

Assessing the Network with Common Security Tools (4e)

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

Student:

Shoumya Rayamajhi

Email:

sxr230169@utdallas.edu

Time on Task:

4 hours, 0 minutes

Progress:

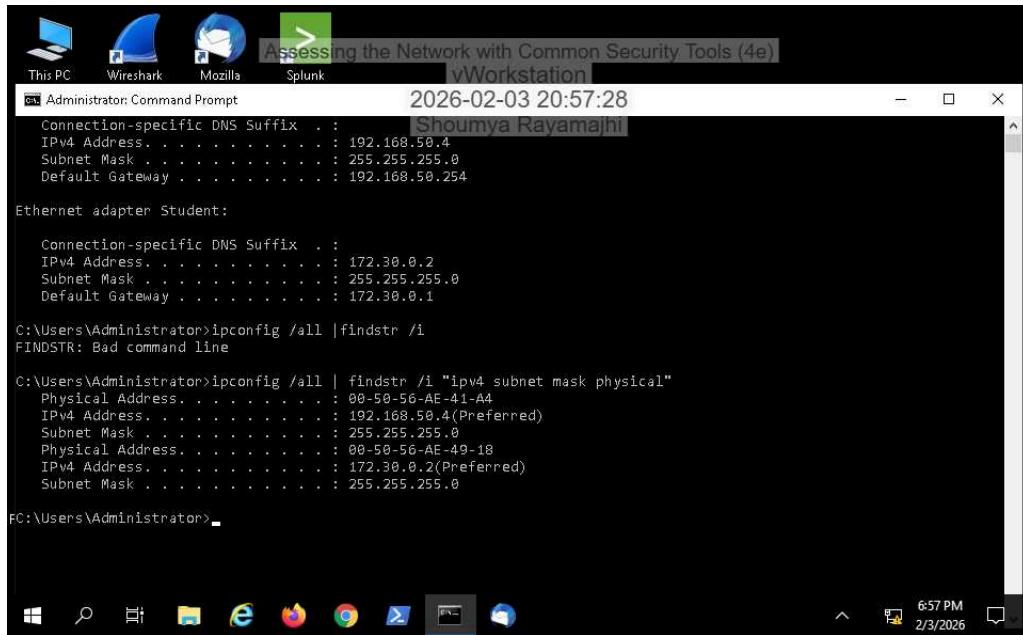
100%

Report Generated: Sunday, February 22, 2026 at 12:23 AM

Hands-On Demonstration

Part 1: Exploring the LAN with Basic Network Utilities

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



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window displays the output of the ipconfig command, specifically focusing on the "Student" network adapter. The adapter has an IPv4 address of 172.30.0.2, a subnet mask of 255.255.255.0, and a default gateway of 172.30.0.1. The prompt shows that a command was entered to filter the results for the physical layer, but it failed ("FINDSTR: Bad command line"). The Command Prompt window is set against a dark background with a light gray title bar. The desktop icons visible include This PC, Wireshark, Mozilla, and Splunk. The taskbar at the bottom shows various open applications like File Explorer, Edge, and a file manager. The system tray indicates the date as 2/3/2026 and the time as 6:57 PM.

```
Administrator: Command Prompt
2026-02-03 20:57:28
Connection-specific DNS Suffix . : Shoumya Rayamajhi
IPv4 Address. . . . . : 192.168.50.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.50.254

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>ipconfig /all | findstr /i
FINDSTR: Bad command line

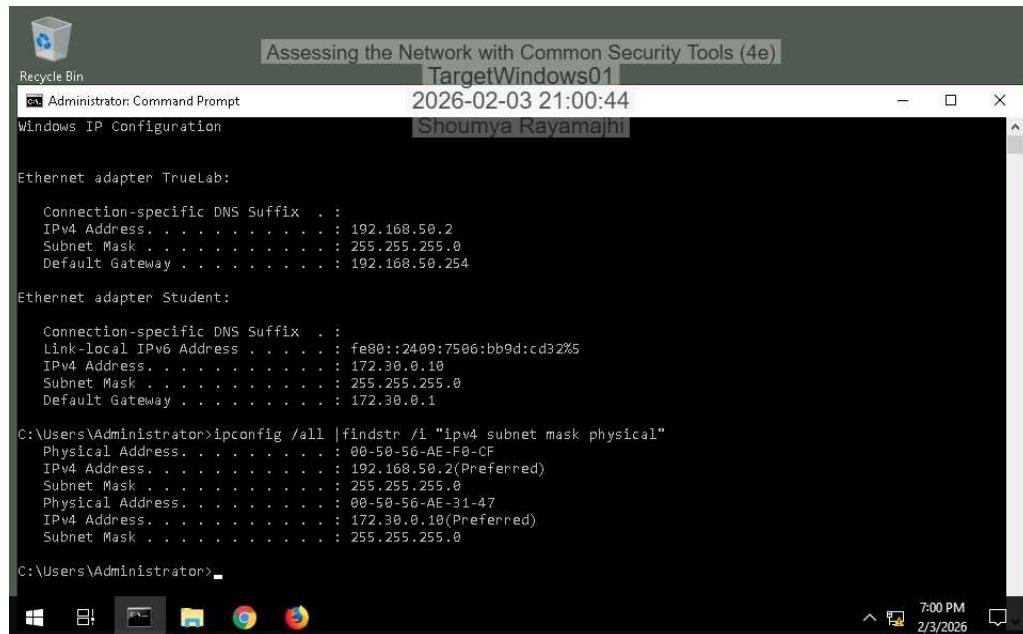
C:\Users\Administrator>ipconfig /all | findstr /i "ipv4 subnet mask physical"
Physical Address. . . . . : 00-50-56-AE-41-A4
IPv4 Address. . . . . : 192.168.50.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Physical Address. . . . . : 00-50-56-AE-49-18
IPv4 Address. . . . . : 172.30.0.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0

C:\Users\Administrator>
```

Assessing the Network with Common Security Tools (4e)

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

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



```
Assessing the Network with Common Security Tools (4e)
TargetWindows01
Administrator: Command Prompt
2026-02-03 21:00:44
Shoumya Rayamajhi

Windows IP Configuration

Ethernet adapter TrueLab:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 192.168.50.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.50.254

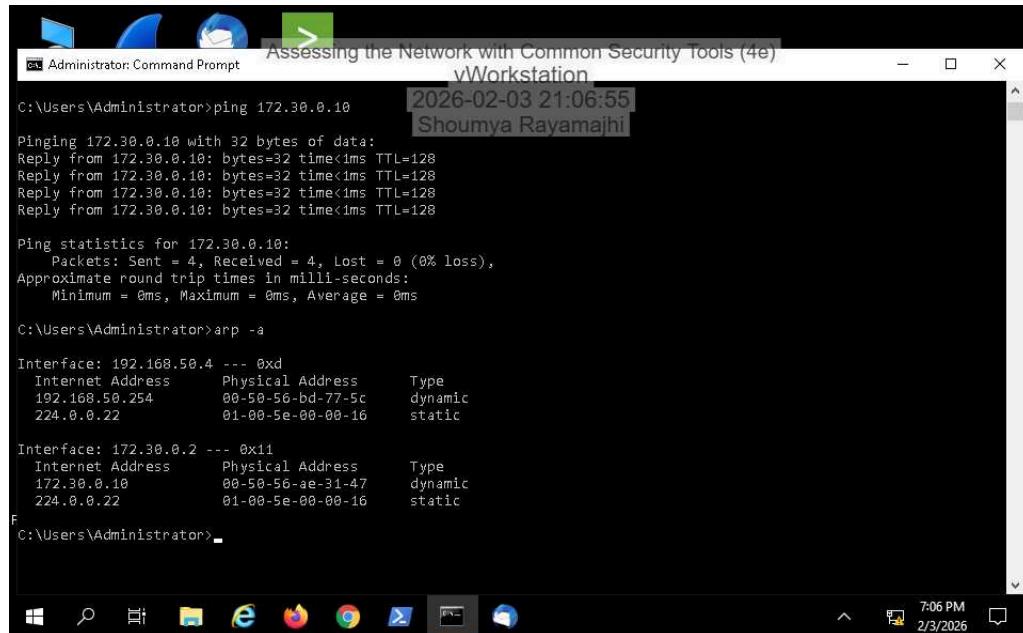
Ethernet adapter Student:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . : fe80::2409:7506:bb9d:cd32%5
IPv4 Address . . . . . : 172.30.0.10
Subnet Mask . . . . . : 255.255.255.0
Physical Address . . . . . : 00-50-56-AE-31-47
IPv4 Address . . . . . : 172.30.0.10(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0

C:\Users\Administrator>ipconfig /all |findstr /i "ipv4 subnet mask physical"
Physical Address . . . . . : 00-50-56-AE-F0-CF
IPv4 Address . . . . . : 192.168.50.2(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Physical Address . . . . . : 00-50-56-AE-31-47
IPv4 Address . . . . . : 172.30.0.10(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0

C:\Users\Administrator>
```

