Assessing the Network with Common Security Tools (3e)

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

Student:	Email:
Corbin Osman	corbin.osman@mycampus.apus.edu

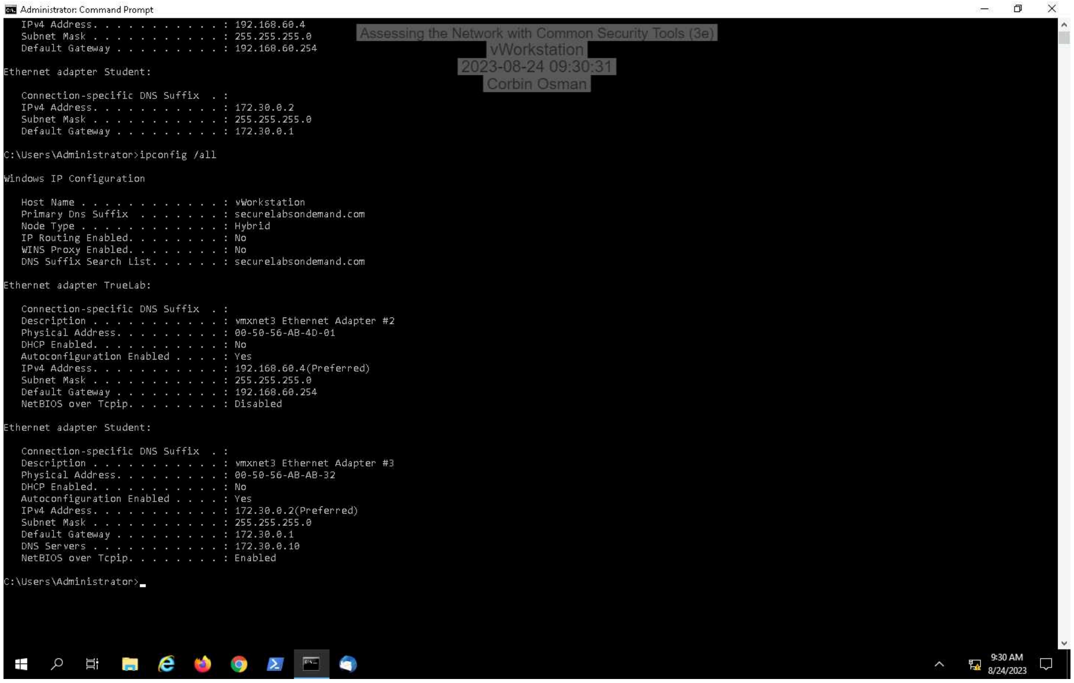
Time on Task:	Progress:
5 hours, 21 minutes	88%

Report Generated: Thursday, August 24, 2023 at 12:55 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**.

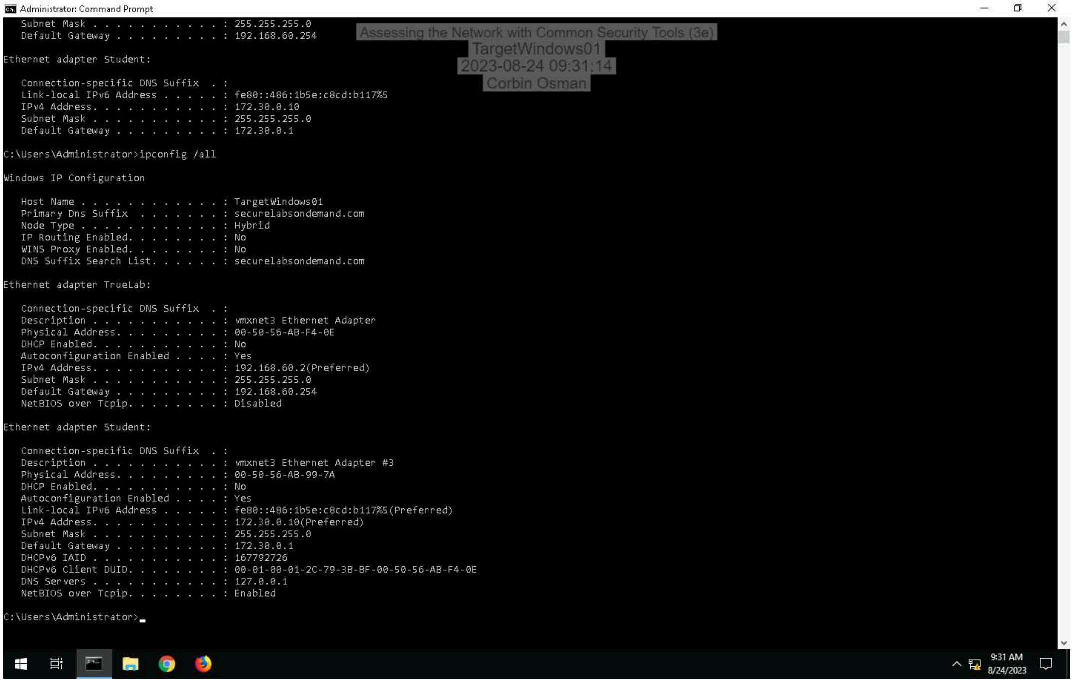


Administrator: Command Prompt

Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-08-24 09:30:31
Corbin Osman

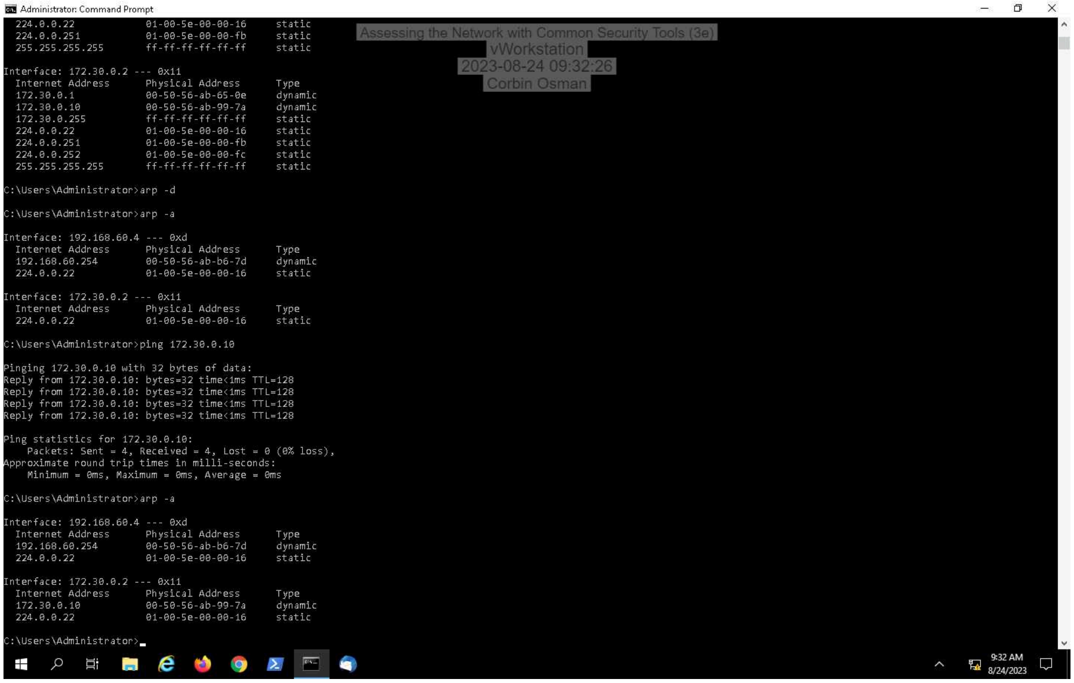
```
   IPv4 Address. . . . . . . . . . . : 192.168.60.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.60.254

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : vWorkstation
   Primary Dns Suffix  . . . . . . . : securelabsondemand.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : securelabsondemand.com

Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-50-56-AB-4D-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.60.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.60.254
   NetBIOS over Tcpip. . . . . . . . : Disabled

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-50-56-AB-AB-32
   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>_
```

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
2023-08-24 09:31:14
Corbin Osman
9:31 AM
8/24/2023

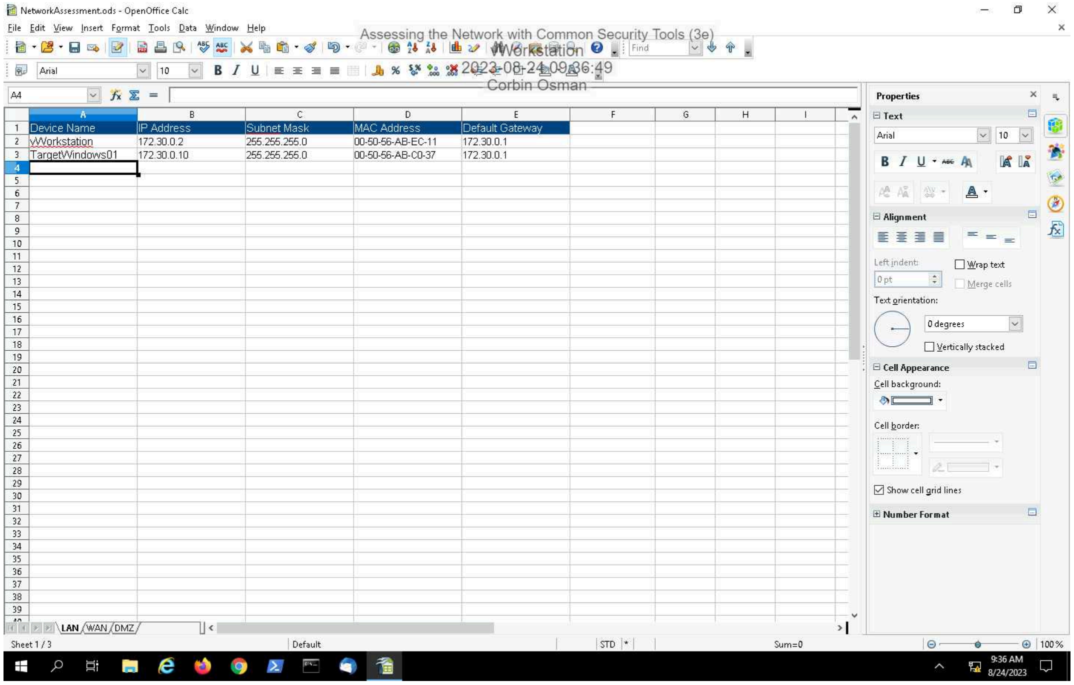
```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.60.254

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::486:1b5e:c8cd:b117%5
   IPv4 Address. . . . . . . . . . . : 172.30.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

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

Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-AB-F4-0E
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.60.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.60.254
   NetBIOS over Tcpip. . . . . . . . : Disabled

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-50-56-AB-99-7A
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::486:1b5e:c8cd:b117%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. . . . . . . . : 00-01-00-01-2C-79-3B-BF-00-50-56-AB-F4-0E
   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
2023-08-24 09:32:26
Corbin Osman
9:32 AM
8/24/2023

```
  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

Interface: 172.30.0.2 --- 0x11
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-ab-65-0e     dynamic
  172.30.0.10           00-50-56-ab-99-7a     dynamic
  172.30.0.255          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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>arp -d

C:\Users\Administrator>arp -a

Interface: 192.168.60.4 --- 0xd
  Internet Address      Physical Address      Type
  192.168.60.254        00-50-56-ab-b6-7d     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: 192.168.60.4 --- 0xd
  Internet Address      Physical Address      Type
  192.168.60.254        00-50-56-ab-b6-7d     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-ab-99-7a     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**.



