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

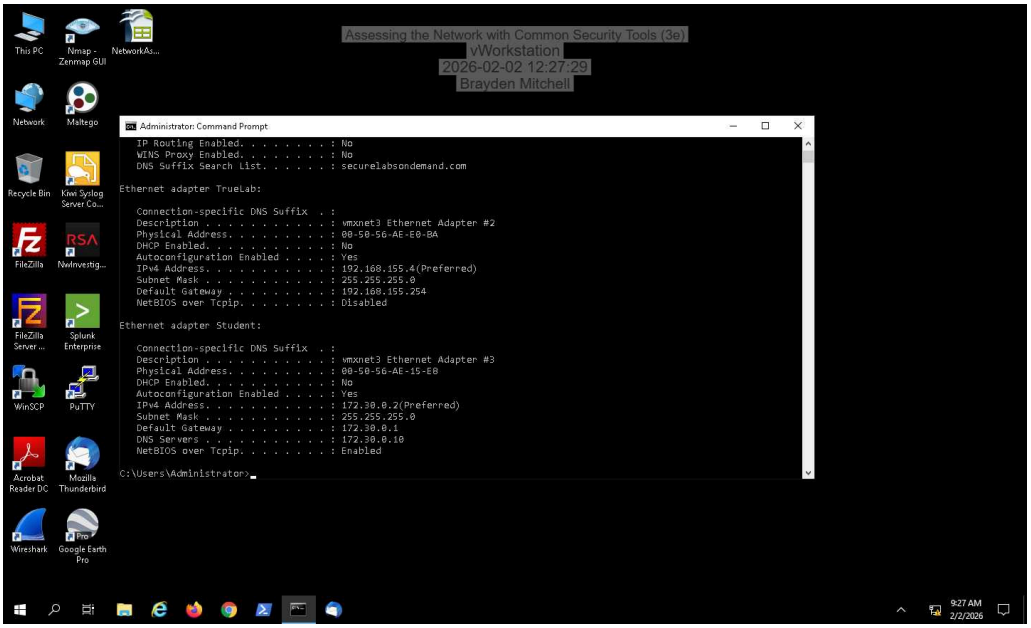
Time on Task:	Progress:
1 hour, 52 minutes	100%