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



```
Assessing the Network with Common Security Tools (4e)
v\Workstation
Administrator: Command Prompt
2026-02-03 21:06:55
Shoumya Rayamajhi

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

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: 192.168.50.4 --- 0xd
    Internet Address      Physical Address      Type
    192.168.50.254        00-50-56-bd-77-5c    dynamic
    224.0.0.22             01-00-5e-00-00-16    static

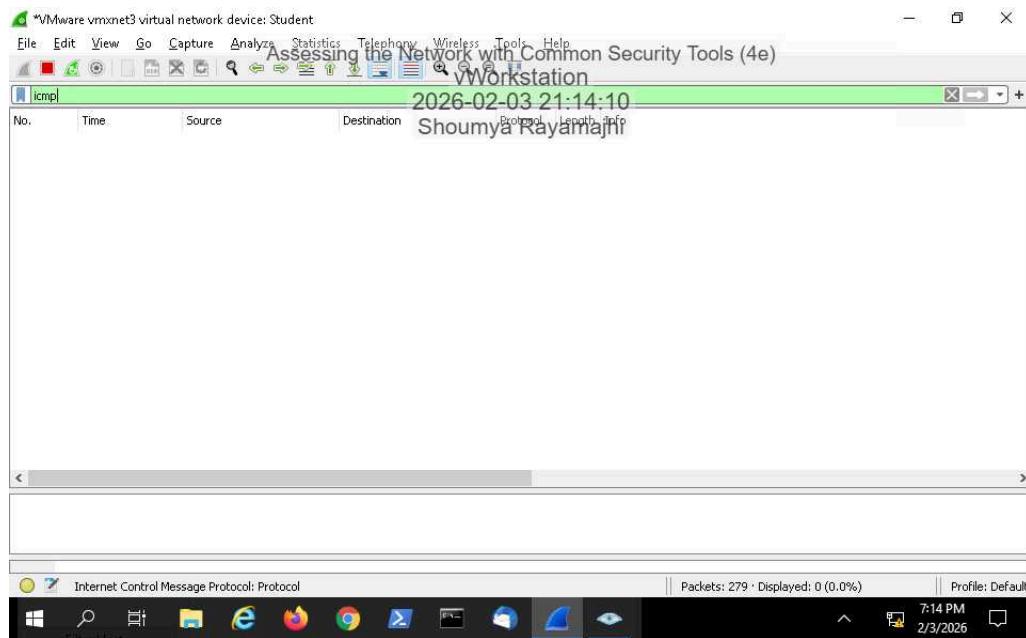
Interface: 172.30.0.2 --- 0x11
    Internet Address      Physical Address      Type
    172.30.0.10            00-50-56-ae-31-47    dynamic
    224.0.0.22             01-00-5e-00-00-16    static
F
C:\Users\Administrator>
```

Part 2: Advanced LAN Analysis with Wireshark and Nmap

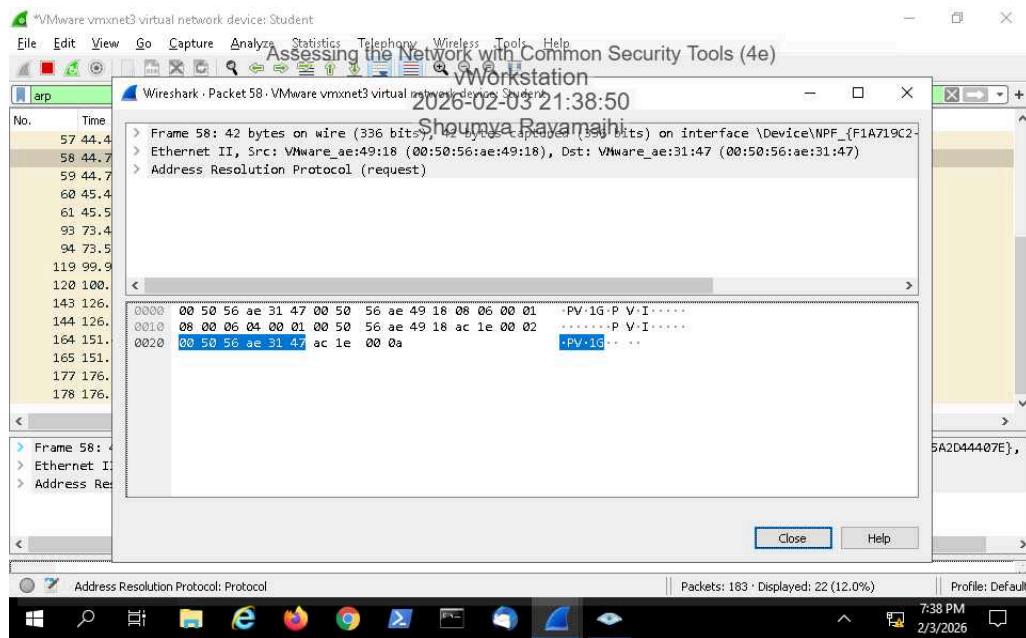
Assessing the Network with Common Security Tools (4e)

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

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



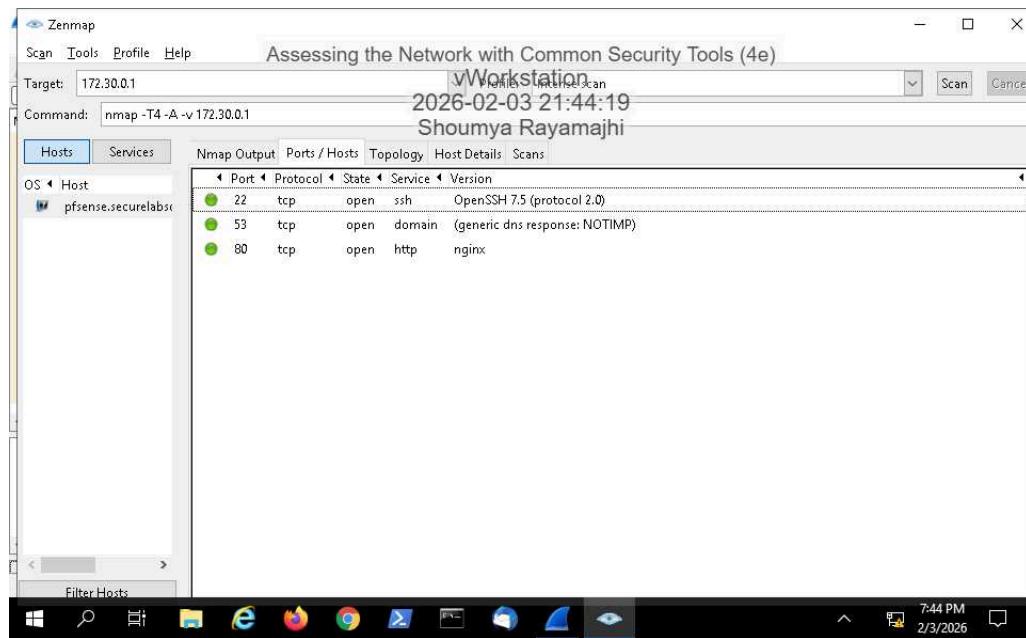
12. Make a screen capture showing the ARP filtered results in Wireshark.



Assessing the Network with Common Security Tools (4e)

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

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



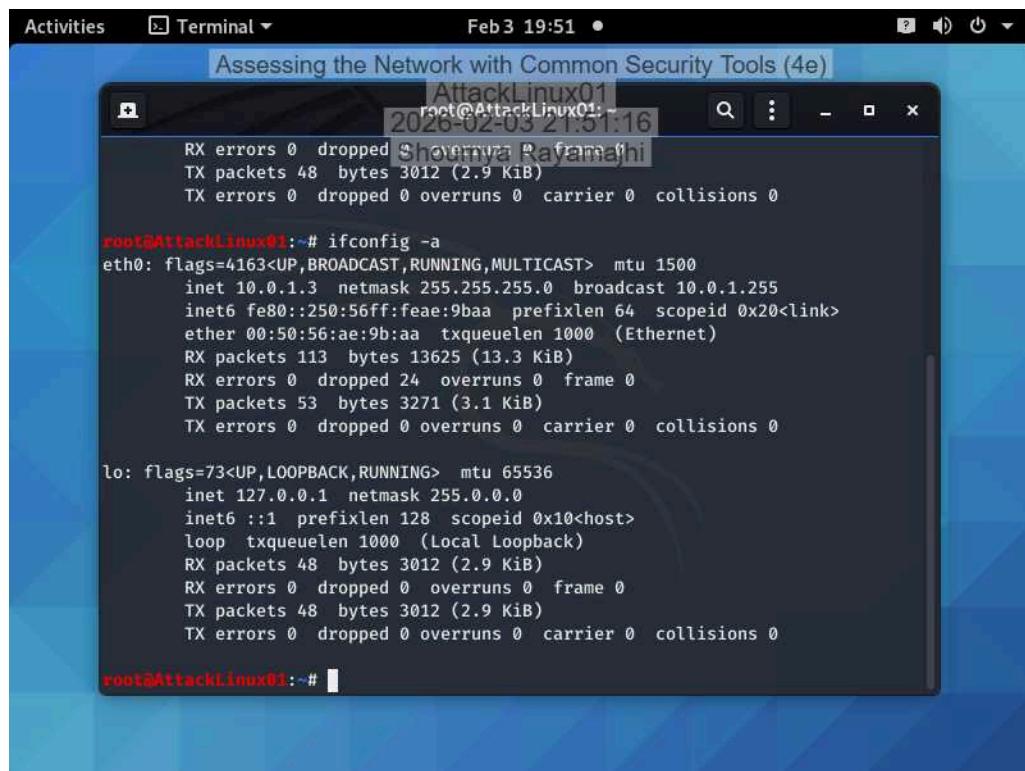
Assessing the Network with Common Security Tools (4e)

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

Applied Learning

Part 1: Exploring the WAN

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



The screenshot shows a terminal window on a Linux desktop environment. The title bar of the window reads "Assessing the Network with Common Security Tools (4e)". The window content displays the output of the "ifconfig -a" command run by root on the interface "AttackLinux01". The output shows two interfaces: "eth0" and "lo".

```
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:9baa prefixlen 64 scopeid 0x20<link>
              ether 00:50:56:ae:9b:aa txqueuelen 1000 (Ethernet)
                  RX packets 113 bytes 13625 (13.3 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 53 bytes 3271 (3.1 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 48 bytes 3012 (2.9 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 48 bytes 3012 (2.9 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@AttackLinux01:~#
```

Assessing the Network with Common Security Tools (4e)

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

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

```
Assessing the Network with Common Security Tools (4e)
Administrator: Command Prompt
2026-02-03 21:52:52
Shoumya Rayamajhi

Connection-specific DNS Suffix . . . . . : vmxnet3 Ethernet Adapter #3
Description . . . . . : vmxnet3 Ethernet Adapter #3
Physical Address . . . . . : 00-50-56-AE-05-42
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::385e:4536:3c51:432f%11(Preferred)
IPv4 Address . . . . . : 10.0.1.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.1.1
DHCPv6 IAID . . . . . : 469782614
DHCPv6 Client DUID. . . . . : 00-01-00-01-31-14-69-2D-00-50-56-AE-05-42
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 . . . . . : vmxnet3 Ethernet Adapter #2
Physical Address . . . . . : 00-50-56-AE-96-04
DHCP Enabled . . . . . : No
F Autoconfiguration Enabled . . . . . : Yes
IPv4 Address . . . . . : 192.168.50.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.50.254
NetBIOS over Tcpip. . . . . : Disabled
```

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

```
Assessing the Network with Common Security Tools (4e)
Administrator: Command Prompt
2026-02-03 21:56:19
Shoumya Rayamajhi

Internet Address      Physical Address      Type
192.168.50.254        00-50-56-bd-77-5c      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

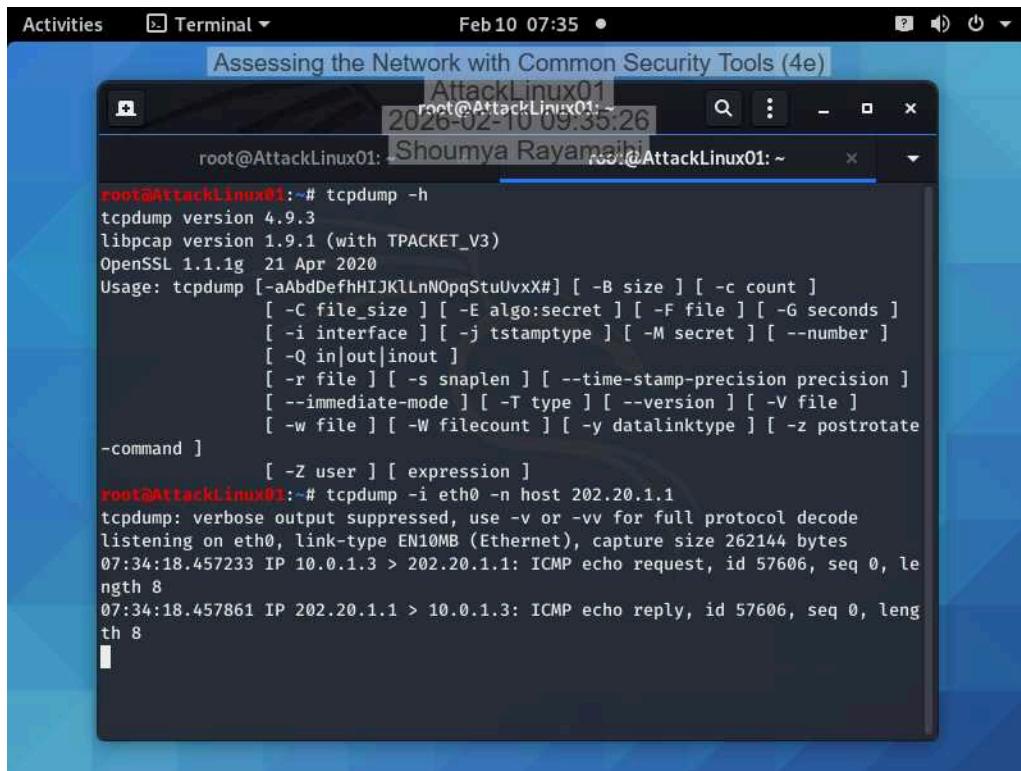
Interface: 10.0.1.2 --- 0xb
Internet Address      Physical Address      Type
10.0.1.1              00-50-56-ae-02-f8      dynamic
224.0.0.22             01-00-5e-00-00-16      static
F Interface: 192.168.50.1 --- 0xe
Internet Address      Physical Address      Type
192.168.50.254        00-50-56-bd-77-5c      dynamic
224.0.0.22             01-00-5e-00-00-16      static
```

Part 2: Advanced WAN Analysis

Assessing the Network with Common Security Tools (4e)

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

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



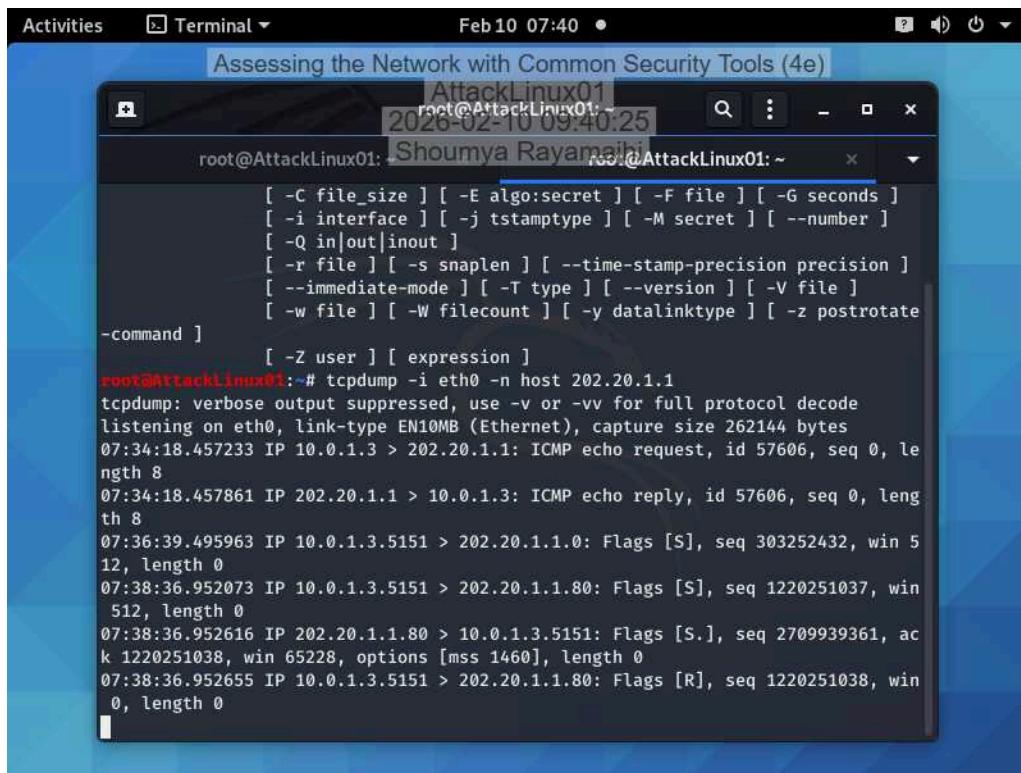
The screenshot shows a terminal window on a Linux system named 'AttackLinux01'. The terminal title bar reads 'Assessing the Network with Common Security Tools (4e)'. The window contains the following text:

```
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 [-aAbdDefhHIJKLnNOpqStuUvxX#] [ -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
07:34:18.457233 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 57606, seq 0, length 8
07:34:18.457861 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 57606, seq 0, length 8
```

Assessing the Network with Common Security Tools (4e)

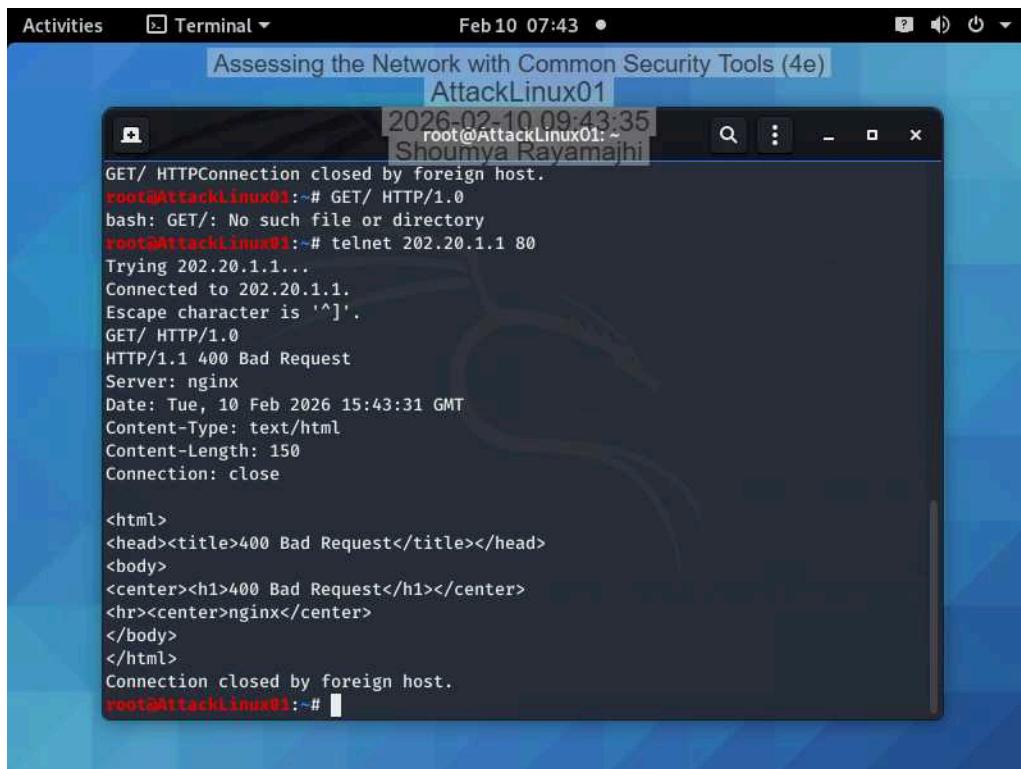
Network Security, Firewalls, and VPNs, Fourth Edition - Lab 01

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



```
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
07:34:18.457233 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 57606, seq 0, length 8
07:34:18.457861 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 57606, seq 0, length 8
07:36:39.495963 IP 10.0.1.3.5151 > 202.20.1.1.0: Flags [S], seq 303252432, win 512, length 0
07:38:36.952073 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [S], seq 1220251037, win 512, length 0
07:38:36.952616 IP 202.20.1.1.80 > 10.0.1.3.5151: Flags [S.], seq 2709939361, ack 1220251038, win 65228, options [mss 1460], length 0
07:38:36.952655 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [R], seq 1220251038, win 0, length 0
```

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



```
root@AttackLinux01:~# GET/ HTTP/1.0
bash: GET/: No such file or directory
root@AttackLinux01:~# telnet 202.20.1.1 80
Trying 202.20.1.1...
Connected to 202.20.1.1.
Escape character is '^]'.
GET/ HTTP/1.0
HTTP/1.1 400 Bad Request
Server: nginx
Date: Tue, 10 Feb 2026 15:43:31 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:~#
```

Assessing the Network with Common Security Tools (4e)

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

Assessing the Network with Common Security Tools (4e)

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

Challenge and Analysis

Part 1

2. Make a screen capture showing the completed DMZ tab of the NetworkAssessment spreadsheet.

The screenshot shows an OpenOffice Calc spreadsheet titled "NetworkAssessmentods - OpenOffice Calc". The spreadsheet has three tabs at the bottom: LAN, WAN, and DMZ. The DMZ tab is selected and contains the following data:

	B	C	D	E
1	IP Address	Subnet Mask	MAC Address	Default Gateway
2	172.40.0.20	255.255.255.0	00:50:56:ae:f9:ea	172.40.0.255
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

5. Briefly summarize your findings in a technical memo to the CISSM (Chief Information Systems Security Manager).

During the regular scan using Zenmap and Wireshark to track the packets, we saw that a ssh port and a tcp ports is open in the firewall (202.20.1.1). ICMP came from 10.0.1.3 and was received by 202.20.1.1. The ARP SRC: VMware_ae:59:88 and dst: VMware_ae:f9:2e. The src for the DNS report came from port 32945 and dst was to port 53