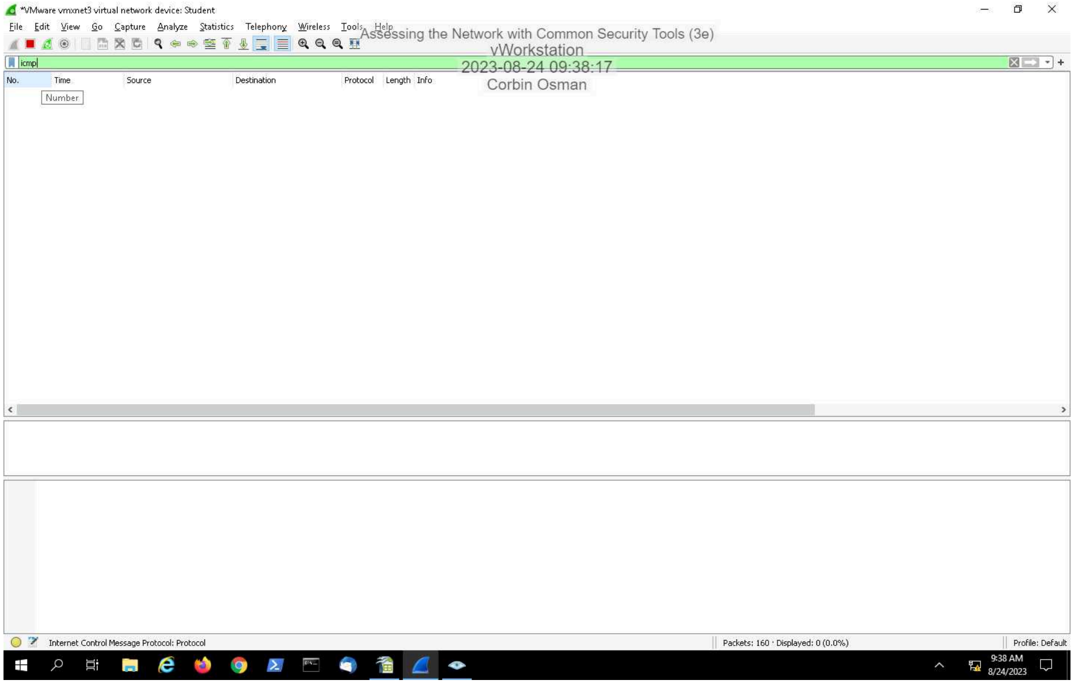
NetworkAssessment.ods - OpenOffice Calc

Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-08-24 09:36:49
Corbin Osman

	A	B	C	D	E
1	Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
2	vWorkstation	172.30.0.2	255.255.255.0	00-50-56-AB-EC-11	172.30.0.1
3	TargetWindows01	172.30.0.10	255.255.255.0	00-50-56-AB-C0-37	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

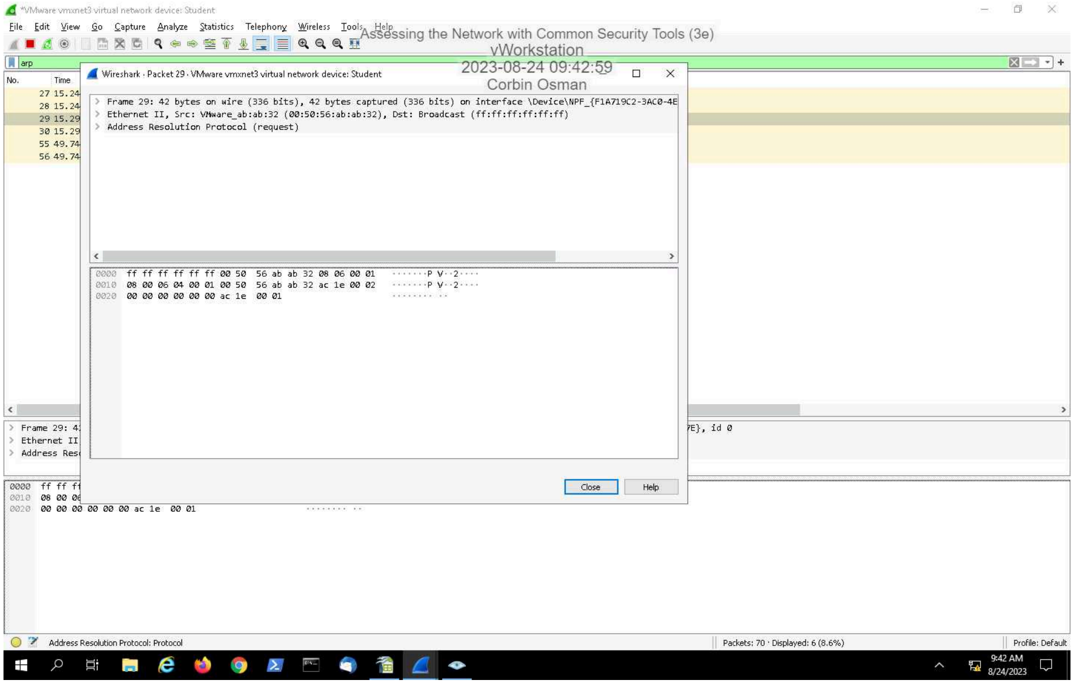
Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-08-24 09:38:17
Corbin Osman

icmp

Packets: 160 · Displayed: 0 (0.0%)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No.
Time
Source
Destination
Protocol
Length
Info
Number
Internet Control Message Protocol: Protocol
Profile: Default
9:38 AM
8/24/2023

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


*VMware vmxnet3 virtual network device: Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time
Close
Help
Address Resolution Protocol: Protocol
Packets: 70 · Displayed: 6 (8.6%)
Profile: Default
9:42 AM
8/24/2023

Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-08-24 09:42:59
Corbin Osman

Wireshark · Packet 29 · VMware vmxnet3 virtual network device: Student

```
27 15.24
28 15.24
29 15.29
30 15.29
55 49.74
56 49.74
```

```
> Frame 29: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F1A719C2-3AC0-4E
> Ethernet II, Src: VMware_ab:ab:32 (00:50:56:ab:ab:32), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 50  56 ab ab 32 08 06 00 01   ·······P V··2····
0010  08 00 06 04 00 01 00 50  56 ab ab 32 ac 1e 00 02   ·······P V··2····
0020  00 00 00 00 00 00 ac 1e  00 01                     ········ ··
```

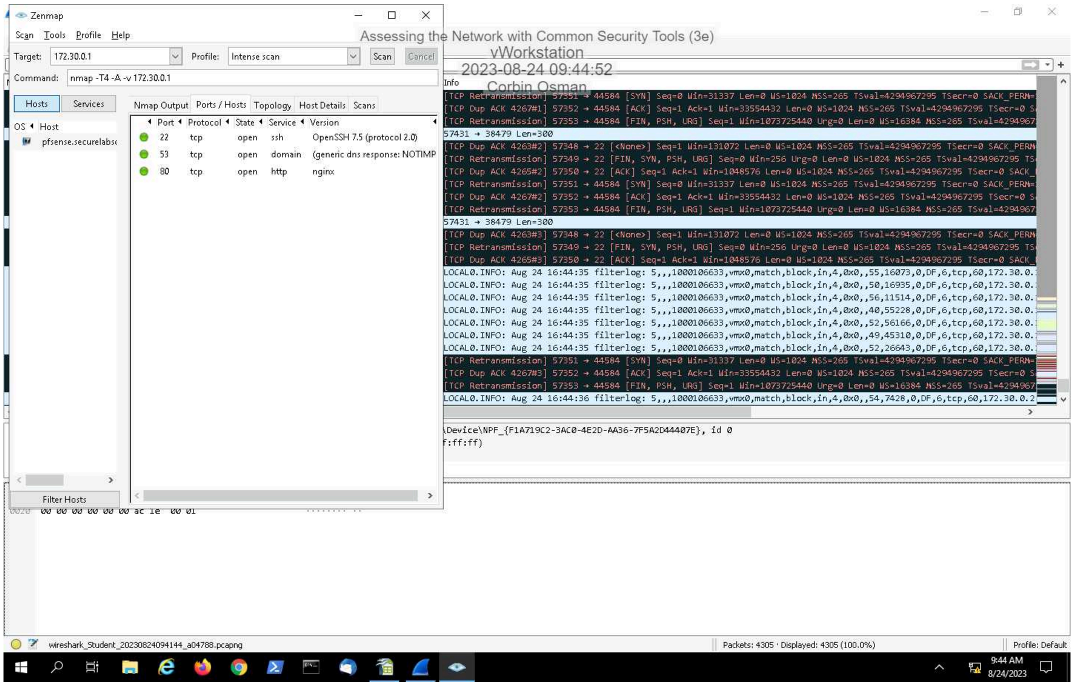
18. **Compare** the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

The regular scan yielded one icmp result, while the original ping scan did not result in any within icmp. The source for this icmp packet was the 172.30.0.2 IP, with the destination of 172.30.0.10. Visibly there doesn’t appear to be much difference between the arp results for the ping and regular scan types, as the arp results continue to grow as wireshark continues to monitor the network traffic.

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

After the intense scan there were several results for the icmp traffic. The info for them were either echo requests and replies or destination unreachable. For the arp traffic there were two instances of the RARP protocol, and the destination was listed as broadcast. The info was asking the question of who a specific physical address belonged to.

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



Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-08-24 09:44:52
Corbin Osman

Target: 172.30.0.1 Profile: Intense scan

Command: nmap -T4 -A -v 172.30.0.1

```
OS  Host
    pfsense.securelabsc

   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
```

```
[TCP Retransmission] 57351 → 44584 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM=
[TCP Dup ACK 4267#1] 57352 → 44584 [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 S
[TCP Retransmission] 57353 → 44584 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967
57431 → 38479 Len=300
[TCP Dup ACK 4263#2] 57348 → 22 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
[TCP Retransmission] 57349 → 22 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TS
[TCP Dup ACK 4265#2] 57350 → 22 [ACK] Seq=1 Ack=1 Win=1048576 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_
[TCP Retransmission] 57351 → 44584 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM=
[TCP Dup ACK 4267#2] 57352 → 44584 [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 S
[TCP Retransmission] 57353 → 44584 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967
57431 → 38479 Len=300
[TCP Dup ACK 4263#3] 57348 → 22 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
[TCP Retransmission] 57349 → 22 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TS
[TCP Dup ACK 4265#3] 57350 → 22 [ACK] Seq=1 Ack=1 Win=1048576 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_
LOCAL0.INFO: Aug 24 16:44:35 filterlog: 5,,,1000106633,vmx0,match,block,in,4,0x0,,55,16073,0,DF,6,tcp,60,172.30.0.
LOCAL0.INFO: Aug 24 16:44:35 filterlog: 5,,,1000106633,vmx0,match,block,in,4,0x0,,50,16935,0,DF,6,tcp,60,172.30.0.
LOCAL0.INFO: Aug 24 16:44:35 filterlog: 5,,,1000106633,vmx0,match,block,in,4,0x0,,56,11514,0,DF,6,tcp,60,172.30.0.
LOCAL0.INFO: Aug 24 16:44:35 filterlog: 5,,,1000106633,vmx0,match,block,in,4,0x0,,40,55228,0,DF,6,tcp,60,172.30.0.
LOCAL0.INFO: Aug 24 16:44:35 filterlog: 5,,,1000106633,vmx0,match,block,in,4,0x0,,52,56166,0,DF,6,tcp,60,172.30.0.
LOCAL0.INFO: Aug 24 16:44:35 filterlog: 5,,,1000106633,vmx0,match,block,in,4,0x0,,49,45310,0,DF,6,tcp,60,172.30.0.
LOCAL0.INFO: Aug 24 16:44:35 filterlog: 5,,,1000106633,vmx0,match,block,in,4,0x0,,52,26643,0,DF,6,tcp,60,172.30.0.
[TCP Retransmission] 57351 → 44584 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM=
[TCP Dup ACK 4267#3] 57352 → 44584 [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 S
[TCP Retransmission] 57353 → 44584 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967
LOCAL0.INFO: Aug 24 16:44:36 filterlog: 5,,,1000106633,vmx0,match,block,in,4,0x0,,54,7428,0,DF,6,tcp,60,172.30.0.2
```

```
\Device\NPF_{F1A719C2-3AC0-4E2D-AA36-7F5A2D44407E}, id 0
f:ff:ff)
```

```
0020  00 00 00 00 00 00 ac 1e  00 01
```

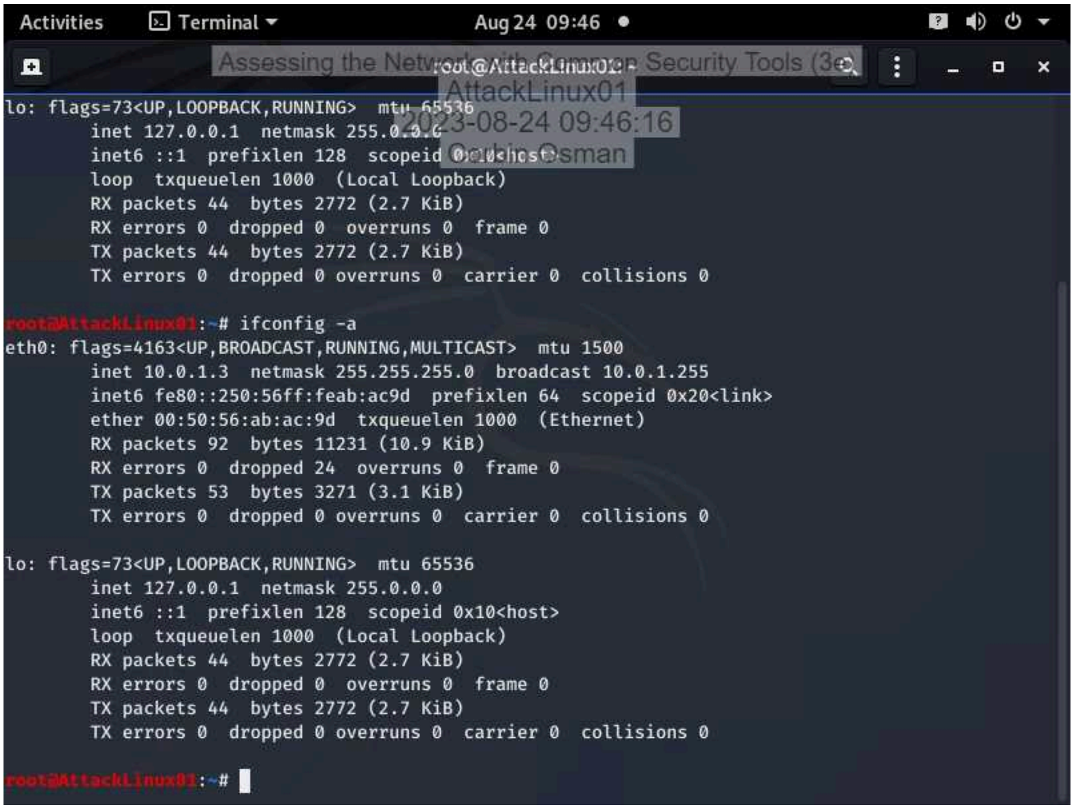
wireshark_Student_20230824094144_a04788.pcapng | Packets: 4305 · Displayed: 4305 (100.0%) | Profile: Default

9:44 AM
8/24/2023

Section 2: Applied Learning

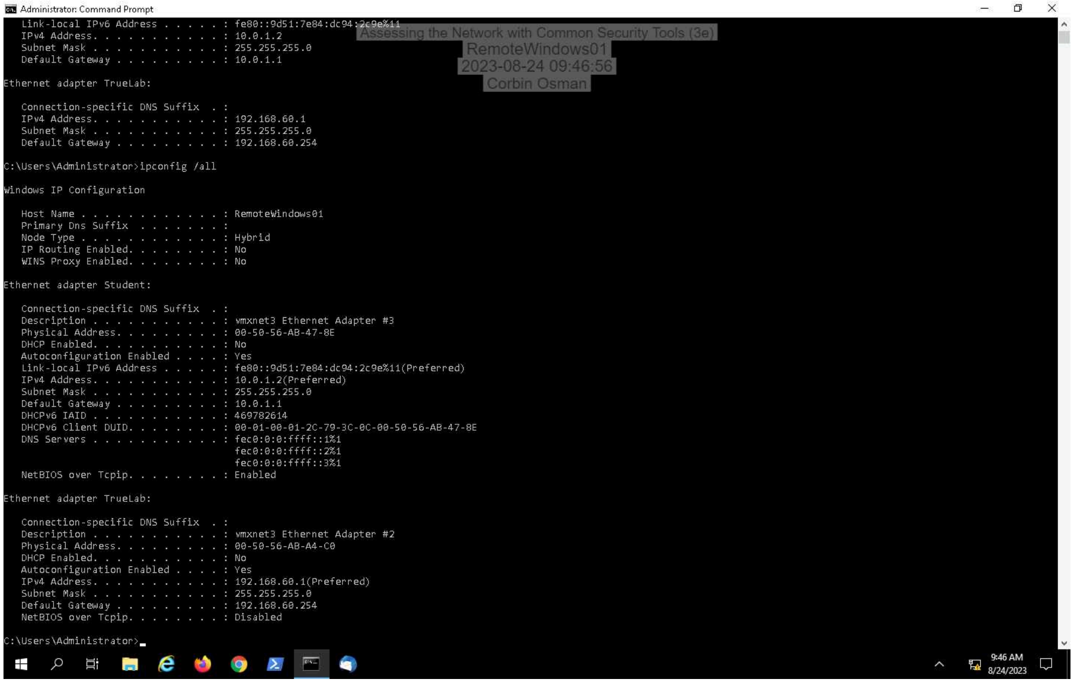
Part 1: Explore the Wide Area Network

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



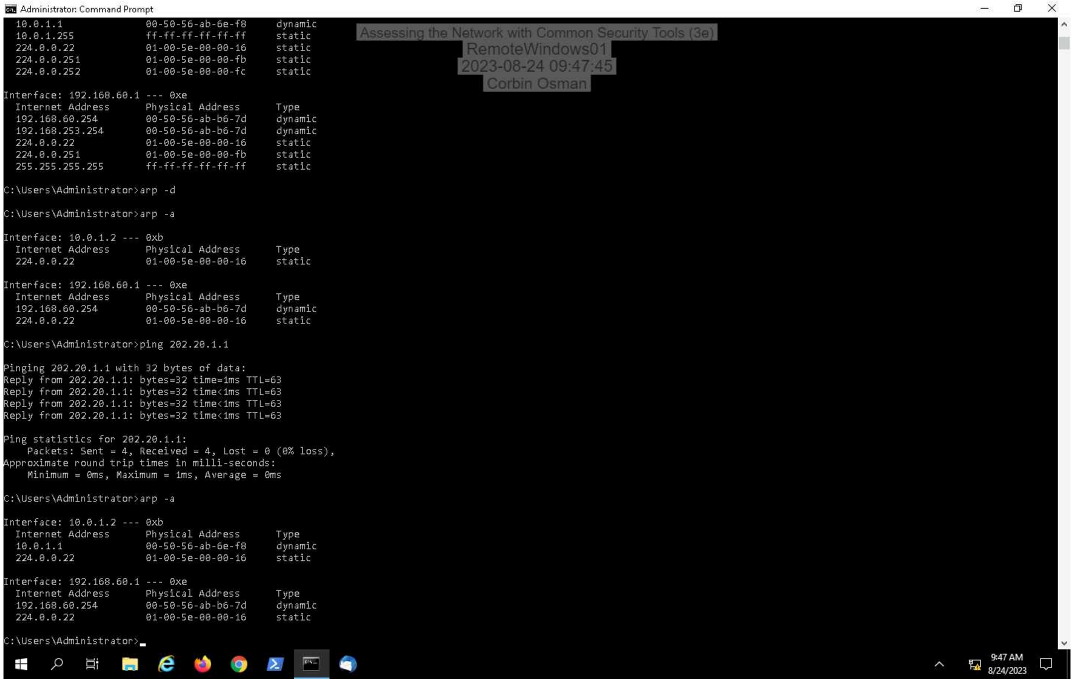
```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 44  bytes 2772 (2.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 2772 (2.7 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:feab:ac9d  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:ab:ac:9d  txqueuelen 1000  (Ethernet)
        RX packets 92  bytes 11231 (10.9 KiB)
        RX errors 0  dropped 24  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 44  bytes 2772 (2.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 2772 (2.7 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**.


Administrator: Command Prompt
Assessing the Network with Common Security Tools (3e)
RemoteWindows01
2023-08-24 09:46:56
Corbin Osman
9:46 AM
8/24/2023

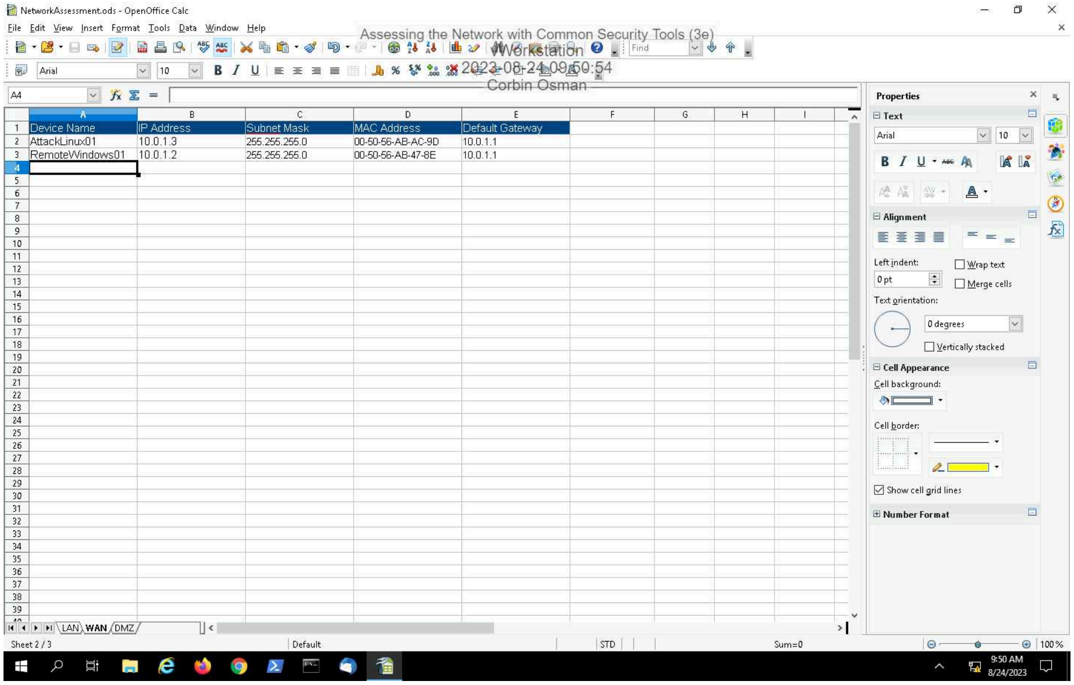
```
   Link-local IPv6 Address . . . . . : fe80::9d51:7e84:dc94:2c9e%11
   IPv4 Address. . . . . . . . . . . : 10.0.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1

Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.60.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.60.254

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-AB-47-8E
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9d51:7e84:dc94:2c9e%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. . . . . . . . : 00-01-00-01-2C-79-3C-0C-00-50-56-AB-47-8E
   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-AB-A4-C0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.60.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.60.254
   NetBIOS over Tcpip. . . . . . . . : Disabled

C:\Users\Administrator>_
```

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


Administrator: Command Prompt
Assessing the Network with Common Security Tools (3e)
RemoteWindows01
2023-08-24 09:47:45
Corbin Osman
9:47 AM
8/24/2023

```
  10.0.1.1              00-50-56-ab-6e-f8     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: 192.168.60.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.60.254        00-50-56-ab-b6-7d     dynamic
  192.168.253.254       00-50-56-ab-b6-7d     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>arp -d

C:\Users\Administrator>arp -a

Interface: 10.0.1.2 --- 0xb
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.60.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.60.254        00-50-56-ab-b6-7d     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-ab-6e-f8     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.60.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.60.254        00-50-56-ab-b6-7d     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>_
```

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

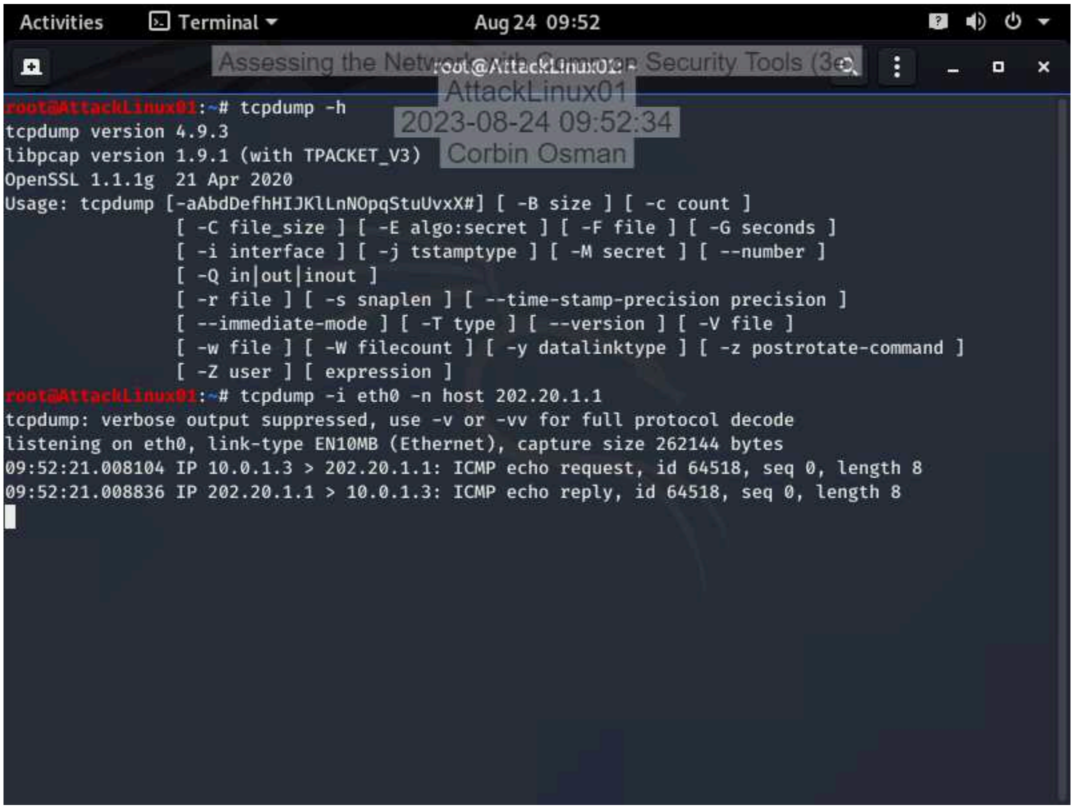


Assessing the Network with Common Security Tools (3e)
vWorkstation
2023-08-24 09:50:54
Corbin Osman

Device Name	IP Address	Subnet Mask	MAC Address	Default Gateway
AttackLinux01	10.0.1.3	255.255.255.0	00-50-56-AB-AC-9D	10.0.1.1
RemoteWindows01	10.0.1.2	255.255.255.0	00-50-56-AB-47-8E	10.0.1.1

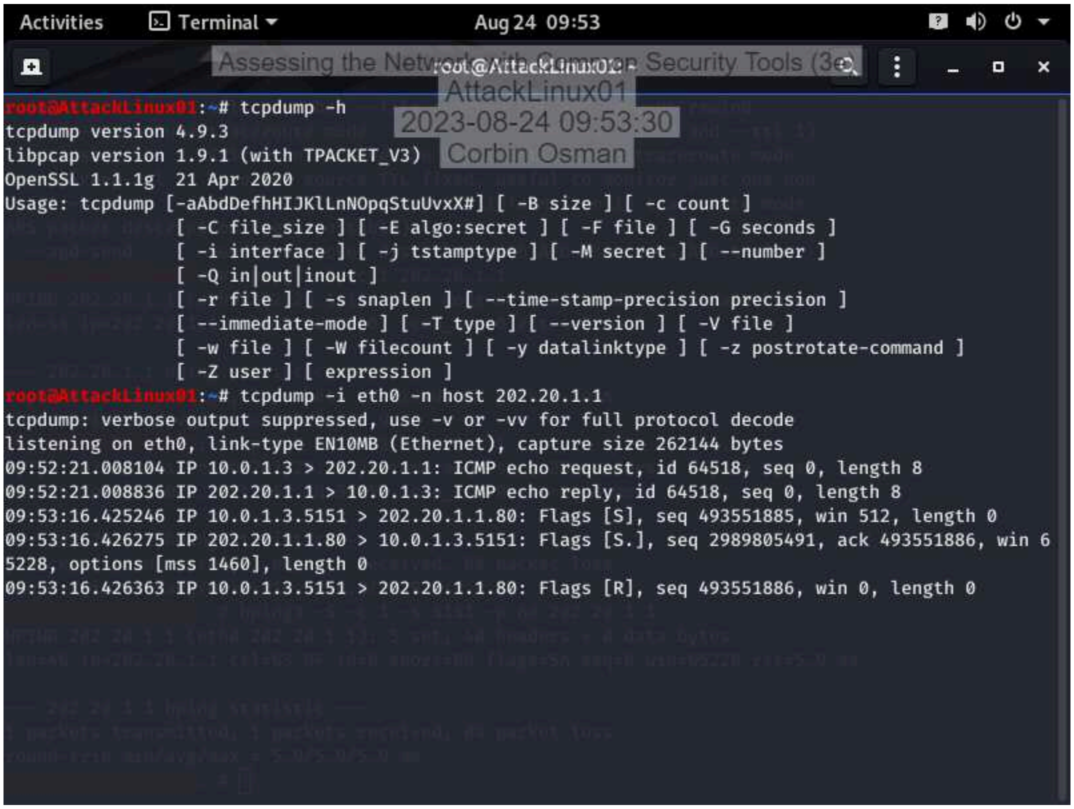
Part 2: Analyze Network Traffic

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



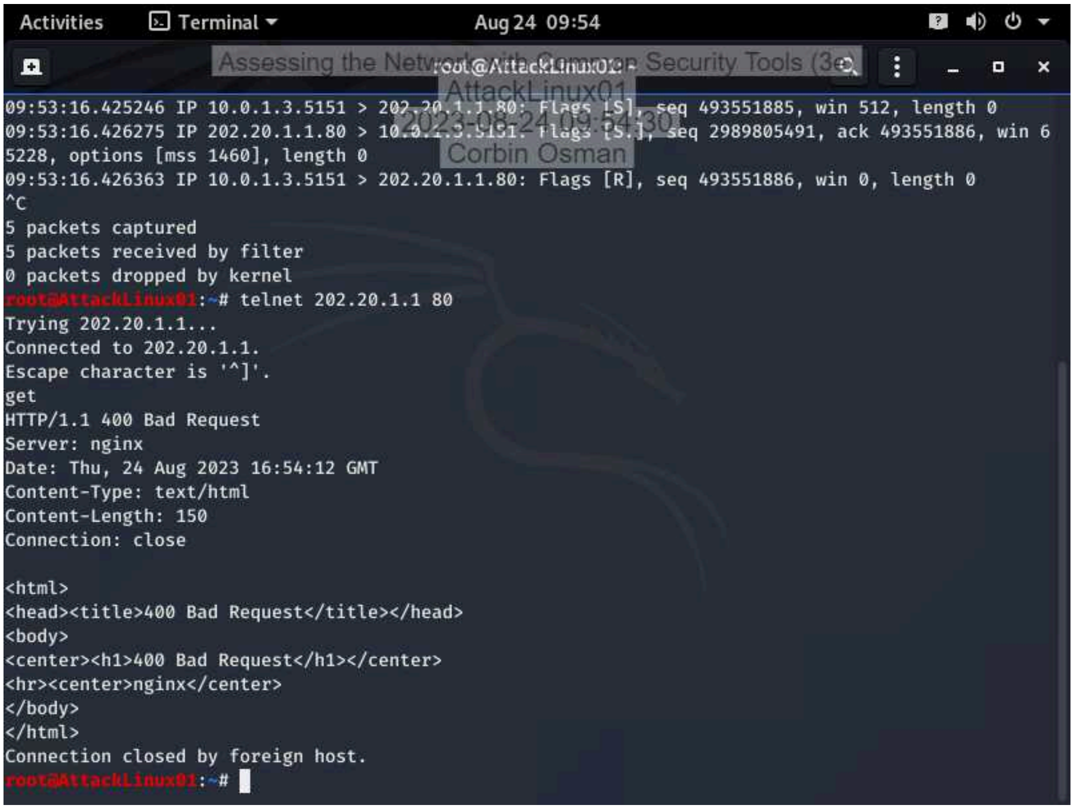
```
root@AttackLinux01:~# tcpdump -h
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1g  21 Apr 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -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 202.20.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:52:21.008104 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 64518, seq 0, length 8
09:52:21.008836 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 64518, seq 0, length 8
```

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



```
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 202.20.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:52:21.008104 IP 10.0.1.3 > 202.20.1.1: ICMP echo request, id 64518, seq 0, length 8
09:52:21.008836 IP 202.20.1.1 > 10.0.1.3: ICMP echo reply, id 64518, seq 0, length 8
09:53:16.425246 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [S], seq 493551885, win 512, length 0
09:53:16.426275 IP 202.20.1.1.80 > 10.0.1.3.5151: Flags [S.], seq 2989805491, ack 493551886, win 6
5228, options [mss 1460], length 0
09:53:16.426363 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [R], seq 493551886, win 0, length 0
```

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



```
09:53:16.425246 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [S], seq 493551885, win 512, length 0
09:53:16.426275 IP 202.20.1.1.80 > 10.0.1.3.5151: Flags [S.], seq 2989805491, ack 493551886, win 6
5228, options [mss 1460], length 0
09:53:16.426363 IP 10.0.1.3.5151 > 202.20.1.1.80: Flags [R], seq 493551886, win 0, length 0
^C
5 packets captured
5 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 '^]'.
get
HTTP/1.1 400 Bad Request
Server: nginx
Date: Thu, 24 Aug 2023 16:54:12 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**.

Incomplete

Part 2: Perform Reconnaissance on the Firewall

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

Incomplete