

Assessing the Network with Common Security Tools (3e)

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

Student:

Stephen Asamoah

Email:

stephen.asamoah@howardcc.edu

Time on Task:

6 hours, 30 minutes

Progress:

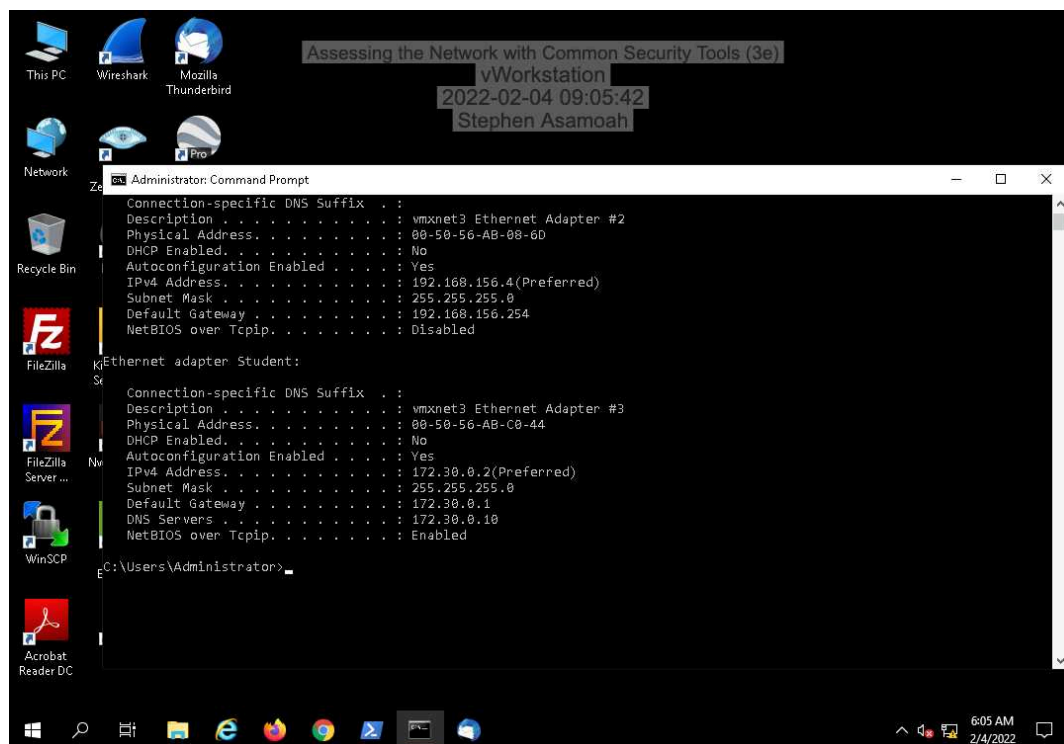
100%

Report Generated: Saturday, February 5, 2022 at 8:26 AM

Section 1: Hands-On Demonstration

Part 1: Explore the Local Area Network

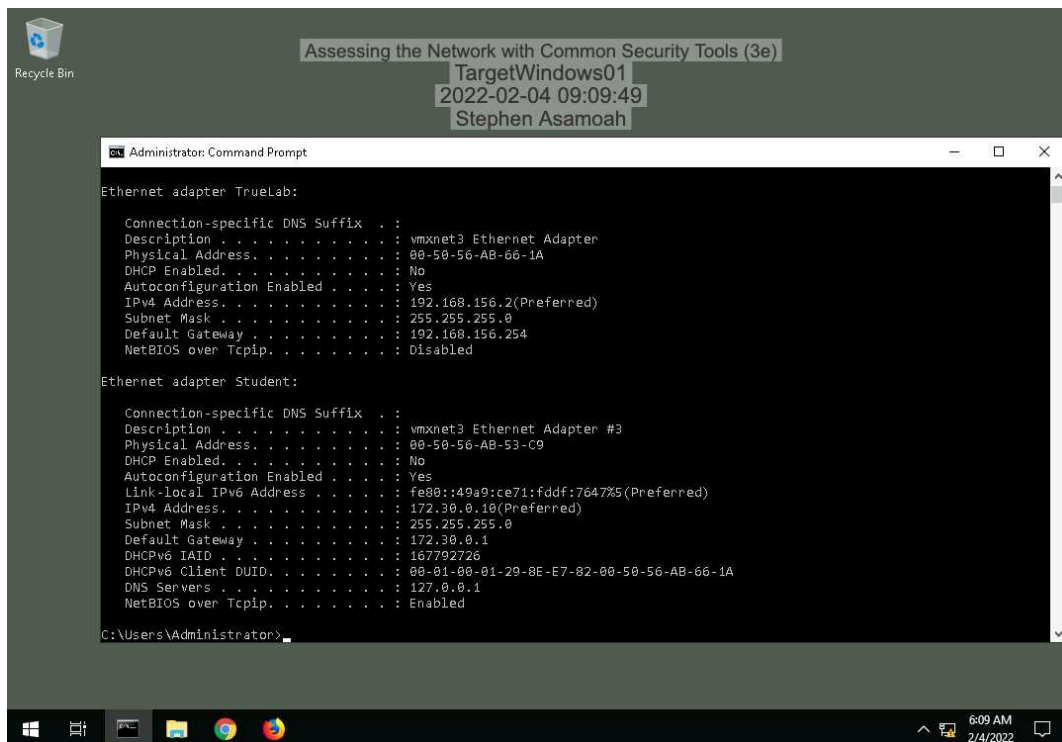
4. **Make a screen capture** showing the **ipconfig** results for the **Student** adapter on the **vWorkstation**.



