

Assessing the Network with Common Security Tools (3e)

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

Student:

Nick Derleth

Email:

nderle02664@fontbonne.edu

Time on Task:

0 hours, 44 minutes

Progress:

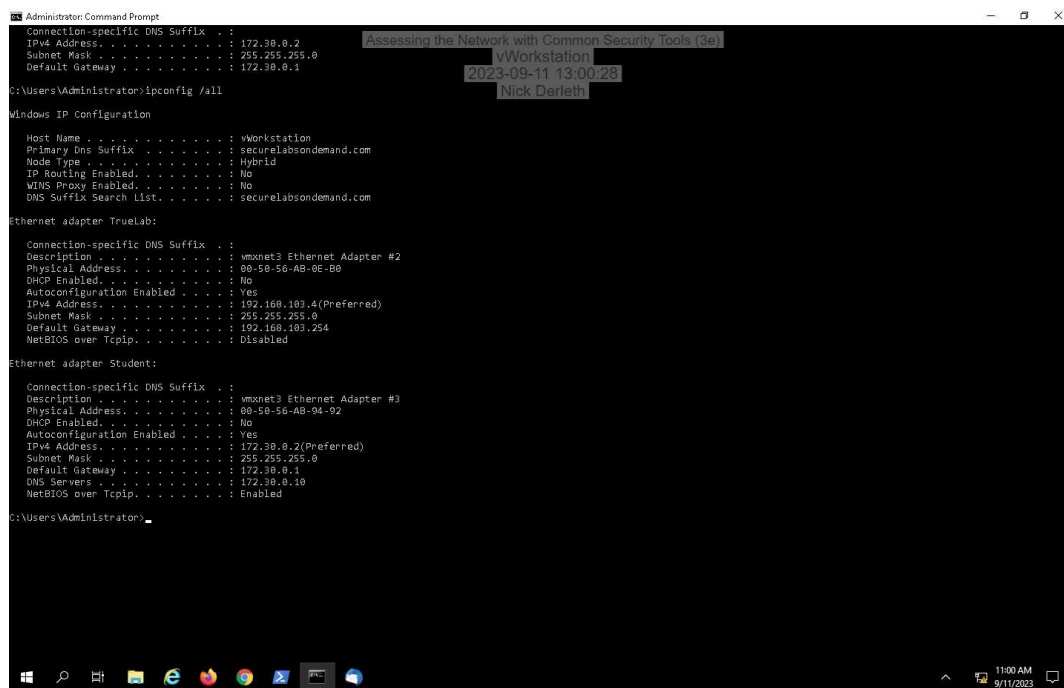
50%

Report Generated: Friday, September 22, 2023 at 8:29 AM

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
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:

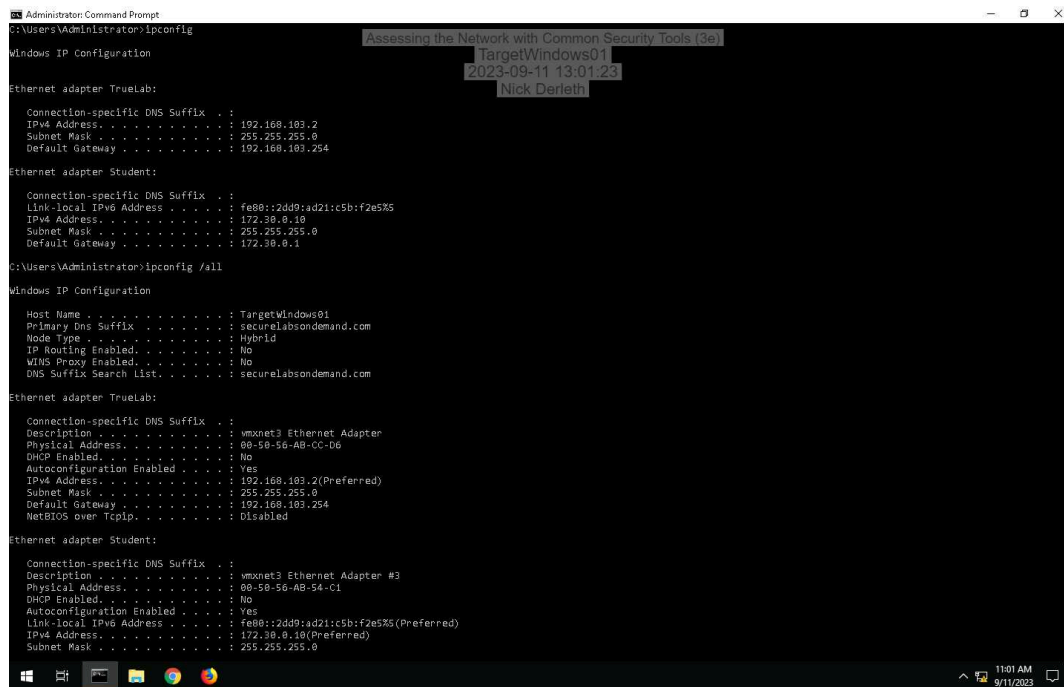
Connection-specific DNS Suffix . : 
Description . . . . . : vmxnet3 Ethernet Adapter #2
Physical Address. . . . . : 00-50-56-AB-0E-B0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.103.4(Prefered)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.103.254
NetBIOS over Tcpip. . . . . : Disabled

Ethernet adapter Student:

Connection-specific DNS Suffix . : 
Description . . . . . : vmxnet3 Ethernet Adapter #3
Physical Address. . . . . : 00-50-56-AB-04-92
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 172.30.0.2(Prefered)
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
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter TrueLab:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.103.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.103.254

Ethernet adapter Student:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2dd9:ad21:c5b:f2e5%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

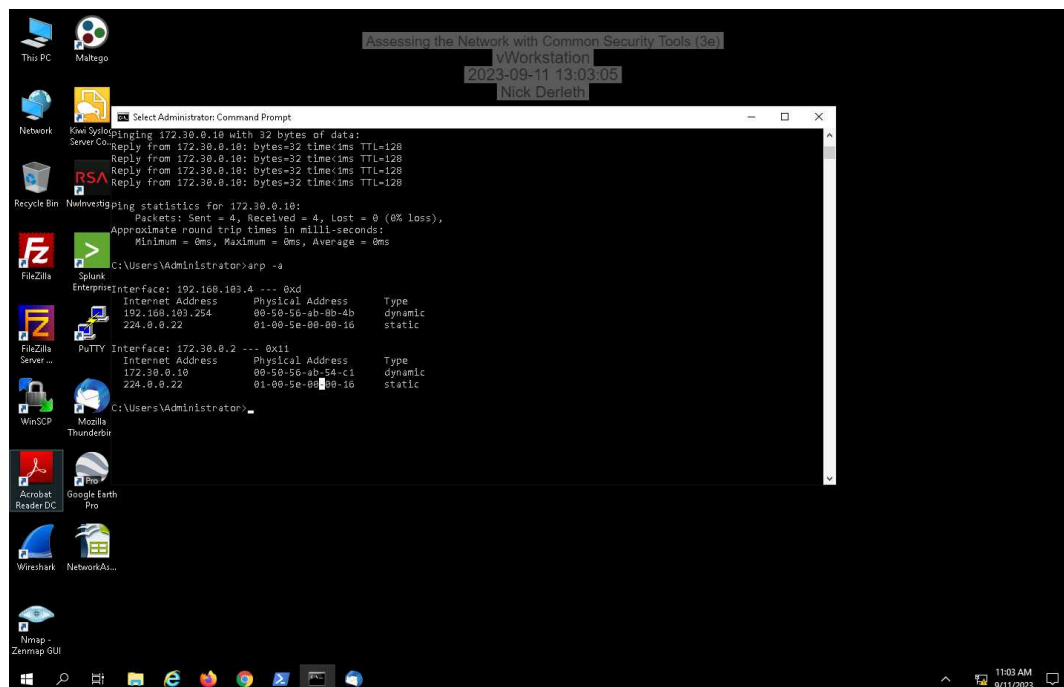
Ethernet adapter TrueLab:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : vmxnet3 Ethernet Adapter
    Physical Address. . . . . : 00-50-56-AB-CC-D6
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.103.2(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.103.254
    NetBIOS over Tcpip. . . . . : Disabled