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

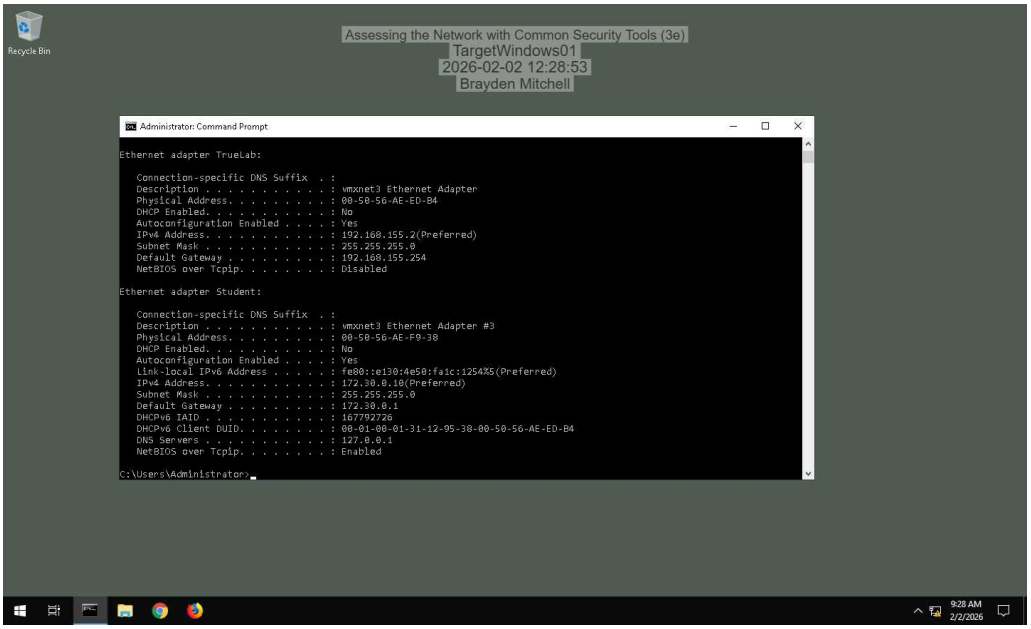
Section 1: Hands-On Demonstration

Part 1: Explore the Local Area Network

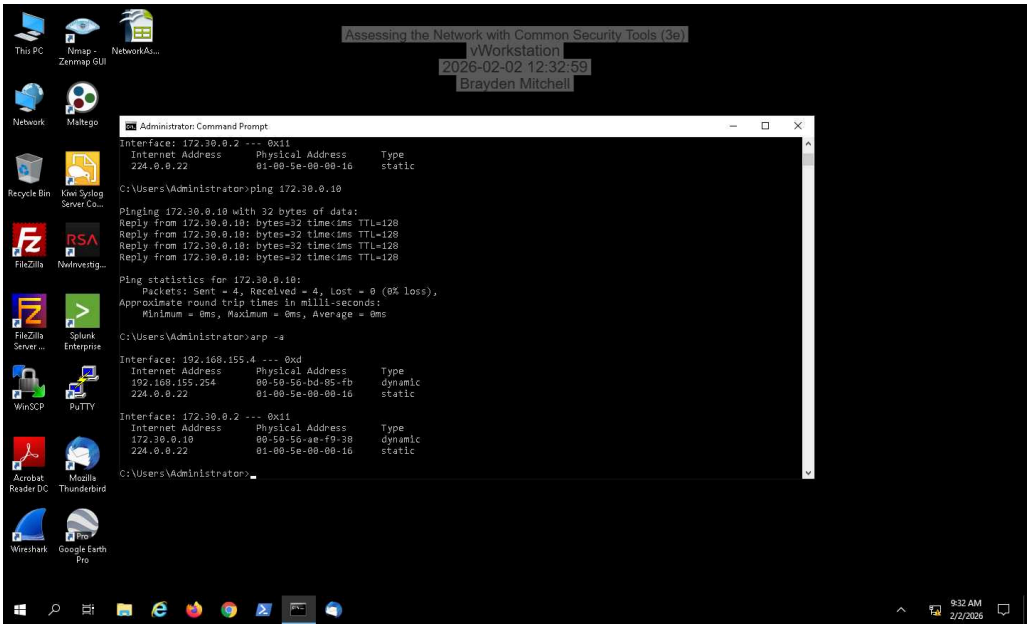
4. **Make a screen capture** showing the **ipconfig results for the Student adapter on the vWorkstation**.



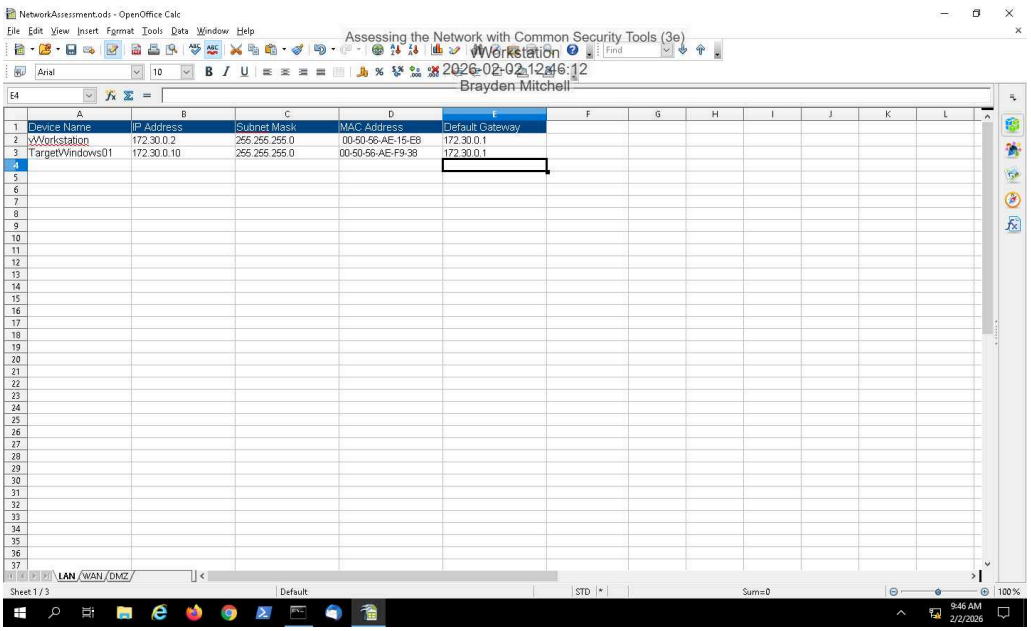
7. **Make a screen capture** showing the **ipconfig results for the Student adapter on TargetWindows01**.



