

# Assessing the Network with Common Security Tools (3e)

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

Student:	Email:
Reginald Gordon	rgordon5002@email.vccs.edu

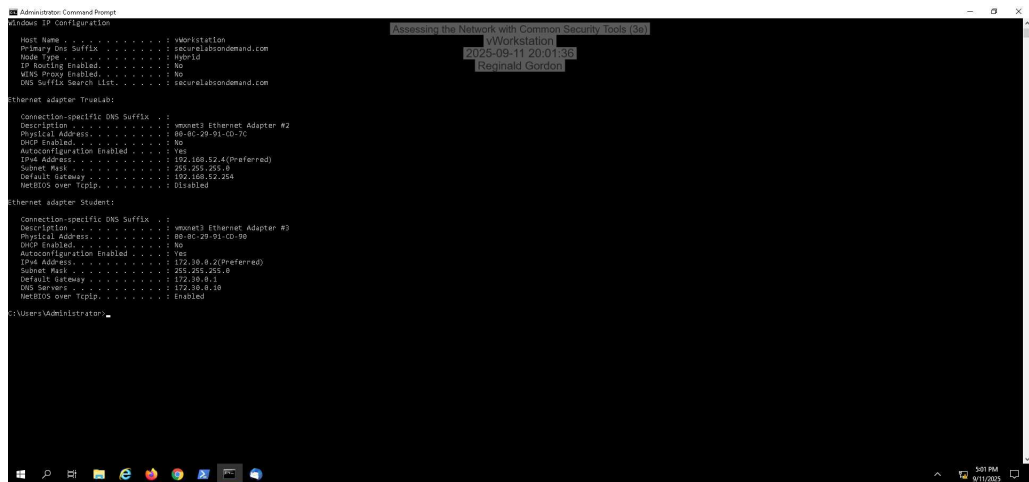
Time on Task:	Progress:
17 hours, 24 minutes	100%

Report Generated: Sunday, September 14, 2025 at 2:39 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**.

```
Administrator: Command Prompt
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.12.254

Ethernet adapter Student:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::1422:5804:190d::da605
IPv6 Address. . . . . : 172.30.8.8
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.30.8.1

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : TargetWindows01
Primary DNS Suffix . . . . . : securelabondemand.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : securelabondemand.com

Ethernet adapter TrueLab:

Connection-specific DNS Suffix . : 
Description . . . . . : VMware3 Ethernet Adapter
Physical Address. . . . . : 08-0C-29-0E-20-A1
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.12.2 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.12.254
NetBIOS over Tcpip. . . . . : Disabled

Ethernet adapter Student:

Connection-specific DNS Suffix . : 
Description . . . . . : VMware3 Ethernet Adapter #3
Physical Address. . . . . : 08-0C-29-0E-20-B5
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1422:5804:190d::da605 (Preferred)
IPv6 Address. . . . . : 172.30.8.18 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.30.8.1
Dhcpv6 IADP . . . . . : 16792720
Dhcpv6 Client DUID. . . . . : 88-63-80-01-30-55-14-E9-00-0C-29-0E-20-A1
DNS Servers . . . . . : 172.8.0.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>
```