Ethernet adapter Student:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : vmxnet3 Ethernet Adapter #3
    Physical Address. . . . . : 00-50-56-AB-54-C1
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::2dd9:ad21:c5b:f2e5%5(Preferred)
    IPv4 Address. . . . . : 172.30.0.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
```

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



```
Select Administrator: Command Prompt

C:\Users\Administrator>arp -a

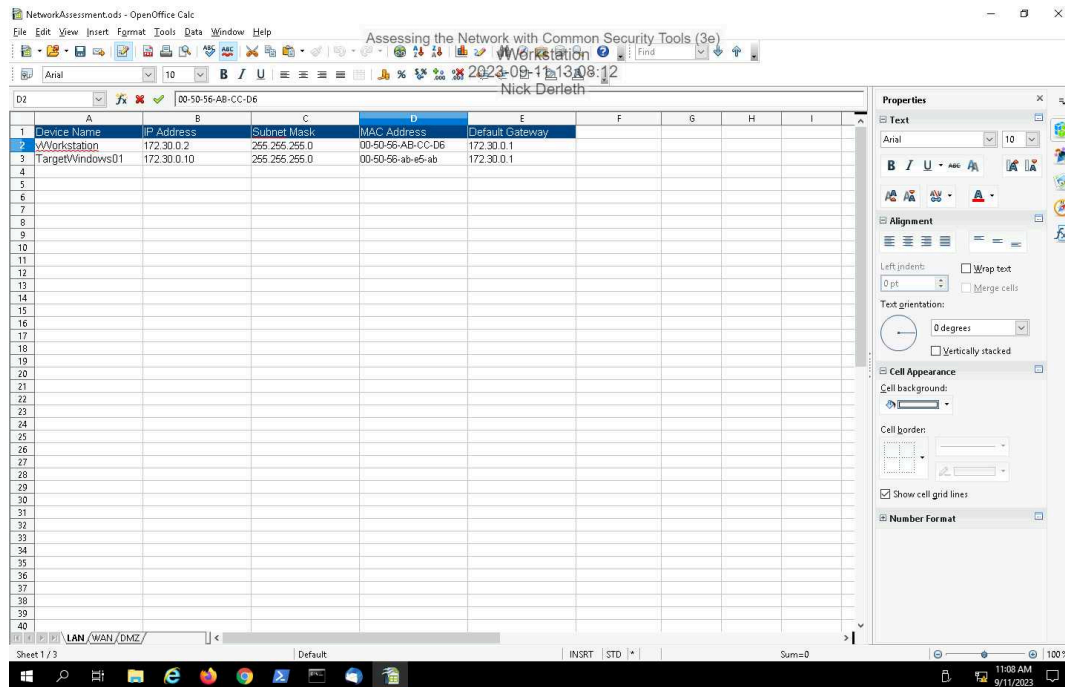
Interface: 192.168.103.4 --- 0xd
Internet Address      Physical Address      Type
192.168.103.254       00-50-56-ab-88-4b     dynamic
224.0.0.22            01-00-5e-00-00-16     static

Interface: 172.30.0.2 --- 0x11
Internet Address      Physical Address      Type
172.30.0.10           00-50-56-ab-54-c1     dynamic
224.0.0.22            01-00-5e-00-00-16     static
```

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.

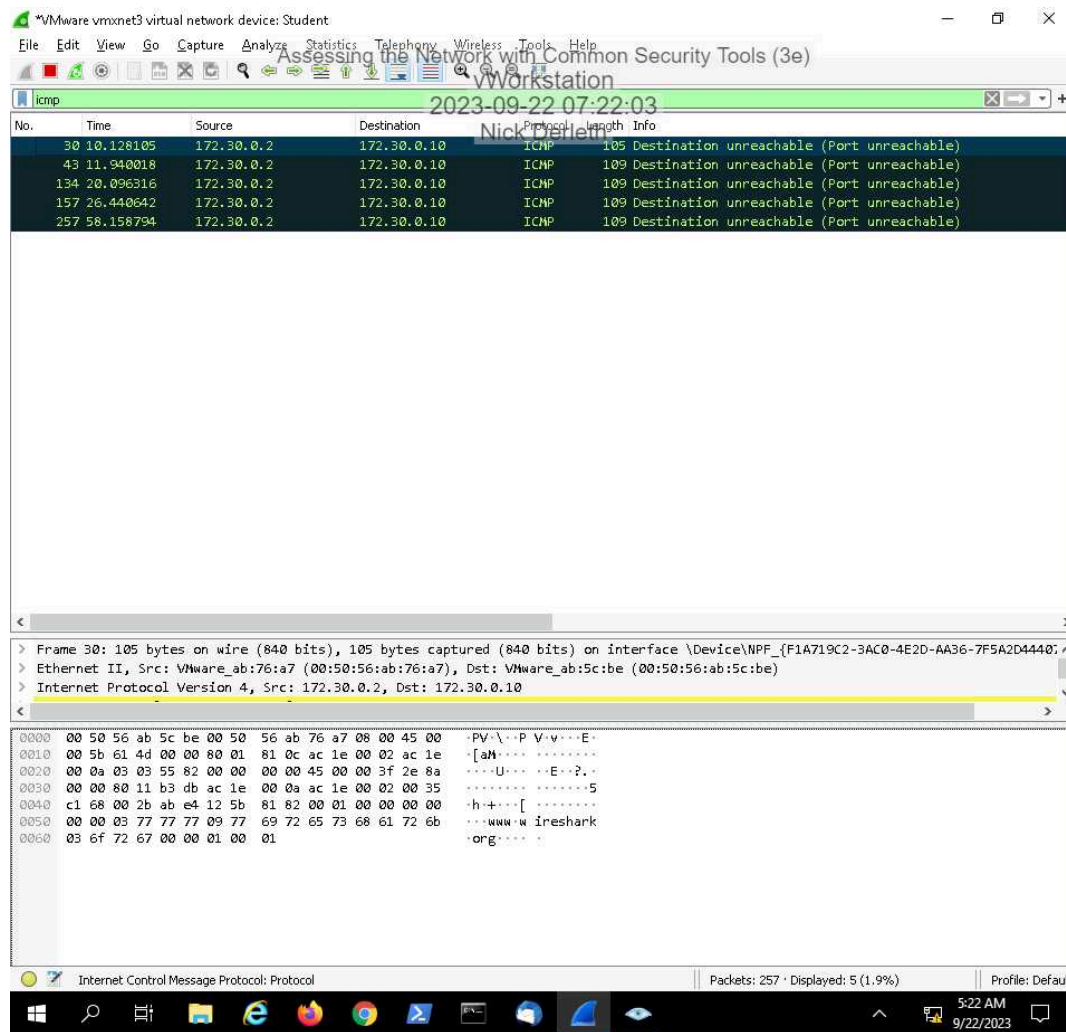


Part 2: Analyze Network Traffic

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

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

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)

2023-09-22 07:24:03

arp

No.	Time	Source	Destination	Protocol	Length	Info
159	26.814882	VNware_ab:5c:be	VNware_ab:50:ed	ARP	60	Who has 172.30.0.1? Tell 172.30.0.10
160	26.814944	VNware_ab:50:ed	VNware_ab:5c:be	ARP	60	172.30.0.1 is at 00:50:56:ab:50:ed
190	34.310826	VNware_ab:76:a7	Broadcast	ARP	42	Who has 172.30.0.1? Tell 172.30.0.2
191	34.311166	VNware_ab:50:ed	VNware_ab:76:a7	ARP	60	172.30.0.1 is at 00:50:56:ab:50:ed
275	63.040186	VNware_ab:76:a7	VNware_ab:5c:be	ARP	42	Who has 172.30.0.10? Tell 172.30.0.2
276	63.040465	VNware_ab:5c:be	VNware_ab:76:a7	ARP	60	172.30.0.10 is at 00:50:56:ab:5c:be
282	64.814834	VNware_ab:5c:be	VNware_ab:50:ed	ARP	60	Who has 172.30.0.1? Tell 172.30.0.10
283	64.815038	VNware_ab:50:ed	VNware_ab:5c:be	ARP	60	172.30.0.1 is at 00:50:56:ab:50:ed
332	102.693432	VNware_ab:50:ed	Broadcast	RARP	60	Who is 00:50:56:ab:50:ed? Tell 00:50:56:ab:50:ed
