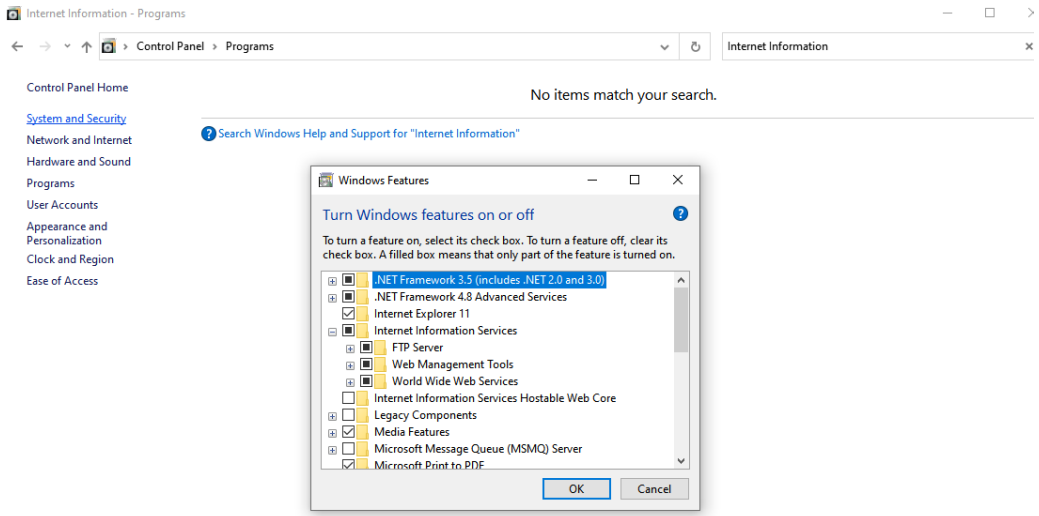
Project 2: IPsec and SSH-Based VPNS

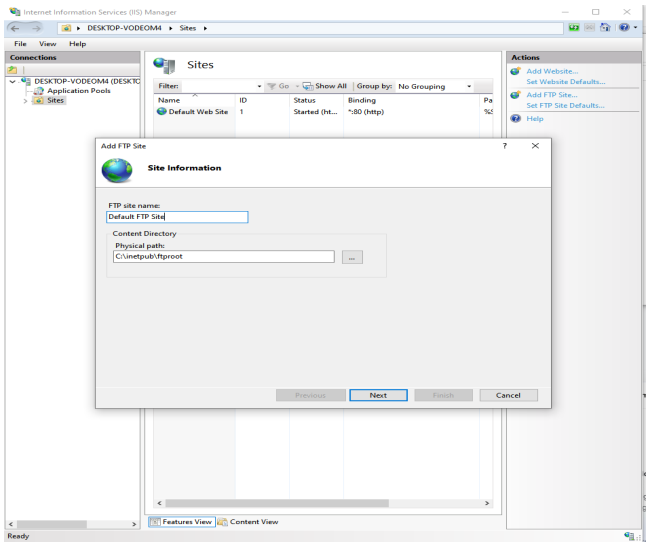
Question 1.1:

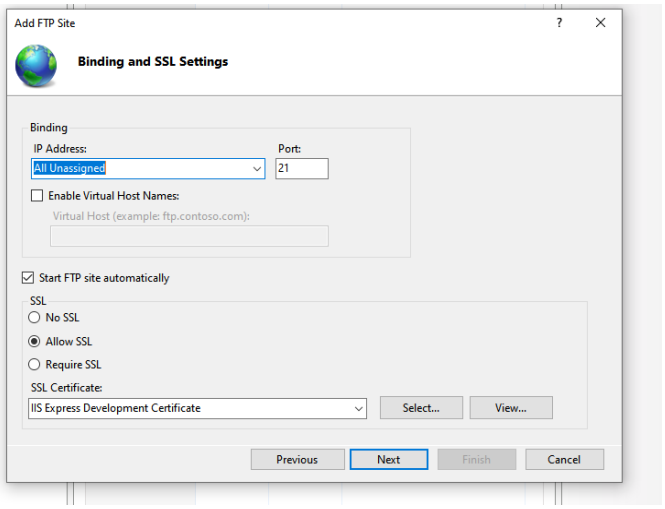
Installation of ISS and FTP Service:

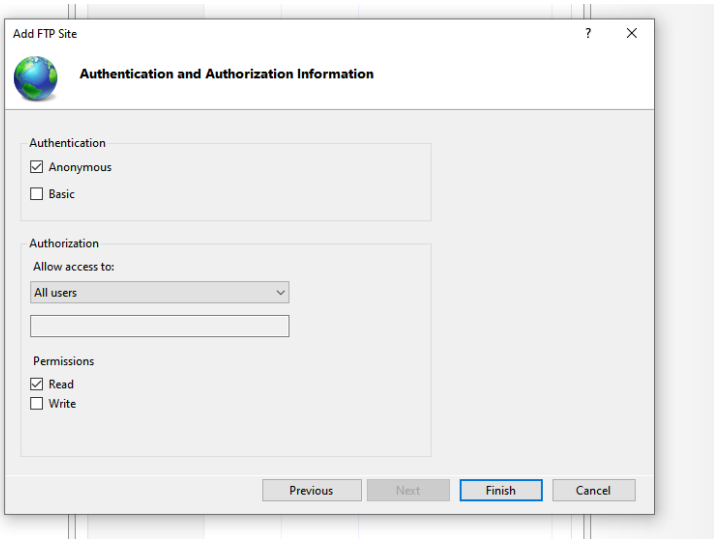


Question 1.2:

Configuring FTP Site through IIS Manager:

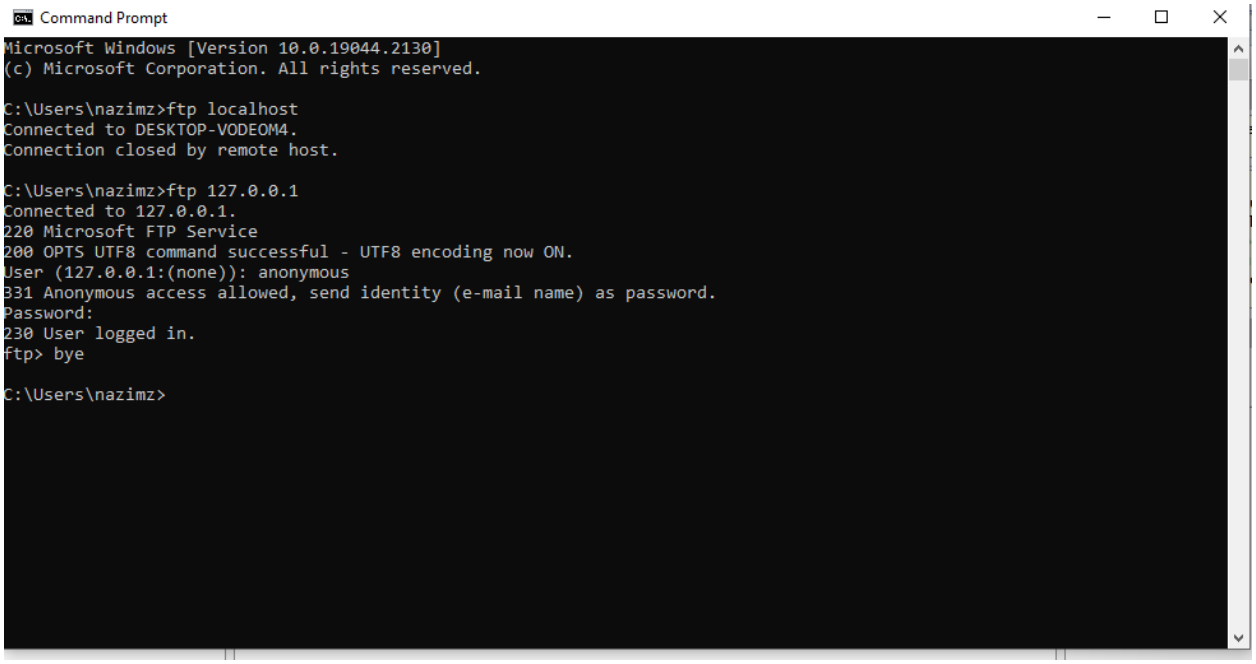






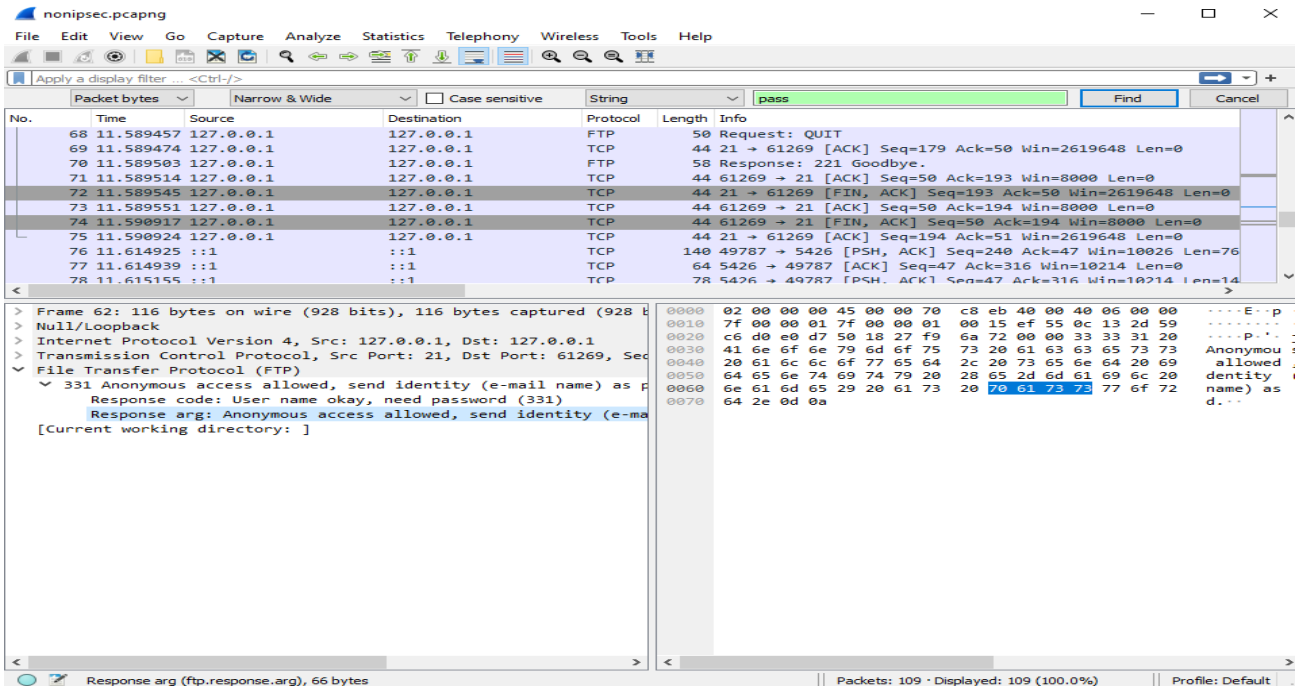
Question 1.3:

Configuring FTP Server:



Question 2:

Captured Packets via WireShark:



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.

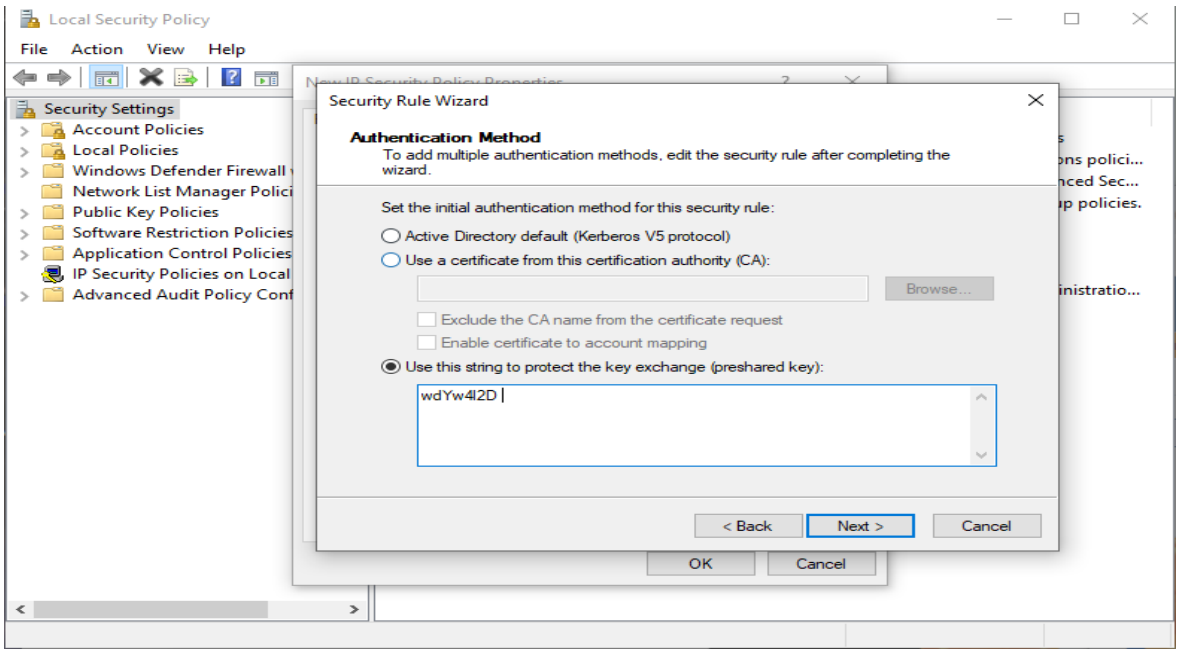
Question 2.1.2:

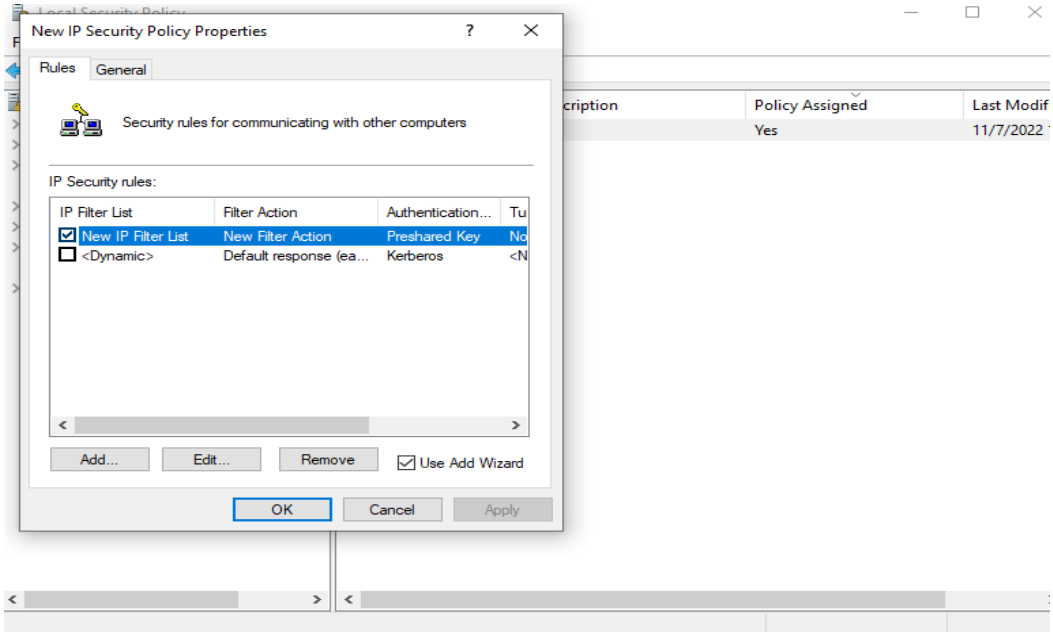
You can sniff out the username and password by going into **Edit -> Find Packet** and from there, you can swap the display filter so that the user can identify the data being sent as explicit strings. Because the data is not encrypted, you can locate the username and password very easily. This makes 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:

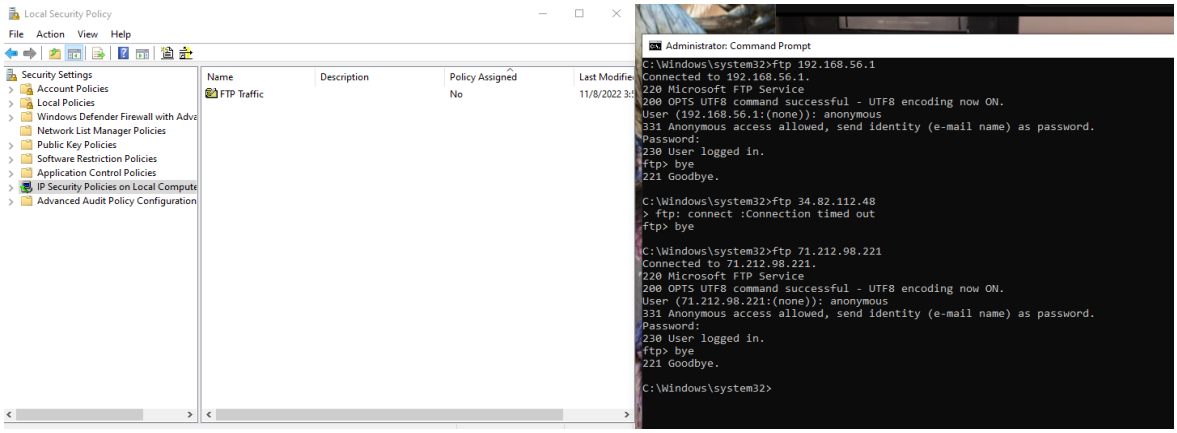
Establishing Security through Local Security Policy MMC:



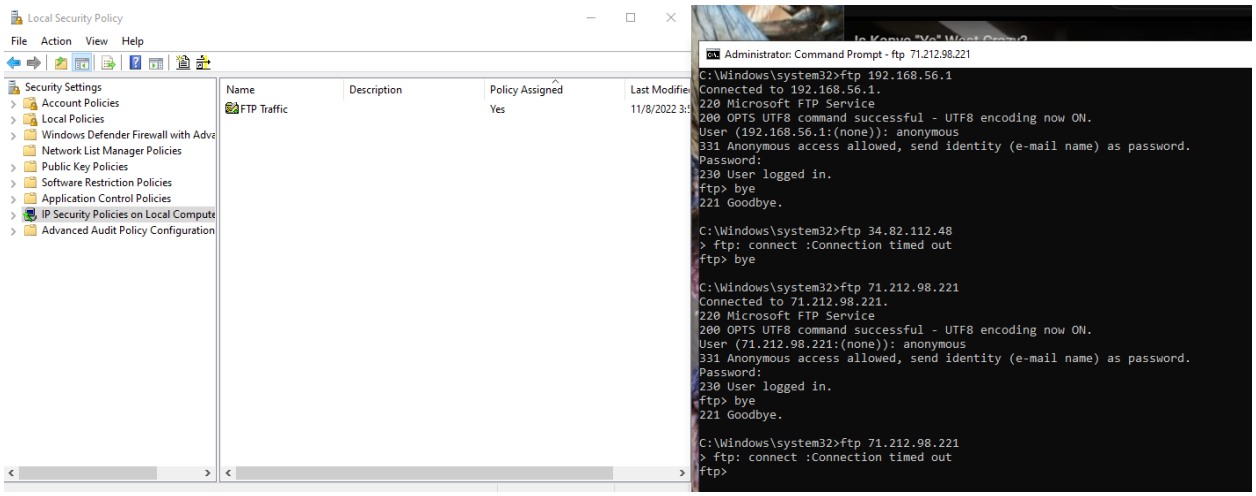


Question 3.1.1:

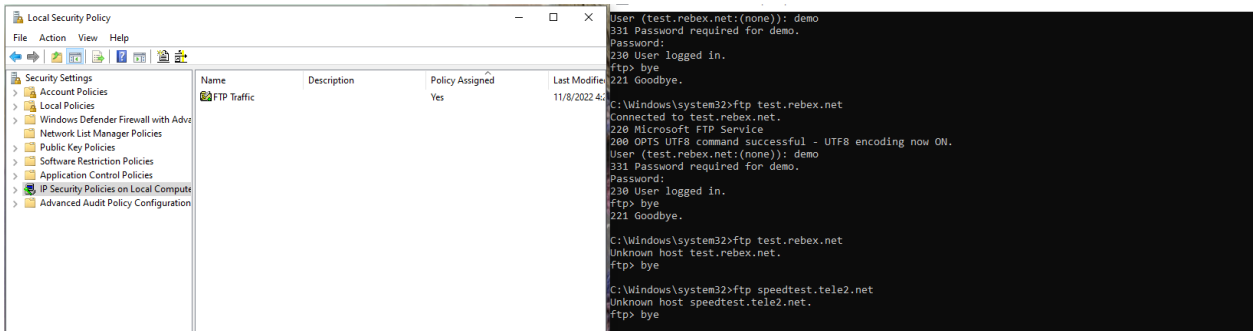
I initially tested the FTP server using localhost but it seems as if there was no way to configure IPSec with localhost. Therefore, I enabled port forwarding on port 21 so that I could access the FTP server through my WAN address. With the above IPSec policy unassigned, the FTP connection was successful.



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.

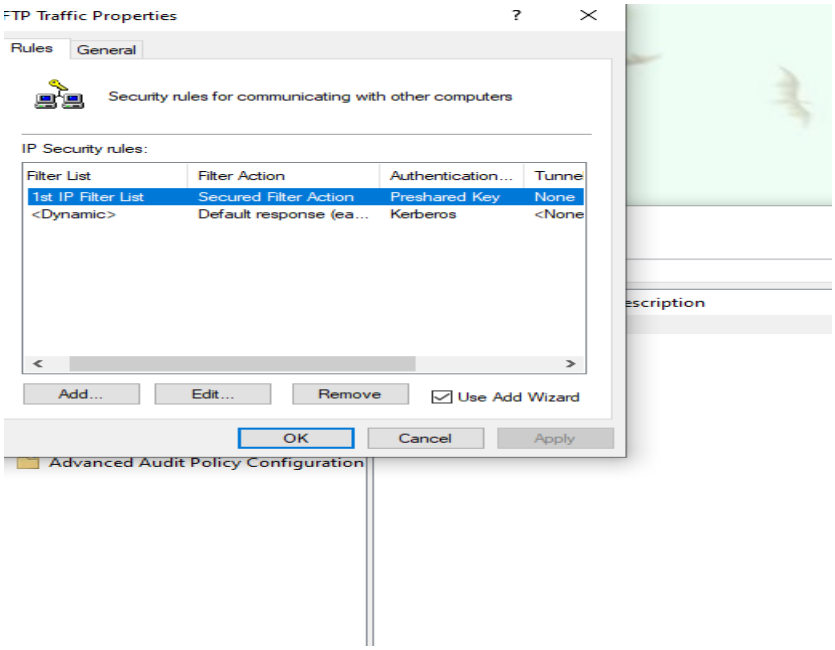


Question 3.1.2:

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.

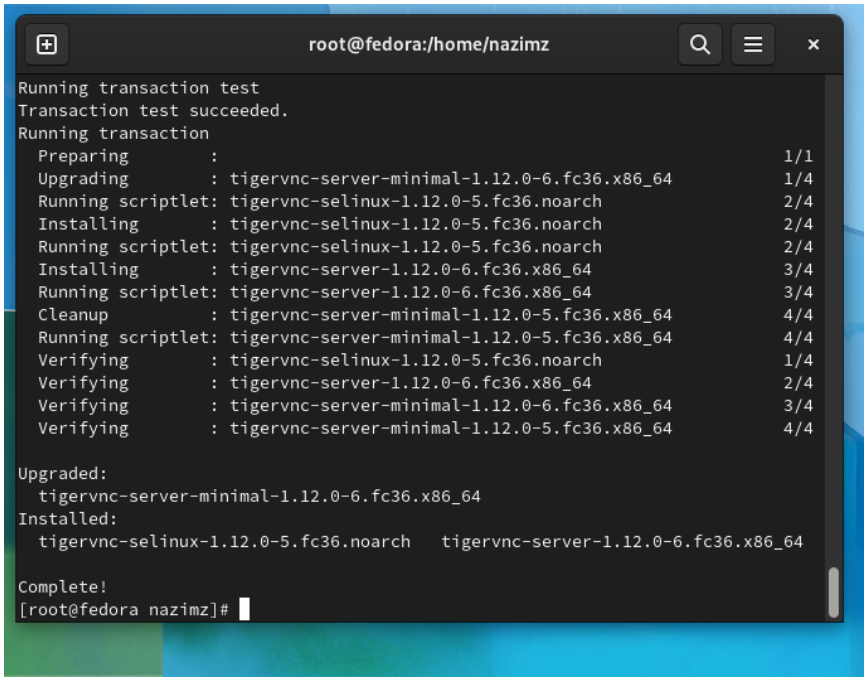
Question 3.3.2:

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

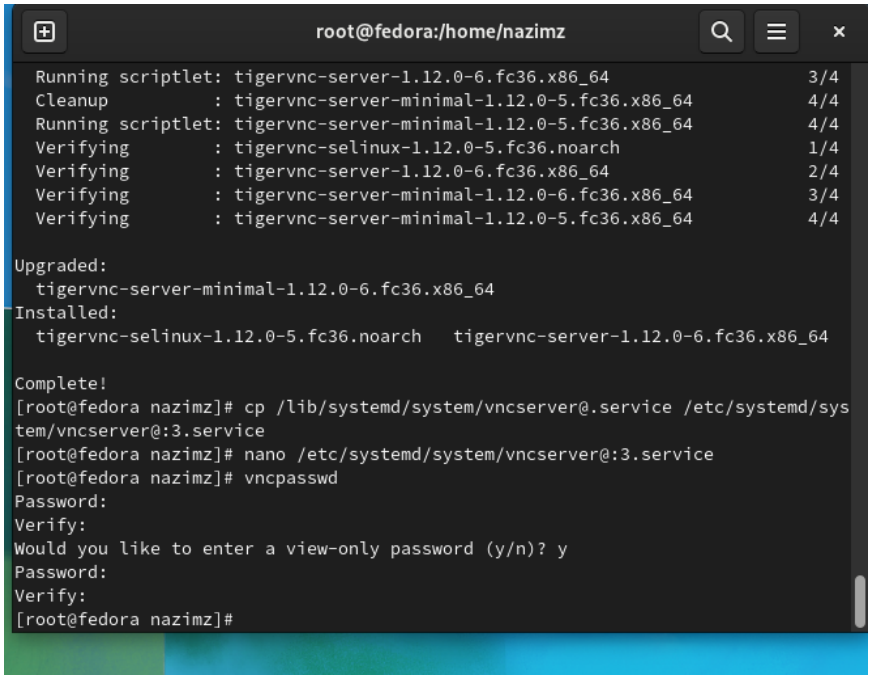
Question 3.3.3:

Question 4.1:

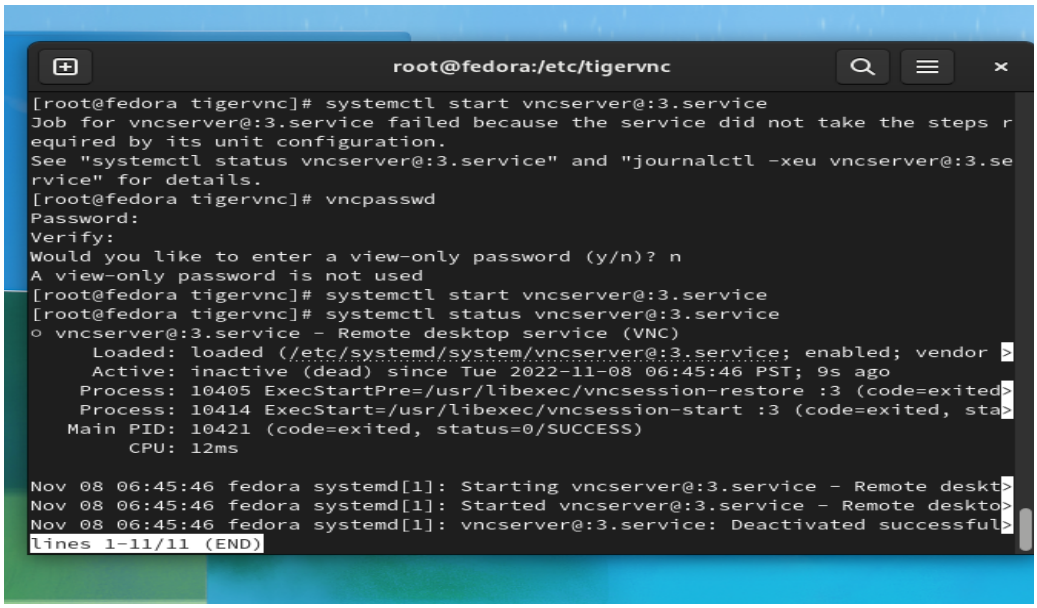
Installation of Tigervnc Server:



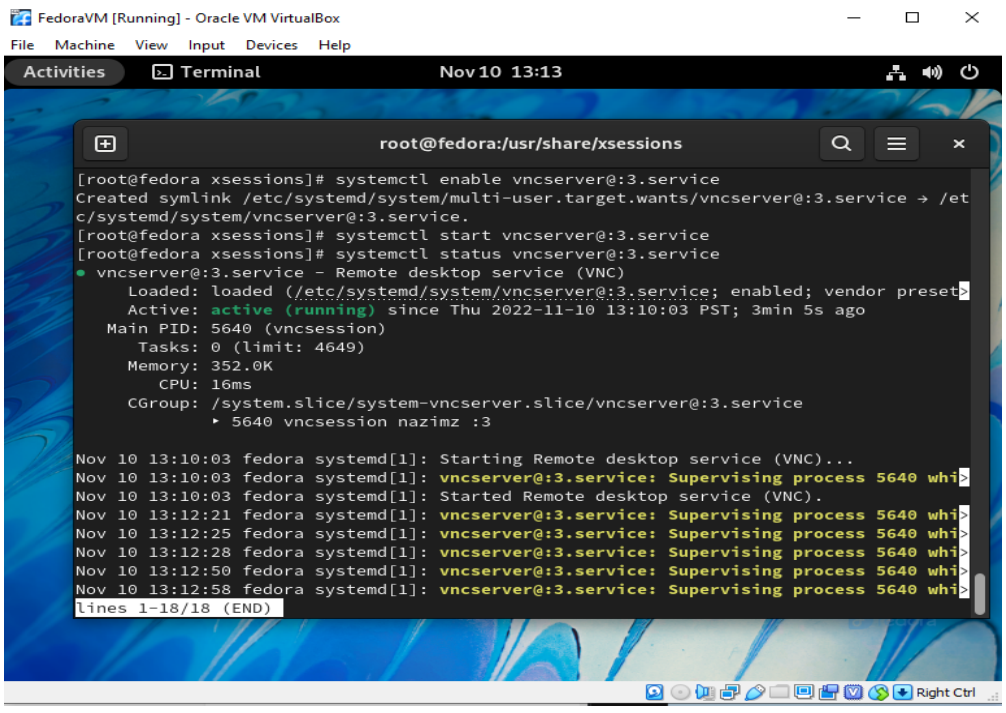
Verify Password:

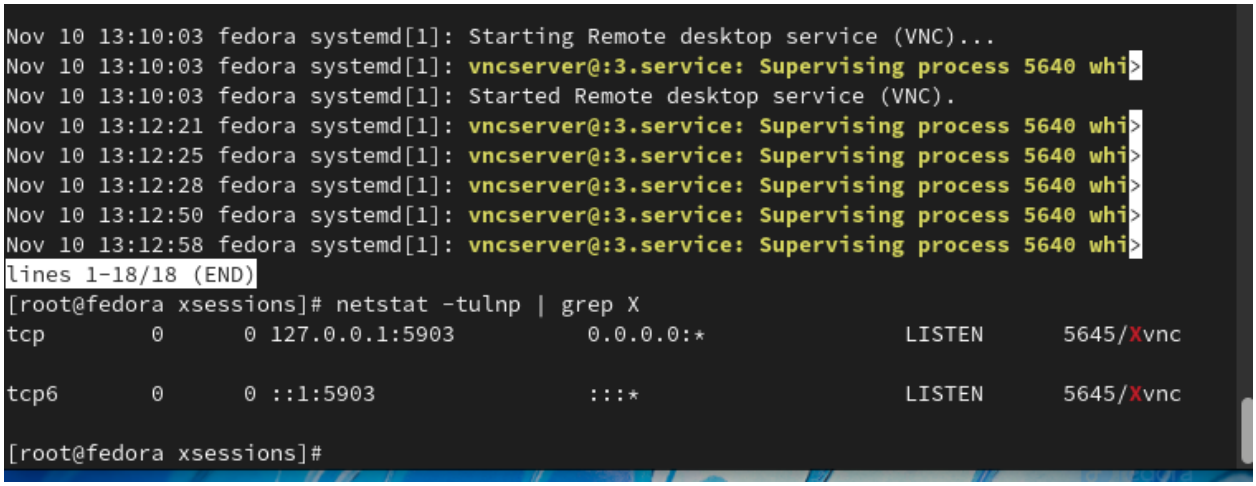


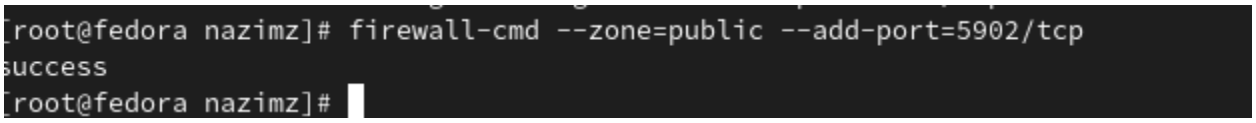
Successful vncserver start-up:



Verification of server running:







Setting up the Wireshark:

Question 4.2: