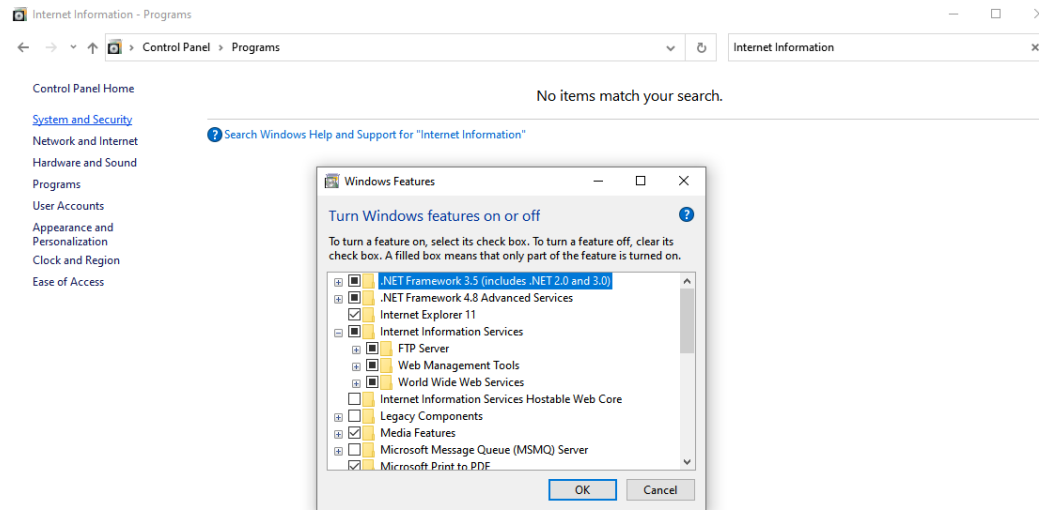


Project 2: IPsec and SSH-Based VPNS

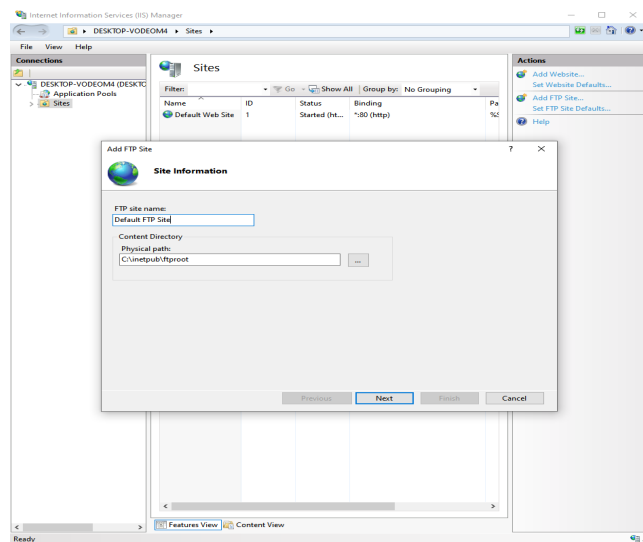
Question 1.1:

Installation of ISS and FTP Service:



Question 1.2:

Configuring FTP Site through IIS Manager:



Add FTP Site

Binding and SSL Settings

Binding

IP Address: Port:

☐ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☒ Start FTP site automatically

SSL

☐ No SSL

☒ Allow SSL

☐ Require SSL

SSL Certificate:

Add FTP Site

Authentication and Authorization Information

Authentication

☒ Anonymous

☐ Basic

Authorization

Allow access to:

Permissions

☒ Read

☐ Write

Question 1.3:

Configuring FTP Server:

```
Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nazimz>ftp localhost
Connected to DESKTOP-VODEOM4.
Connection closed by remote host.

C:\Users\nazimz>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> bye

C:\Users\nazimz>
```

Question 2:

Captured Packets via WireShark:

nonipsec.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Packet bytes Narrow & Wide Case sensitive String Length Info

No.	Time	Source	Destination	Protocol	Length	Info
68	11.589457	127.0.0.1	127.0.0.1	FTP	50	Request: QUIT
69	11.589474	127.0.0.1	127.0.0.1	TCP	44	21 → 61269 [ACK] Seq=179 Ack=50 Win=2619648 Len=0
70	11.589503	127.0.0.1	127.0.0.1	FTP	58	Response: 221 Goodbye.
71	11.589514	127.0.0.1	127.0.0.1	TCP	44	61269 → 21 [ACK] Seq=50 Ack=193 Win=8000 Len=0
72	11.589545	127.0.0.1	127.0.0.1	TCP	44	21 → 61269 [FIN, ACK] Seq=193 Ack=50 Win=2619648 Len=0
73	11.589551	127.0.0.1	127.0.0.1	TCP	44	61269 → 21 [ACK] Seq=50 Ack=194 Win=8000 Len=0
74	11.590917	127.0.0.1	127.0.0.1	TCP	44	61269 → 21 [FIN, ACK] Seq=50 Ack=194 Win=8000 Len=0
75	11.590924	127.0.0.1	127.0.0.1	TCP	44	21 → 61269 [ACK] Seq=194 Ack=51 Win=2619648 Len=0
76	11.614925	:::1	:::1	TCP	140	49787 → 5426 [PSH, ACK] Seq=240 Ack=47 Win=10026 Len=76
77	11.614939	:::1	:::1	TCP	64	5426 → 49787 [ACK] Seq=47 Ack=316 Win=10214 Len=0
78	11.615155	:::1	:::1	TCP	78	5426 → 49787 [PSH, ACK] Seq=47 Ack=316 Win=10214 Len=14

Frame 62: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 21, Dst Port: 61269, Seq=193, Win=0, Len=0

File Transfer Protocol (FTP)

331 Anonymous access allowed, send identity (e-mail name) as password

Response code: User name okay, need password (331)

Response arg: Anonymous access allowed, send identity (e-mail name) as password

[Current working directory:]

0000 02 00 00 00 45 00 00 70 c8 eb 40 00 40 06 00 00E..p
0010 7f 00 00 01 7f 00 00 01 00 15 ef 55 0c 13 2d 59
0020 c6 d0 e0 d7 50 18 27 f9 6a 72 00 00 33 33 31 20P...
0030 41 6e 6f 6e 79 6d 6f 75 73 20 61 63 63 65 73 73 Anonymou
0040 20 61 6c 6c 6f 77 65 64 2c 20 73 65 6e 64 20 69 allowed
0050 64 65 6e 74 69 74 79 20 28 65 2d 6d 61 69 6c 20 identity
0060 6e 61 6d 65 29 20 61 73 20 70 61 73 73 77 6f 72 (name) as
0070 64 2e 0d 0a d...

Response arg (ftp.response.arg), 66 bytes

Packets: 109 · Displayed: 109 (100.0%) Profile: Default

The Destination Port is 21 which is the port of the FTP Server. This is proof that the Wireshark captured the packets from the FTP server.

Question 2.1.1:

You can determine the source and destination port of the FTP server. The source port is 21 which is the port of the FtP server and the destination port is 61269 which is the port of the client. This is a TCP protocol executed using localhost as the IP address for the FTP server. There is a three-way handshake as shown above.

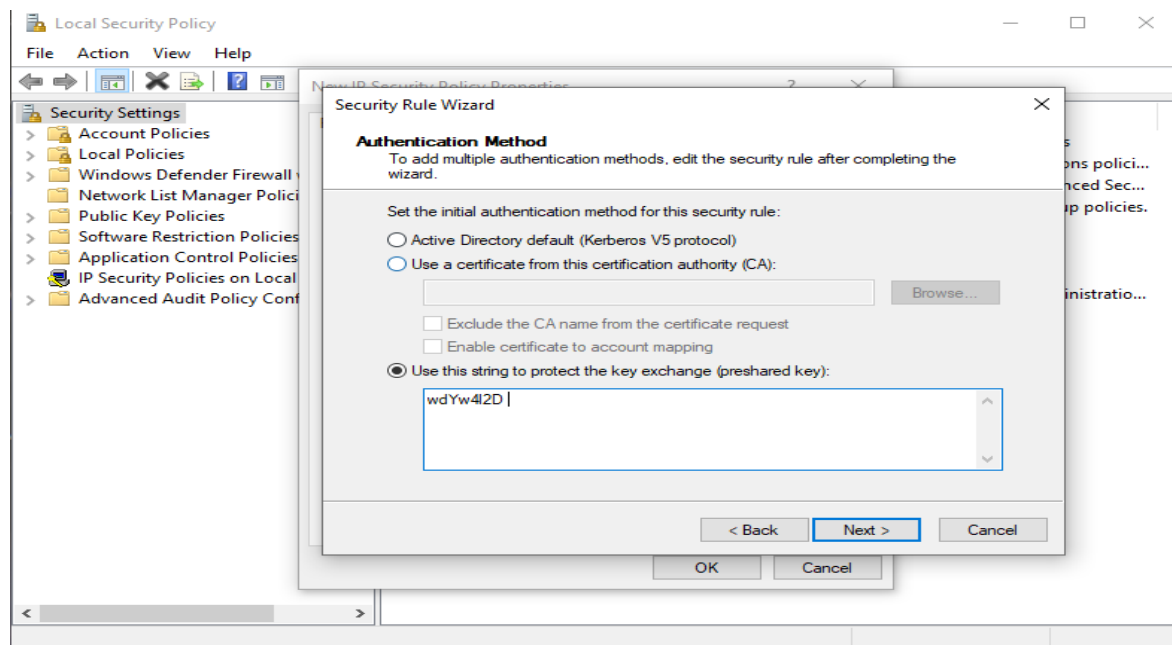
Question 2.1.2:

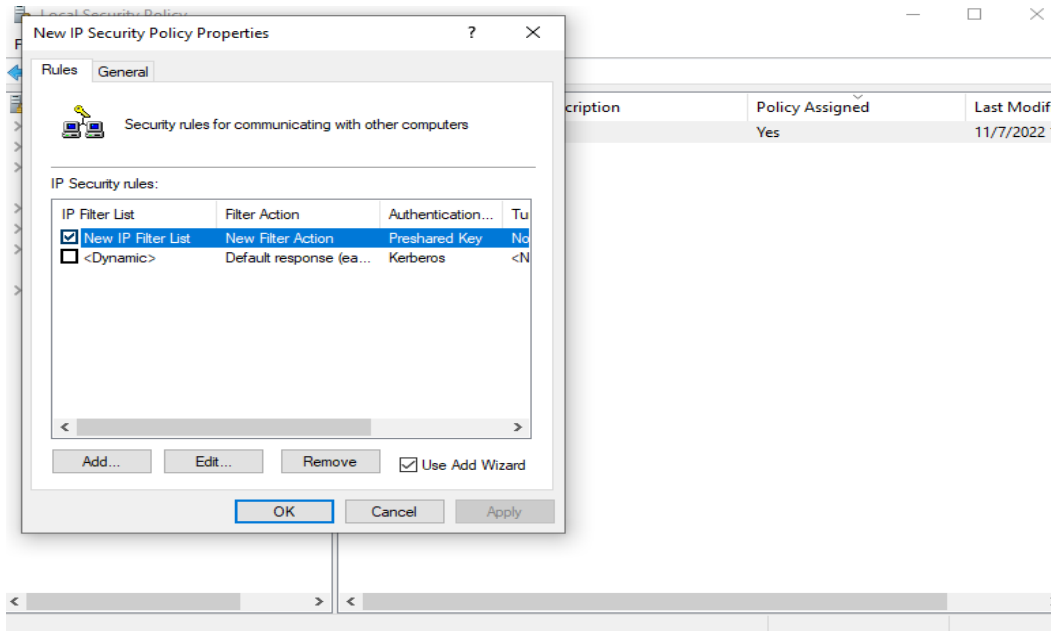
You can sniff out the username and password by going into **Edit -> Find Packet** and from there, you can swap the display filter so that the user can identify the data being sent as explicit strings. Because the data is not encrypted, you can locate the username and password very easily. This makes the FTP server a very faulty method in transferring data over the internet. The screenshot is proof of this given that fulfilling this prompt clearly shows that the client requested anonymous access in which the server responds with an explicit request for a password. This is bad because this string is not encrypted.

The file was saved as nonipsec.pcapng as shown at the very top of the screenshot.

Question 3.1:

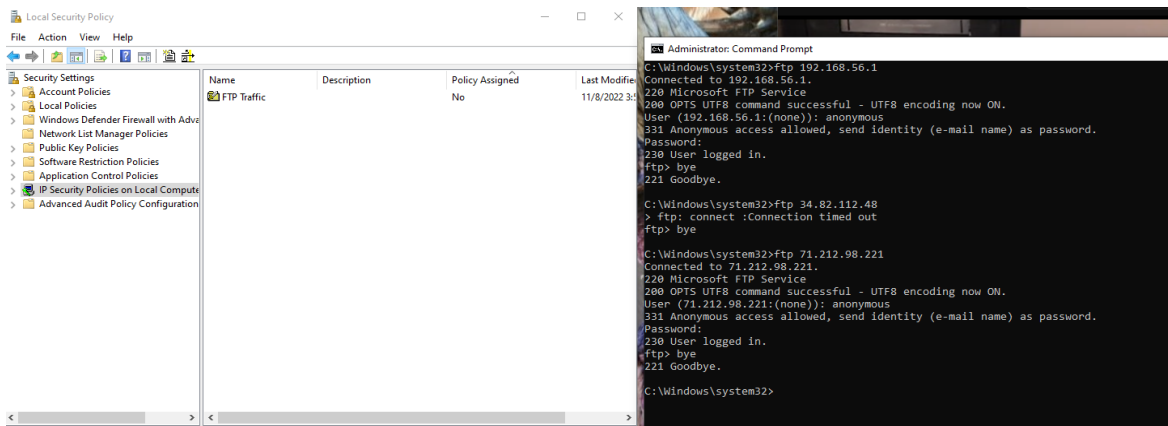
Establishing Security through Local Security Policy MMC:



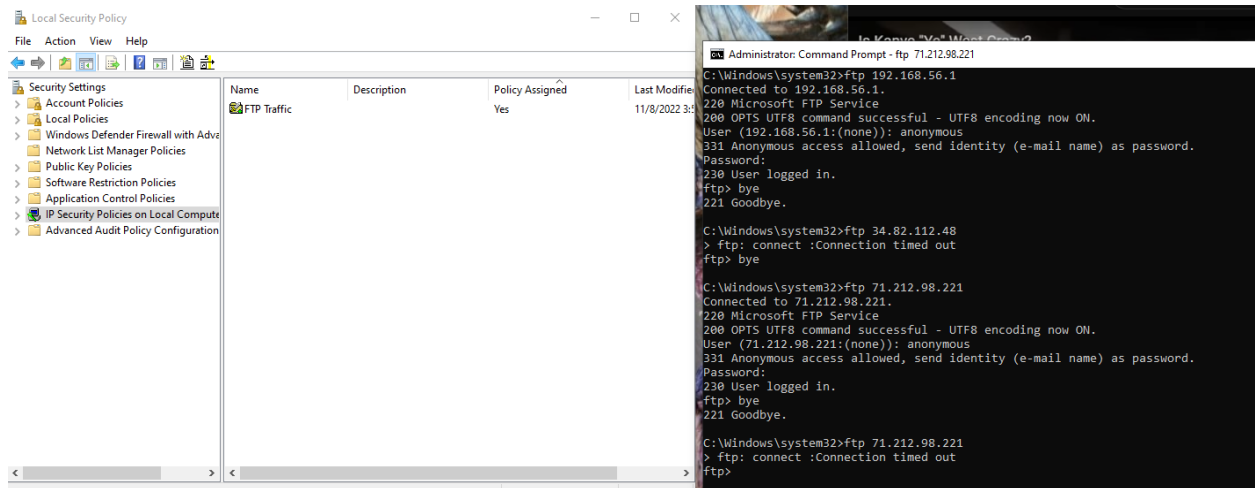


Question 3.1.1:

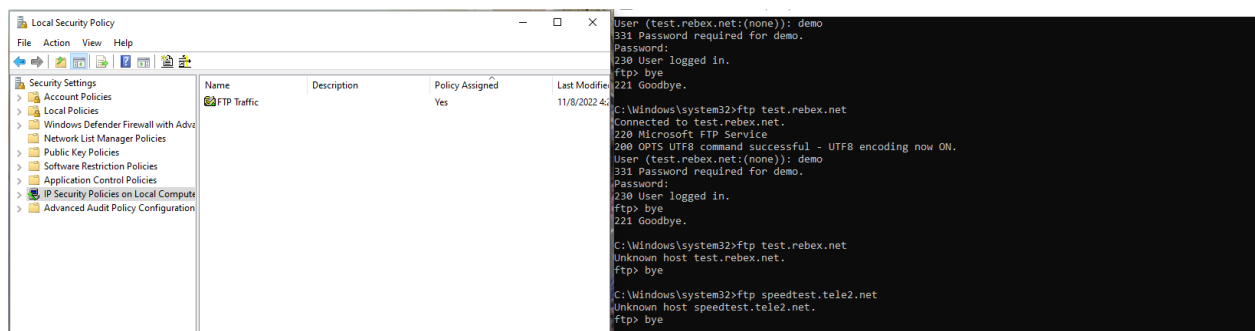
I initially tested the FTP server using localhost but it seems as if there was no way to configure IPsec with localhost. Therefore, I enabled port forwarding on port 21 so that I could access the FTP server through my WAN address. With the above IPsec policy unassigned, the FTP connection was successful.



