

Assessing the Network with Common Security Tools (3e)

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

Student:

Vidhi Kadakia

Email:

jinsukrishna108@gmail.com

Time on Task:

4 hours, 3 minutes

Progress:

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**.

Assessing the Network with Common Security Tools (3e)

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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.121]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter TrueLab:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.132.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.132.254

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>
```

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

Assessing the Network with Common Security Tools (3e)

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

```
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 TrueLab:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.132.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.132.254

Ethernet adapter Student:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f142:2a28:ed77:9395%5
    IPv4 Address. . . . . : 172.30.0.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.30.0.1

C:\Users\Administrator>
```

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

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

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>
```

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.

NetworkAssessment.xls - OpenOffice Calc

Assessing the Network with Common Security Tools (3e)

2025-10-19 16:37:17

Vidhi-Kadakia

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
vboxnet0	172.30.0.2	255.255.255.0	00:60:60:ae:0e:03	172.30.0.1
TargetWindows01	172.30.0.10	255.255.255.0	00:60:60:ae:0e:46	172.30.0.1
vmxnet3	172.30.0.1	255.255.255.0	00:60:60:bd:ad:4e	

Properties

Text

Align

Alignment

Left indent: 0 pt

Text orientation: 0 degrees

Cell Appearance

Cell background: Default

Cell border: Default

Show cell grid lines: ☒

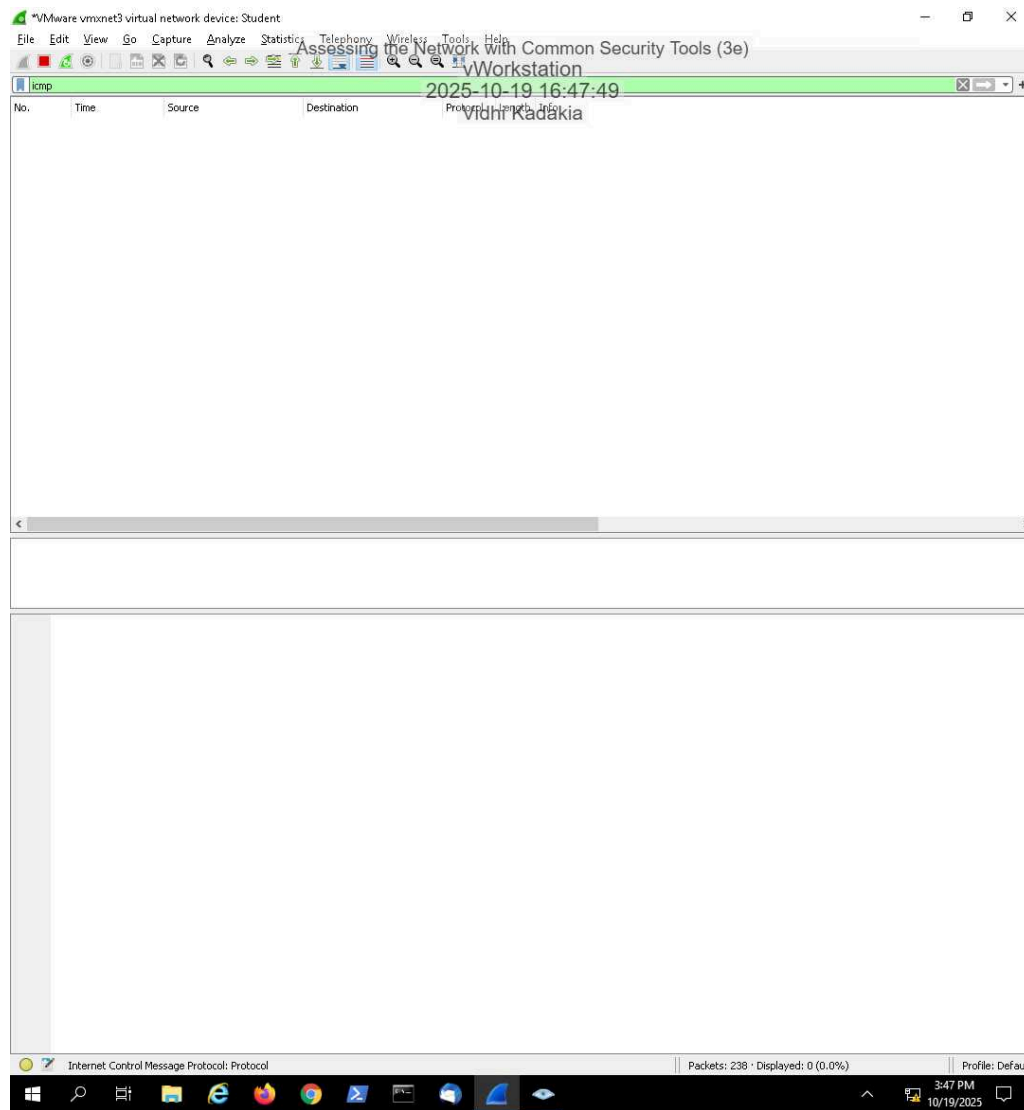
Number Format

Part 2: Analyze Network Traffic

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

Assessing the Network with Common Security Tools (3e)

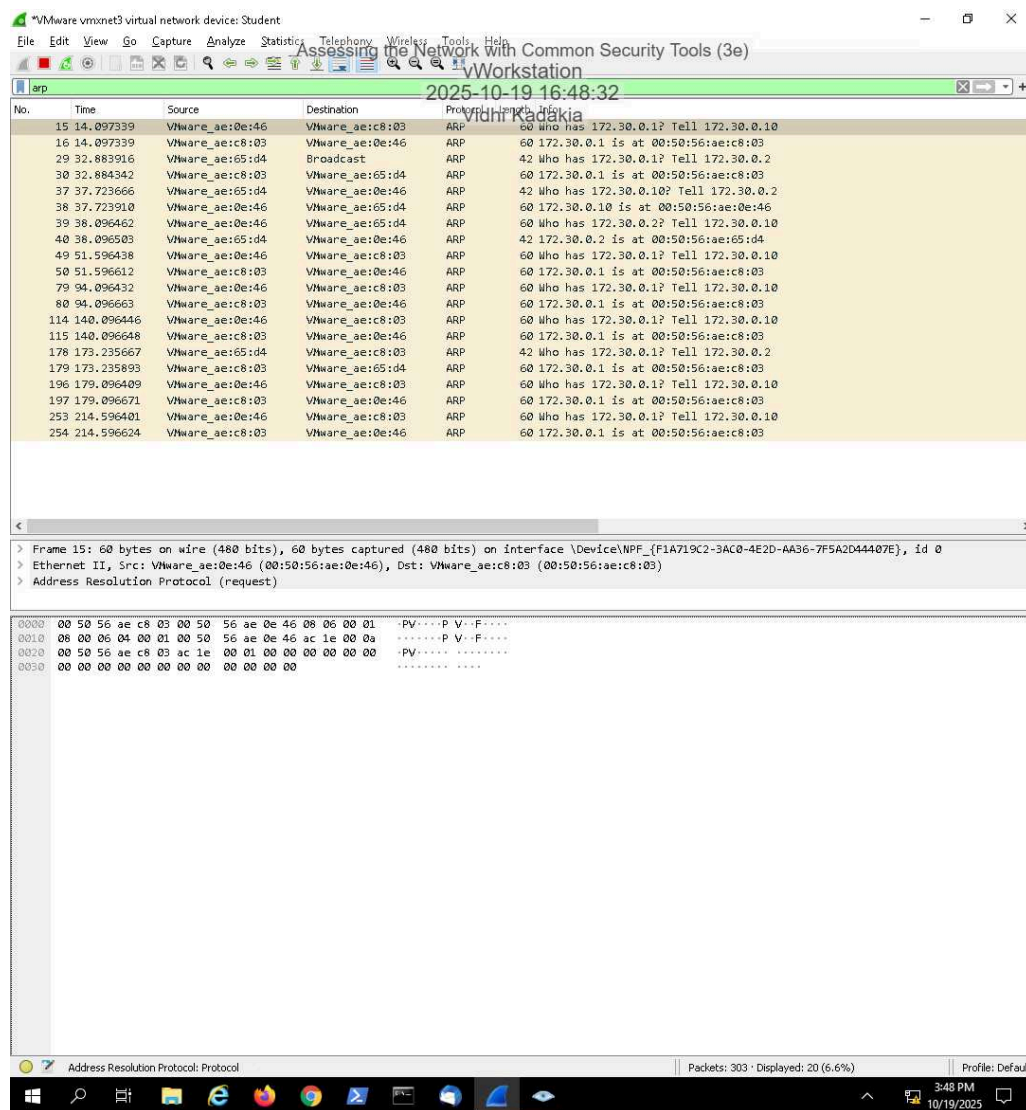
Network Security, Firewalls, and VPNs, Third Edition - Lab 01



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

Assessing the Network with Common Security Tools (3e)

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



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.

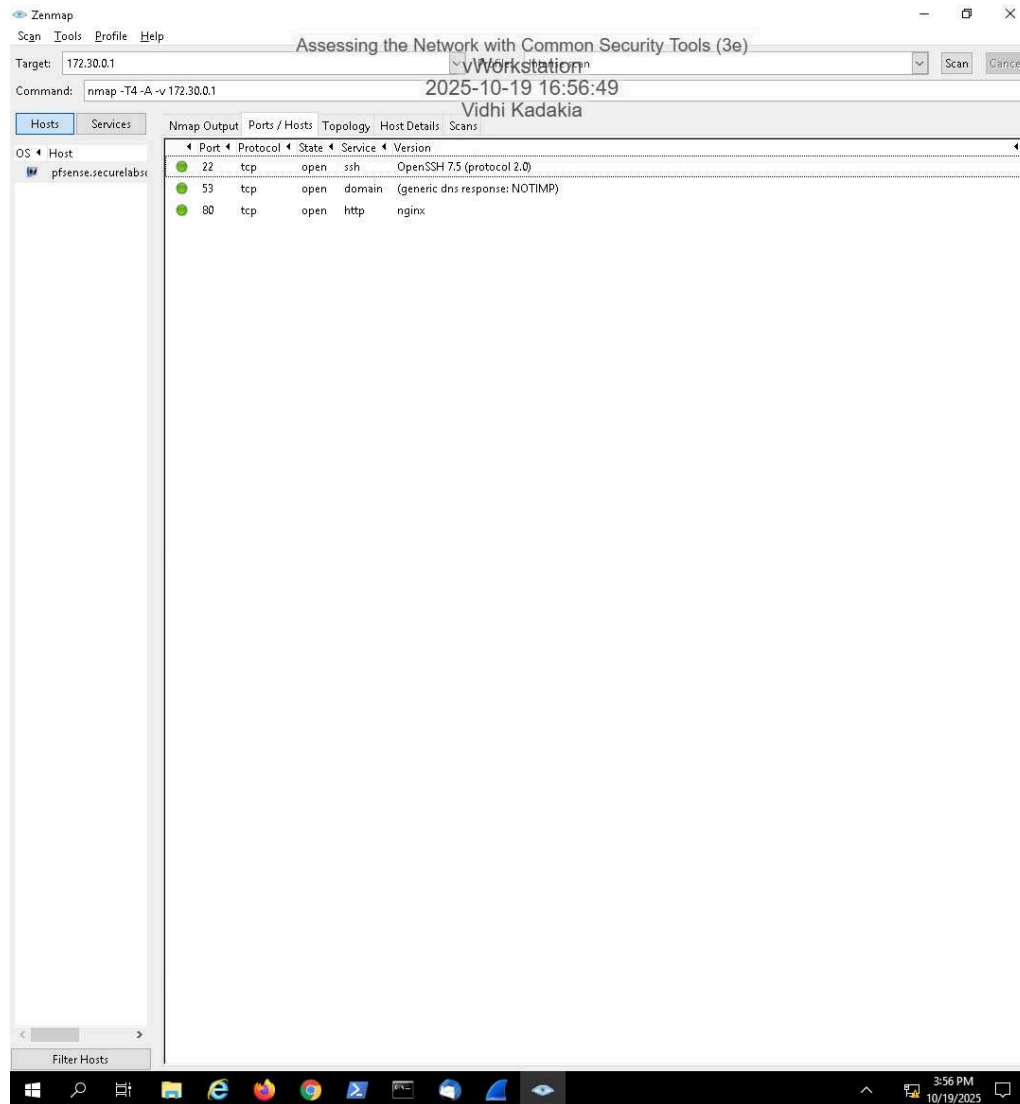
24. **Compare** the Intense scan results with the results from the Ping scan.

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.

Assessing the Network with Common Security Tools (3e)

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

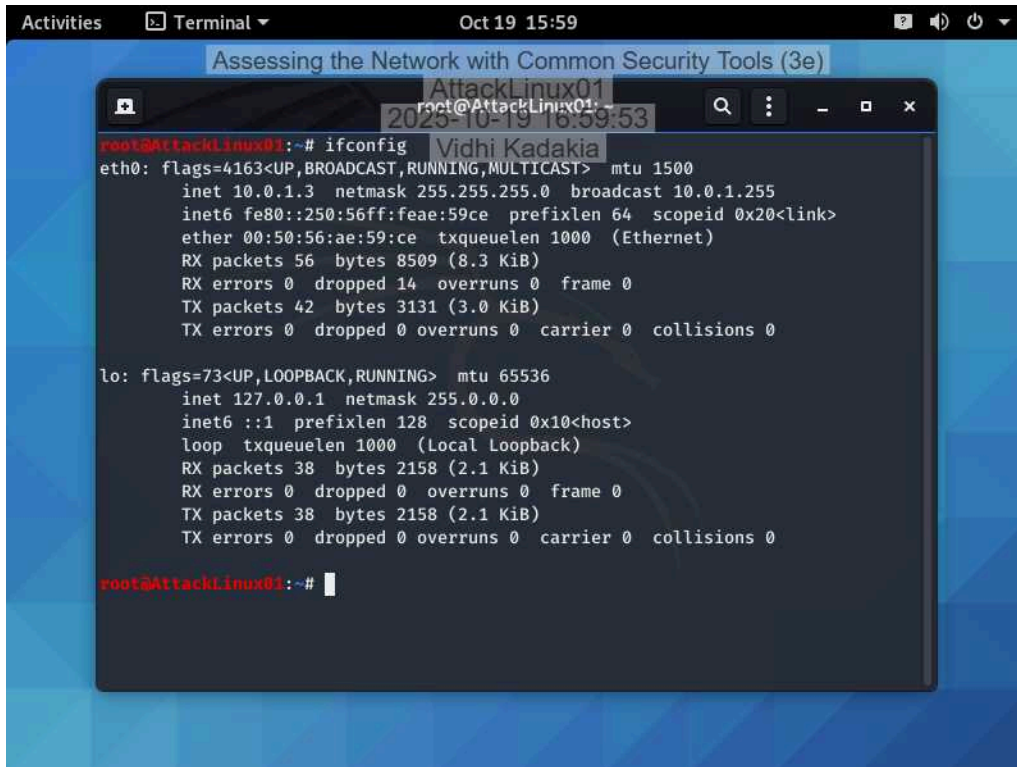
28. Make a screen capture showing the contents of the Ports/Hosts tab.



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 "Oct 19 15:59". The terminal is running the `ifconfig` command on the `AttackLinux01` machine. The output displays the configuration for the `eth0` and `lo` interfaces. The `eth0` interface is configured with IP address `10.0.1.3`, netmask `255.255.255.0`, and broadcast address `10.0.1.255`. The `lo` interface is configured with IP address `127.0.0.1` and netmask `255.0.0.0`. The terminal window also shows the user `root` and the machine name `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::250:56ff:feae:59ce prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ae:59:ce txqueuelen 1000 (Ethernet)
    RX packets 56 bytes 8509 (8.3 KiB)
    RX errors 0 dropped 14 overruns 0 frame 0
    TX packets 42 bytes 3131 (3.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

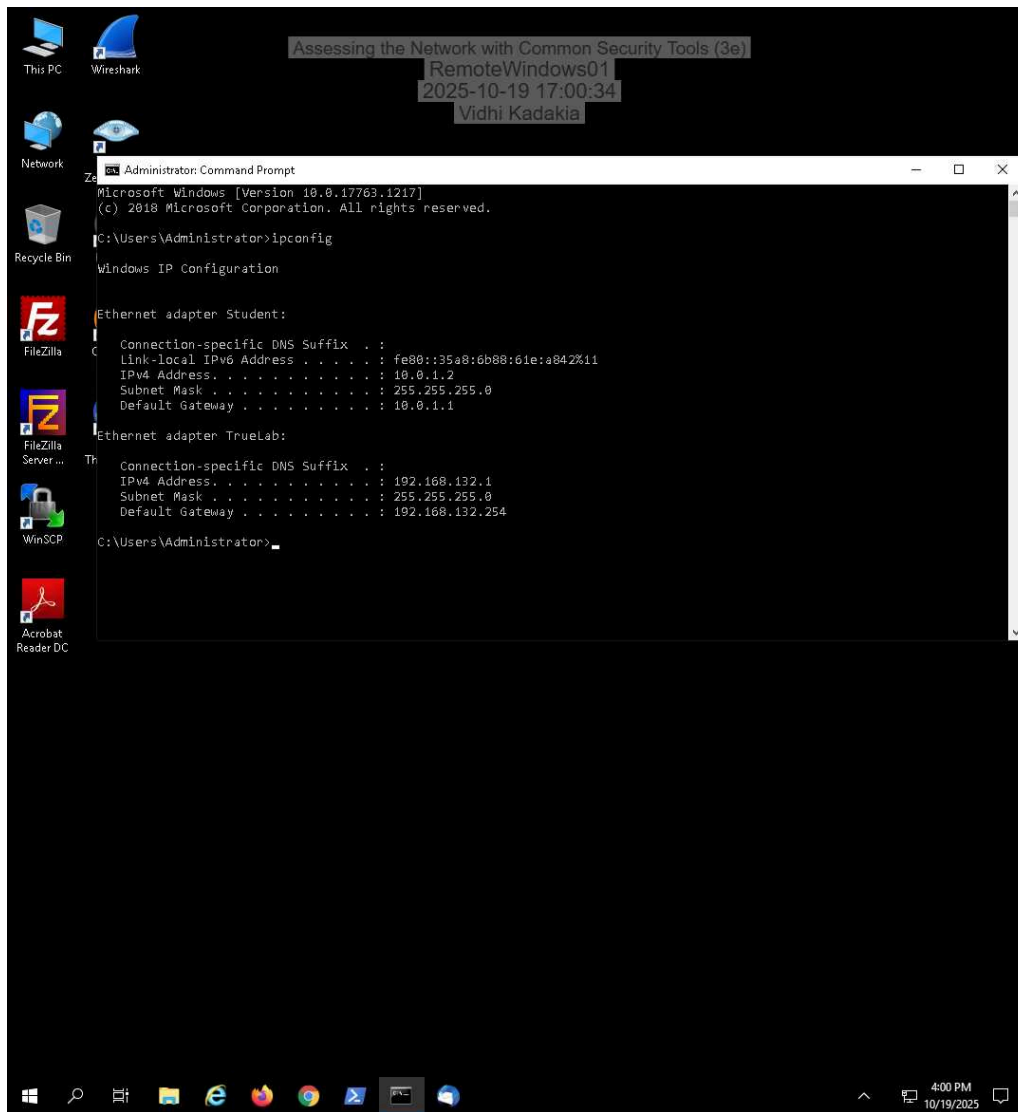
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 38 bytes 2158 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 38 bytes 2158 (2.1 KiB)
    TX errors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

root@AttackLinux01:~#
```

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

Assessing the Network with Common Security Tools (3e)

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



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

```
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 --- 0xa
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)

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 shows the OpenOffice Calc application window titled "NetworkAssessment.xls - OpenOffice Calc". The spreadsheet is titled "Assessing the Network with Common Security Tools (3e)" and is located in the "vWorkstation" folder. The user is "Vidhi Kadakia". The spreadsheet has a tab labeled "WAN" selected. The data is as follows:

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
AttackLinux01	10.0.1.3	255.255.255.0	00-50-56-ae-59-c8	10.0.1.1
RemoteWindows01	10.0.1.2	255.255.255.0	80-50-56-ae-e1-c4	10.0.1.1
pfSense (WAN)	10.0.1.1	255.255.255.0	80-50-56-ae-e1-c4	-

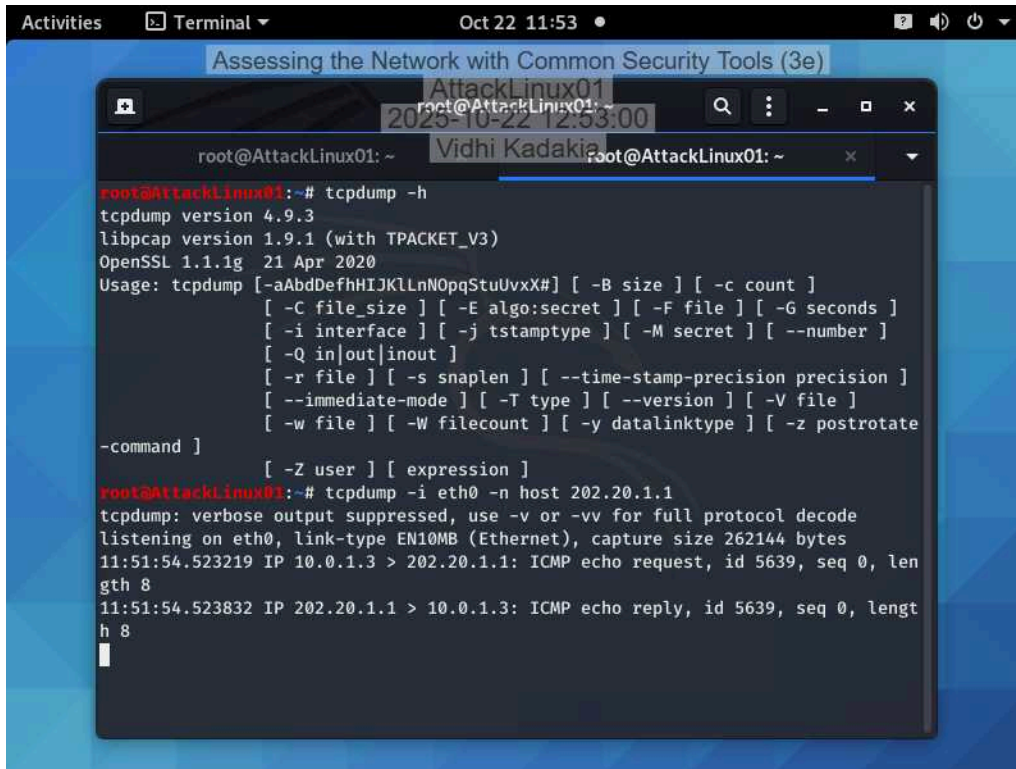
The Properties sidebar on the right shows the Text, Alignment, and Cell Appearance sections. The Text section shows the font is Arial, size 10. The Alignment section shows the text is left-aligned. The Cell Appearance section shows the cell background is white and the cell border is none. The Number Format section is empty.

Part 2: Analyze Network Traffic

Assessing the Network with Common Security Tools (3e)

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

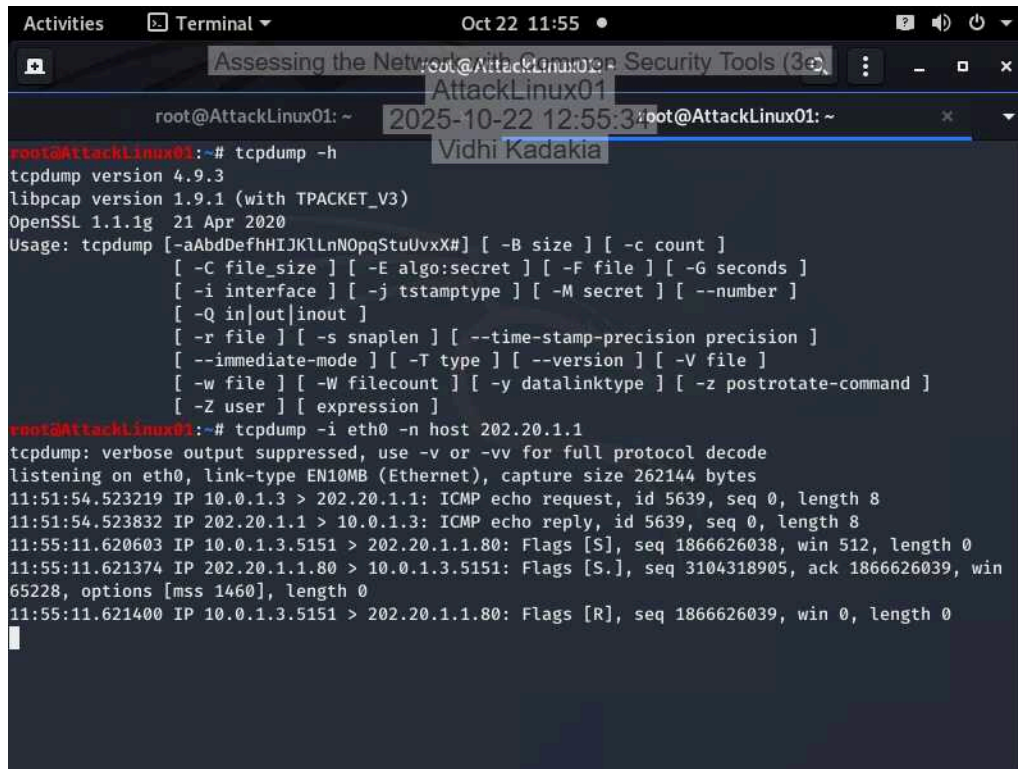
9. Make a screen capture showing **tcpdump** echo back the captured packets.



The screenshot shows a terminal window titled "Assessing the Network with Common Security Tools (3e)" with a subtitle "AttackLinux01". The terminal output shows the help for tcpdump, followed by a command to capture ICMP echo requests from 10.0.1.3 on interface eth0. The output shows two packets: an ICMP echo request from 10.0.1.3 to 202.20.1.1 and an ICMP echo reply from 202.20.1.1 to 10.0.1.3.

```
root@AttackLinux01: ~  
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 [-aAbDefhHIJKLlnNOpqStuUvVxX#] [-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  
11:51:54.523219 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 5639, seq 0, len  
gth 8  
11:51:54.523832 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 5639, seq 0, lengt  
h 8  
[
```

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

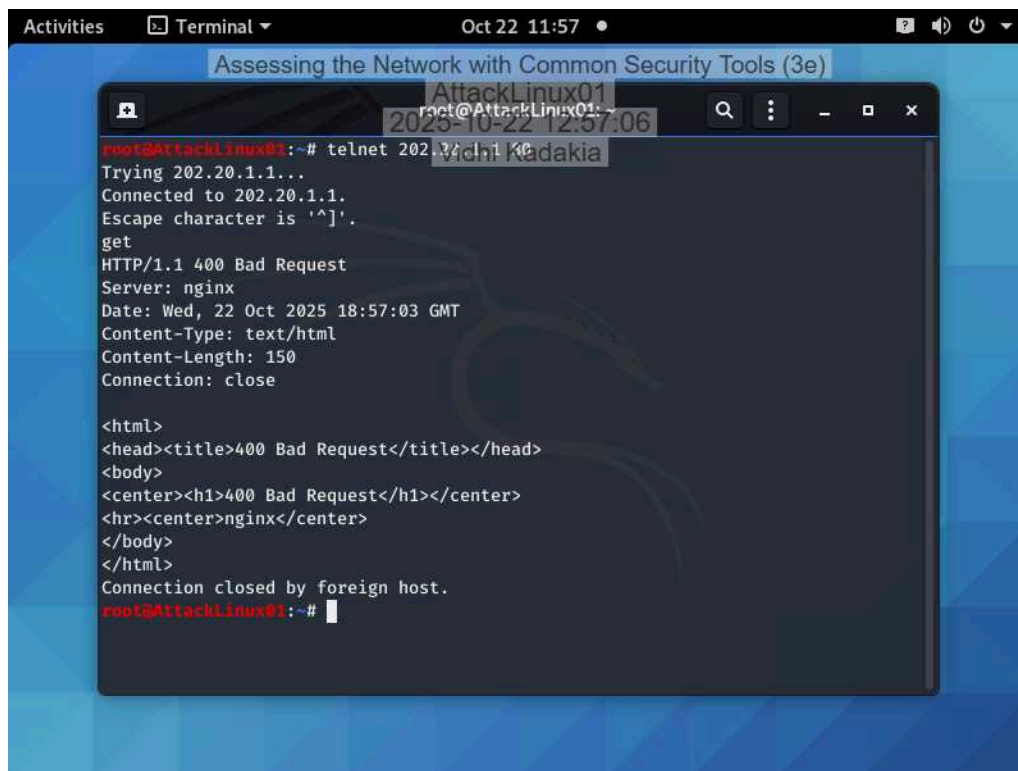


A terminal window titled "Assessing the Network with Common Security Tools (3e)" on a system named "AttackLinux01". The user "root" has executed the command `tcpdump -h`, displaying the help text for tcpdump version 4.9.3. Then, the user has executed `tcpdump -i eth0 -n host 202.20.1.1`. The output shows several network packets, including ICMP echo requests and replies, and a TCP SYN packet from 10.0.1.3 to 202.20.1.1:80, indicating an attempted three-way handshake.

```
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
11:51:54.523219 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 5639, seq 0, length 8
11:51:54.523832 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 5639, seq 0, length 8
11:55:11.620603 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [S], seq 1866626038, win 512, length 0
11:55:11.621374 IP 202.20.1.1.80 > 10.0.1.3.5151: Flags [S.], seq 3104318905, ack 1866626039, win 65228, options [mss 1460], length 0
11:55:11.621400 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [R], seq 1866626039, win 0, length 0
```

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



A terminal window titled "Assessing the Network with Common Security Tools (3e)" on a system named "AttackLinux01". The user "root" has executed the command `telnet 202.20.1.1 80`. The output shows a successful connection to 202.20.1.1 on port 80. The user then enters the command `get`, which results in a "400 Bad Request" response from the nginx server. The response includes headers like "Server: nginx", "Date: Wed, 22 Oct 2025 18:57:03 GMT", "Content-Type: text/html", and "Content-Length: 150". The body of the response is an HTML document with a title "400 Bad Request" and a message "400 Bad Request" from nginx. The connection is then closed by the 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: Wed, 22 Oct 2025 18:57:03 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:~#
```


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.