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

```
Administrator: Command Prompt
C:\Users\Administrator>arp -d

C:\Users\Administrator>arp -a

Interface: 192.168.12.4 --- 0ad
Internet Address Physical Address Type
192.168.12.254 08-50-56-bd-62-ee dynamic
224.0.0.22 01-00-5e-00-00-16 static

Interface: 172.30.8.2 --- 0a11
Internet Address Physical Address Type
224.0.0.22 01-00-5e-00-00-16 static

C:\Users\Administrator>ping 172.30.8.10

Pinging 172.30.8.10 with 32 bytes of data:
Reply from 172.30.8.10: bytes=32 time=1ms TTL=120
Reply from 172.30.8.10: bytes=32 time=1ms TTL=120
Reply from 172.30.8.10: bytes=32 time=1ms TTL=120
Reply from 172.30.8.10: bytes=32 time=1ms TTL=120

Ping statistics for 172.30.8.10:
    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: 192.168.12.4 --- 0ad
Internet Address Physical Address Type
192.168.12.254 08-50-56-bd-62-ee dynamic
224.0.0.22 01-00-5e-00-00-16 static

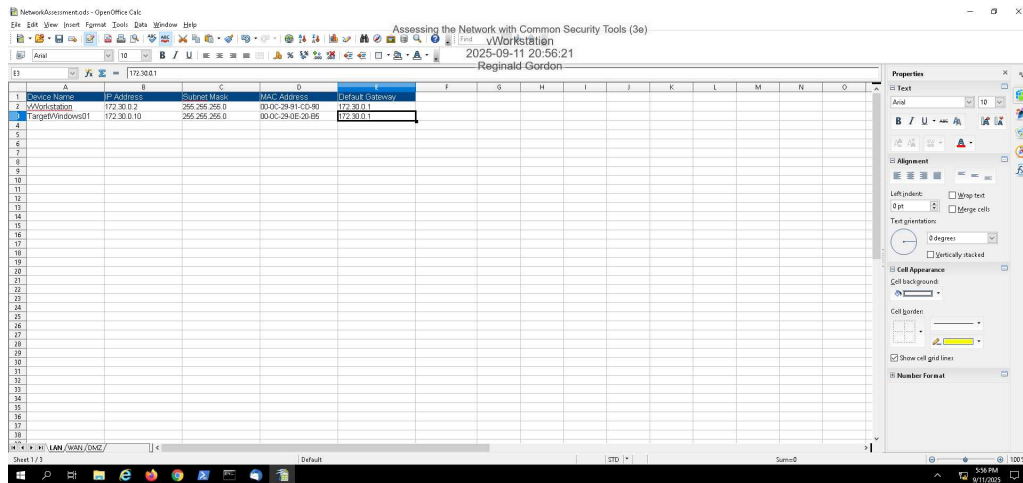
Interface: 172.30.8.2 --- 0a11
Internet Address Physical Address Type
172.30.8.10 08-0c-29-0e-20-b5 dynamic
224.0.0.22 01-00-5e-00-00-16 static

C:\Users\Administrator>
```

# Assessing the Network with Common Security Tools (3e)

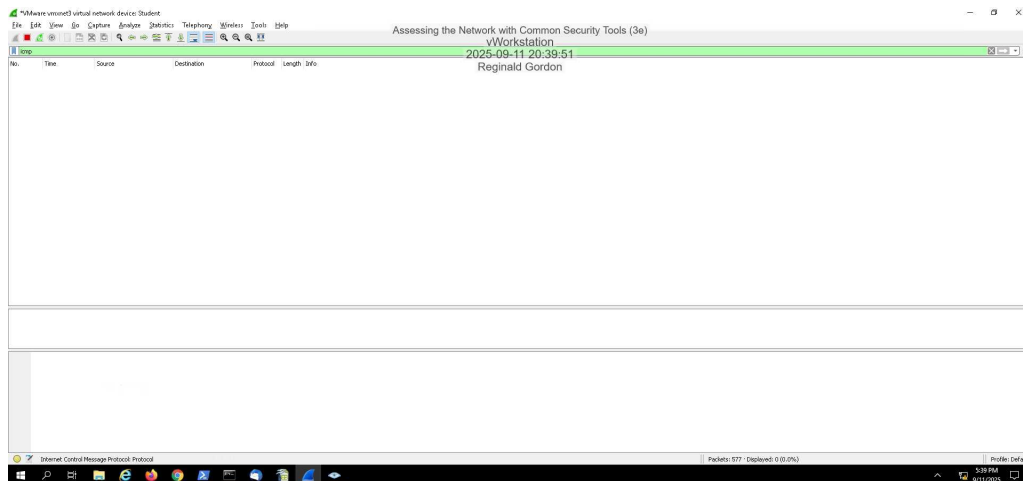
## Network Security, Firewalls, and VPNs, Third Edition - Lab 01

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

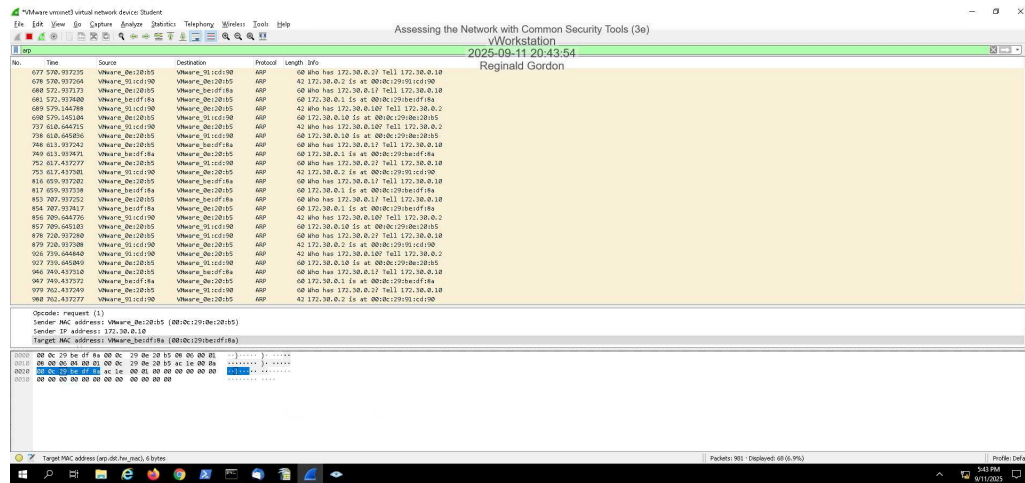


## Part 2: Analyze Network Traffic

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



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



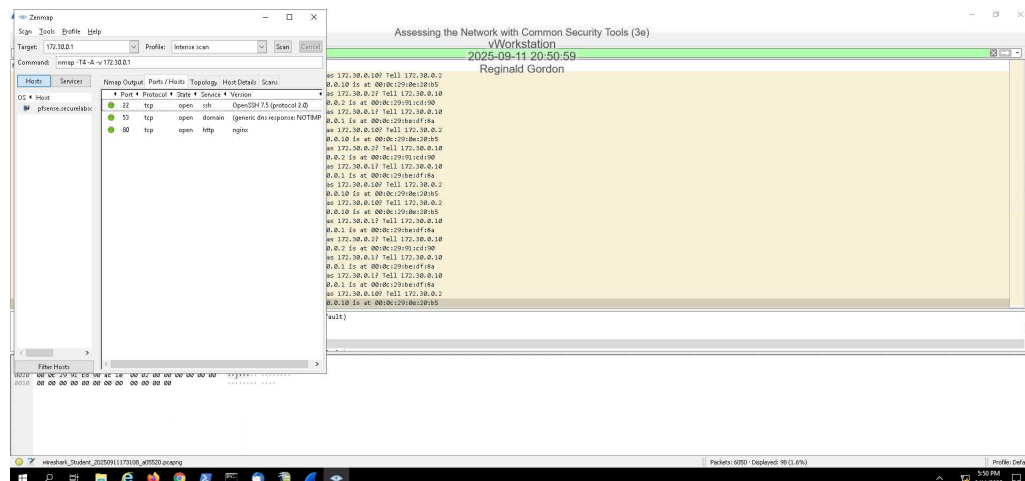
### 18. Compare the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

The regular scan generated more ARP traffic, but no ICMP traffic.

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

The Intense scan was able to generate traffic for ICMP, and ARP.

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

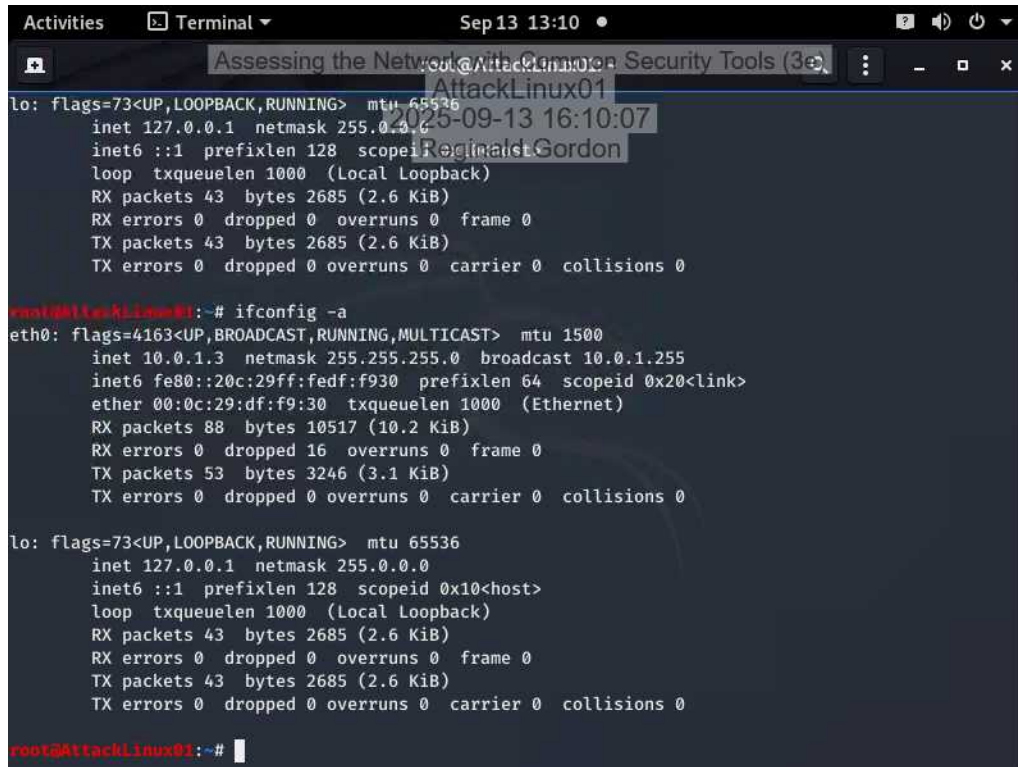




### Section 2: Applied Learning

#### Part 1: Explore the Wide Area Network

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



A terminal window titled 'Terminal' with a timestamp of 'Sep 13 13:10'. The prompt is 'root@AttackLinux01:~#'. The command 'ifconfig -a' has been executed, showing network configuration for three interfaces: 'lo' (loopback), 'eth0' (ethernet), and another 'lo' (loopback). The output for 'lo' shows 'inet 127.0.0.1 netmask 255.0.0.0' and 'inet6 ::1 prefixlen 128 scopeid 0x10<host>'. The output for 'eth0' shows 'inet 10.0.1.3 netmask 255.255.255.0 broadcast 10.0.1.255' and 'ether 00:0c:29:df:f9:30 txqueuelen 1000 (Ethernet)'. The output for the second 'lo' shows 'inet 127.0.0.1 netmask 255.0.0.0' and 'inet6 ::1 prefixlen 128 scopeid 0x10<host>'. The prompt is now 'root@AttackLinux01:~#'.


```
root@AttackLinux01:~# ifconfig -a
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 43 bytes 2685 (2.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 2685 (2.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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::20c:29ff:fedf:f930 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:df:f9:30 txqueuelen 1000 (Ethernet)
    RX packets 88 bytes 10517 (10.2 KiB)
    RX errors 0 dropped 16 overruns 0 frame 0
    TX packets 53 bytes 3246 (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 43 bytes 2685 (2.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 2685 (2.6 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**.



An Administrator Command Prompt window showing the output of the 'ipconfig /all' command. The output displays network configuration for the host 'RemoteWindows01', including host name, primary DNS suffix, node type, IP routing, NetBIOS, Ethernet adapter 'Student', and Ethernet adapter 'TrueLab'. The 'Student' adapter shows 'Physical Address' as '80-0C-29-AF-03-09' and 'IP Address' as '192.168.51.1'. The 'TrueLab' adapter shows 'Physical Address' as '80-0C-29-AF-03-75' and 'IP Address' as '192.168.51.1'. The prompt is 'C:\Users\Administrator>'.

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

Windows IP Configuration

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

Ethernet adapter Student:

Connection-specific DNS Suffix . :
Description . . . . . : VMware3 Ethernet Adapter #3
Physical Address. . . . . : 80-0C-29-AF-03-09
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80:2da2:5300:6aa2:a37811(Prefered)
IPv4 Address. . . . . : 192.168.51.1(Prefered)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.51.1
Dhcpv6 IAID . . . . . : 46072614
Dhcpv6 Client DUID. . . . . : 00-01-80-01-30-57-05-98-00-00-29-AF-03-09
DNS Servers . . . . . : fe80:8b8:ffff::121
                        fe80:8b8:ffff::121
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter TrueLab:

Connection-specific DNS Suffix . :
Description . . . . . : VMware3 Ethernet Adapter #2
Physical Address. . . . . : 80-0C-29-AF-03-75
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80:2da2:5300:6aa2:a37811(Prefered)
IPv4 Address. . . . . : 192.168.51.1(Prefered)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.51.1
NetBIOS over Tcpip. . . . . : Disabled

C:\Users\Administrator>
```

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



```
Administrator Command Prompt
2025-09-13 16:22:11 01:00:50:00:00:01 static
255.255.255.255 ff:ff:ff:ff:ff:ff static

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

Interface: 10.0.1.2 --- Bdb
Interface: Physical Address Type
224.0.0.22 01:00:5a:00:00:16 static

Interface: 192.168.53.1 --- Bdb
Interface: Physical Address Type
192.168.53.254 00:50:56:a0:64:59 dynamic
224.0.0.22 01:00:5a:00:00:16 static

C:\Users\Administrator>ping 202.28.1.1.
Ping request could not find host 202.28.1.1. Please check the name and try again.
C:\Users\Administrator>ping 202.28.1.1

Pinging 202.28.1.1 with 32 bytes of data:
Reply from 202.28.1.1: bytes=32 time=1ms TTL=63
Reply from 202.28.1.1: bytes=32 time=1ms TTL=63
Reply from 202.28.1.1: bytes=32 time=1ms TTL=63
Reply from 202.28.1.1: bytes=32 time=1ms TTL=63

Ping statistics for 202.28.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

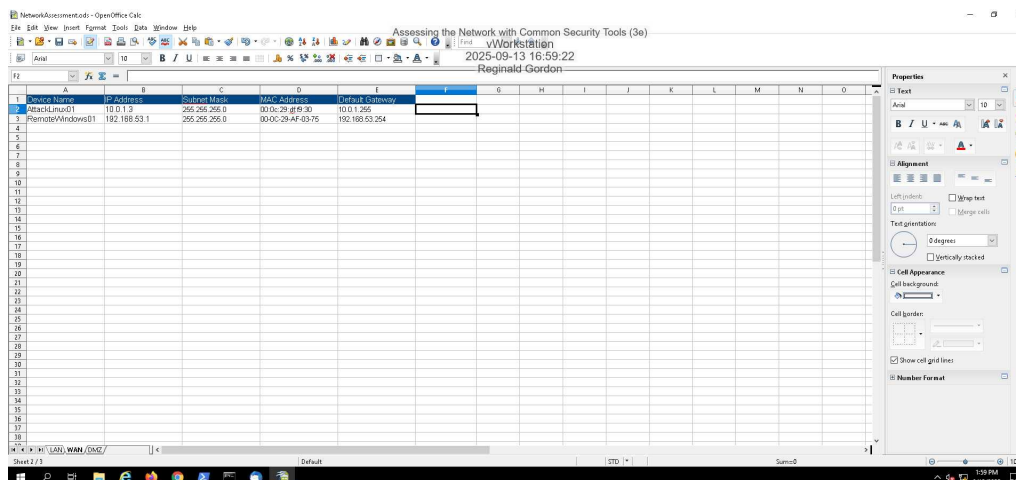
C:\Users\Administrator>arp -a

Interface: 10.0.1.2 --- Bdb
Interface: Physical Address Type
10.0.1.1 00:0c:29:6d:00:00 dynamic
10.0.1.255 ff:ff:ff:ff:ff:ff static
224.0.0.22 01:00:5a:00:00:16 static

Interface: 192.168.53.1 --- Bdb
Interface: Physical Address Type
192.168.53.254 00:50:56:a0:64:59 dynamic
224.0.0.22 01:00:5a:00:00:16 static

C:\Users\Administrator>
```

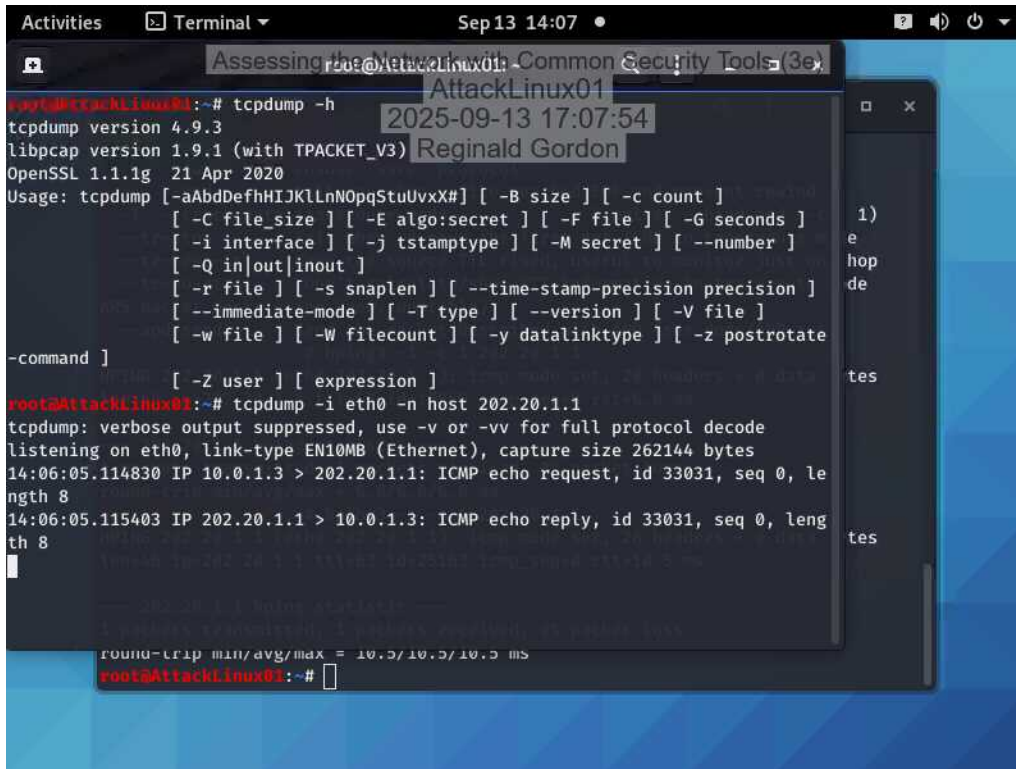
### 22. Make a screen capture showing the completed WAN tab of the Network Assessment spreadsheet.



Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
AttackLinux01	10.0.1.3	255.255.255.0	00:0c:29:6d:00:00	10.0.1.255
RemoteWindows01	192.168.53.1	255.255.255.0	00:0c:29:af:03:75	192.168.53.254

## 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 the date and time "Sep 13 14:07". The terminal output shows the user running `tcpdump -h` to see usage options, then `tcpdump -i eth0 -n host 202.20.1.1` to capture traffic. The output shows a successful ping test with the following details:

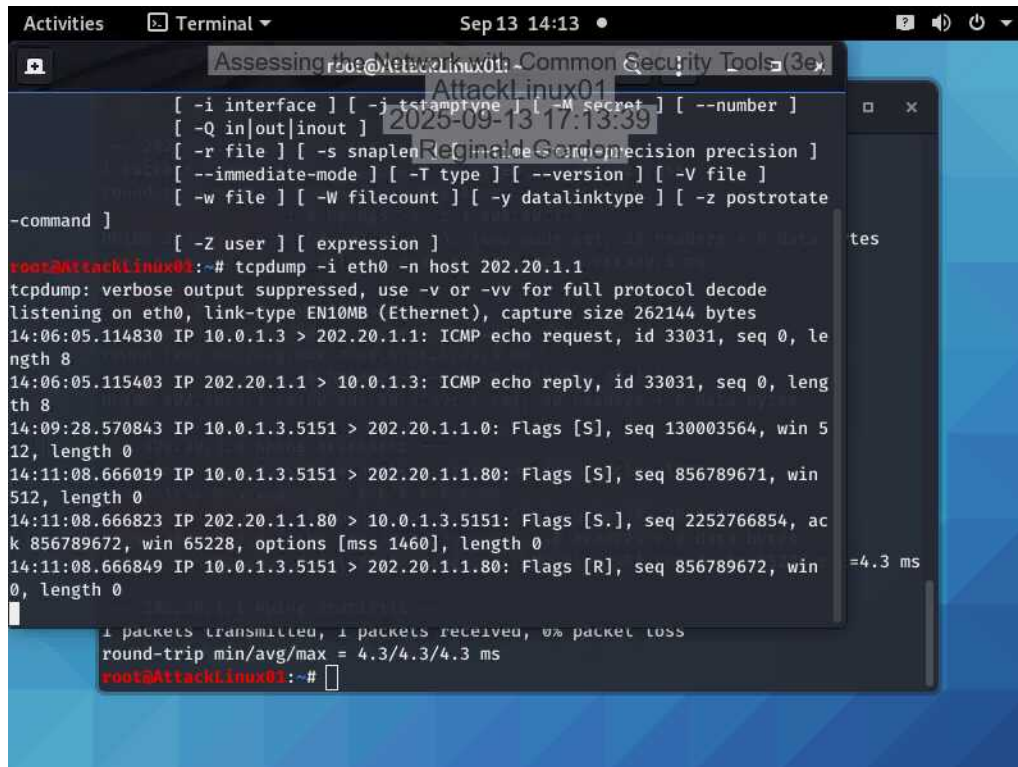
```
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1g 21 Apr 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvXx#] [-B size] [-c count]
        [-C file_size] [-E algo:secret] [-F file] [-G seconds]
        [-i interface] [-j tstamptype] [-M secret] [--number]
        [-Q in|out|inout]
        [-r file] [-s snaplen] [--time-stamp-precision precision]
        [--immediate-mode] [-T type] [--version] [-V file]
        [-w file] [-W filecount] [-y datalinktype] [-z postrotate]
        [-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
14:06:05.114830 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 33031, seq 0, length 8
14:06:05.115403 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 33031, seq 0, length 8

round-trip min/avg/max = 10.5/10.5/10.5 ms
root@AttackLinux01:~#
```



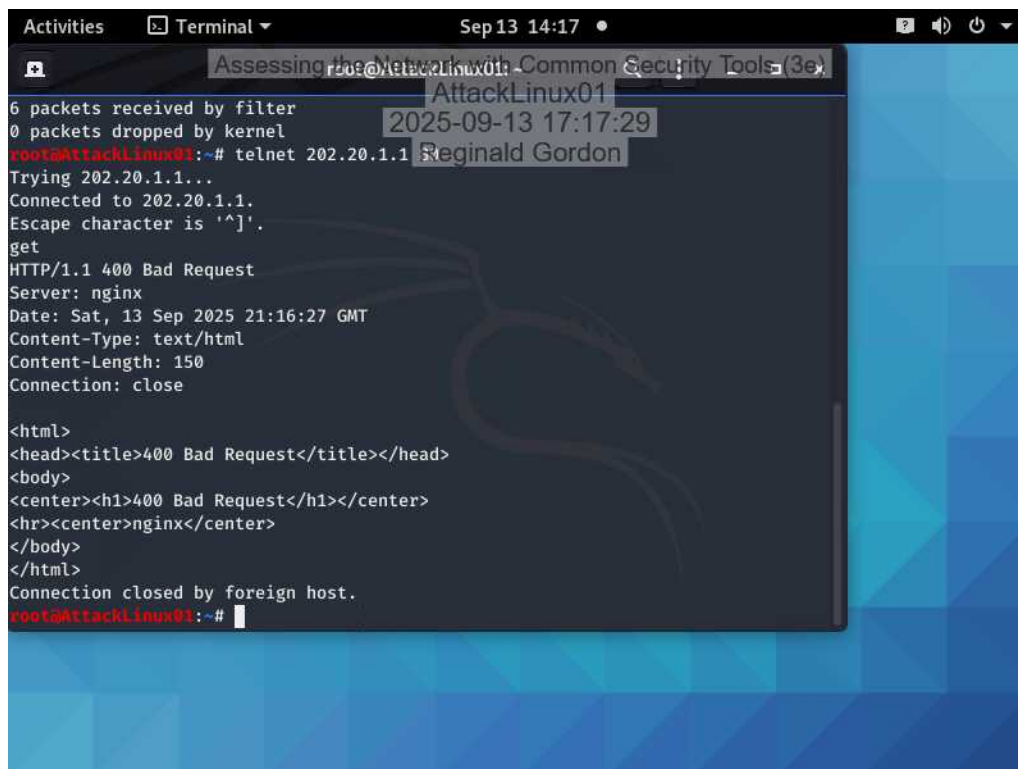
12. Make a screen capture showing the attempted three-way handshake in tcpdump.



A terminal window titled "Assessing the Network with Common Security Tools (3e)" and "AttackLinux01" showing the output of the tcpdump command. The command is `tcpdump -i eth0 -n host 202.20.1.1`. The output shows several ICMP echo requests and replies, and a sequence of flags (S, S., R) indicating an attempted three-way handshake. The round-trip time is shown as 4.3 ms.

```
[ -i interface ] [ -j timestamp ] [ -l secret ] [ --number ]
[ -Q in|out|inout ]
[ -r file ] [ -s snaplen ] [ -e 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
14:06:05.114830 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 33031, seq 0, length 8
14:06:05.115403 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 33031, seq 0, length 8
14:09:28.570843 IP 10.0.1.3.5151 > 202.20.1.1.0: Flags [S], seq 130003564, win 512, length 0
14:11:08.666019 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [S], seq 856789671, win 512, length 0
14:11:08.666823 IP 202.20.1.1.80 > 10.0.1.3.5151: Flags [S.], seq 2252766854, ack 856789672, win 65228, options [mss 1460], length 0
14:11:08.666849 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [R], seq 856789672, win 0, length 0
=4.3 ms
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.3/4.3/4.3 ms
root@AttackLinux01:~#
```

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



A terminal window titled "Assessing the Network with Common Security Tools (3e)" and "AttackLinux01" showing the output of the telnet command. The command is `telnet 202.20.1.1`. The output shows a connection to 202.20.1.1, followed by the results of the `get` command, which returns a 400 Bad Request status from the nginx server.

```
6 packets received by filter
0 packets dropped by kernel
root@AttackLinux01:~# telnet 202.20.1.1
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, 13 Sep 2025 21:16:27 GMT
Content-Type: text/html
Content-Length: 150
Connection: close

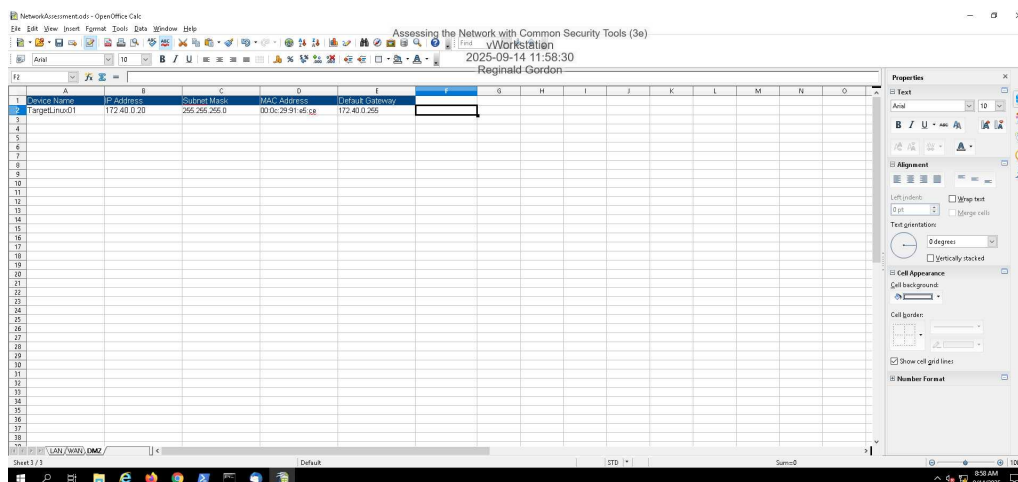
<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
Connection closed by foreign host.
root@AttackLinux01:~#
```



### Section 3: Challenge and Analysis

#### Part 1: Explore the DMZ

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



#### Part 2: Perform Reconnaissance on the Firewall

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

ICMP packets showed up after running an Intense scan in Zenmap. ARP packets didn't appear in the pfSense firewall MAC add search. DNS packets had several inquiries. Ports 22 (Ubuntu) and 80 (Apache) were open on the pfSense firewall.