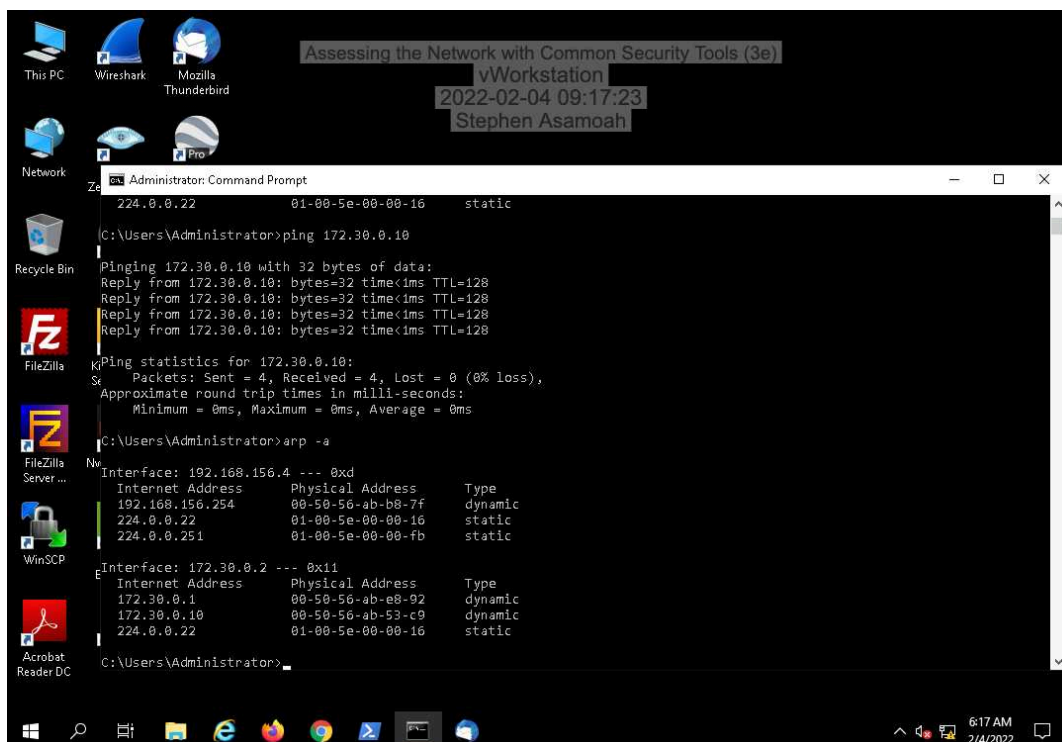
Assessing the Network with Common Security Tools (3e)

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**.

The screenshot displays the OpenOffice Calc application window titled "NetworkAssessment.xls - OpenOffice Calc". The spreadsheet is titled "Assessing the Network with Common Security Tools (3e)" and contains a table with the following data:

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
vWorkstation	172.30.0.2	255.255.255.0	00-50-56-AB-C0-44	172.30.0.1
TargetWindows01	172.30.0.10	255.255.255.0	00-50-56-ab-53-c9	172.30.0.1

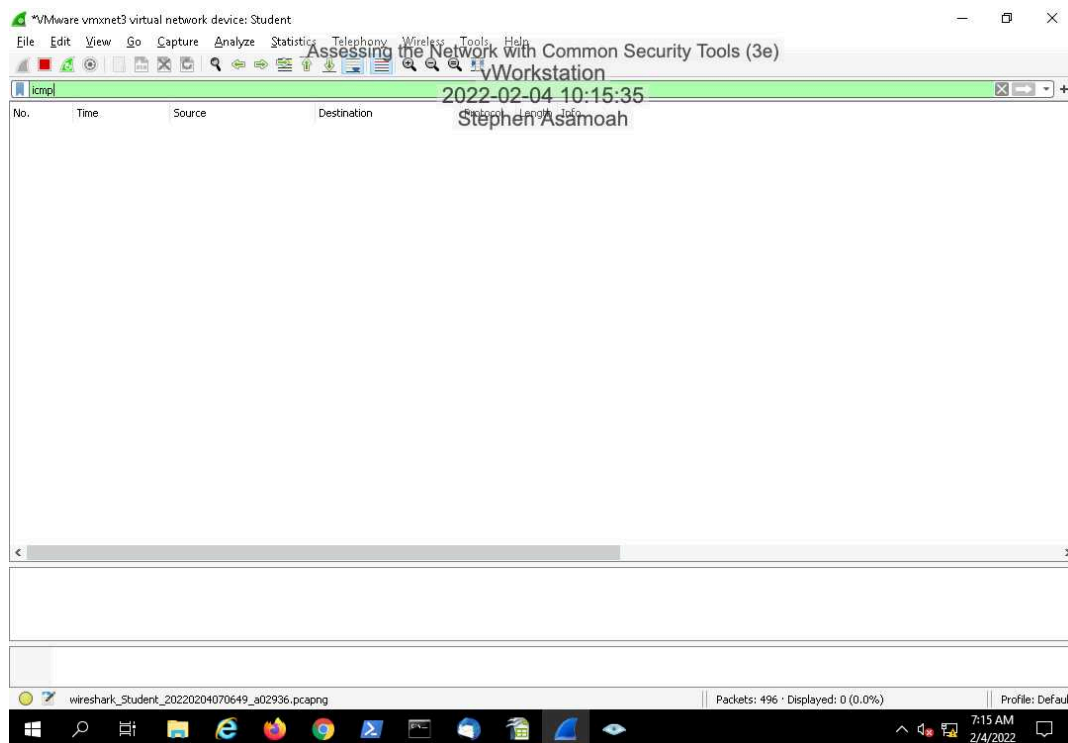
The spreadsheet is currently showing the "LAN/WAN/DMZ/" tab. The "Properties" sidebar on the right is open, showing the "Text" and "Cell Appearance" sections. The "Text" section shows the font is "Arial" and size is "10". The "Cell Appearance" section shows the "Cell background" is set to a light blue color and the "Cell border" is set to a thin black line. The "Show cell grid lines" checkbox is checked.

Part 2: Analyze Network Traffic

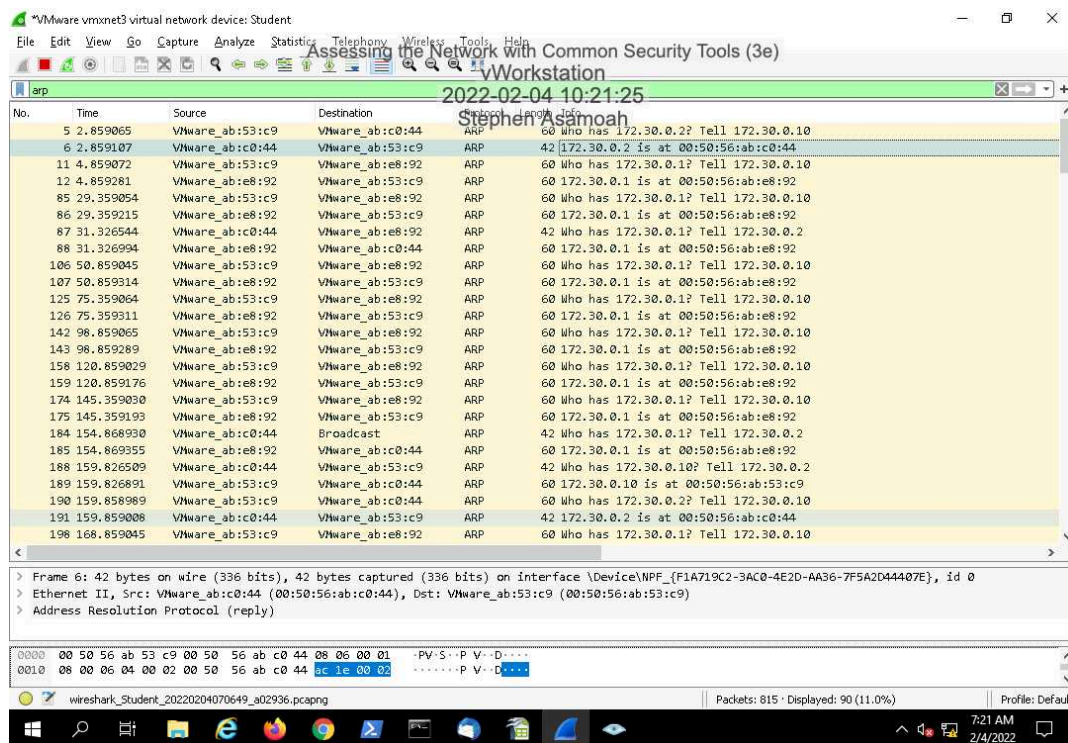
Assessing the Network with Common Security Tools (3e)

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

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



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



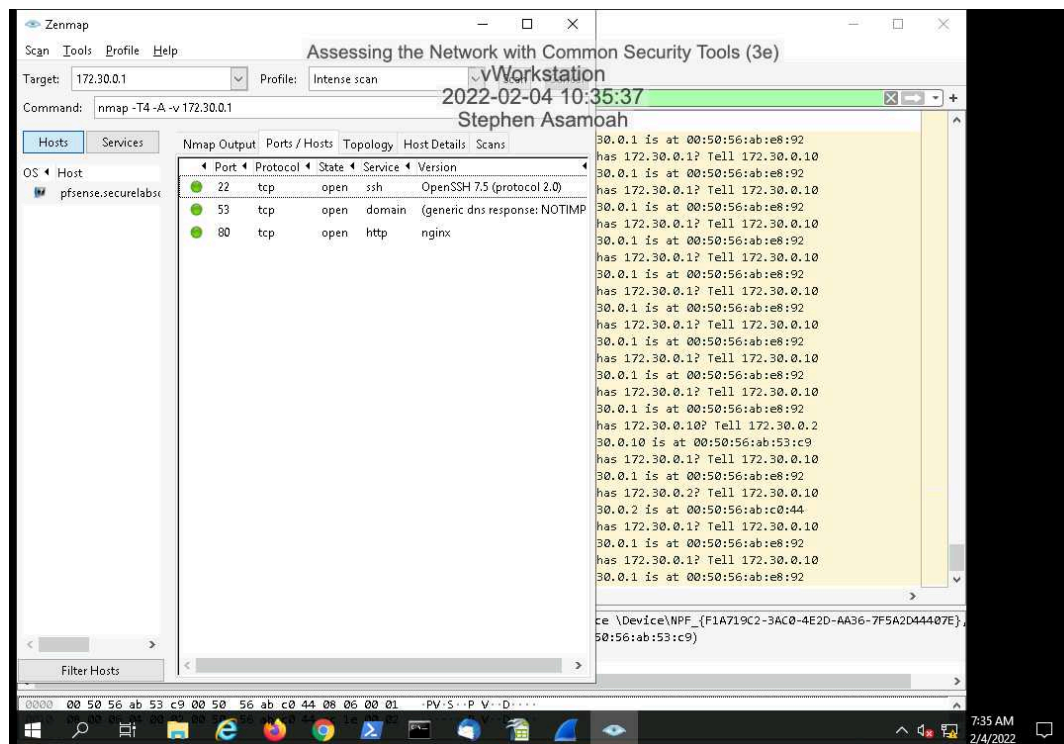
18. **Compare** the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

There is still no results for ICMP and ARP shows the same results

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

With the Intense scan, There is now ICMP results in the filter

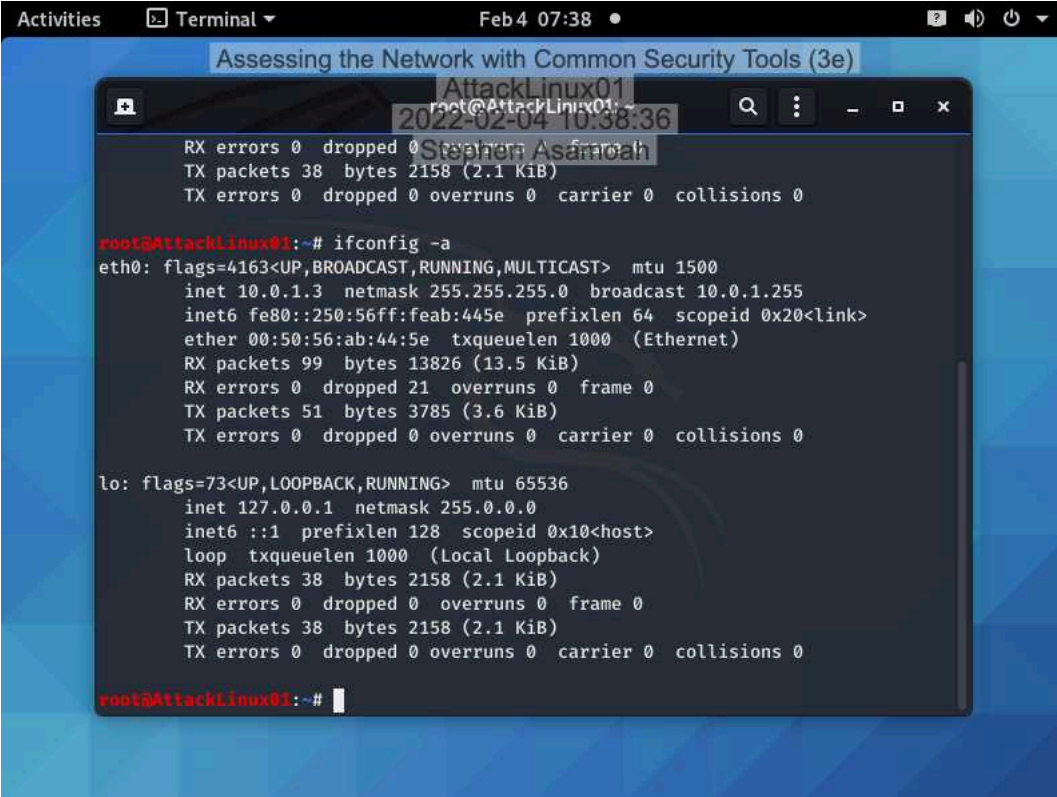
28. **Make a screen capture** showing the contents of the Ports/Hosts tab.



Section 2: Applied Learning

Part 1: Explore the Wide Area Network

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



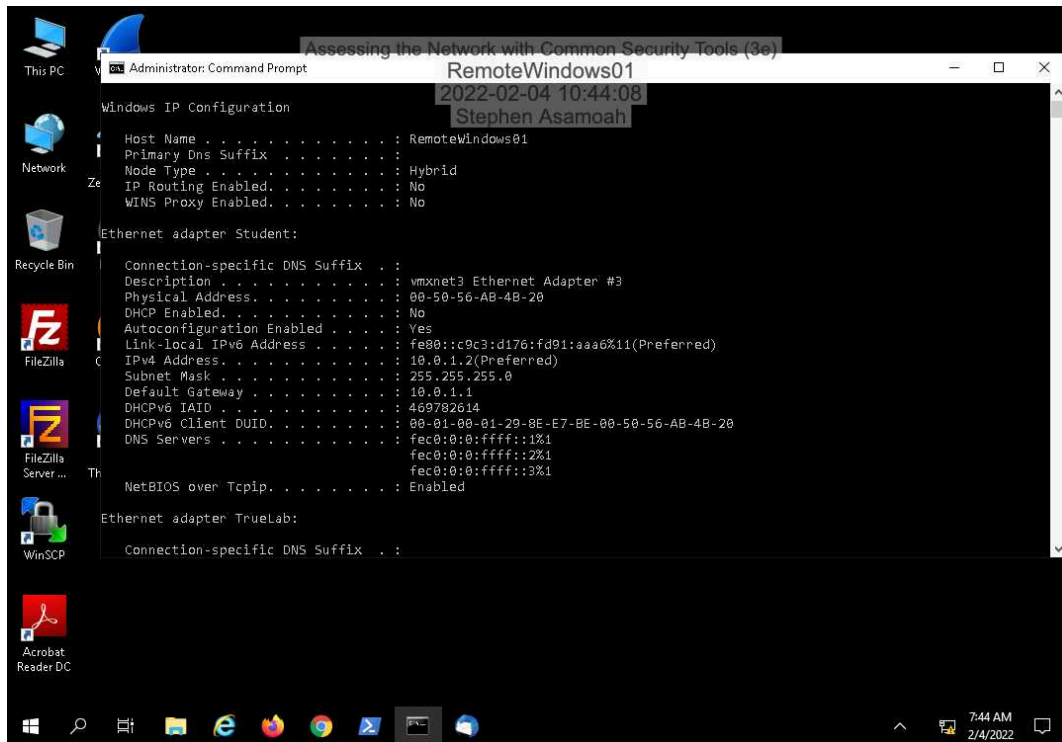
The screenshot shows a terminal window titled "Terminal" with a date and time of "Feb 4 07:38". The terminal output displays the results of the `ifconfig -a` command. The output is as follows:

```
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:feab:445e prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:44:5e txqueuelen 1000 (Ethernet)
    RX packets 99 bytes 13826 (13.5 KiB)
    RX errors 0 dropped 21 overruns 0 frame 0
    TX packets 51 bytes 3785 (3.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

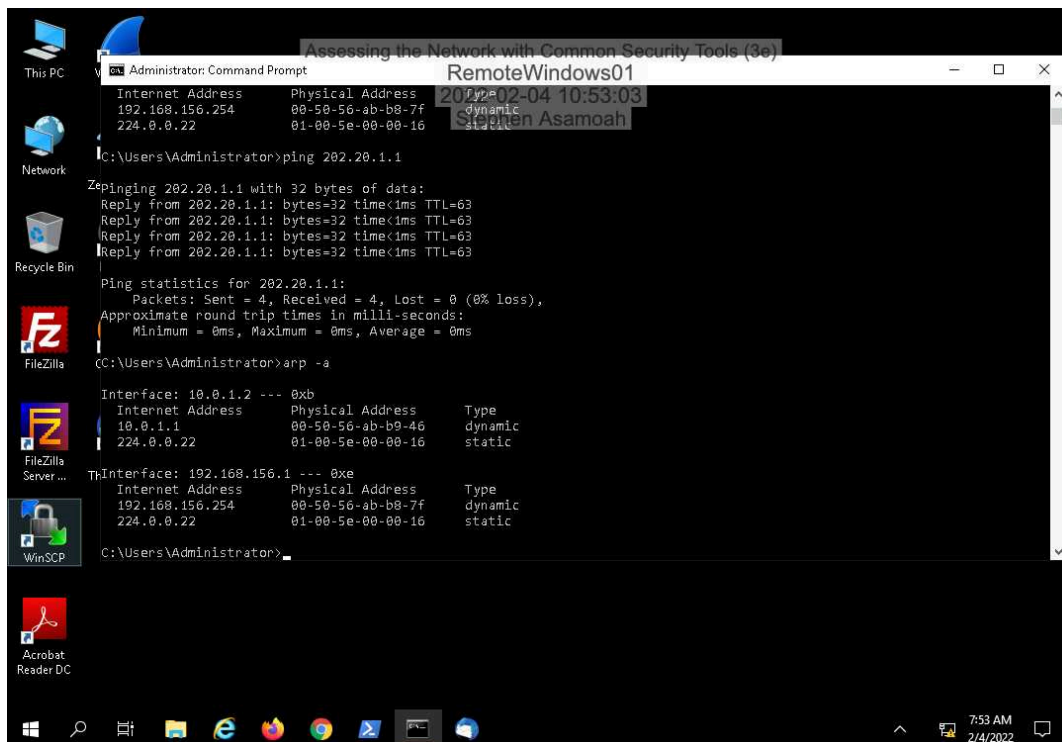
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 38 bytes 2158 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 38 bytes 2158 (2.1 KiB)
    TX errors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

root@AttackLinux01:~#
```


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



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



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**.

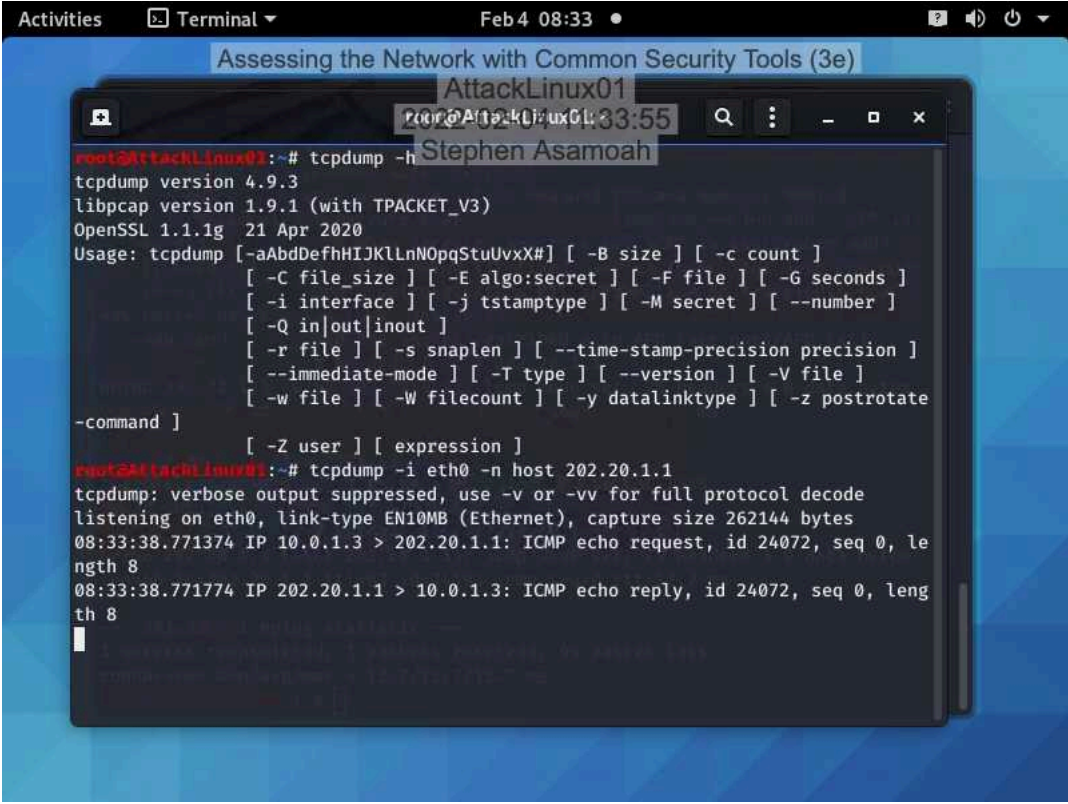
The screenshot displays the OpenOffice Calc application window titled "NetworkAssessment.ods - OpenOffice Calc". The spreadsheet is titled "Assessing the Network with Common Security Tools (3e)" and is the second sheet in the workbook, labeled "WAN". The spreadsheet contains a table with the following data:

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
AttackLinux01	10.0.1.3	255.255.255.0	00:50:56:ab:44:5e	10.0.1.1
RemoteWindows01	10.0.1.2	255.255.255.0	00:50:56:AB:4B:20	10.0.1.1

The spreadsheet is open in the "vWorkstation" environment. The status bar at the bottom indicates "Sheet 2 / 3", "Default", "STD", and "Sum=0". The system tray shows the time as 8:05 AM on 2/4/2022.

Part 2: Analyze Network Traffic

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



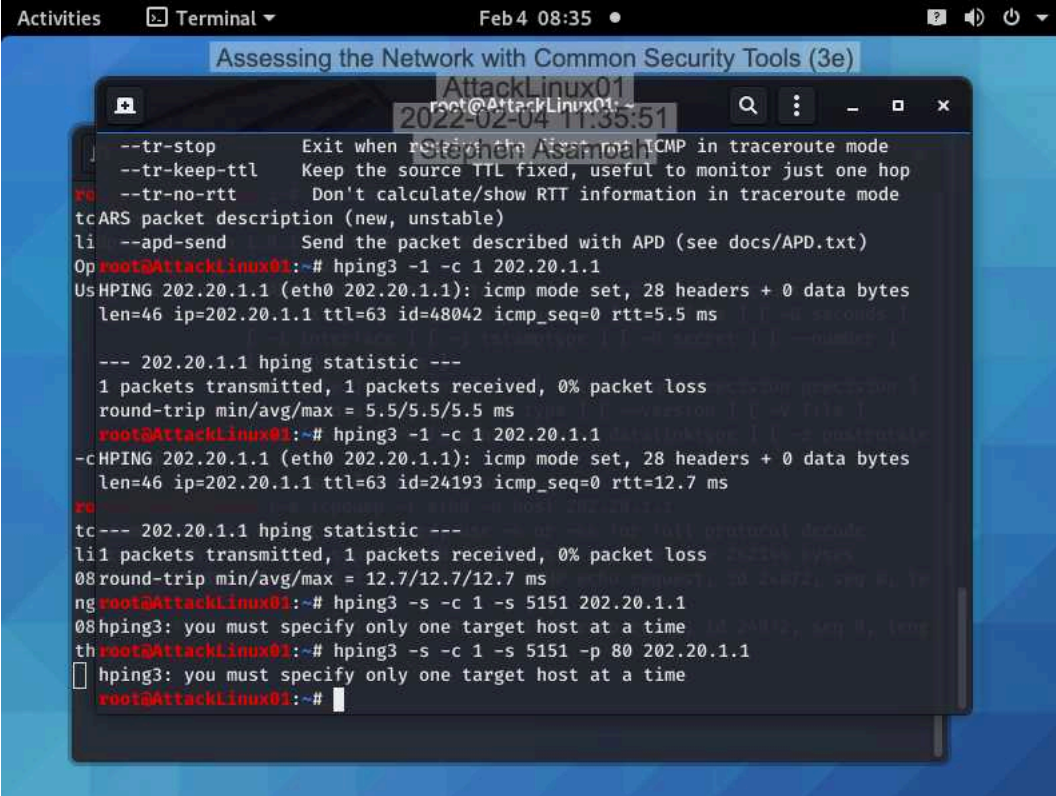
The screenshot shows a terminal window titled "Terminal" with a date and time of "Feb 4 08:33". The terminal is running on a system named "AttackLinux01". The user has entered the command `tcpdump -h`, which displays the usage and options for the `tcpdump` tool. The output shows the version (4.9.3), the libpcap version (1.9.1), and the OpenSSL version (1.1.1g). The usage text lists various options for specifying capture parameters. The user then enters the command `tcpdump -i eth0 -n host 202.20.1.1`, which starts a live capture on the `eth0` interface, listening for traffic to or from the host `202.20.1.1`. The terminal output shows the capture size (262144 bytes) and the link type (EN10MB Ethernet). The first two packets captured are an ICMP echo request from `10.0.1.3` to `202.20.1.1` at `08:33:38.771374`, and an ICMP echo reply from `202.20.1.1` to `10.0.1.3` at `08:33:38.771774`. Both packets have an ID of 24072 and a sequence number of 0.

```
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 [-aAbdDefhHIJKLLnOpqStuUvxxX#] [-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
08:33:38.771374 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 24072, seq 0, le
ngth 8
08:33:38.771774 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 24072, seq 0, leng
th 8
```

Assessing the Network with Common Security Tools (3e)

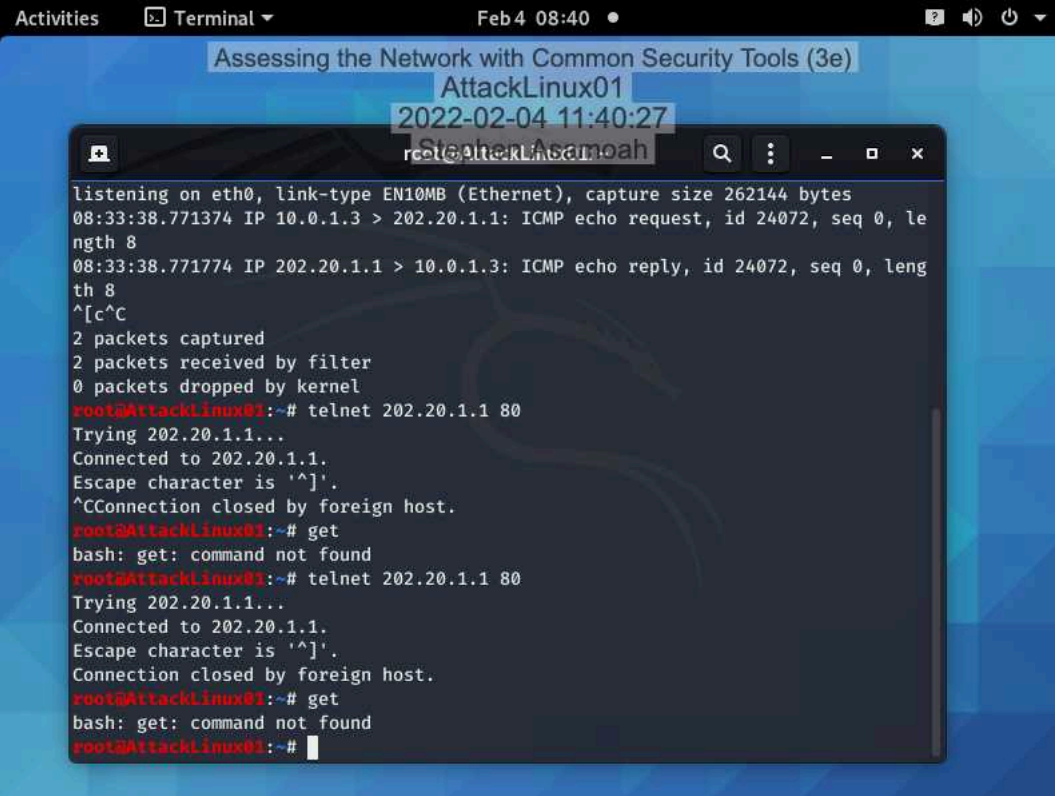
Network Security, Firewalls, and VPNs, Third Edition - Lab 01

