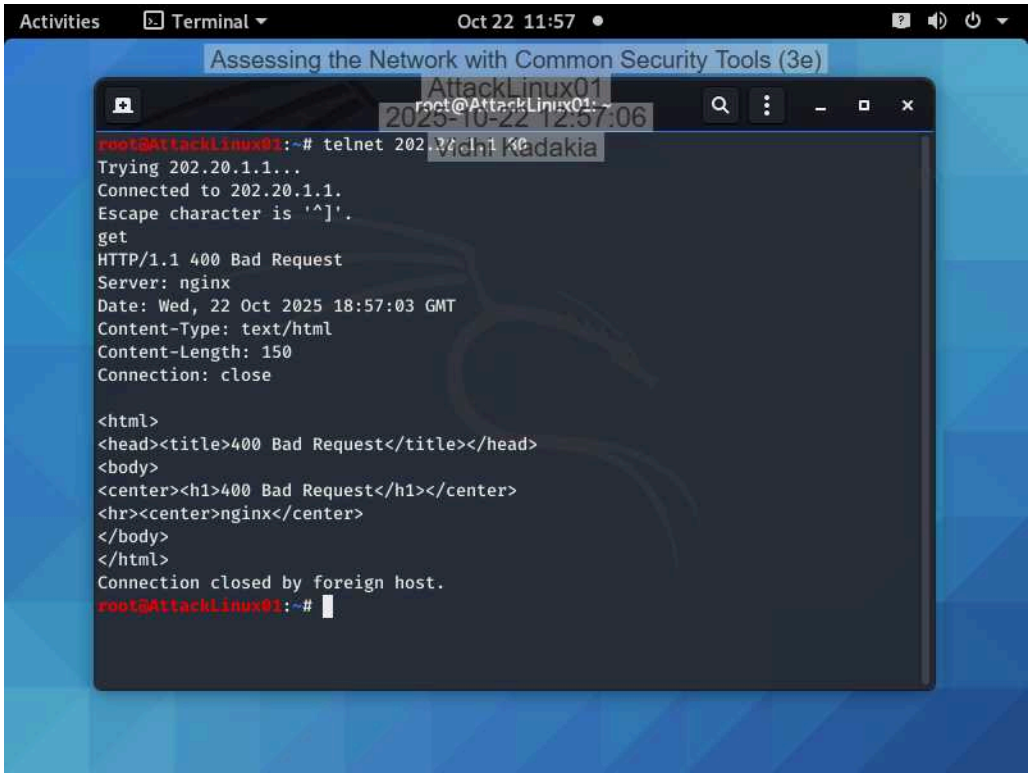
9. **Make a screen capture** showing **tcpdump echo back the captured packets**.



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



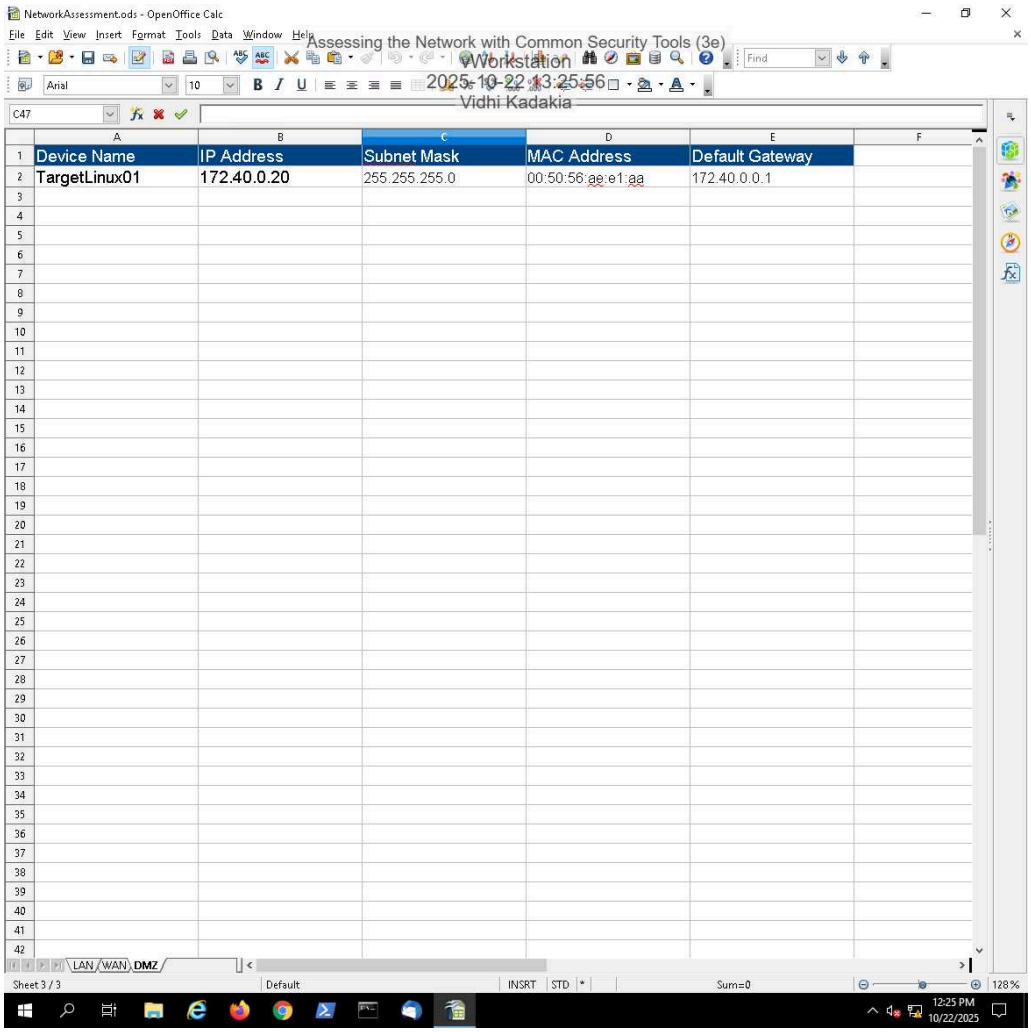
17. **Make a screen capture** showing the **results of the get command**.



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.

I ran a basic Nmap scan from the AttackLinux01 machine (IP: 10.0.1.3) to test the pfSense firewall (IP: 10.0.1.1). While the scan was running, I used tcpdump to capture packets and later looked at the capture with tshark. The goal was to see what kinds of packets were sent and what ports on the firewall were open.

No ICMP packets were captured this means the firewall didn't respond to any of the pings which is good because that makes firewall less visible to attackers.
I saw two ARP packets and I saw that my system can talk to the hardware (Layer 2) level network.

DNS packets; none were found even though the port 53 was open but it didn't send any.

Open Ports (from Nmap):
Port 53/tcp — domain (DNS)
Port 80/tcp — http (web)Everything else was filtered or closed. This means the firewall is only letting a couple of services answer on the network.
The pfSense firewall seems to be working well.It only showed ports 53 and 80 as open, no ping replies, and normal ARP behavior.Overall, the system looks secure, but the open ports should be double-checked to make sure they’re meant to be public.