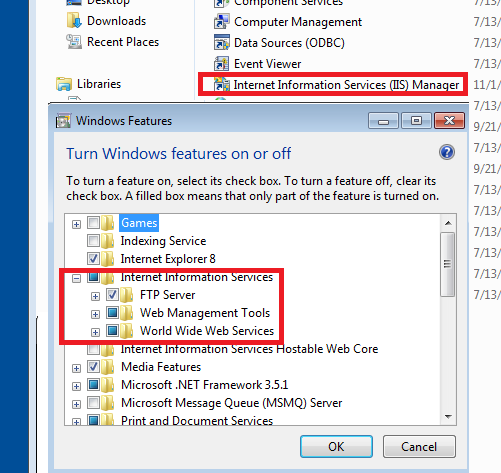
**Project 2: IPsec and SSH based VPNs**

**TCSS 431: Network Security**

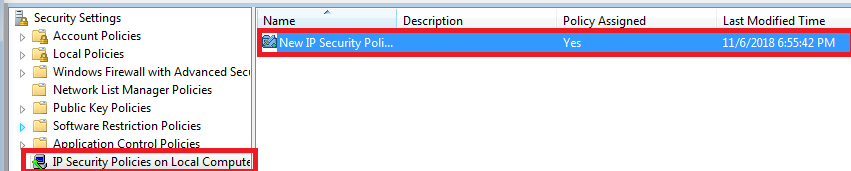
**Professor Wei Cheng**

**By Eduard Klimenko & Kyle Beveridge**

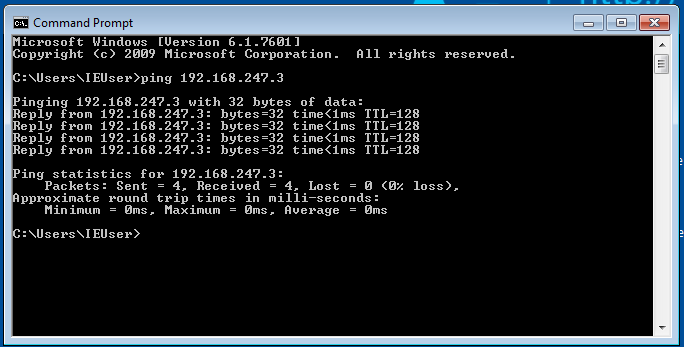
**Install Internet Information Services and the FTP Service (6 points)**

****

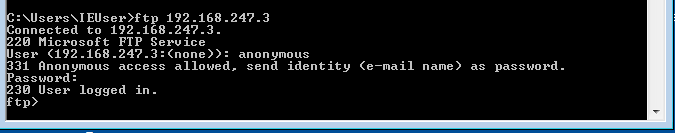
**Configure the FTP Service (6 points)**

****

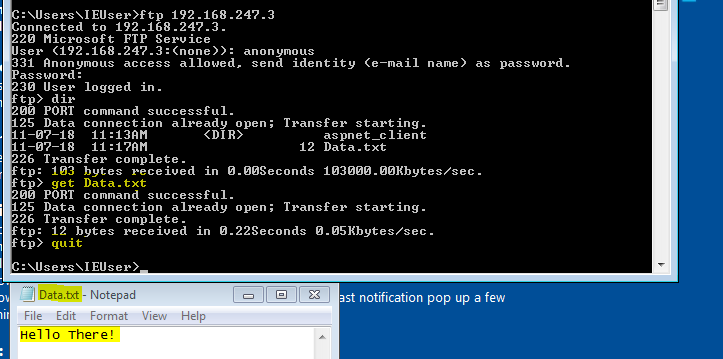
**Use your Windows client machine to make certain that you have connectivity to the FTP Server by pinging the server. (3 points)**

****

**Use the anonymous username and any password at the FTP prompt. (3 points)**

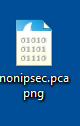
****

**When confirmed that FTP is working properly, quit the FTP connection (bye). (2 points)**

****

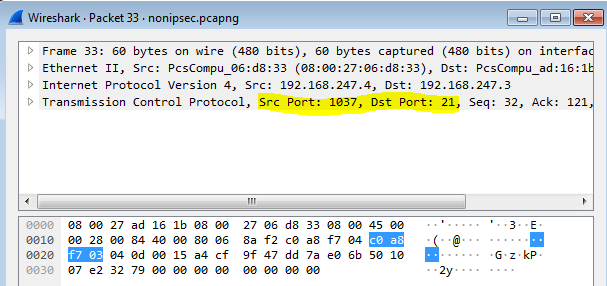
**Start capturing packets using the Wireshark. (3 points)**

**Save the file as nonipsec. (3 points)**

****

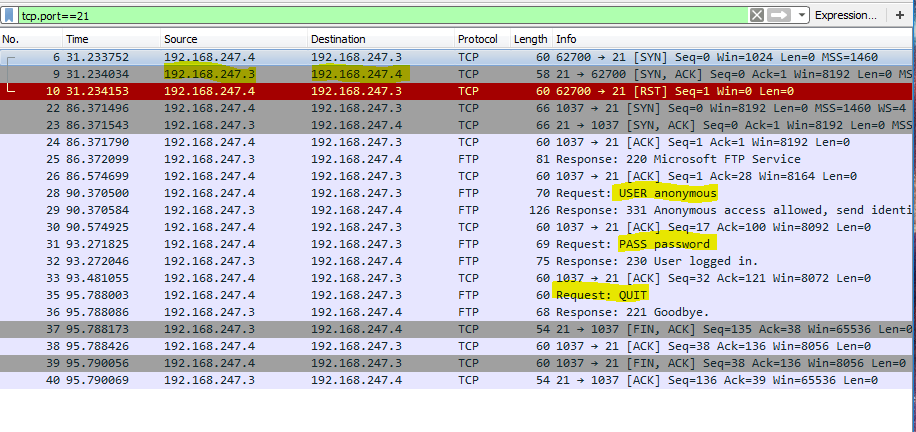
**Were you able to determine the source and destination port of the FTP connection? If so, what are they? (3 points)**

As you can see the source port was 1037(client), destination was 21 (server). These would be switched if the server was responding to the client.

****

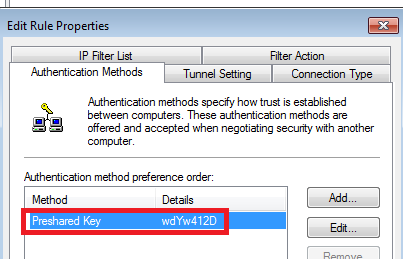
**Were you able to sniff the FTP username and password? Make certain to explain this answer. (3 points)**

The username and password were visible, and since this isn't an sftp setup, they are in plain text, not encrypted at all.

****

**Alter the Secure Server policy to use a preshared-key of wdYw4l2D (what do you want for lunch today) for both IP and ICMP traffic. (5 points)**

**Assign these settings on the Secure Server policy (3 points)**

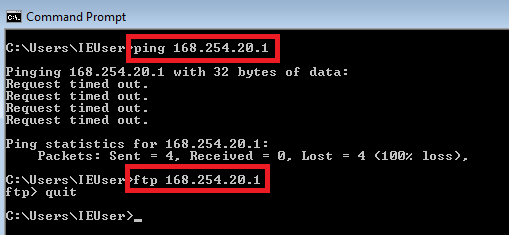
****

**Ping the server from client machine What response did you get? (3 points)**

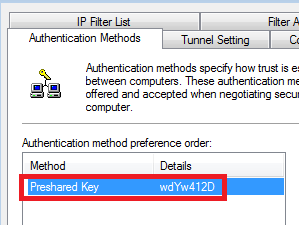
The request timed out, this means the server did not respond (unreachable).

**FTP to the Server machine from the client. What message did you receive? (3 points)**

No authentication handshake was initiated (connection timeout).

****

**Setting the IPSec policy for the Windows client machine (4 points)**

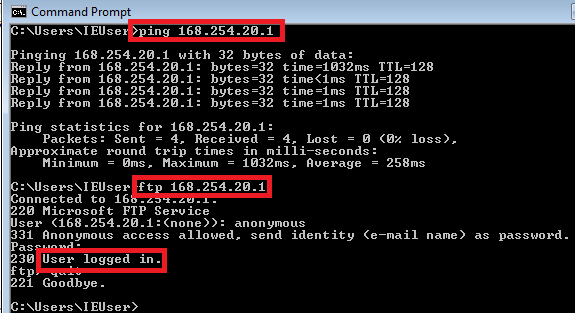
****

**Ping the server from Windows client machine What response did you get? (3 points)**

No packet loss, all packets were sent and received just fine.

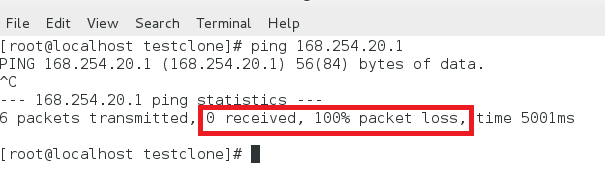
**FTP to the Server machine from the client What message did you receive? (3 points)**

Server asked for user and password as it normally would.

****

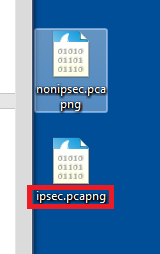
**Try to ping, ftp your Windows client and Server from your Linux machine. Can you get through? Why or why not? (3 points)**

No, the linux machine does not have the preshared key so connection is refused.