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

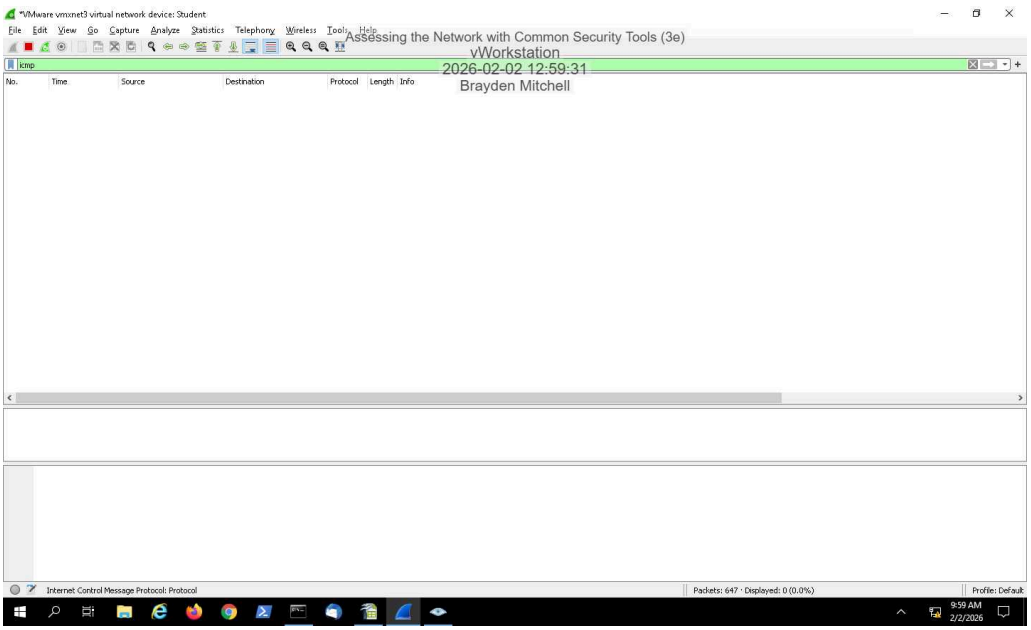


19. **Make a screen capture** showing the **completed LAN tab of the Network Assessment spreadsheet**.

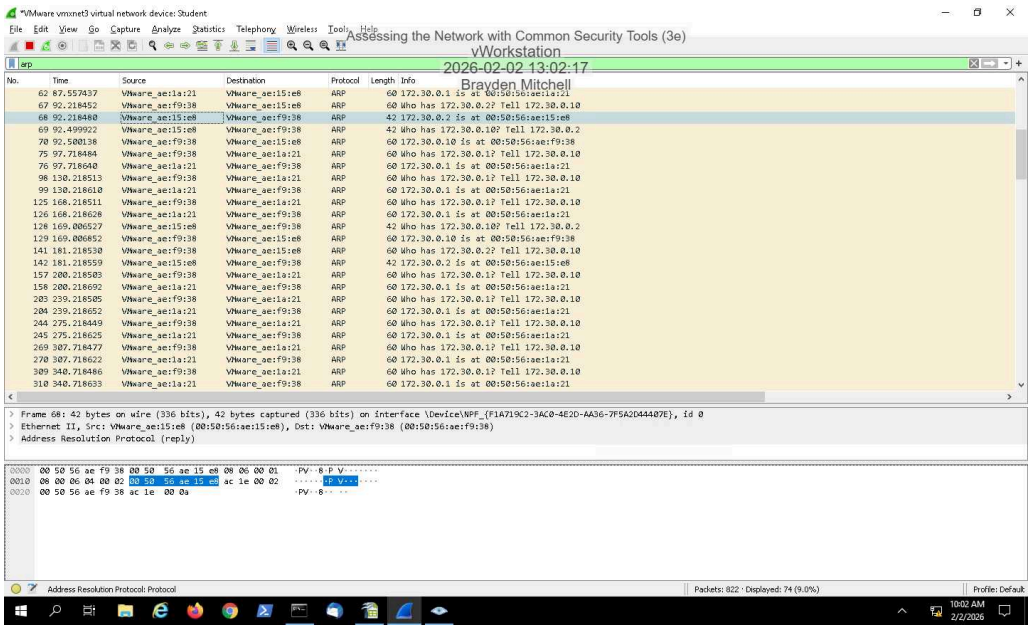


Part 2: Analyze Network Traffic

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



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



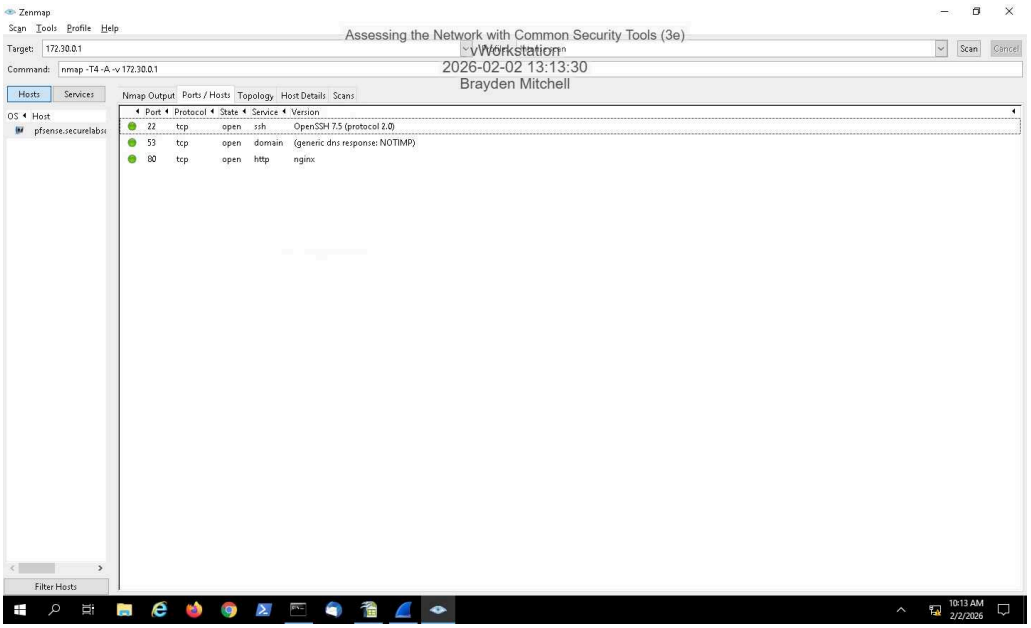
18. **Compare** the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

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

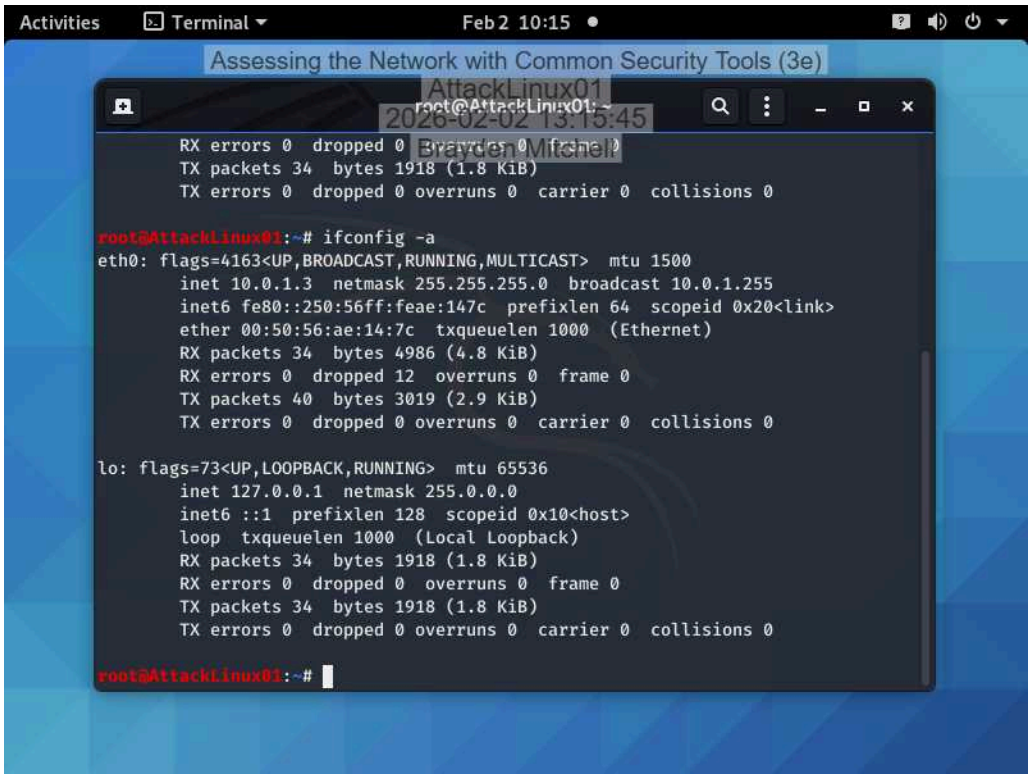
28. **Make a screen capture** showing the **contents of the Ports/Hosts tab**.