333	102.814913	VNware_ab:5c:be	VNware_ab:50:ed	ARP	60	Who has 172.30.0.1? Tell 172.30.0.10
334	102.814995	VNware_ab:50:ed	VNware_ab:5c:be	ARP	60	172.30.0.1 is at 00:50:56:ab:50:ed
397	141.330924	VNware_ab:76:a7	Broadcast	ARP	42	Who has 172.30.0.1? Tell 172.30.0.2
398	141.331256	VNware_ab:50:ed	VNware_ab:76:a7	ARP	60	172.30.0.1 is at 00:50:56:ab:50:ed
405	142.814888	VNware_ab:5c:be	VNware_ab:50:ed	ARP	60	Who has 172.30.0.1? Tell 172.30.0.10
406	142.814999	VNware_ab:50:ed	VNware_ab:5c:be	ARP	60	172.30.0.1 is at 00:50:56:ab:50:ed
407	144.696219	VNware_ab:5c:be	Broadcast	RARP	60	Who is 00:50:56:ab:5c:be? Tell 00:50:56:ab:5c:be
408	146.039195	VNware_ab:76:a7	VNware_ab:5c:be	ARP	42	Who has 172.30.0.10? Tell 172.30.0.2
409	146.039450	VNware_ab:5c:be	VNware_ab:76:a7	ARP	60	172.30.0.10 is at 00:50:56:ab:5c:be
415	146.314806	VNware_ab:5c:be	VNware_ab:76:a7	ARP	60	Who has 172.30.0.2? Tell 172.30.0.10
416	146.314830	VNware_ab:76:a7	VNware_ab:5c:be	ARP	42	172.30.0.2 is at 00:50:56:ab:76:a7
472	173.543641	VNware_ab:76:a7	VNware_ab:5c:be	ARP	42	Who has 172.30.0.10? Tell 172.30.0.2
473	173.543848	VNware_ab:5c:be	VNware_ab:76:a7	ARP	60	172.30.0.10 is at 00:50:56:ab:5c:be

> Frame 416: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F1A719C2-3AC0-4E2D-AA36-7F5A2D44407E},
> Ethernet II, Src: VNware_ab:76:a7 (00:50:56:ab:76:a7), Dst: VNware_ab:5c:be (00:50:56:ab:5c:be)
> Address Resolution Protocol (reply)

0000 00 50 56 ab 5c be 00 50 56 ab 76 a7 08 06 00 01 -PV-...P V-ψ-...
0010 08 00 06 04 00 02 00 50 56 ab 76 a7 ac 1e 00 02 -...-P V-ψ-...
0020 00 50 56 ab 5c be ac 1e 00 0a -PV-... ..

Address Resolution Protocol: Protocol

Packets: 479 · Displayed: 22 (4.6%)

Profile: Default

5:24 AM
9/22/2023

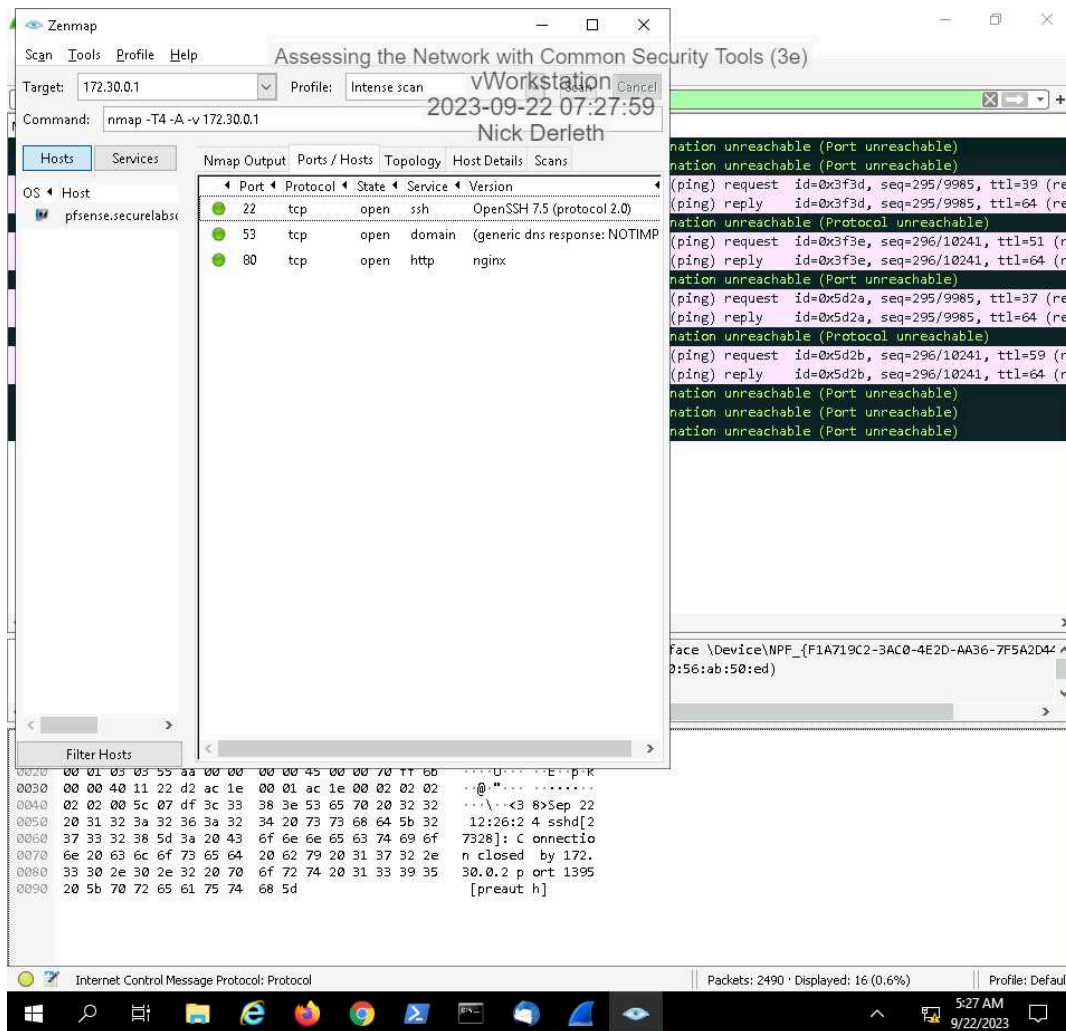
18. **Compare** the Regular scan results for ICMP and ARP traffic with the results from the Ping scan.

ICMP traffic seemed the same on both scans but ARP had much more traffic on the regular scan than the ping scan.

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

ICMP seemed to be sending more requests and getting more replies while ARP stayed the same.

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**.

Incomplete

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

Incomplete

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

Incomplete

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

Incomplete

Part 2: Analyze Network Traffic

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

Incomplete

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

Incomplete

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

Incomplete

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