****

**Capture IPsec protected FTP traffic using Wireshark (3 points)**

**Save the file as IPsec (3 points)**

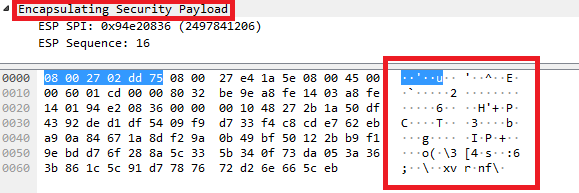
****

**Were you able to determine the source and destination port of the FTP connection? Why or why not? (3 points)**

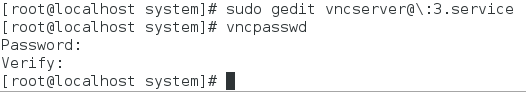
No, the packets were encrypted!

**Were you able to sniff the FTP username and password? Make certain to explain this answer. (3 points)**

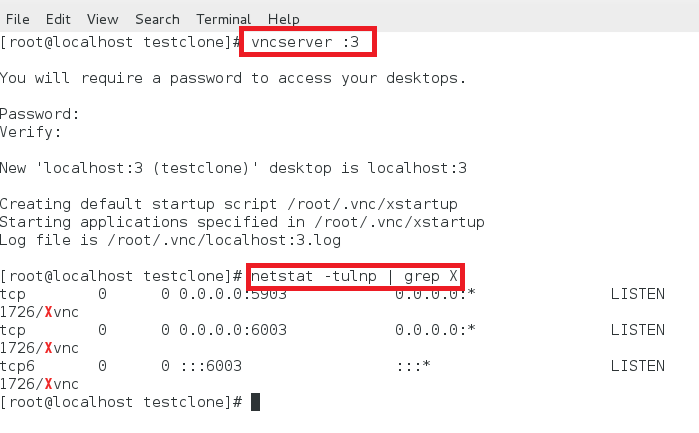
Similar to the previous question, the packets were encrypted so unless a third party had the preshared key they won’t be able to decrypt the packet and find the username and password (packets not in plain text).

****

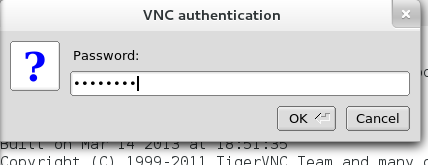
**Configure the VNC service (2 points)**

****

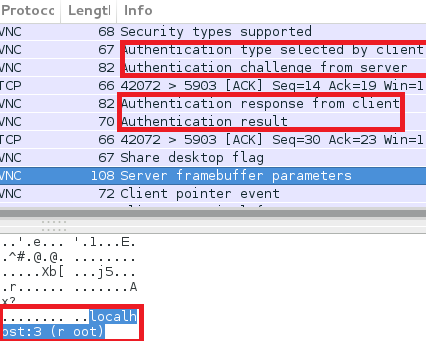
**Then, verify the vnc service is running: (3 points)**

****

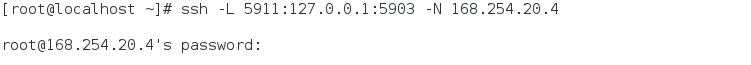
**Login with the password you have just created. (3 points)**

****

**Verify that you can see the authentication procedure and information exchange in the captured data. (3 points)**

****

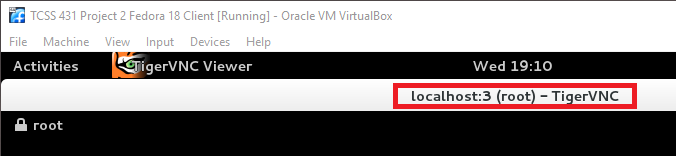
**On your client side, as the root user, issue the following commands: (3 points)**

****

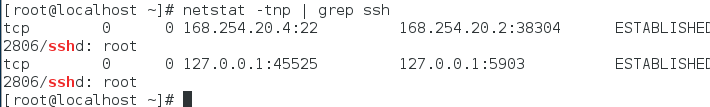
**Open another terminal; verify that your loopback address is listening on port 5911. (3 points)**

****

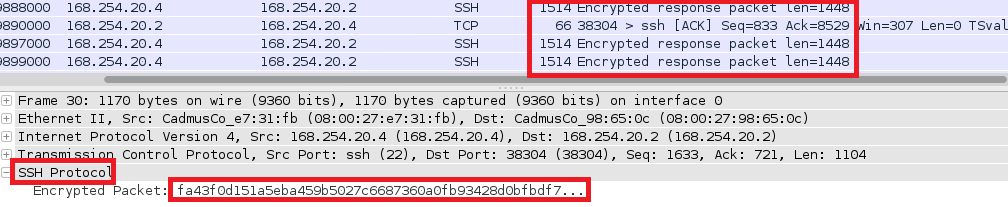
**Now you can VNC connect to the local port 5911: (3 points)**

****

**Go to your server side, verify that the ssh connection is established: (3 points)**

****

**Verify that you cannot see the authentication procedure and information exchange. (2 points)**

****

**Explain how SSH tunneling (port forwarding) works (3 points)**

SSH is a remote login shell that connects computers using encrypted connection. SSH tunneling is routing the network traffic through this SSH connection effectively making all packets encrypted over this connection.

**To stop your vncserver on the service side, type: (2 points)**

****