Section 2: Applied Learning

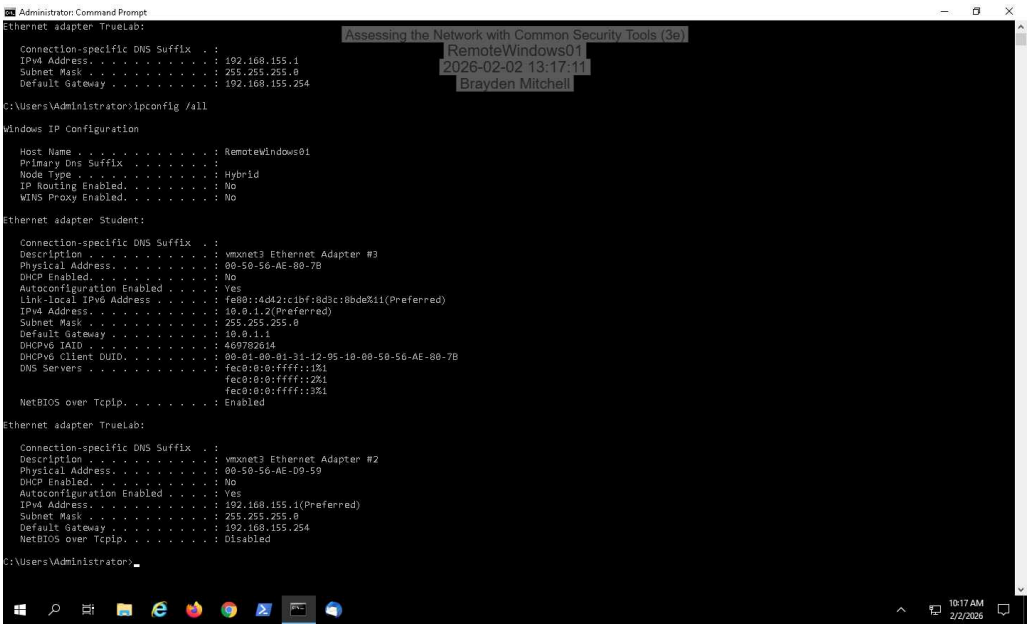
Part 1: Explore the Wide Area Network

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

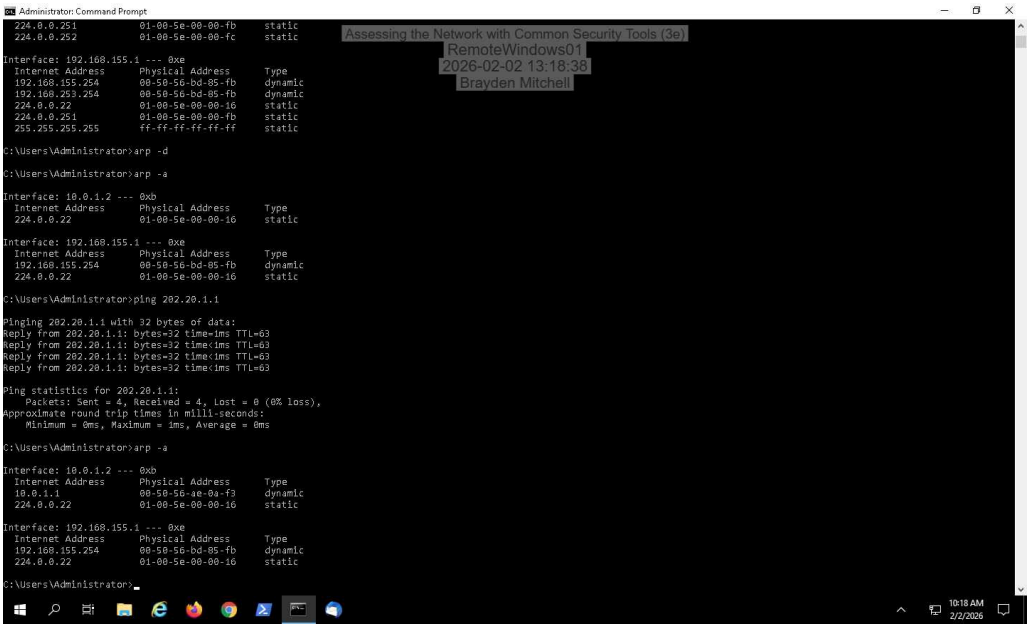


10.0.1.3 255.255.255.0 00:50:56:ae:14:7c

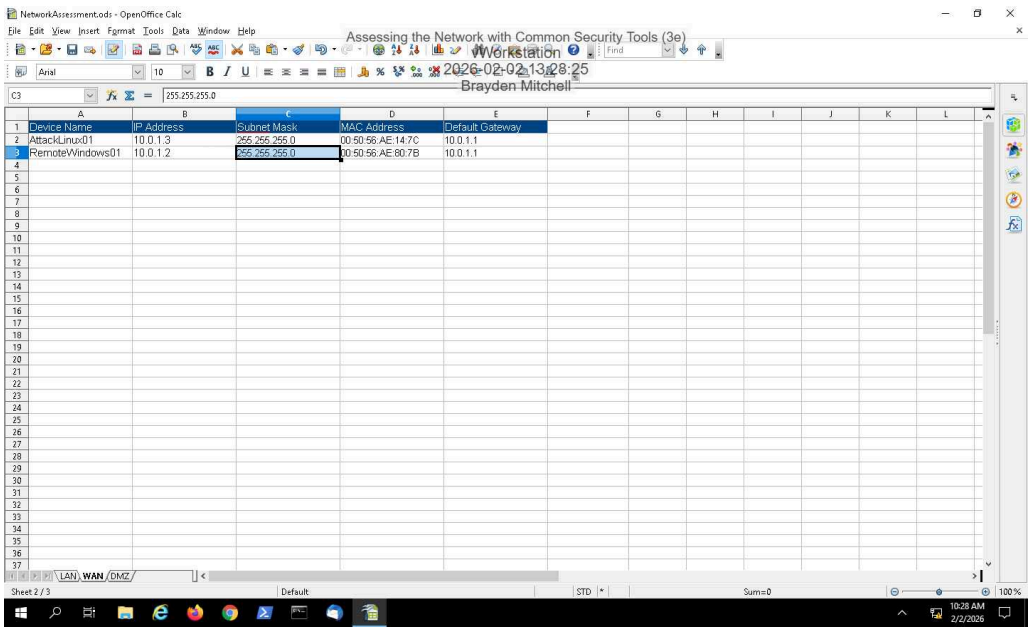
12. **Make a screen capture** showing the **ipconfig results on RemoteWindows01**.



