Jason Hodge

Lab 02 – Analyzing Network Traffic using Packet Capture Software

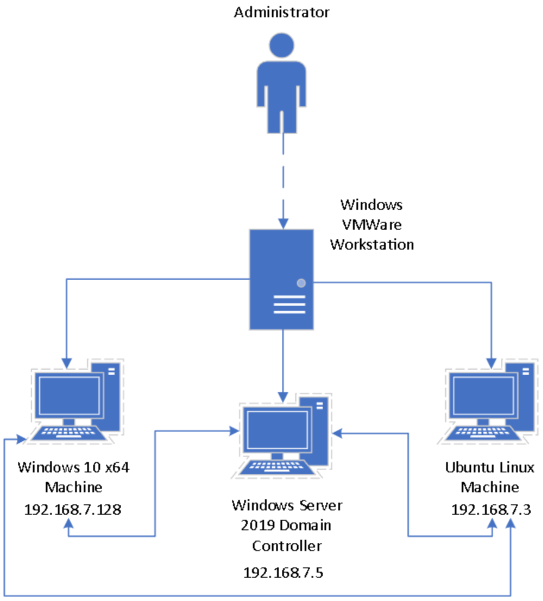
October 10, 2023

Description:

The primary objective of this lab was to set up an Ubuntu Linux virtual machine (VM) on VMware Workstation to utilize as a "Sniffer" machine where we ran our packet capture software, Wireshark. We had to make sure these virtual machines were on the same network to ensure they could communicate with each other when analyzing through network traffic between our Windows 10 client VM and Windows 10 server VM.

We then verified and traced the path a packet takes from the Windows client to the Windows server. Next, we displayed the ARP cache, which we used to verify the mac addresses of our VMs compared to the information from the ipconfig command. In addition, we opened a remote desktop connection and logged in as the administrator to map a network drive from the client machine to the server. Lastly, we generated a couple additional types of network traffic from the client to the server.

Topology:



This is an overview of the three virtual machines built and utilized in this lab within VMWare Workstation. All three of these virtual machines are interconnected as they were all configured on the same network 192.168.7.1.

Key Syntax:

We utilized Command Prompt (CMD) to check the hostname and IPv4 address, subnet mask, default gateway and DNS Servers. This was used as a second verification to see the changes have been made.

Commands:

‘hostname’: Provides the computer’s host name.

‘ipconfig /all’: Provides full detailed adapter configuration information (IPv4 address, subnet mask, default gateway, DNS Servers, etc.)

‘ipconfig /release’: Forces the client to immediately give up its Ip address lease.

‘ipconfig /renew’: Allows your DHCP client to gain a new Ip address lease.

‘sudo wireshark’: Runs Wireshark in Ubuntu terminal.

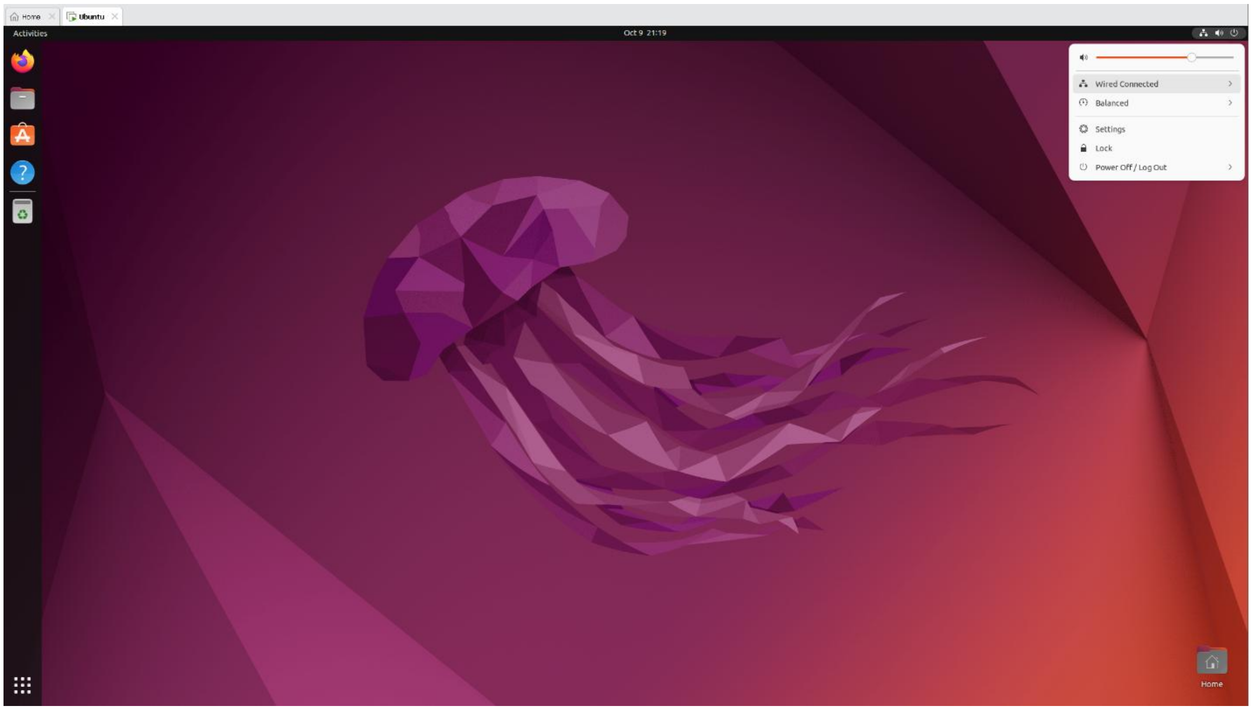
‘mstsc’: Pulls up windows remote desktop when run.

‘\\(host Ip)’: Pulls up the shared folder in run.

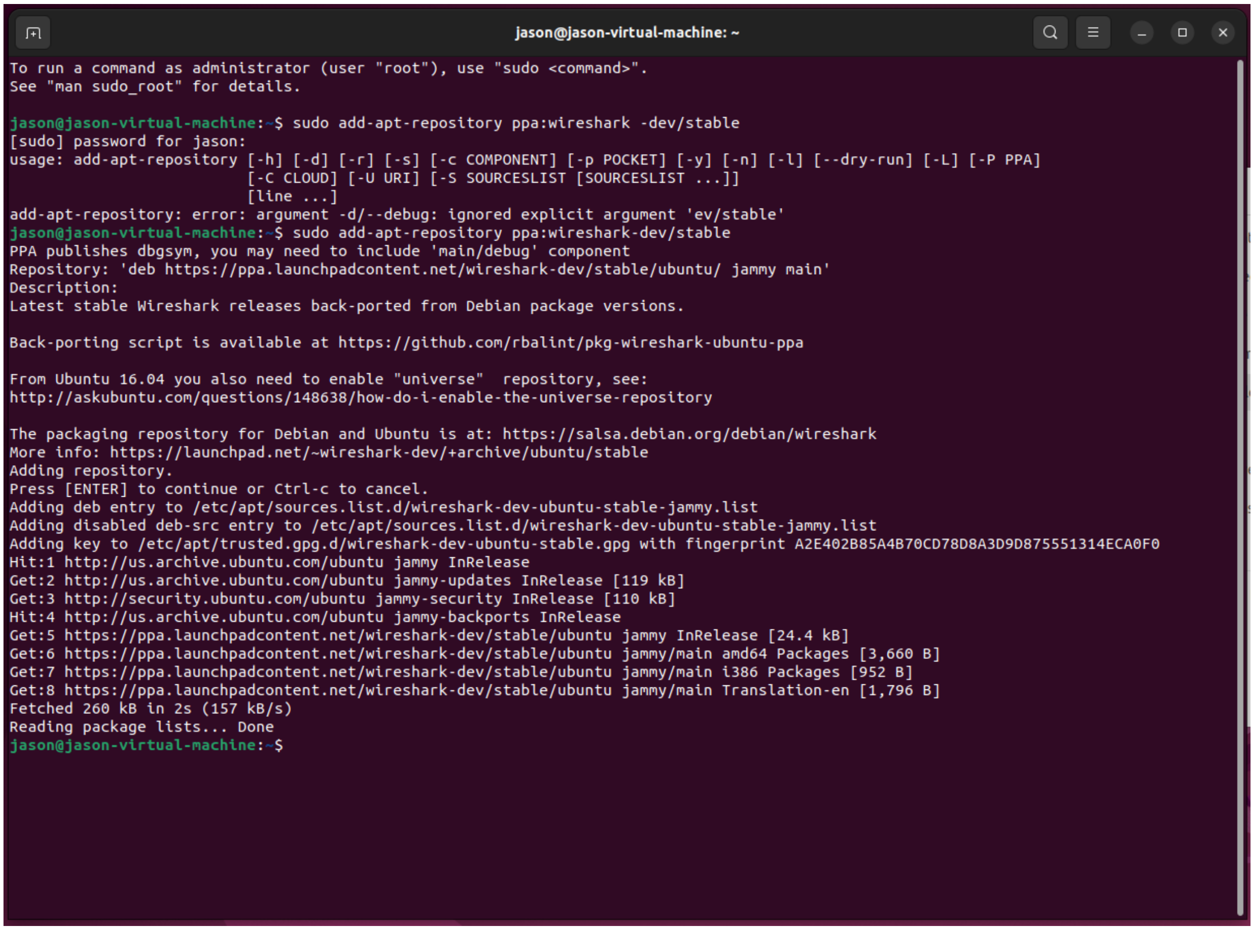
‘ping (host Ip address)’: Tests ping connectivity.

Verification:

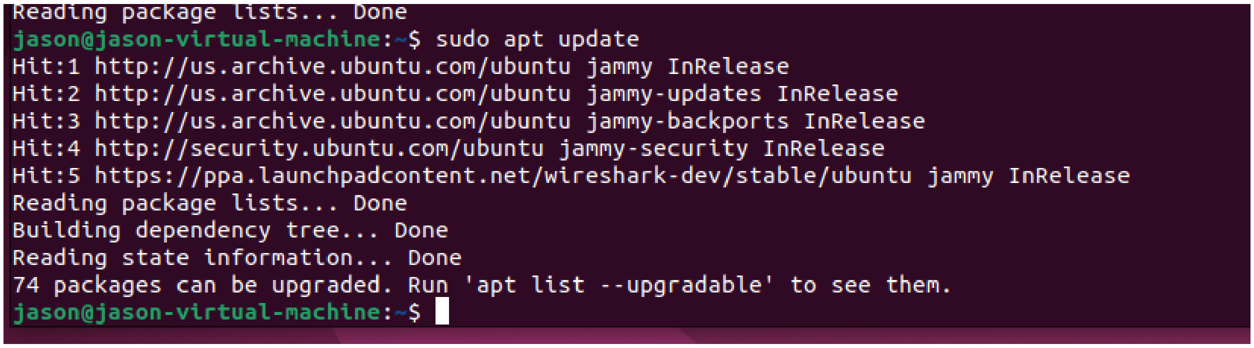
TASK ONE: VM and Wireshark Installation



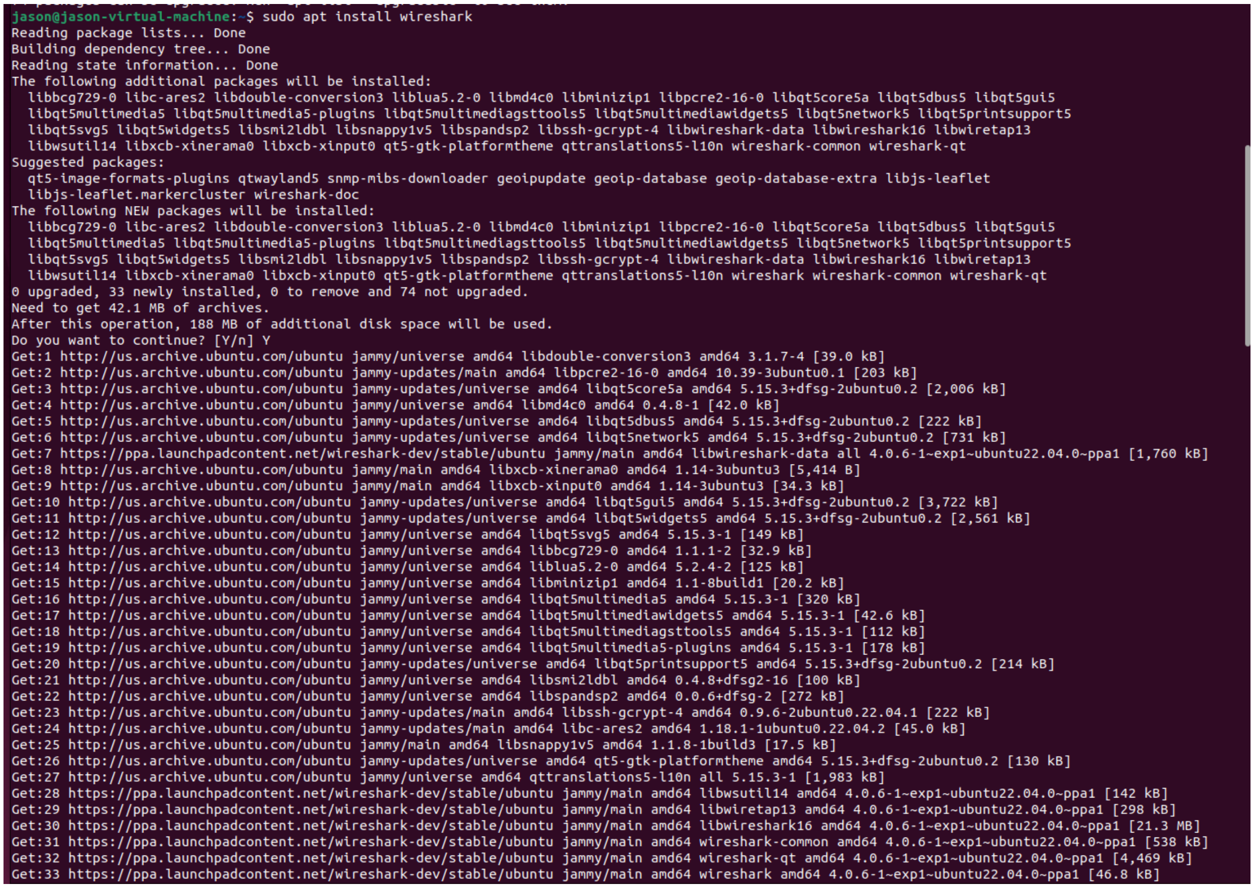
This screenshot is of my Ubuntu VM connected to the internet.



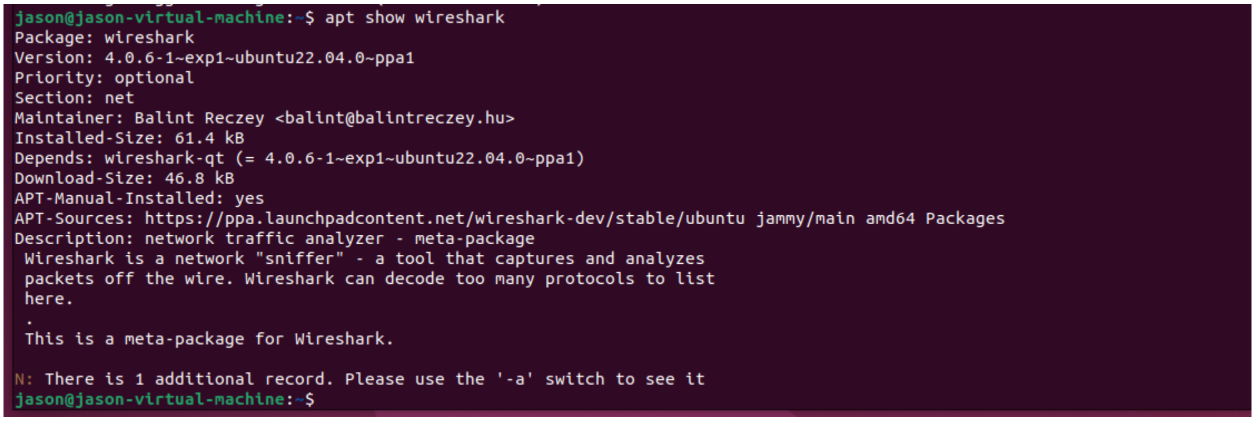
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jason@jason-virtual-machine:~$ sudo add-apt-repository ppa:wireshark -dev/stable
[sudo] password for jason:
usage: add-apt-repository [-h] [-d] [-r] [-s] [-c COMPONENT] [-p POCKET] [-y] [-n] [-l] [--dry-run] [-L] [-P PPA]
                          [-C CLOUD] [-U URI] [-S SOURCESLIST [SOURCESLIST ...]]
                          [line ...]
add-apt-repository: error: argument -d/--debug: ignored explicit argument 'ev/stable'
jason@jason-virtual-machine:~$ sudo add-apt-repository ppa:wireshark-dev/stable
PPA publishes dbgsym, you may need to include 'main/debug' component
Repository: 'deb https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu/ jammy main'
Description:
Latest stable Wireshark releases back-ported from Debian package versions.

Back-porting script is available at https://github.com/rbalint/pkg-wireshark-ubuntu-ppa

From Ubuntu 16.04 you also need to enable "universe"  repository, see:
http://askubuntu.com/questions/148638/how-do-i-enable-the-universe-repository

The packaging repository for Debian and Ubuntu is at: https://salsa.debian.org/debian/wireshark
More info: https://launchpad.net/~wireshark-dev/+archive/ubuntu/stable
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.
Adding deb entry to /etc/apt/sources.list.d/wireshark-dev-ubuntu-stable-jammy.list
Adding disabled deb-src entry to /etc/apt/sources.list.d/wireshark-dev-ubuntu-stable-jammy.list
Adding key to /etc/apt/trusted.gpg.d/wireshark-dev-ubuntu-stable.gpg with fingerprint A2E402B85A4B70CD78D8A3D9D875551314ECA0F0
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:5 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy InRelease [24.4 kB]
Get:6 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 Packages [3,660 B]
Get:7 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main i386 Packages [952 B]
Get:8 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main Translation-en [1,796 B]
Fetched 260 kB in 2s (157 kB/s)
Reading package lists... Done
jason@jason-virtual-machine:~$
```



```
Reading package lists... Done
jason@jason-virtual-machine:~$ sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
74 packages can be upgraded. Run 'apt list --upgradable' to see them.
jason@jason-virtual-machine:~$
```

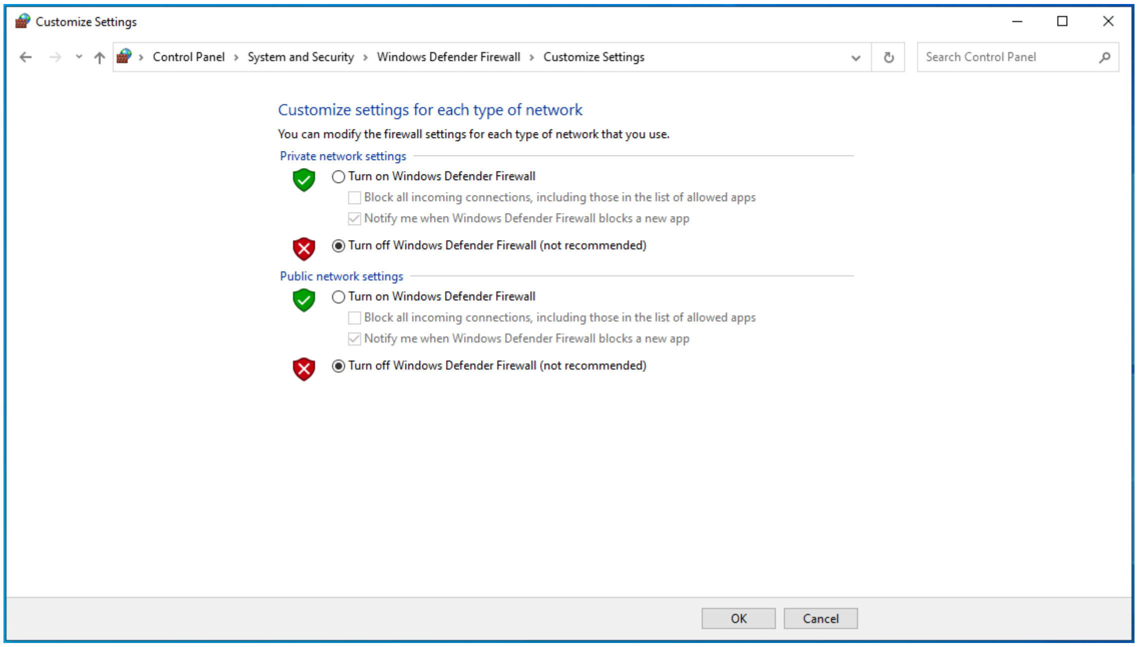


```
jason@jason-virtual-machine:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0 libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5 libqt5printsupport5
  libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark16 libwiretap13
  libwsutil14 libxcb-xinerama0 libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0 libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5 libqt5printsupport5
  libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark16 libwiretap13
  libwsutil14 libxcb-xinerama0 libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common wireshark-qt
0 upgraded, 33 newly installed, 0 to remove and 74 not upgraded.
Need to get 42.1 MB of archives.
After this operation, 188 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libdouble-conversion3 amd64 3.1.7-4 [39.0 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpcre2-16-0 amd64 10.39-3ubuntu0.1 [203 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libqt5core5a amd64 5.15.3+dfsg-2ubuntu0.2 [2,006 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libmd4c0 amd64 0.4.8-1 [42.0 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libqt5dbus5 amd64 5.15.3+dfsg-2ubuntu0.2 [222 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libqt5network5 amd64 5.15.3+dfsg-2ubuntu0.2 [731 kB]
Get:7 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 libwireshark-data all 4.0.6-1~exp1~ubuntu22.04.0~ppa1 [1,760 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 libxcb-xinerama0 amd64 1.14-3ubuntu3 [5,414 B]
Get:9 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 libxcb-xinput0 amd64 1.14-3ubuntu3 [34.3 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libqt5gui5 amd64 5.15.3+dfsg-2ubuntu0.2 [3,722 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libqt5widgets5 amd64 5.15.3+dfsg-2ubuntu0.2 [2,561 kB]
Get:12 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libqt5svg5 amd64 5.15.3-1 [149 kB]
Get:13 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libbcg729-0 amd64 1.1.1-2 [32.9 kB]
Get:14 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 liblua5.2-0 amd64 5.2.4-2 [125 kB]
Get:15 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libminizip1 amd64 1.1-8build1 [20.2 kB]
Get:16 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libqt5multimedia5 amd64 5.15.3-1 [320 kB]
Get:17 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libqt5multimediawidgets5 amd64 5.15.3-1 [42.6 kB]
Get:18 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libqt5multimediagsttools5 amd64 5.15.3-1 [112 kB]
Get:19 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libqt5multimedia5-plugins amd64 5.15.3-1 [178 kB]
Get:20 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libqt5printsupport5 amd64 5.15.3+dfsg-2ubuntu0.2 [214 kB]
Get:21 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libsmi2ldbl amd64 0.4.8+dfsg2-16 [100 kB]
Get:22 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libspandsp2 amd64 0.0.6+dfsg-2 [272 kB]
Get:23 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libssh-gcrypt-4 amd64 0.9.6-2ubuntu0.22.04.1 [222 kB]
Get:24 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libc-ares2 amd64 1.18.1-1ubuntu0.22.04.2 [45.0 kB]
Get:25 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 libsnappy1v5 amd64 1.1.8-1build3 [17.5 kB]
Get:26 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 qt5-gtk-platformtheme amd64 5.15.3+dfsg-2ubuntu0.2 [130 kB]
Get:27 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 qttranslations5-l10n all 5.15.3-1 [1,983 kB]
Get:28 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 libwsutil14 amd64 4.0.6-1~exp1~ubuntu22.04.0~ppa1 [142 kB]
Get:29 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 libwiretap13 amd64 4.0.6-1~exp1~ubuntu22.04.0~ppa1 [298 kB]
Get:30 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 libwireshark16 amd64 4.0.6-1~exp1~ubuntu22.04.0~ppa1 [21.3 MB]
Get:31 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 wireshark-common amd64 4.0.6-1~exp1~ubuntu22.04.0~ppa1 [538 kB]
Get:32 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 wireshark-qt amd64 4.0.6-1~exp1~ubuntu22.04.0~ppa1 [4,469 kB]
Get:33 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 wireshark amd64 4.0.6-1~exp1~ubuntu22.04.0~ppa1 [46.8 kB]
```



```
jason@jason-virtual-machine:~$ apt show wireshark
Package: wireshark
Version: 4.0.6-1~exp1~ubuntu22.04.0~ppa1
Priority: optional
Section: net
Maintainer: Balint Reczey <balint@balintreczey.hu>
Installed-Size: 61.4 kB
Depends: wireshark-qt (= 4.0.6-1~exp1~ubuntu22.04.0~ppa1)
Download-Size: 46.8 kB
APT-Manual-Installed: yes
APT-Sources: https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy/main amd64 Packages
Description: network traffic analyzer - meta-package
 Wireshark is a network "sniffer" - a tool that captures and analyzes
 packets off the wire. Wireshark can decode too many protocols to list
 here.
 .
 This is a meta-package for Wireshark.

N: There is 1 additional record. Please use the '-a' switch to see it
jason@jason-virtual-machine:~$
```

These screenshots are the steps in which it takes to install the packet capture software Wireshark via Ubuntu terminal.


Customize Settings
Control Panel › System and Security › Windows Defender Firewall › Customize Settings
Search Control Panel
OK
Cancel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

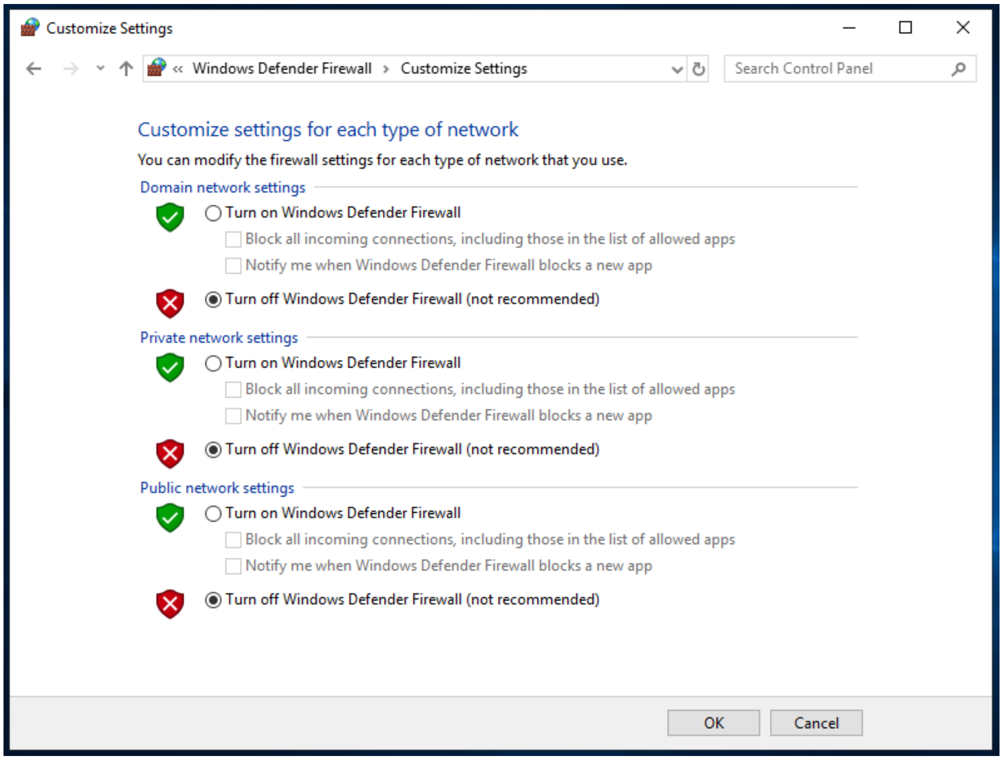
Public network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall

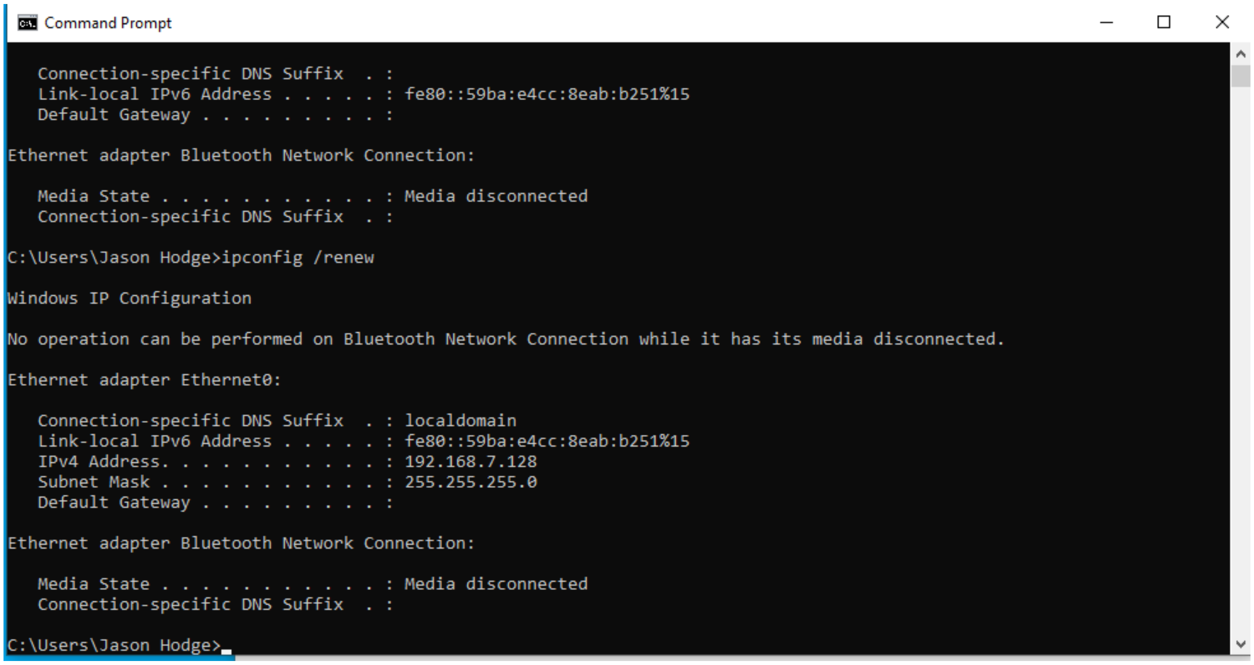
□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

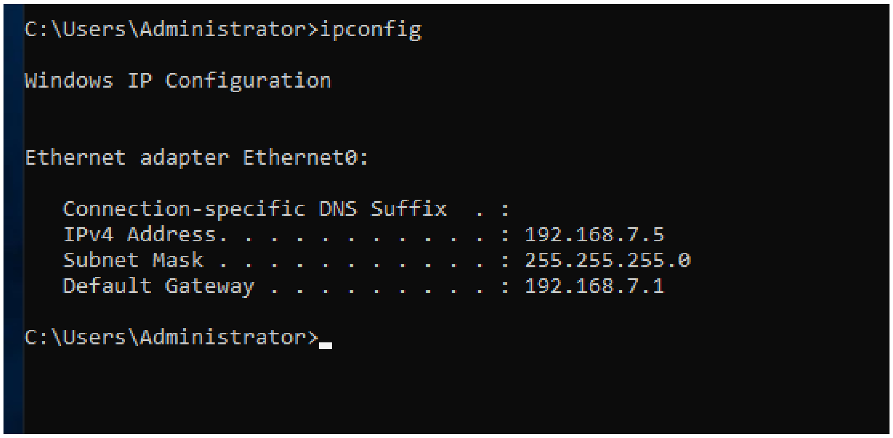
These screenshots show the disabling of the Windows Firewall, which is necessary for allowing remote access among other things.

TASK TWO: Generate and Capture Network Traffic



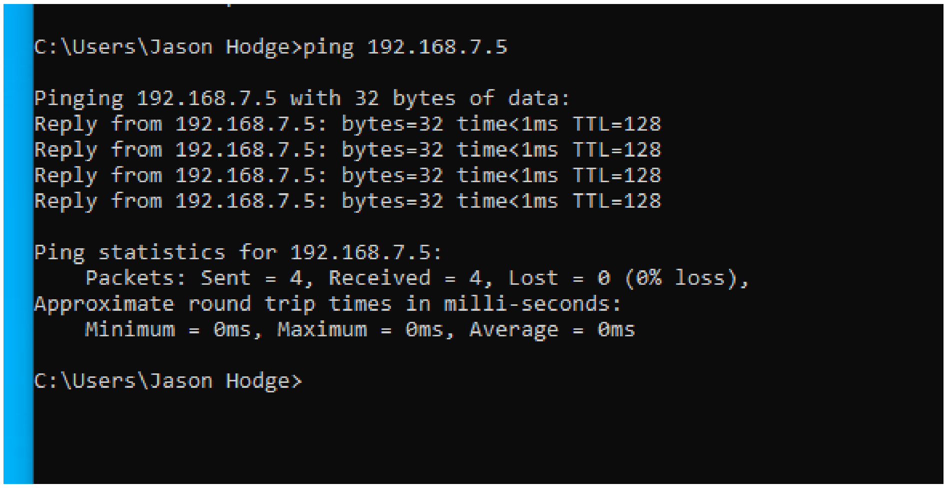
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::59ba:e4cc:8eab:b251%15
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Jason Hodge>ipconfig /renew

Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::59ba:e4cc:8eab:b251%15
   IPv4 Address. . . . . . . . . . . : 192.168.7.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Jason Hodge>
```

Here we see the Windows client address has been changed to network 7.



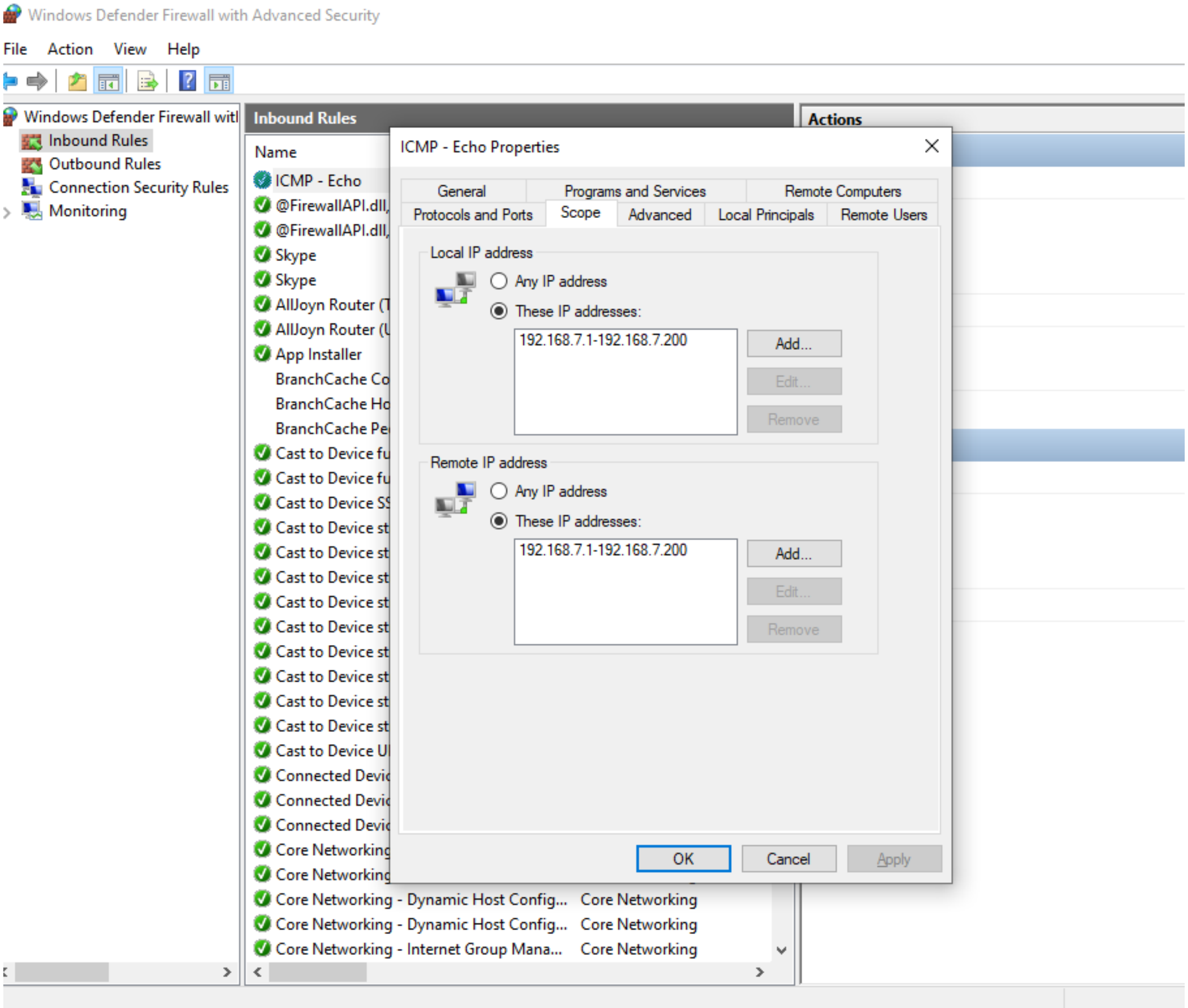
```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.7.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.7.1

C:\Users\Administrator>
```

In this screenshot we see the Windows server IPv4 Address is apart of the same network as the client VM.



```
C:\Users\Jason Hodge>ping 192.168.7.5

Pinging 192.168.7.5 with 32 bytes of data:
Reply from 192.168.7.5: bytes=32 time<1ms TTL=128
Reply from 192.168.7.5: bytes=32 time<1ms TTL=128
Reply from 192.168.7.5: bytes=32 time<1ms TTL=128
Reply from 192.168.7.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.7.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Jason Hodge>
```

Here is a successful ping to the Windows server from the client.



Local IP address

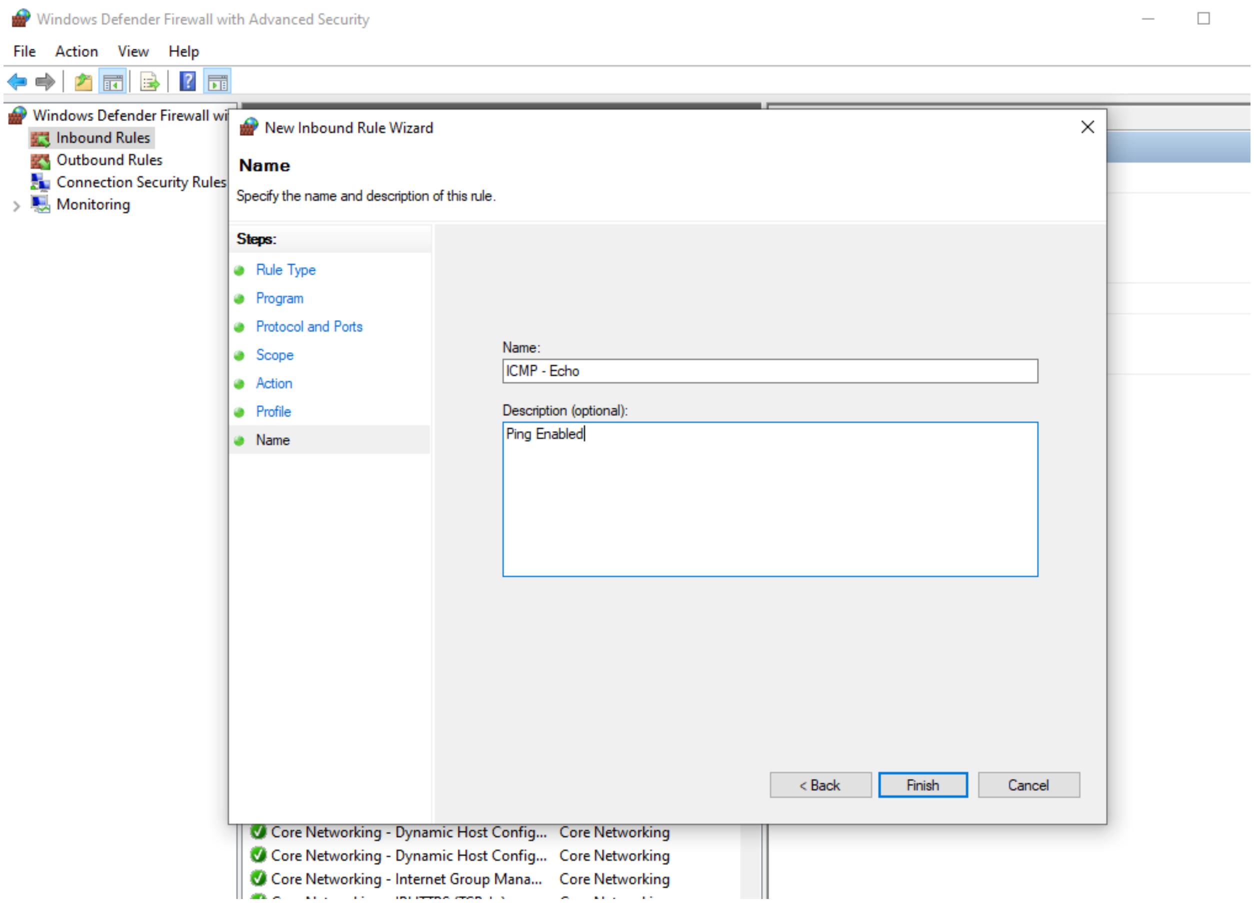
○ Any IP address
● These IP addresses:

192.168.7.1-192.168.7.200

Remote IP address

○ Any IP address
● These IP addresses:

192.168.7.1-192.168.7.200



Name

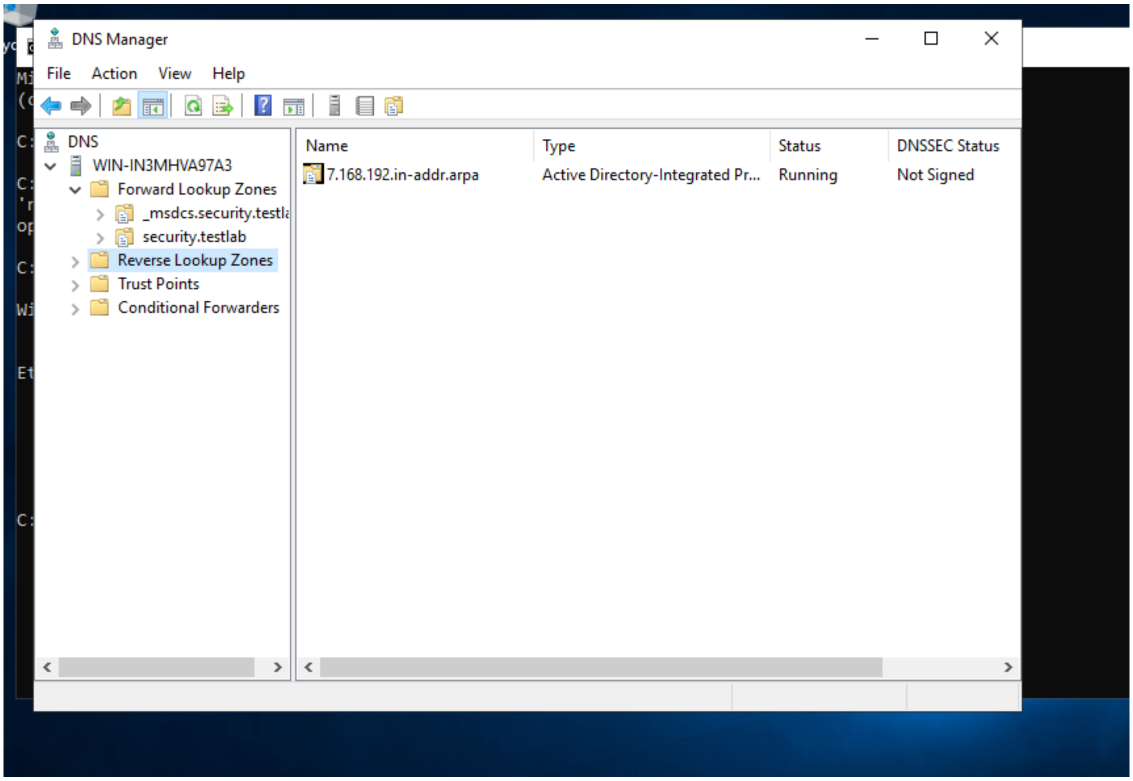
Specify the name and description of this rule.

Name: ICMP - Echo

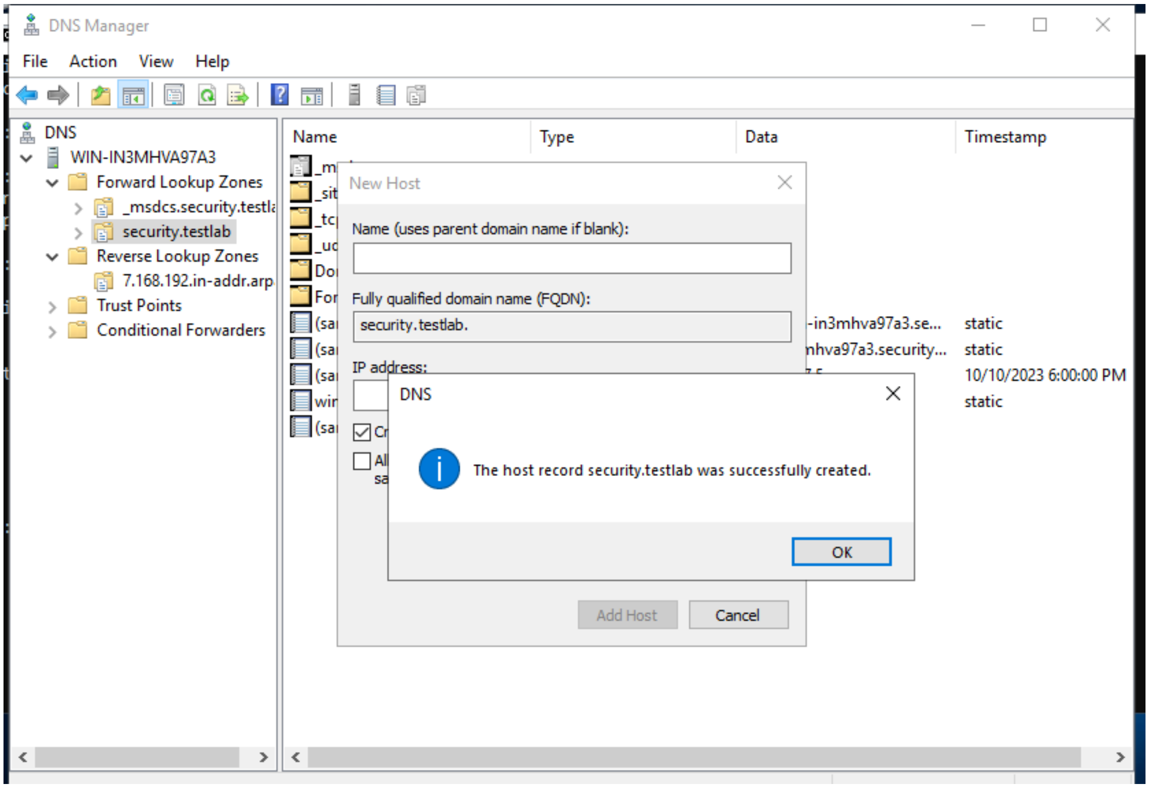
Description (optional): Ping Enabled

Core Networking - Dynamic Host Config...	Core Networking
Core Networking - Dynamic Host Config...	Core Networking
Core Networking - Internet Group Mana...	Core Networking

In these screenshots I added a new rule to the Windows Defender Firewall allowing for inbound ICMP Echo packets to be visible within a selected Ip address range.



Name	Type	Status	DNSSEC Status
7.168.192.in-addr.arpa	Active Directory-Integrated Pr...	Running	Not Signed



New Host

Name (uses parent domain name if blank):

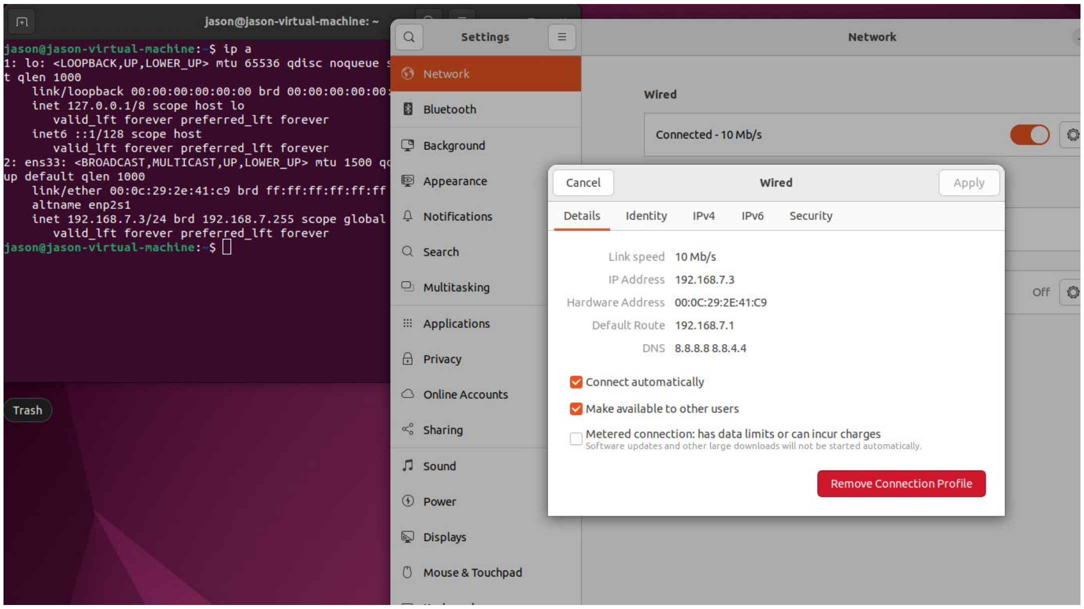
Fully qualified domain name (FQDN): security.testlab.

IP address:

DNS

The host record security.testlab was successfully created.

These two screenshots show the successful configuration of the DNS Windows Server with lookup zones for mapping host names to Ip addresses and vice versa.



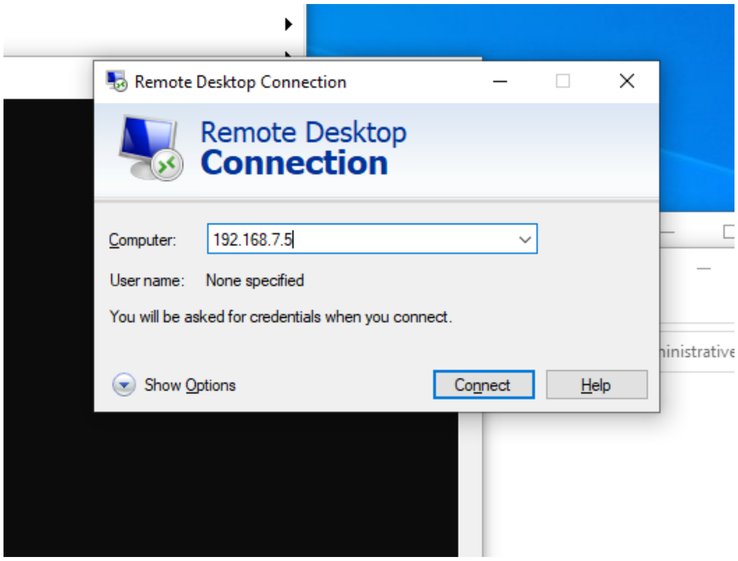
```
jason@jason-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue s
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qd
up default qlen 1000
    link/ether 00:0c:29:2e:41:c9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.7.3/24 brd 192.168.7.255 scope global
       valid_lft forever preferred_lft forever
jason@jason-virtual-machine:~$
```

Connected - 10 Mb/s

Link speed 10 Mb/s
IP Address 192.168.7.3
Hardware Address 00:0C:29:2E:41:C9
Default Route 192.168.7.1
DNS 8.8.8.8 8.8.4.4

☑ Connect automatically
☑ Make available to other users
□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

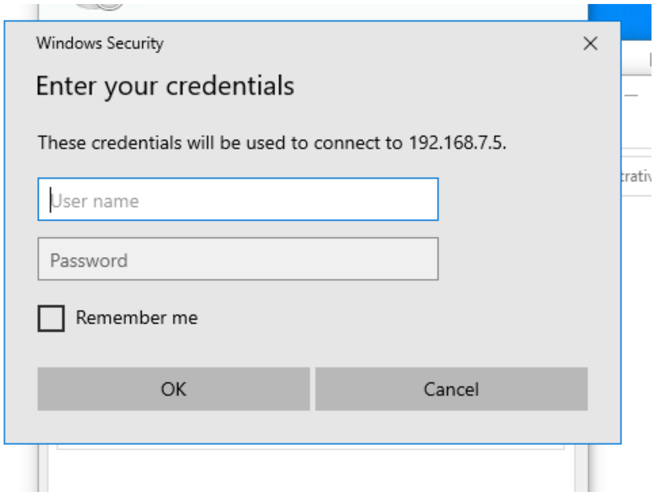
To get all three machines to exist on the same network I changed the Ip address on the ‘sniffer’ Ubuntu machine.



Computer: 192.168.7.5

User name: None specified

You will be asked for credentials when you connect.



Windows Security

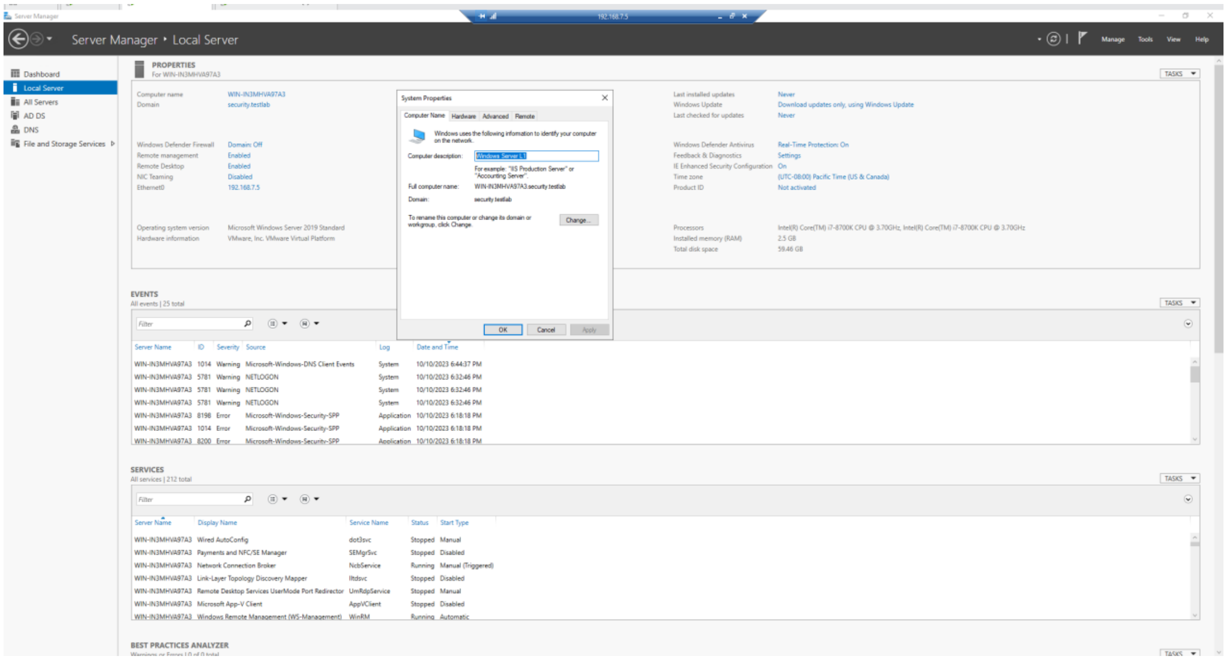
Enter your credentials

These credentials will be used to connect to 192.168.7.5.

User name

Password

□ Remember me



PROPERTIES
For WIN-IN3MHVA97A3

Computer name	WIN-IN3MHVA97A3
Domain	security.testlab
Windows Defender Firewall	Domain: Off
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Disabled
Ethernet0	192.168.7.5
Operating system version	Microsoft Windows Server 2019 Standard
Hardware information	VMware, Inc. VMware Virtual Platform
Last installed updates	Never
Windows Update	Download updates only, using Windows Update
Last checked for updates	Never
Windows Defender Antivirus	Real-Time Protection: On
Feedback & Diagnostics	Settings
IE Enhanced Security Configuration	On
Time zone	(UTC-08:00) Pacific Time (US & Canada)
Product ID	Not activated
Processors	Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz, Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
Installed memory (RAM)	2.5 GB
Total disk space	59.46 GB

System Properties

Windows uses the following information to identify your computer on the network.

Computer description: Windows Server L1

For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-IN3MHVA97A3.security.testlab

Domain: security.testlab

To rename this computer or change its domain or workgroup, click Change.

EVENTS
All events | 25 total

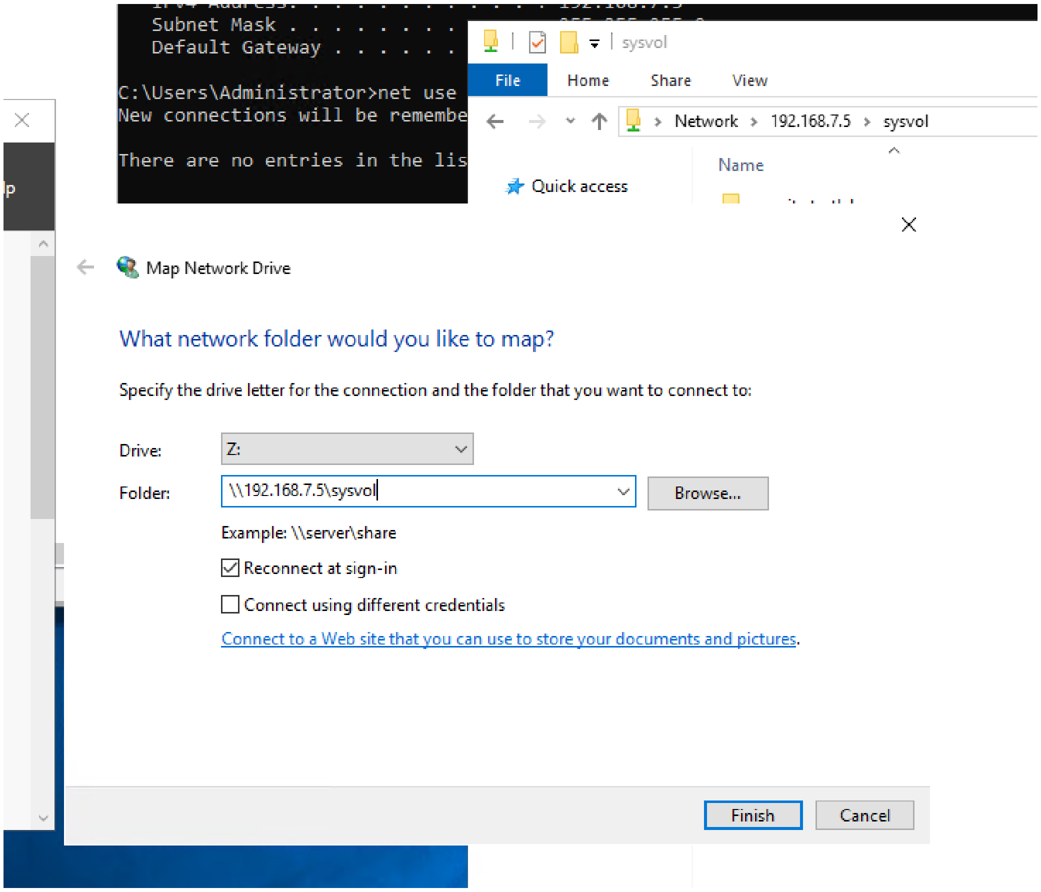
Server Name	ID	Severity	Source	Log	Date and Time
WIN-IN3MHVA97A3	1014	Warning	Microsoft-Windows-DNS Client Events	System	10/10/2023 6:44:37 PM
WIN-IN3MHVA97A3	5781	Warning	NETLOGON	System	10/10/2023 6:32:46 PM
WIN-IN3MHVA97A3	5781	Warning	NETLOGON	System	10/10/2023 6:32:46 PM
WIN-IN3MHVA97A3	5781	Warning	NETLOGON	System	10/10/2023 6:32:46 PM
WIN-IN3MHVA97A3	8198	Error	Microsoft-Windows-Security-SPP	Application	10/10/2023 6:18:18 PM
WIN-IN3MHVA97A3	1014	Error	Microsoft-Windows-Security-SPP	Application	10/10/2023 6:18:18 PM
WIN-IN3MHVA97A3	8200	Error	Microsoft-Windows-Security-SPP	Application	10/10/2023 6:18:18 PM

SERVICES
All services | 212 total

Server Name	Display Name	Service Name	Status	Start Type
WIN-IN3MHVA97A3	Wired AutoConfig	dot3svc	Stopped	Manual
WIN-IN3MHVA97A3	Payments and NFC/SE Manager	SEMgrSvc	Stopped	Disabled
WIN-IN3MHVA97A3	Network Connection Broker	NcbService	Running	Manual (Triggered)
WIN-IN3MHVA97A3	Link-Layer Topology Discovery Mapper	lltdsvc	Stopped	Disabled
WIN-IN3MHVA97A3	Remote Desktop Services UserMode Port Redirector	UmRdpService	Stopped	Manual
WIN-IN3MHVA97A3	Microsoft App-V Client	AppVClient	Stopped	Disabled
WIN-IN3MHVA97A3	Windows Remote Management (WS-Management)	WinRM	Running	Automatic

BEST PRACTICES ANALYZER
Warnings or Errors | 0 of 0 total

These three screenshots show how a remote desktop connection was opened from the Windows client machine to the Windows server. After the **'mstsc'** command is run the initial connection page is opened where one can follow the prompts to connect to another machine.



```
   Subnet Mask . . . . . . . .
   Default Gateway . . . . . .

C:\Users\Administrator>net use
New connections will be remembe

There are no entries in the lis
```

Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

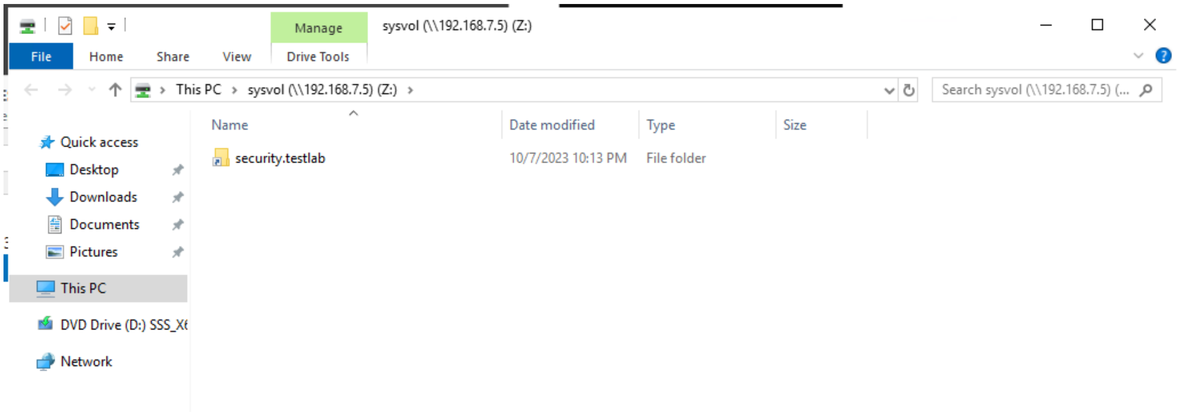
Folder: \\192.168.7.5\sysvol

Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

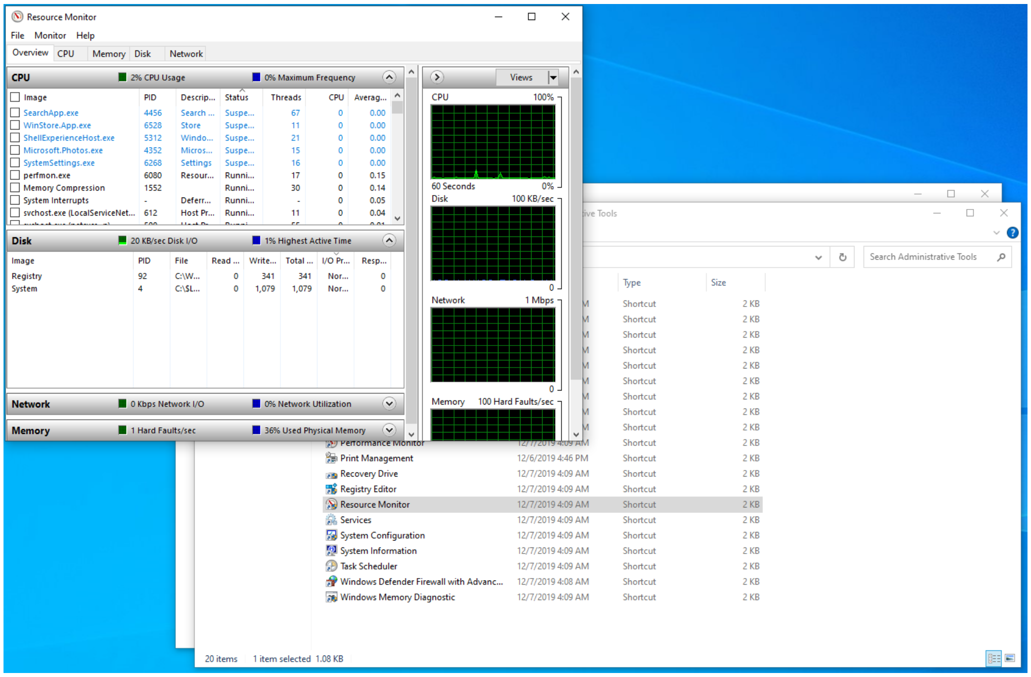
Connect to a Web site that you can use to store your documents and pictures.



Name	Date modified	Type	Size
security.testlab	10/7/2023 10:13 PM	File folder	

This shows the successful completion of mapping the network drive so both the client and the server can have access to the same resources. The command **‘\\(host Ip)’** was utilized where the host Ip was 192.168.7.5 (Server).

TASK THREE: Analyze Network Traffic:



CPU ■ 2% CPU Usage ■ 0% Maximum Frequency

□ Image	PID	Descrip...	Status	Threads	CPU	Averag...
□ SearchApp.exe	4456	Search ...	Suspe...	67	0	0.00
□ WinStore.App.exe	6528	Store	Suspe...	11	0	0.00
□ ShellExperienceHost.exe	5312	Windo...	Suspe...	21	0	0.00
□ Microsoft.Photos.exe	4352	Micros...	Suspe...	15	0	0.00
□ SystemSettings.exe	6268	Settings	Suspe...	16	0	0.00
□ perfmon.exe	6080	Resour...	Runni...	17	0	0.15
□ Memory Compression	1552		Runni...	30	0	0.14
□ System Interrupts	-	Deferr...	Runni...	-	0	0.05
□ svchost.exe (LocalServiceNet...	612	Host Pr...	Runni...	11	0	0.04

Disk ■ 20 KB/sec Disk I/O ■ 1% Highest Active Time

Image	PID	File	Read ...	Write...	Total ...	I/O Pr...	Resp...
Registry	92	C:\W...	0	341	341	Nor...	0
System	4	C:\$L...	0	1,079	1,079	Nor...	0

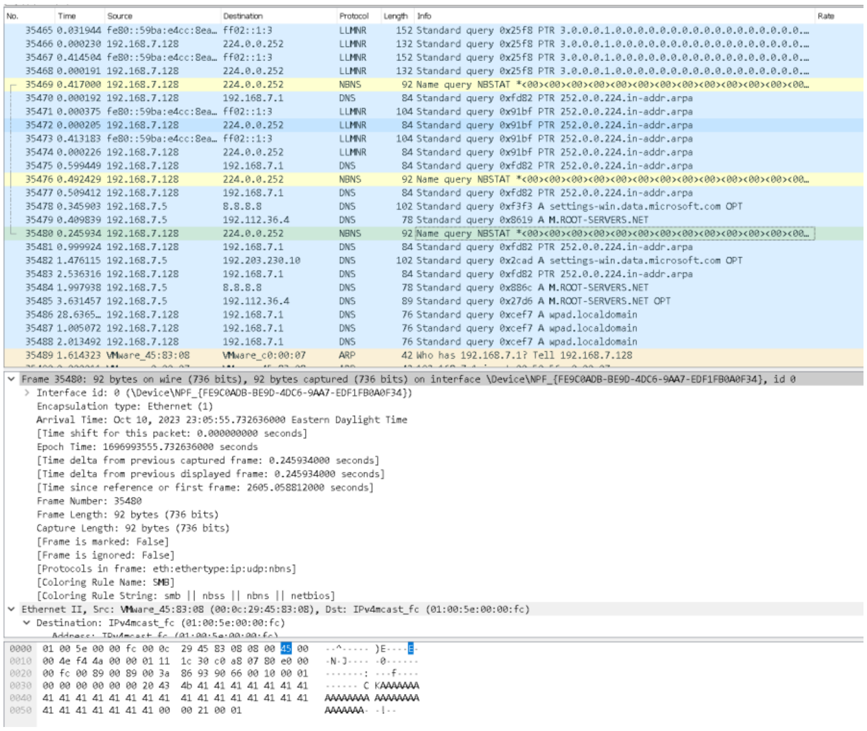
Network ■ 0 Kbps Network I/O ■ 0% Network Utilization

Memory ■ 1 Hard Faults/sec ■ 36% Used Physical Memory

Name	Date modified	Type	Size
Print Management	12/6/2019 4:46 PM	Shortcut	2 KB
Recovery Drive	12/7/2019 4:09 AM	Shortcut	2 KB
Registry Editor	12/7/2019 4:09 AM	Shortcut	2 KB
Resource Monitor	12/7/2019 4:09 AM	Shortcut	2 KB
Services	12/7/2019 4:09 AM	Shortcut	2 KB
System Configuration	12/7/2019 4:09 AM	Shortcut	2 KB
System Information	12/7/2019 4:09 AM	Shortcut	2 KB
Task Scheduler	12/7/2019 4:09 AM	Shortcut	2 KB
Windows Defender Firewall with Advanc...	12/7/2019 4:08 AM	Shortcut	2 KB
Windows Memory Diagnostic	12/7/2019 4:09 AM	Shortcut	2 KB

20 items 1 item selected 1.08 KB

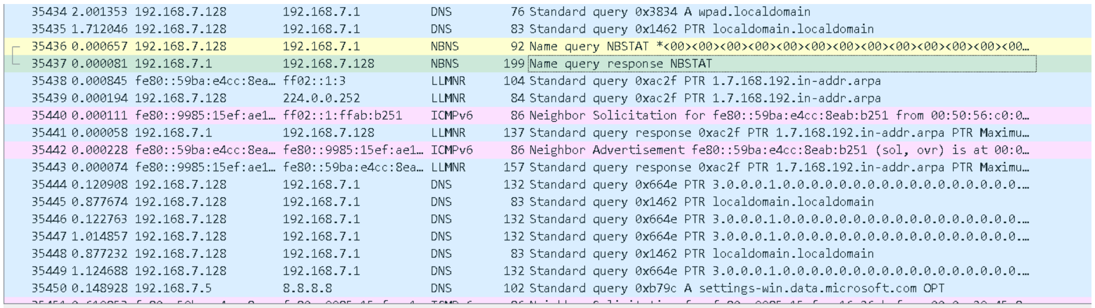
The resource monitor tool generated NBNS network traffic, or NetBIOS Name Service. I believe this appeared when I was viewing the resource monitor tool likely because it deals with internal parts and processes that are interconnected with a systems BIOS.



```
No.    Time     Source                Destination     Protocol Length Info                                                                        Rate
 35465 0.031944 fe80::59ba:e4cc:8ea… ff02::1:3        LLMNR     152 Standard query 0x25f8 PTR 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.…
 35466 0.000230 192.168.7.128         224.0.0.252      LLMNR     132 Standard query 0x25f8 PTR 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.…
 35467 0.414504 fe80::59ba:e4cc:8ea… ff02::1:3        LLMNR     152 Standard query 0x25f8 PTR 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.…
 35468 0.000191 192.168.7.128         224.0.0.252      LLMNR     132 Standard query 0x25f8 PTR 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.…
 35469 0.417000 192.168.7.128         224.0.0.252      NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00…
 35470 0.000192 192.168.7.128         192.168.7.1      DNS        84 Standard query 0xfd82 PTR 252.0.0.224.in-addr.arpa
 35471 0.000375 fe80::59ba:e4cc:8ea… ff02::1:3        LLMNR     104 Standard query 0x91bf PTR 252.0.0.224.in-addr.arpa
 35472 0.000205 192.168.7.128         224.0.0.252      LLMNR      84 Standard query 0x91bf PTR 252.0.0.224.in-addr.arpa
 35473 0.413183 fe80::59ba:e4cc:8ea… ff02::1:3        LLMNR     104 Standard query 0x91bf PTR 252.0.0.224.in-addr.arpa
 35474 0.000226 192.168.7.128         224.0.0.252      LLMNR      84 Standard query 0x91bf PTR 252.0.0.224.in-addr.arpa
 35475 0.599449 192.168.7.128         192.168.7.1      DNS        84 Standard query 0xfd82 PTR 252.0.0.224.in-addr.arpa
 35476 0.492429 192.168.7.128         224.0.0.252      NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00…
 35477 0.509412 192.168.7.128         192.168.7.1      DNS        84 Standard query 0xfd82 PTR 252.0.0.224.in-addr.arpa
 35478 0.345903 192.168.7.5           8.8.8.8          DNS       102 Standard query 0xf3f3 A settings-win.data.microsoft.com OPT
 35479 0.409839 192.168.7.5           192.112.36.4     DNS        78 Standard query 0x8619 A M.ROOT-SERVERS.NET
 35480 0.245934 192.168.7.128         224.0.0.252      NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00…
 35481 0.999924 192.168.7.128         192.168.7.1      DNS        84 Standard query 0xfd82 PTR 252.0.0.224.in-addr.arpa
 35482 1.476115 192.168.7.5           192.203.230.10   DNS       102 Standard query 0x2cad A settings-win.data.microsoft.com OPT
 35483 2.536316 192.168.7.128         192.168.7.1      DNS        84 Standard query 0xfd82 PTR 252.0.0.224.in-addr.arpa
 35484 1.997938 192.168.7.5           8.8.8.8          DNS        78 Standard query 0x886c A M.ROOT-SERVERS.NET
 35485 3.631457 192.168.7.5           192.112.36.4     DNS        89 Standard query 0x27d6 A M.ROOT-SERVERS.NET OPT
 35486 28.6365… 192.168.7.128         192.168.7.1      DNS        76 Standard query 0xcef7 A wpad.localdomain
 35487 1.005072 192.168.7.128         192.168.7.1      DNS        76 Standard query 0xcef7 A wpad.localdomain
 35488 2.013492 192.168.7.128         192.168.7.1      DNS        76 Standard query 0xcef7 A wpad.localdomain
 35489 1.614323 VMware_45:83:08       VMware_c0:00:07  ARP        42 Who has 192.168.7.1? Tell 192.168.7.128
```

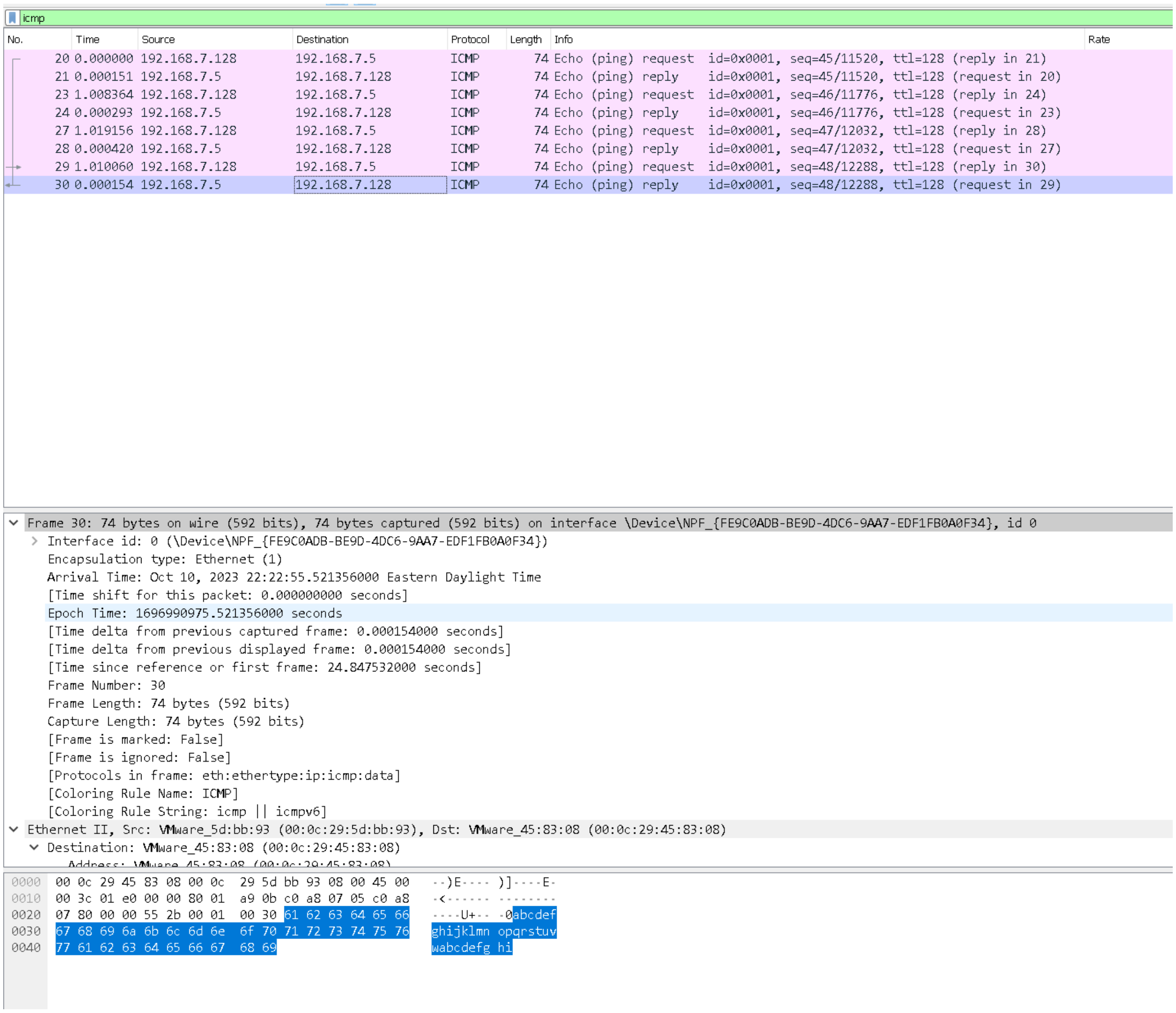
```
v Frame 35480: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{FE9C0ADB-BE9D-4DC6-9AA7-EDF1FB0A0F34}, id 0
  > Interface id: 0 (\Device\NPF_{FE9C0ADB-BE9D-4DC6-9AA7-EDF1FB0A0F34})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2023 23:05:55.732636000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1696993555.732636000 seconds
    [Time delta from previous captured frame: 0.245934000 seconds]
    [Time delta from previous displayed frame: 0.245934000 seconds]
    [Time since reference or first frame: 2605.058812000 seconds]
    Frame Number: 35480
    Frame Length: 92 bytes (736 bits)
    Capture Length: 92 bytes (736 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:nbns]
    [Coloring Rule Name: SMB]
    [Coloring Rule String: smb || nbss || nbns || netbios]
v Ethernet II, Src: VMware_45:83:08 (00:0c:29:45:83:08), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
  v Destination: IPv4mcast_fc (01:00:5e:00:00:fc)
```

```
0000  01 00 5e 00 00 fc 00 0c  29 45 83 08 08 00 45 00   ··^····· )E····E·
0010  00 4e f4 4a 00 00 01 11  1c 30 c0 a8 07 80 e0 00   ·N·J···· ·0······
0020  00 fc 00 89 00 89 00 3a  86 93 90 66 00 10 00 01   ·······: ···f····
0030  00 00 00 00 00 00 20 43  4b 41 41 41 41 41 41 41   ······ C KAAAAAAA
0040  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0050  41 41 41 41 41 41 41 00  00 21 00 01               AAAAAAA· ·!··
```



```
35434 2.001353 192.168.7.128         192.168.7.1           DNS          76 Standard query 0x3834 A wpad.localdomain
35435 1.712046 192.168.7.128         192.168.7.1           DNS          83 Standard query 0x1462 PTR localdomain.localdomain
35436 0.000657 192.168.7.128         192.168.7.1           NBNS         92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00…
35437 0.000081 192.168.7.1           192.168.7.128         NBNS        199 Name query response NBSTAT
35438 0.000845 fe80::59ba:e4cc:8ea… ff02::1:3             LLMNR       104 Standard query 0xac2f PTR 1.7.168.192.in-addr.arpa
35439 0.000194 192.168.7.128         224.0.0.252           LLMNR        84 Standard query 0xac2f PTR 1.7.168.192.in-addr.arpa
35440 0.000111 fe80::9985:15ef:ae1… ff02::1:ffab:b251     ICMPv6       86 Neighbor Solicitation for fe80::59ba:e4cc:8eab:b251 from 00:50:56:c0:0…
35441 0.000058 192.168.7.1           192.168.7.128         LLMNR       137 Standard query response 0xac2f PTR 1.7.168.192.in-addr.arpa PTR Maximu…
35442 0.000228 fe80::59ba:e4cc:8ea… fe80::9985:15ef:ae1… ICMPv6       86 Neighbor Advertisement fe80::59ba:e4cc:8eab:b251 (sol, ovr) is at 00:0…
35443 0.000074 fe80::9985:15ef:ae1… fe80::59ba:e4cc:8ea… LLMNR       157 Standard query response 0xac2f PTR 1.7.168.192.in-addr.arpa PTR Maximu…
35444 0.120908 192.168.7.128         192.168.7.1           DNS         132 Standard query 0x664e PTR 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0…
35445 0.877674 192.168.7.128         192.168.7.1           DNS          83 Standard query 0x1462 PTR localdomain.localdomain
35446 0.122763 192.168.7.128         192.168.7.1           DNS         132 Standard query 0x664e PTR 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0…
35447 1.014857 192.168.7.128         192.168.7.1           DNS         132 Standard query 0x664e PTR 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0…
35448 0.877232 192.168.7.128         192.168.7.1           DNS          83 Standard query 0x1462 PTR localdomain.localdomain
35449 1.124688 192.168.7.128         192.168.7.1           DNS         132 Standard query 0x664e PTR 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0…
35450 0.148928 192.168.7.5           8.8.8.8               DNS         102 Standard query 0xb79c A settings-win.data.microsoft.com OPT
```

This is the NBNS protocol response.



```
icmp

No.   Time     Source          Destination     Protocol  Length  Info                                                                              Rate
   20 0.000000 192.168.7.128   192.168.7.5     ICMP        74 Echo (ping) request  id=0x0001, seq=45/11520, ttl=128 (reply in 21)
   21 0.000151 192.168.7.5     192.168.7.128   ICMP        74 Echo (ping) reply    id=0x0001, seq=45/11520, ttl=128 (request in 20)
   23 1.008364 192.168.7.128   192.168.7.5     ICMP        74 Echo (ping) request  id=0x0001, seq=46/11776, ttl=128 (reply in 24)
   24 0.000293 192.168.7.5     192.168.7.128   ICMP        74 Echo (ping) reply    id=0x0001, seq=46/11776, ttl=128 (request in 23)
   27 1.019156 192.168.7.128   192.168.7.5     ICMP        74 Echo (ping) request  id=0x0001, seq=47/12032, ttl=128 (reply in 28)
   28 0.000420 192.168.7.5     192.168.7.128   ICMP        74 Echo (ping) reply    id=0x0001, seq=47/12032, ttl=128 (request in 27)
   29 1.010060 192.168.7.128   192.168.7.5     ICMP        74 Echo (ping) request  id=0x0001, seq=48/12288, ttl=128 (reply in 30)
   30 0.000154 192.168.7.5     192.168.7.128   ICMP        74 Echo (ping) reply    id=0x0001, seq=48/12288, ttl=128 (request in 29)
```

```
v Frame 30: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{FE9C0ADB-BE9D-4DC6-9AA7-EDF1FB0A0F34}, id 0
  > Interface id: 0 (\Device\NPF_{FE9C0ADB-BE9D-4DC6-9AA7-EDF1FB0A0F34})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2023 22:22:55.521356000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1696990975.521356000 seconds
    [Time delta from previous captured frame: 0.000154000 seconds]
    [Time delta from previous displayed frame: 0.000154000 seconds]
    [Time since reference or first frame: 24.847532000 seconds]
    Frame Number: 30
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
v Ethernet II, Src: VMware_5d:bb:93 (00:0c:29:5d:bb:93), Dst: VMware_45:83:08 (00:0c:29:45:83:08)
  v Destination: VMware_45:83:08 (00:0c:29:45:83:08)
      Address: VMware_45:83:08 (00:0c:29:45:83:08)
```

```
0000  00 0c 29 45 83 08 00 0c  29 5d bb 93 08 00 45 00   ··)E···· )]····E·
0010  00 3c 01 e0 00 00 80 01  a9 0b c0 a8 07 05 c0 a8   ·<······ ········
0020  07 80 00 00 55 2b 00 01  00 30 61 62 63 64 65 66   ····U+·· ·0abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Here we see the ICMP protocol response and replies to the ping between the Windows client and server machines.

Everything by this point was what I was expecting to see. I wish I played around with some more default tools and utilities in windows before ending the capture as this would have provided more data for me to work with when it came to this part of the lab. This would have likely included more data transfer protocols.

The NBNS and LLMNR protocols can be vulnerable to spoofing attacks where a bad actor could pretend to be the server and accept the incoming traffic as it comes in. (Triaxiomsecurity) According to Triaxiom Security, these packets are recommended to be disabled, if possible, with less and acuate DNS entries, as well as utilizing a WPAD. A WPAD, Web Proxy Auto-Discover, can be pointed to a corporate proxy service or can act as one. A WPAD cannot be impersonated by an attacker, so this provides a great sense of security.

Conclusion:

Throughout the course of completing this lab I hit some bumps in the road. For some reason no matter what I tried I could not get the ICMP packets to show in Wireshark within the Ubuntu client, with no success there and hours of time debugging, I ran Wireshark on my local machine and the packets and correct corresponding pings were there from the processes running on the virtual machines. I was relieved to see this and with that I was able to complete this lab.

References:

https://manage.accuwebhosting.com/knowledgebase/2609/How-to-Allow-Pingor-ICMP-Echo-Request-in-Windows-Firewall.html

https://youtu.be/6l2T7-4dJis?si=uN4V_qFuvh3j64oB

https://www.triaxiomsecurity.com/vulnerability-walkthrough-nbns-and-llmnr-spoofing/