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

A screenshot of a Linux terminal window titled "AttackLinux01" with a timestamp of "2022-02-04 11:35:51". The terminal shows the output of the 'hping3' command. It lists various options like --tr-stop, --tr-keep-ttl, --tr-no-rtt, --apd-send, and --tr-keep-ttl. Then, it shows the execution of 'hping3 -1 -c 1 202.20.1.1', which results in an ICMP echo request being sent to 202.20.1.1. The output shows the packet details: 'len=46 ip=202.20.1.1 ttl=63 id=48042 icmp_seq=0 rtt=5.5 ms'. It then shows the hping3 statistics: '1 packets transmitted, 1 packets received, 0% packet loss round-trip min/avg/max = 5.5/5.5/5.5 ms'. Finally, it shows the execution of 'hping3 -s -c 1 -s 5151 202.20.1.1', which results in an error message: 'hping3: you must specify only one target host at a time'.

```
Activities Terminal Feb 4 08:35
Assessing the Network with Common Security Tools (3e)
AttackLinux01
root@AttackLinux01:~# hping3 --tr-stop Exit when receiving the first non-ICMP in traceroute mode
--tr-keep-ttl Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt Don't calculate/show RTT information in traceroute mode
tcARS packet description (new, unstable)
li --apd-send Send the packet described with APD (see docs/APD.txt)
Op root@AttackLinux01:~# hping3 -1 -c 1 202.20.1.1
UsHPING 202.20.1.1 (eth0 202.20.1.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=202.20.1.1 ttl=63 id=48042 icmp_seq=0 rtt=5.5 ms
--- 202.20.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.5/5.5/5.5 ms
root@AttackLinux01:~# hping3 -1 -c 1 202.20.1.1
HPING 202.20.1.1 (eth0 202.20.1.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=202.20.1.1 ttl=63 id=24193 icmp_seq=0 rtt=12.7 ms
--- 202.20.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.7/12.7/12.7 ms
root@AttackLinux01:~# hping3 -s -c 1 -s 5151 202.20.1.1
hping3: you must specify only one target host at a time
root@AttackLinux01:~# hping3 -s -c 1 -s 5151 -p 80 202.20.1.1
hping3: you must specify only one target host at a time
root@AttackLinux01:~#
```

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



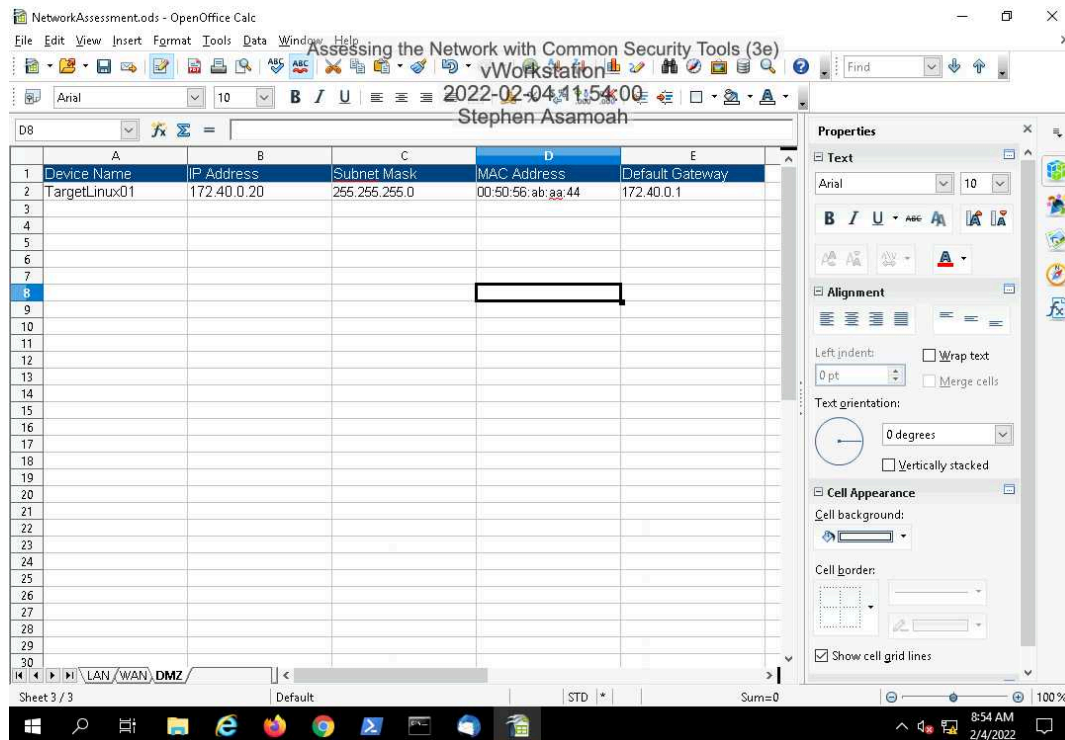
The screenshot shows a terminal window titled "AttackLinux01" with a timestamp of "2022-02-04 11:40:27". The user is logged in as root. The terminal displays the output of a packet capture on eth0, showing an ICMP echo request from 10.0.1.3 to 202.20.1.1 and its corresponding reply. Subsequently, the user runs a telnet command to connect to 202.20.1.1 on port 80. The connection is established, but the user's attempt to run the 'get' command results in a "bash: get: command not found" error. The connection is then closed by the foreign host. The user repeats the telnet connection and command execution, again receiving the "command not found" error.

```
Activities Terminal Feb 4 08:40
Assessing the Network with Common Security Tools (3e)
AttackLinux01
2022-02-04 11:40:27
root@AttackLinux01:~#
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
08:33:38.771374 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 24072, seq 0, length 8
08:33:38.771774 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 24072, seq 0, length 8
^[c^C
2 packets captured
2 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 '^]'.
^CConnection closed by foreign host.
root@AttackLinux01:~# get
bash: get: command not found
root@AttackLinux01:~# telnet 202.20.1.1 80
Trying 202.20.1.1...
Connected to 202.20.1.1.
Escape character is '^]'.
Connection closed by foreign host.
root@AttackLinux01:~# get
bash: get: command not found
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.

Received 8 ICMP packets, 28 ARP packets and 153 DNS packets. Total packet captured is 2190 with no drop. Port 22(ssh) and 80 (Http) are the only open ports on the pfSense firewall