Assessing the Network with Common Security Tools (3e)

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

Student:	Email:
Valeria Brochero	v0broc01@louisville.edu

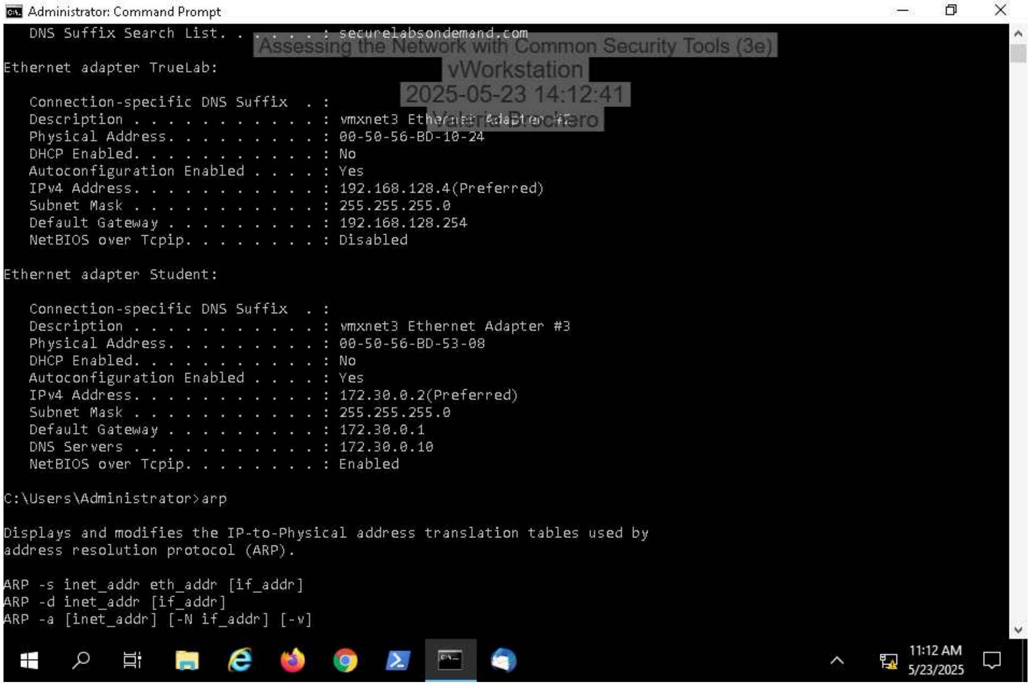
Time on Task:	Progress:
5 hours, 50 minutes	100%

Report Generated: Friday, July 11, 2025 at 11:22 PM

Section 1: Hands-On Demonstration

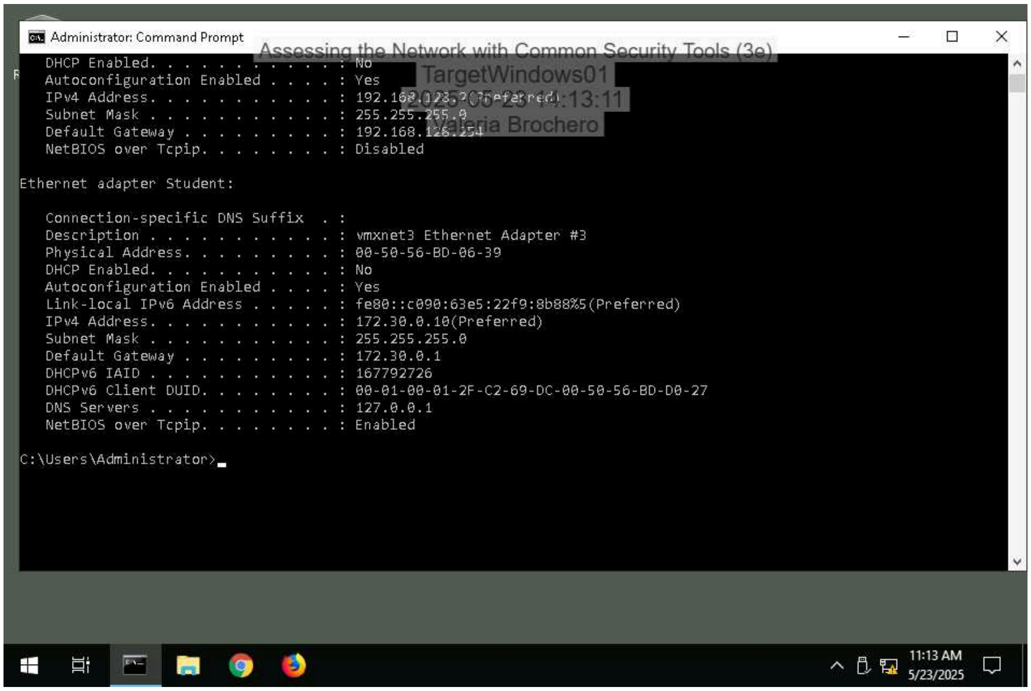
Part 1: Explore the Local Area Network

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


Administrator: Command Prompt
Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-05-23 14:12:41
Valeria Brochero
11:12 AM
5/23/2025

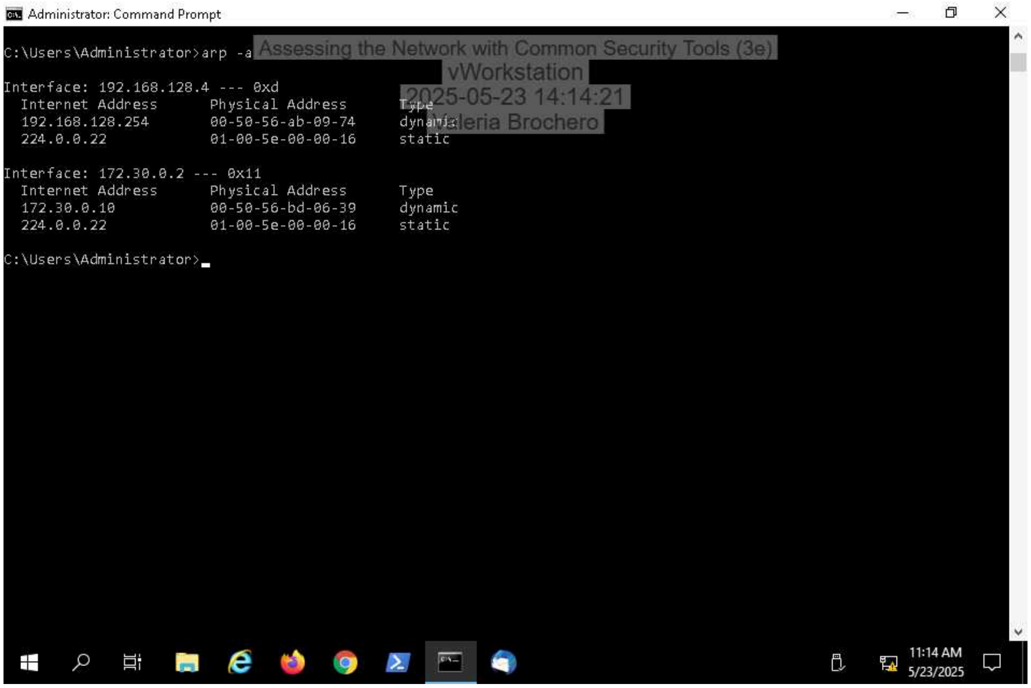
```
   DNS Suffix Search List. . . . . . : securelabsondemand.com

Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-50-56-BD-10-24
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.128.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.128.254
   NetBIOS over Tcpip. . . . . . . . : Disabled

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-50-56-BD-53-08
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.30.0.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1
   DNS Servers . . . . . . . . . . . : 172.30.0.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]
```

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


Administrator: Command Prompt
Assessing the Network with Common Security Tools (3e)
TargetWindows01
2025-05-23 14:13:11
Valeria Brochero
11:13 AM
5/23/2025

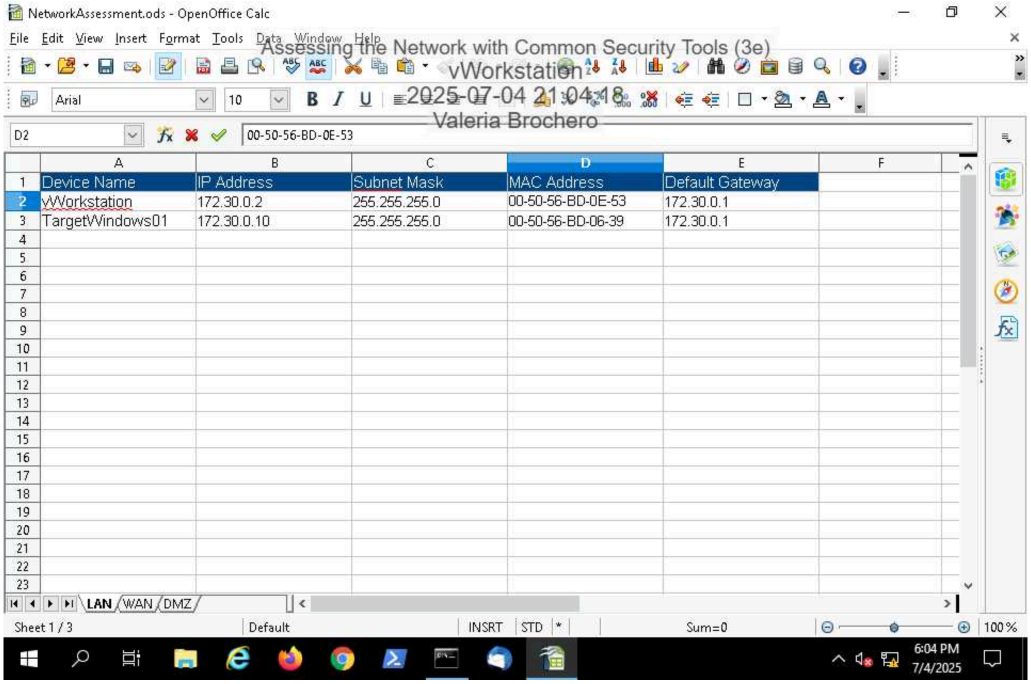
```
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.128.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.128.254
   NetBIOS over Tcpip. . . . . . . . : Disabled

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-50-56-BD-06-39
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c090:63e5:22f9:8b88%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.30.0.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1
   DHCPv6 IAID . . . . . . . . . . . : 167792726
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-C2-69-DC-00-50-56-BD-D0-27
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>
```

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


Administrator: Command Prompt
Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-05-23 14:14:21
Valeria Brochero
11:14 AM
5/23/2025

```
C:\Users\Administrator>arp -a

Interface: 192.168.128.4 --- 0xd
  Internet Address      Physical Address      Type
  192.168.128.254       00-50-56-ab-09-74     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-bd-06-39     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>
```

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

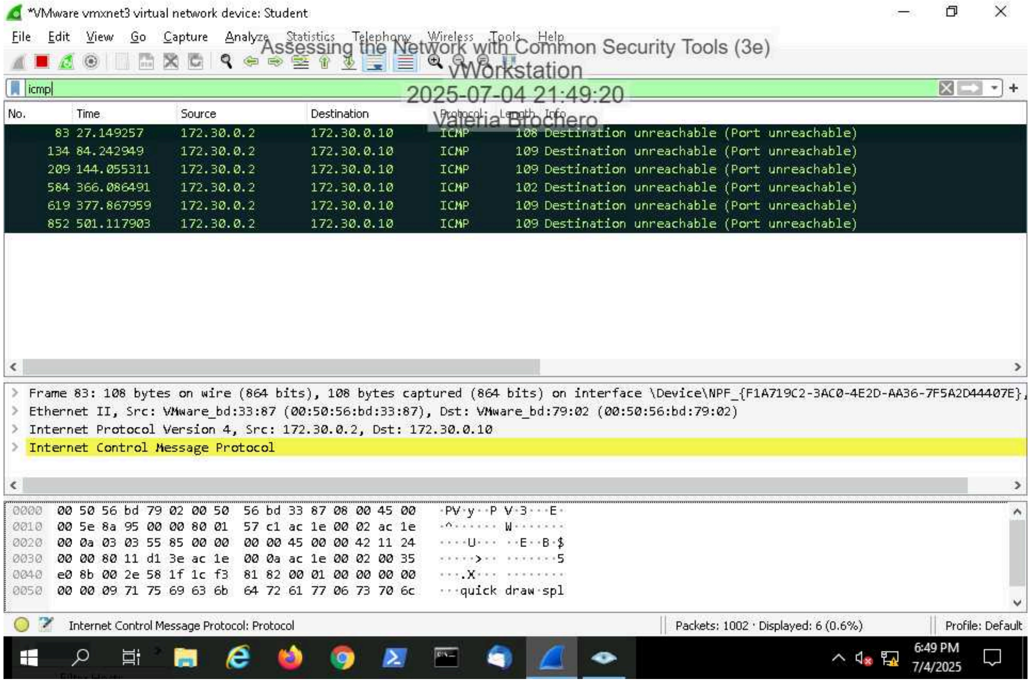

NetworkAssessment.ods - OpenOffice Calc
File Edit View Insert Format Tools Data Window Help
Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-07-04 21:04:18
Valeria Brochero
Arial
10
LAN
WAN
DMZ
Sheet 1 / 3
Default
INSRT
STD
Sum=0
100 %
6:04 PM
7/4/2025

D2 00-50-56-BD-0E-53

	A	B	C	D	E	F
1	Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway	
2	vWorkstation	172.30.0.2	255.255.255.0	00-50-56-BD-0E-53	172.30.0.1	
3	TargetWindows01	172.30.0.10	255.255.255.0	00-50-56-BD-06-39	172.30.0.1	

Part 2: Analyze Network Traffic

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


*VMware vmxnet3 virtual network device: Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-07-04 21:49:20
Valeria Brochero
6:49 PM
7/4/2025

icmp

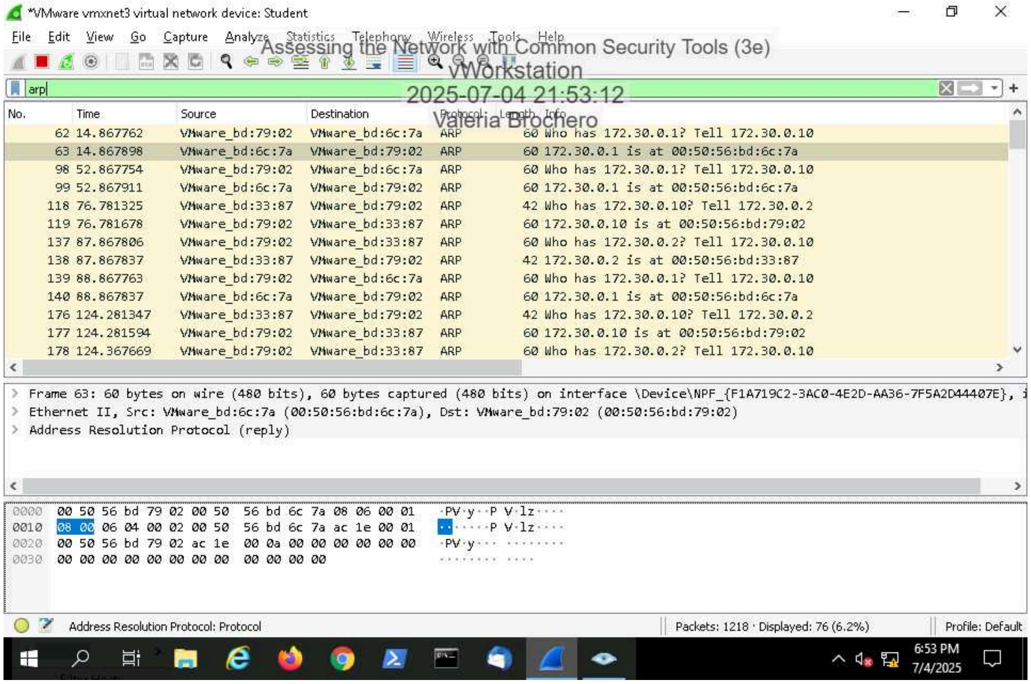
```
No.   Time        Source       Destination   Protocol Length Info
   83 27.149257   172.30.0.2   172.30.0.10   ICMP     108 Destination unreachable (Port unreachable)
  134 84.242949   172.30.0.2   172.30.0.10   ICMP     109 Destination unreachable (Port unreachable)
  209 144.055311  172.30.0.2   172.30.0.10   ICMP     109 Destination unreachable (Port unreachable)
  584 366.086491  172.30.0.2   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
  619 377.867959  172.30.0.2   172.30.0.10   ICMP     109 Destination unreachable (Port unreachable)
  852 501.117903  172.30.0.2   172.30.0.10   ICMP     109 Destination unreachable (Port unreachable)
```

```
> Frame 83: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface \Device\NPF_{F1A719C2-3AC0-4E2D-AA36-7F5A2D44407E},
> Ethernet II, Src: VMware_bd:33:87 (00:50:56:bd:33:87), Dst: VMware_bd:79:02 (00:50:56:bd:79:02)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.10
> Internet Control Message Protocol
```

```
0000  00 50 56 bd 79 02 00 50  56 bd 33 87 08 00 45 00   ·PV·y··P V·3···E·
0010  00 5e 8a 95 00 00 80 01  57 c1 ac 1e 00 02 ac 1e   ·^······ W·······
0020  00 0a 03 03 55 85 00 00  00 00 45 00 00 42 11 24   ····U··· ··E··B·$
0030  00 00 80 11 d1 3e ac 1e  00 0a ac 1e 00 02 00 35   ·····>·· ·······5
0040  e0 8b 00 2e 58 1f 1c f3  81 82 00 01 00 00 00 00   ····.X·· ········
0050  00 00 09 71 75 69 63 6b  64 72 61 77 06 73 70 6c   ···quick draw·spl
```

Internet Control Message Protocol: Protocol | Packets: 1002 · Displayed: 6 (0.6%) | Profile: Default

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



arp

```
No.     Time         Source             Destination        Protocol Length Info
     62 14.867762    VMware_bd:79:02    VMware_bd:6c:7a    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
     63 14.867898    VMware_bd:6c:7a    VMware_bd:79:02    ARP      60 172.30.0.1 is at 00:50:56:bd:6c:7a
     98 52.867754    VMware_bd:79:02    VMware_bd:6c:7a    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
     99 52.867911    VMware_bd:6c:7a    VMware_bd:79:02    ARP      60 172.30.0.1 is at 00:50:56:bd:6c:7a
    118 76.781325    VMware_bd:33:87    VMware_bd:79:02    ARP      42 Who has 172.30.0.10? Tell 172.30.0.2
    119 76.781678    VMware_bd:79:02    VMware_bd:33:87    ARP      60 172.30.0.10 is at 00:50:56:bd:79:02
    137 87.867806    VMware_bd:79:02    VMware_bd:33:87    ARP      60 Who has 172.30.0.2? Tell 172.30.0.10
    138 87.867837    VMware_bd:33:87    VMware_bd:79:02    ARP      42 172.30.0.2 is at 00:50:56:bd:33:87
    139 88.867763    VMware_bd:79:02    VMware_bd:6c:7a    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
    140 88.867837    VMware_bd:6c:7a    VMware_bd:79:02    ARP      60 172.30.0.1 is at 00:50:56:bd:6c:7a
    176 124.281347   VMware_bd:33:87    VMware_bd:79:02    ARP      42 Who has 172.30.0.10? Tell 172.30.0.2
    177 124.281594   VMware_bd:79:02    VMware_bd:33:87    ARP      60 172.30.0.10 is at 00:50:56:bd:79:02
    178 124.367669   VMware_bd:79:02    VMware_bd:33:87    ARP      60 Who has 172.30.0.2? Tell 172.30.0.10
```

```
> Frame 63: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{F1A719C2-3AC0-4E2D-AA36-7F5A2D44407E}, i
> Ethernet II, Src: VMware_bd:6c:7a (00:50:56:bd:6c:7a), Dst: VMware_bd:79:02 (00:50:56:bd:79:02)
> Address Resolution Protocol (reply)
```

```
0000  00 50 56 bd 79 02 00 50  56 bd 6c 7a 08 06 00 01   ·PV·y··P V·lz····
0010  08 00 06 04 00 02 00 50  56 bd 6c 7a ac 1e 00 01   ········P V·lz····
0020  00 50 56 bd 79 02 ac 1e  00 0a 00 00 00 00 00 00   ·PV·y··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Address Resolution Protocol: Protocol | Packets: 1218 · Displayed: 76 (6.2%) | Profile: Default

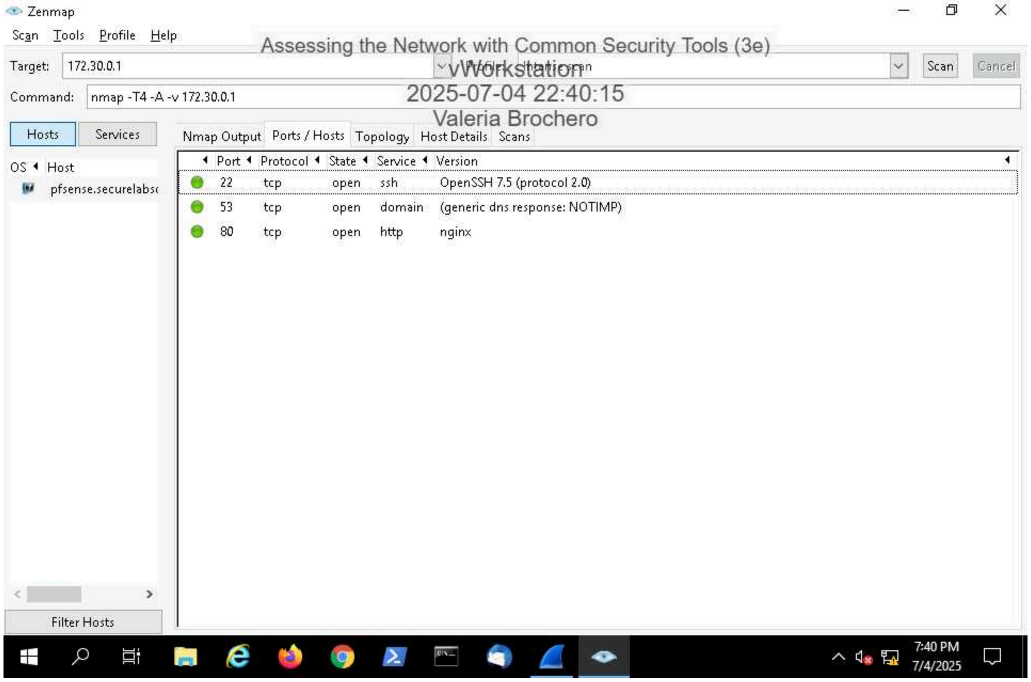
18. **Compare** the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

The difference between the two is that the ping scan identifies the host on our network and all IP addresses currently online which are sending packet requests. On the other hand, the regular scan syncs all TCP ports via an ICMP echo request.

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

The intense scan results are more numerous than both previous scans, yet similar to the regular scan. The TCP ports use SYN packets, which also scan for UDP ports.

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



Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-07-04 22:40:15
Valeria Brochero

Target: 172.30.0.1

Command: nmap -T4 -A -v 172.30.0.1

OS	Host
	pfsense.securelabs(

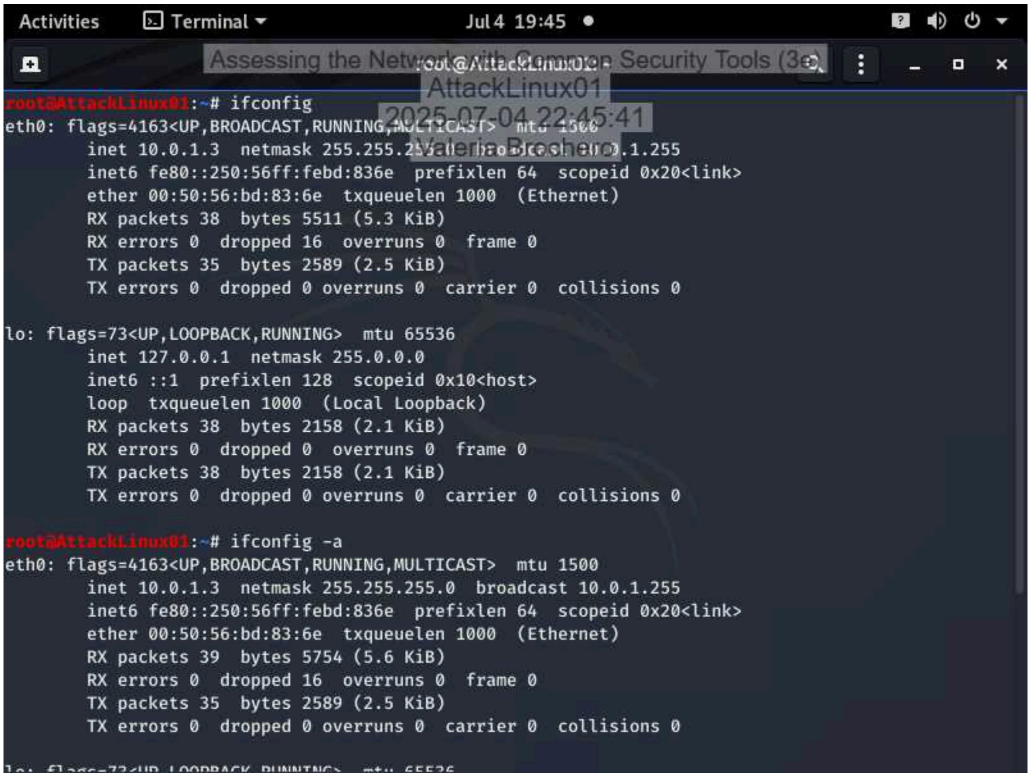
	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 7.5 (protocol 2.0)
●	53	tcp	open	domain	(generic dns response: NOTIMP)
●	80	tcp	open	http	nginx

7:40 PM
7/4/2025

Section 2: Applied Learning

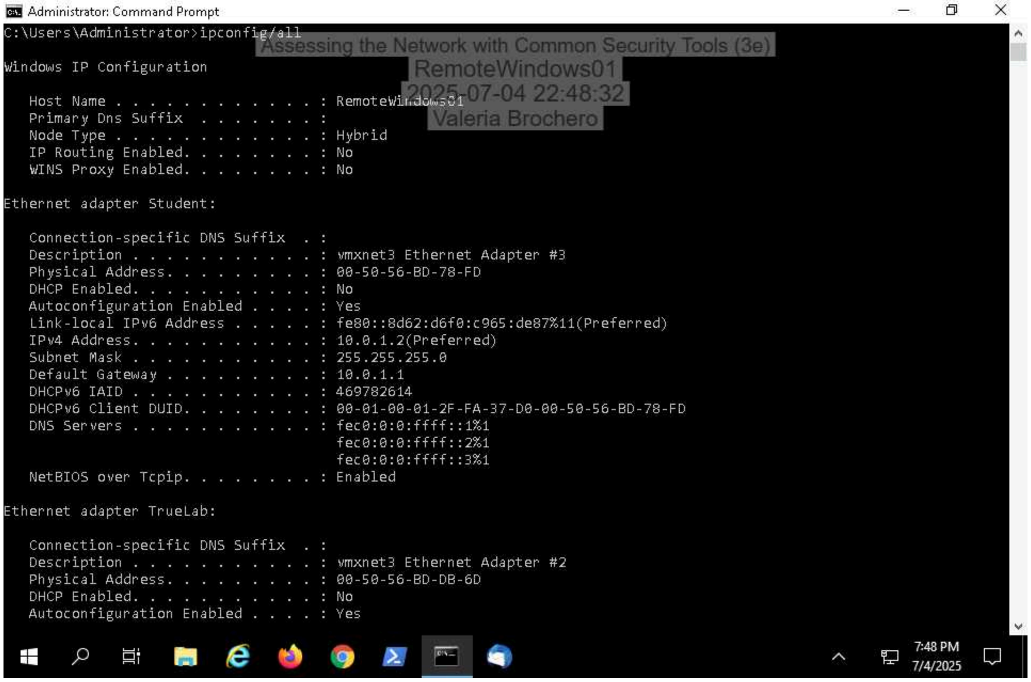
Part 1: Explore the Wide Area Network

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



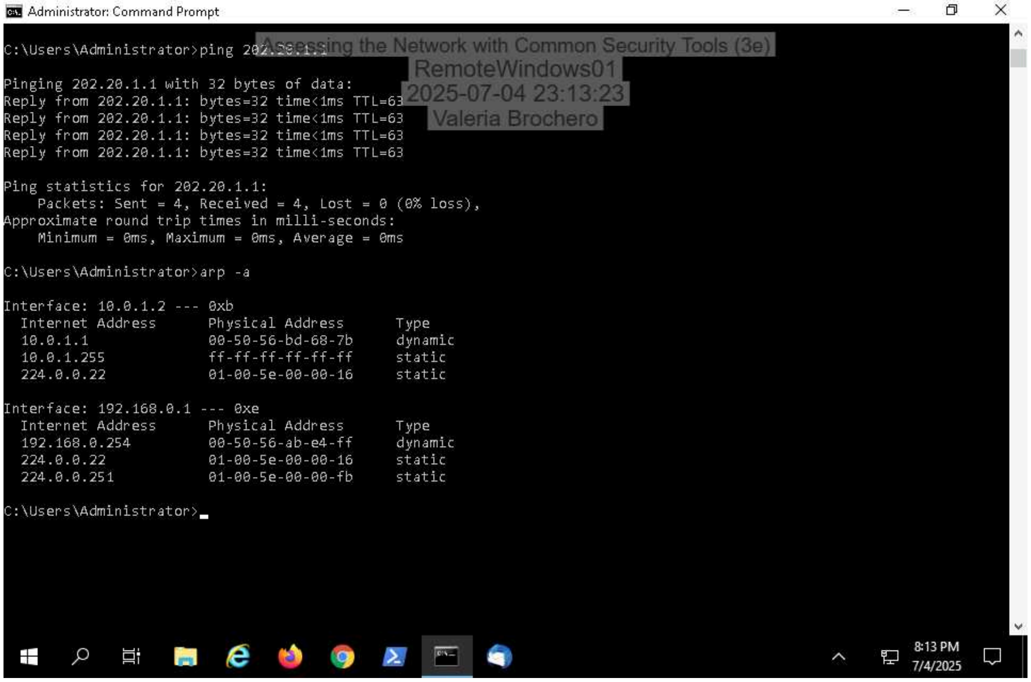
```
root@AttackLinux01:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.3  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::250:56ff:febd:836e  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:bd:83:6e  txqueuelen 1000  (Ethernet)
        RX packets 38  bytes 5511 (5.3 KiB)
        RX errors 0  dropped 16  overruns 0  frame 0
        TX packets 35  bytes 2589 (2.5 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:~# 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:febd:836e  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:bd:83:6e  txqueuelen 1000  (Ethernet)
        RX packets 39  bytes 5754 (5.6 KiB)
        RX errors 0  dropped 16  overruns 0  frame 0
        TX packets 35  bytes 2589 (2.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

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


Administrator: Command Prompt
Assessing the Network with Common Security Tools (3e)
RemoteWindows01
2025-07-04 22:48:32
Valeria Brochero
7:48 PM
7/4/2025

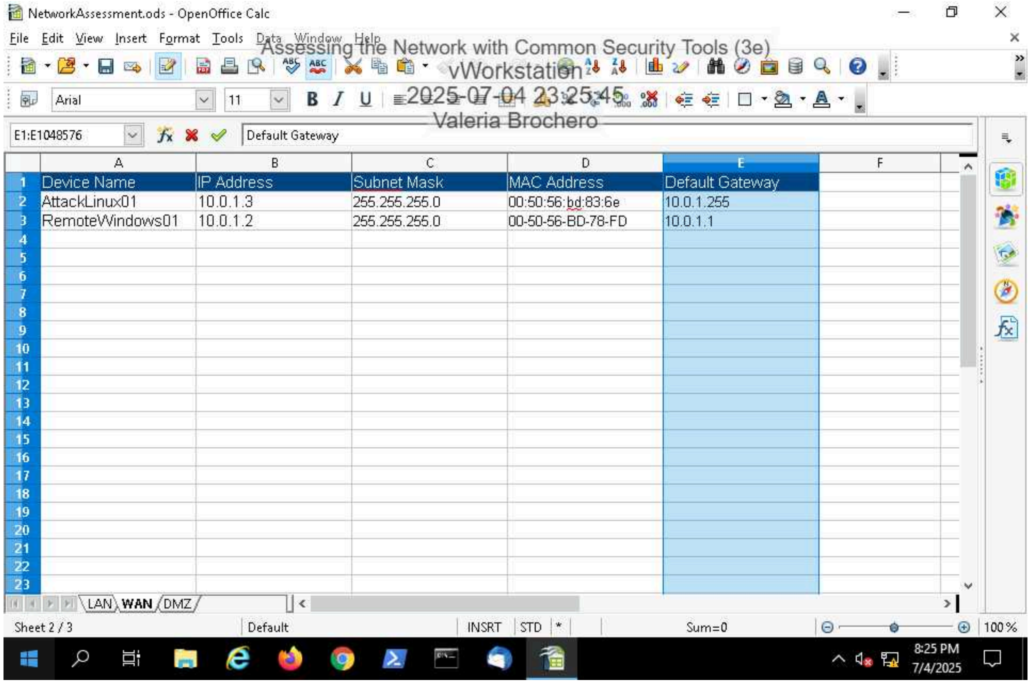
```
C:\Users\Administrator>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : RemoteWindows01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-50-56-BD-78-FD
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8d62:d6f0:c965:de87%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. . . . . . . . : 00-01-00-01-2F-FA-37-D0-00-50-56-BD-78-FD
   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-BD-DB-6D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

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


Administrator: Command Prompt
Assessing the Network with Common Security Tools (3e)
RemoteWindows01
2025-07-04 23:13:23
Valeria Brochero
8:13 PM
7/4/2025

```
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 = 0ms, 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-bd-68-7b     dynamic
  10.0.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.0.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.254         00-50-56-ab-e4-ff     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static

C:\Users\Administrator>
```

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



NetworkAssessment.ods - OpenOffice Calc
File Edit View Insert Format Tools Data Window Help
Arial
11
E1:E1048576

Assessing the Network with Common Security Tools (3e)
vWorkstation
2025-07-04 23:25:45
Valeria Brochero

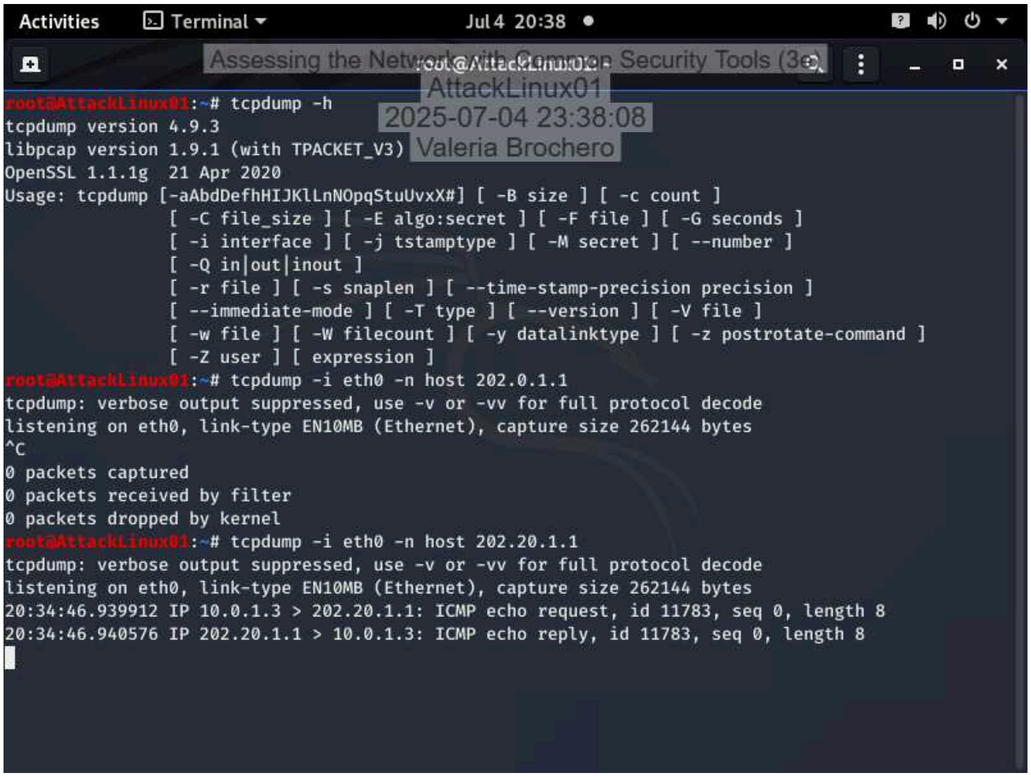
Default Gateway

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
AttackLinux01	10.0.1.3	255.255.255.0	00:50:56:bd:83:6e	10.0.1.255
RemoteWindows01	10.0.1.2	255.255.255.0	00-50-56-BD-78-FD	10.0.1.1

LAN
WAN
DMZ
Sheet 2 / 3
Default
INSRT
STD
Sum=0
100 %
8:25 PM
7/4/2025

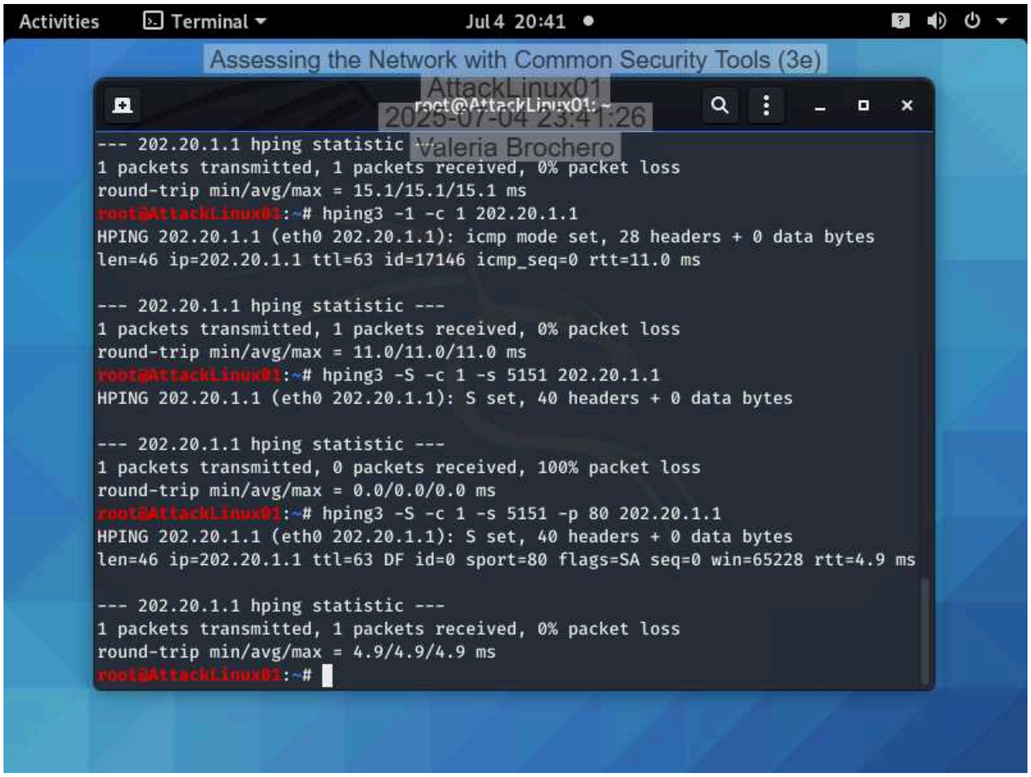
Part 2: Analyze Network Traffic

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



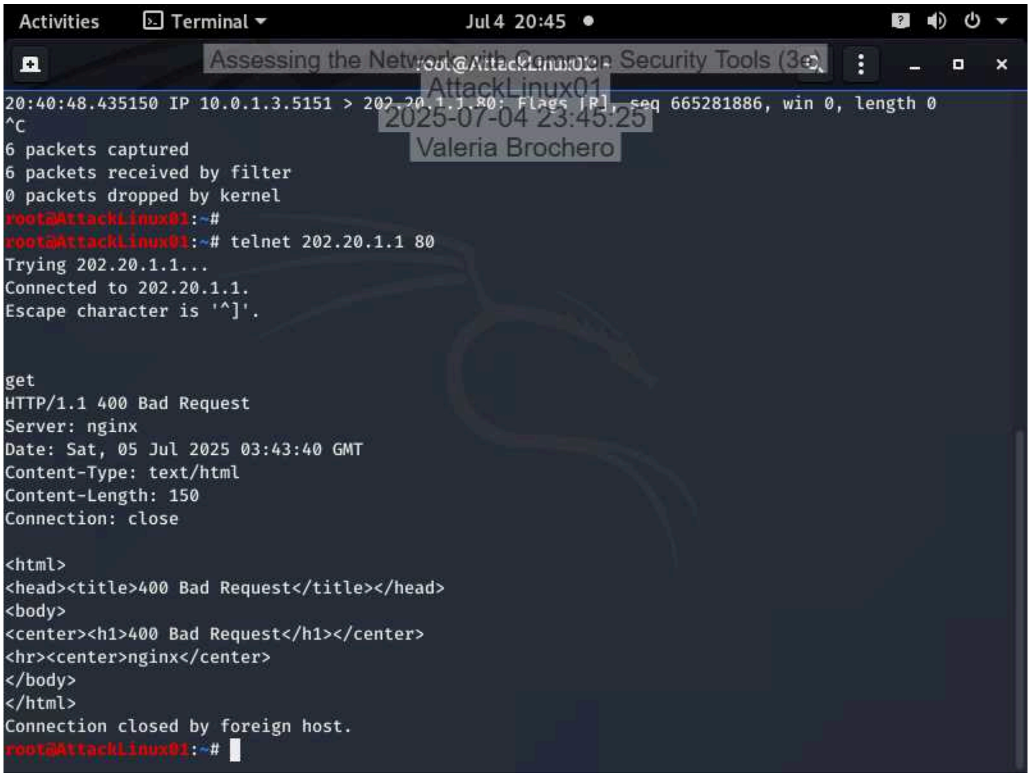
```
root@AttackLinux01:~# tcpdump -h
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1g  21 Apr 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -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 202.0.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
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
20:34:46.939912 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 11783, seq 0, length 8
20:34:46.940576 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 11783, seq 0, length 8
```

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



```
--- 202.20.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 15.1/15.1/15.1 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=17146 icmp_seq=0 rtt=11.0 ms

--- 202.20.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 11.0/11.0/11.0 ms
root@AttackLinux01:~# hping3 -S -c 1 -s 5151 202.20.1.1
HPING 202.20.1.1 (eth0 202.20.1.1): S set, 40 headers + 0 data bytes

--- 202.20.1.1 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@AttackLinux01:~# hping3 -S -c 1 -s 5151 -p 80 202.20.1.1
HPING 202.20.1.1 (eth0 202.20.1.1): S set, 40 headers + 0 data bytes
len=46 ip=202.20.1.1 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=65228 rtt=4.9 ms

--- 202.20.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.9/4.9/4.9 ms
root@AttackLinux01:~#
```

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

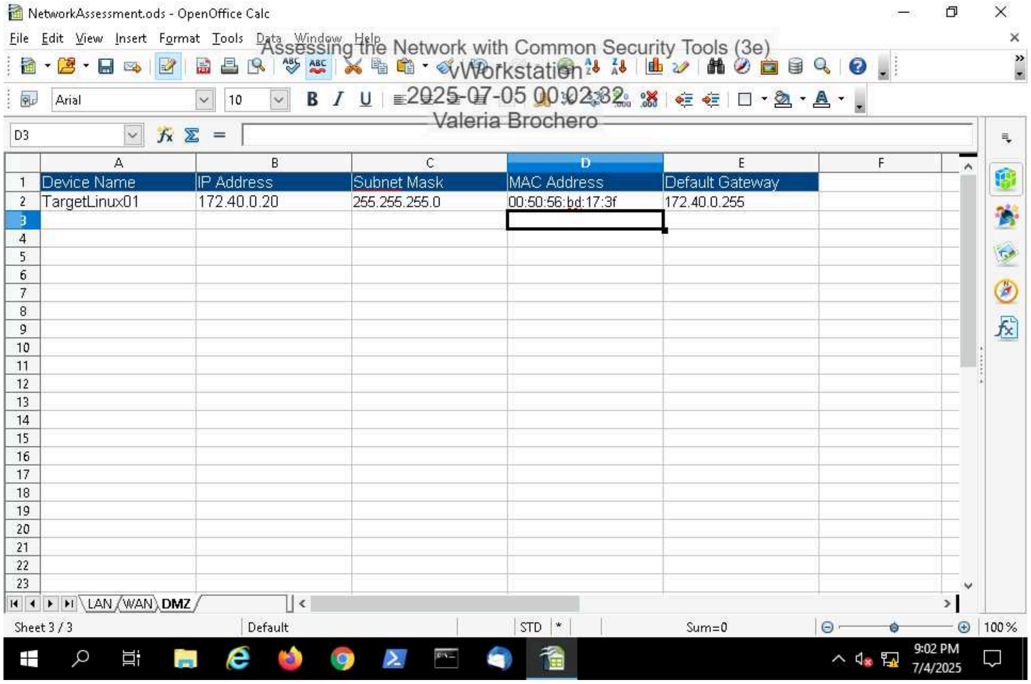


```
20:40:48.435150 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [R], seq 665281886, win 0, length 0
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
root@AttackLinux01:~#
root@AttackLinux01:~# telnet 202.20.1.1 80
Trying 202.20.1.1...
Connected to 202.20.1.1.
Escape character is '^]'.


get
HTTP/1.1 400 Bad Request
Server: nginx
Date: Sat, 05 Jul 2025 03:43:40 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:~#
```

Section 3: Challenge and Analysis

Part 1: Explore the DMZ

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


NetworkAssessment.ods - OpenOffice Calc
File Edit View Insert Format Tools Data Window Help
Arial
10
D3
LAN
WAN
DMZ
Sheet 3 / 3
Default
STD
Sum=0
100 %
9:02 PM
7/4/2025

	A	B	C	D	E
1	Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
2	TargetLinux01	172.40.0.20	255.255.255.0	00:50:56:bd:17:3f	172.40.0.255

Part 2: Perform Reconnaissance on the Firewall

Briefly summarize and analyze your findings in a technical memo to your boss.

There were 2 ICMP, 4 ARP, and 4 DNS packets sent to the firewall. Ports 22 (ssh) and 111 (rpcbind) are both tcp protocol and open on the pfSense firewall.