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

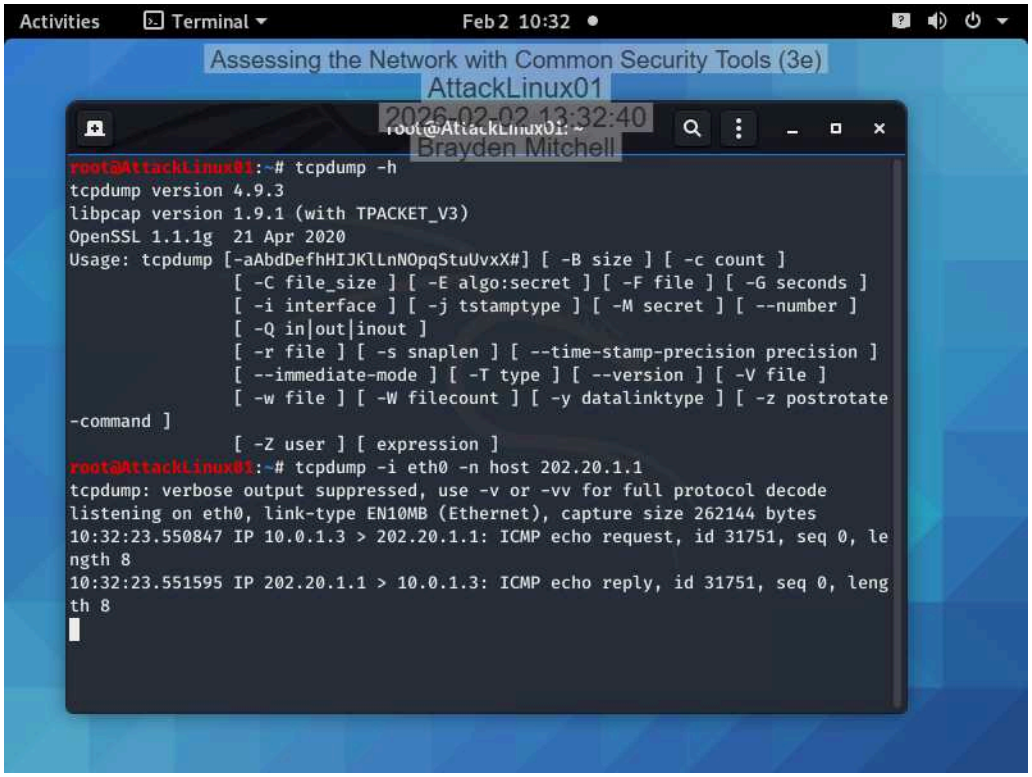


22. **Make a screen capture** showing the **completed WAN tab of the Network Assessment spreadsheet**.

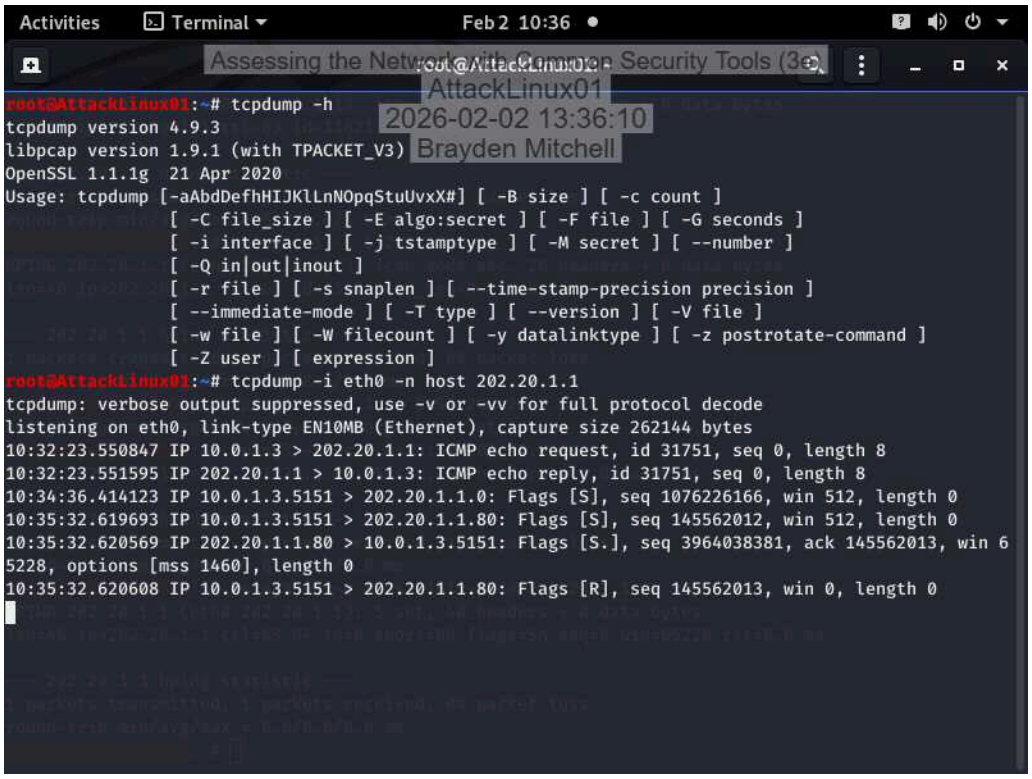


Part 2: Analyze Network Traffic

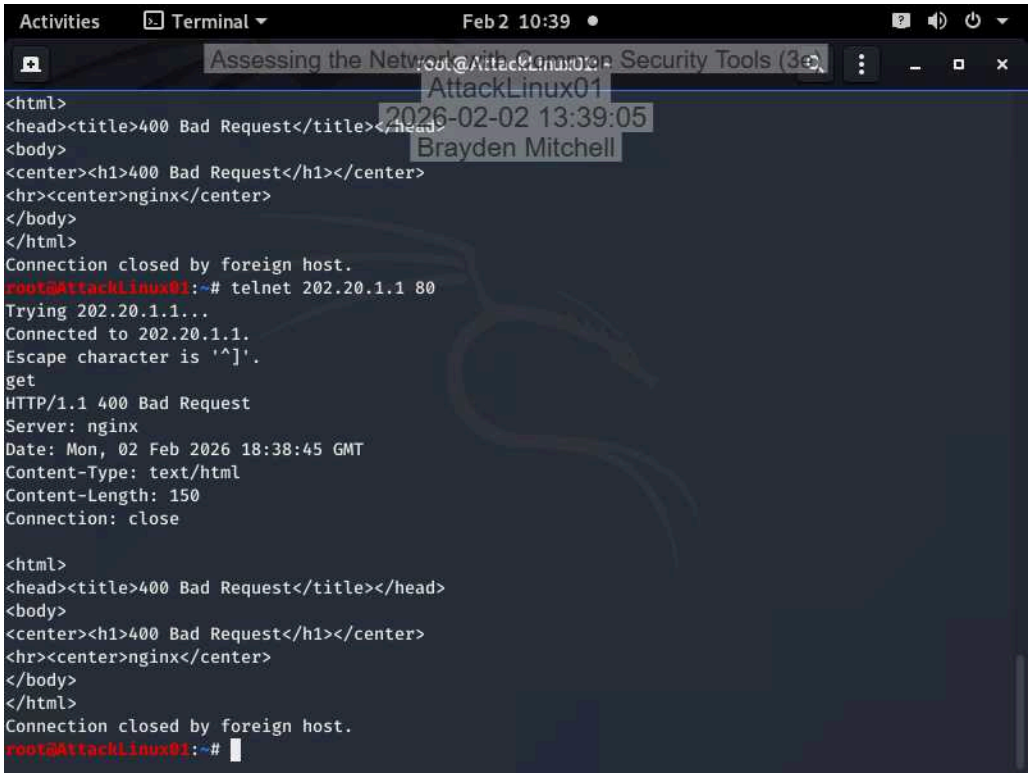
9. **Make a screen capture** showing **tcpdump echo back the captured packets**.



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



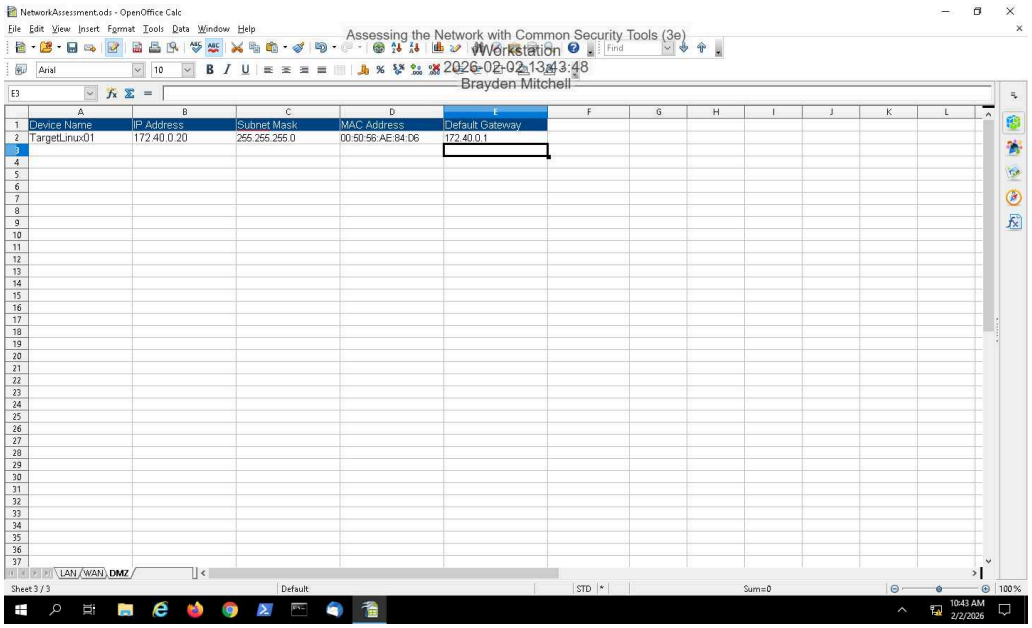
17. **Make a screen capture** showing the **results of the get command**.



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.

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).