With the IPsec policy assigned, this was the result:



The client machine was unable to connect to the server. Testing this on any available FTP server available produces this result in which the host is stated to be unknown.

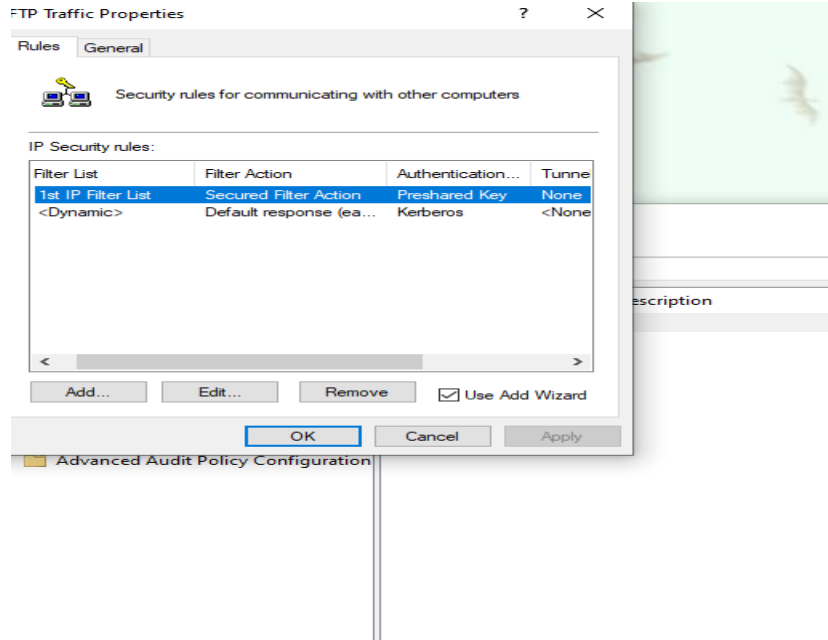


Question 3.1.2:

Upon initiating the “bye” prompt to disconnect, there was no response because an authentic connection was not established.

Question 3.2:

Same procedure was initiated for client.



Question 3.3.1:

Similar response was above. Either a connection was not established or it was stated that the host was unknown.

Question 3.3.2:

No response was given because an authentic connection to the server could not be established.

Question 3.3.3:

Question 4.1:

Installation of Tigervnc Server:

```
root@fedora:/home/nazimz
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Upgrading      : tigervnc-server-minimal-1.12.0-6.fc36.x86_64 1/4
  Running scriptlet: tigervnc-selinux-1.12.0-5.fc36.noarch      2/4
  Installing     : tigervnc-selinux-1.12.0-5.fc36.noarch      2/4
  Running scriptlet: tigervnc-selinux-1.12.0-5.fc36.noarch      2/4
  Installing     : tigervnc-server-1.12.0-6.fc36.x86_64        3/4
  Running scriptlet: tigervnc-server-1.12.0-6.fc36.x86_64        3/4
  Cleanup       : tigervnc-server-minimal-1.12.0-5.fc36.x86_64 4/4
  Running scriptlet: tigervnc-server-minimal-1.12.0-5.fc36.x86_64 4/4
  Verifying      : tigervnc-selinux-1.12.0-5.fc36.noarch      1/4
  Verifying      : tigervnc-server-1.12.0-6.fc36.x86_64        2/4
  Verifying      : tigervnc-server-minimal-1.12.0-6.fc36.x86_64 3/4
  Verifying      : tigervnc-server-minimal-1.12.0-5.fc36.x86_64 4/4

Upgraded:
  tigervnc-server-minimal-1.12.0-6.fc36.x86_64
Installed:
  tigervnc-selinux-1.12.0-5.fc36.noarch  tigervnc-server-1.12.0-6.fc36.x86_64

Complete!
[root@fedora nazimz]#
```

Verify Password:

```
root@fedora:/home/nazimz
Running scriptlet: tigervnc-server-1.12.0-6.fc36.x86_64 3/4
Cleanup       : tigervnc-server-minimal-1.12.0-5.fc36.x86_64 4/4
Running scriptlet: tigervnc-server-minimal-1.12.0-5.fc36.x86_64 4/4
Verifying      : tigervnc-selinux-1.12.0-5.fc36.noarch      1/4
Verifying      : tigervnc-server-1.12.0-6.fc36.x86_64        2/4
Verifying      : tigervnc-server-minimal-1.12.0-6.fc36.x86_64 3/4
Verifying      : tigervnc-server-minimal-1.12.0-5.fc36.x86_64 4/4

Upgraded:
  tigervnc-server-minimal-1.12.0-6.fc36.x86_64
Installed:
  tigervnc-selinux-1.12.0-5.fc36.noarch  tigervnc-server-1.12.0-6.fc36.x86_64

Complete!
[root@fedora nazimz]# cp /lib/systemd/system/vncserver@.service /etc/systemd/system/vncserver@:3.service
[root@fedora nazimz]# nano /etc/systemd/system/vncserver@:3.service
[root@fedora nazimz]# vncpasswd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
[root@fedora nazimz]#
```


Successful vncserver start-up:

```
root@fedora:/etc/tigervnc
[root@fedora tigervnc]# systemctl start vncserver@:3.service
Job for vncserver@:3.service failed because the service did not take the steps r
equired by its unit configuration.
See "systemctl status vncserver@:3.service" and "journalctl -xeu vncserver@:3.se
rvice" for details.
[root@fedora tigervnc]# vncpasswd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
A view-only password is not used
[root@fedora tigervnc]# systemctl start vncserver@:3.service
[root@fedora tigervnc]# systemctl status vncserver@:3.service
● vncserver@:3.service - Remote desktop service (VNC)
   Loaded: loaded (/etc/systemd/system/vncserver@:3.service; enabled; vendor p
   Active: inactive (dead) since Tue 2022-11-08 06:45:46 PST; 9s ago
     Process: 10405 ExecStartPre=/usr/libexec/vncsession-restore :3 (code=exited
     Process: 10414 ExecStart=/usr/libexec/vncsession-start :3 (code=exited, sta
   Main PID: 10421 (code=exited, status=0/SUCCESS)
      CPU: 12ms

Nov 08 06:45:46 fedora systemd[1]: Starting vncserver@:3.service - Remote deskto
Nov 08 06:45:46 fedora systemd[1]: Started vncserver@:3.service - Remote deskto
Nov 08 06:45:46 fedora systemd[1]: vncserver@:3.service: Deactivated successfully
lines 1-11/11 (END)
```

Verification of server running:

```
FedoraVM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 10 13:13
root@fedora:/usr/share/xsessions
[root@fedora xsessions]# systemctl enable vncserver@:3.service
Created symlink /etc/systemd/system/multi-user.target.wants/vncserver@:3.service → /et
c/systemd/system/vncserver@:3.service.
[root@fedora xsessions]# systemctl start vncserver@:3.service
[root@fedora xsessions]# systemctl status vncserver@:3.service
● vncserver@:3.service - Remote desktop service (VNC)
   Loaded: loaded (/etc/systemd/system/vncserver@:3.service; enabled; vendor preset
   Active: active (running) since Thu 2022-11-10 13:10:03 PST; 3min 5s ago
     Main PID: 5640 (vncsession)
       Tasks: 0 (limit: 4649)
      Memory: 352.0K
         CPU: 16ms
    CGroup: /system.slice/system-vncserver.slice/vncserver@:3.service
            └─ 5640 vncsession nazimz :3

Nov 10 13:10:03 fedora systemd[1]: Starting Remote desktop service (VNC)...
Nov 10 13:10:03 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi
Nov 10 13:10:03 fedora systemd[1]: Started Remote desktop service (VNC).
Nov 10 13:12:21 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi
Nov 10 13:12:25 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi
Nov 10 13:12:28 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi
Nov 10 13:12:50 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi
Nov 10 13:12:58 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi
lines 1-18/18 (END)
```

```

Nov 10 13:10:03 fedora systemd[1]: Starting Remote desktop service (VNC)...
Nov 10 13:10:03 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi>
Nov 10 13:10:03 fedora systemd[1]: Started Remote desktop service (VNC).
Nov 10 13:12:21 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi>
Nov 10 13:12:25 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi>
Nov 10 13:12:28 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi>
Nov 10 13:12:50 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi>
Nov 10 13:12:58 fedora systemd[1]: vncserver@:3.service: Supervising process 5640 whi>
lines 1-18/18 (END)
[root@fedora xsessions]# netstat -tulnp | grep X
tcp        0      0 127.0.0.1:5903          0.0.0.0:*               LISTEN      5645/Xvnc
tcp6       0      0 :::1:5903              :::*                   LISTEN      5645/Xvnc
[root@fedora xsessions]#

[root@fedora nazimz]# firewall-cmd --zone=public --add-port=5902/tcp
success
[root@fedora nazimz]#

```

Setting up the Wireshark:

Question 4.2: