Basic IT Security

Windows 10 Security

Name: _____ Class: _____

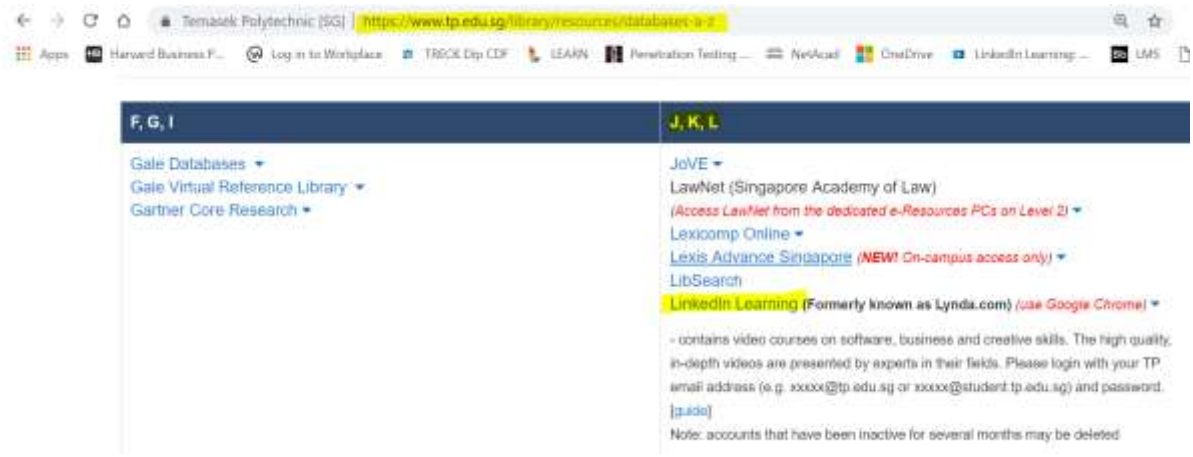
Objectives:

At the end of the lab session, you will learn on

- Setting up passwords
- Creating groups and assigning permissions
- Assigning permissions
- Encrypting full disk, file transfers, and networks
- Using anti-virus and anti-malware solutions
- Configuring firewall settings
- Securing remote desktop connections

To access the lab video, you need to login to LinkedIn Learn via TP Library website.

https://www.tp.edu.sg/library/resources/databases-a-z



1. Authentication and Account

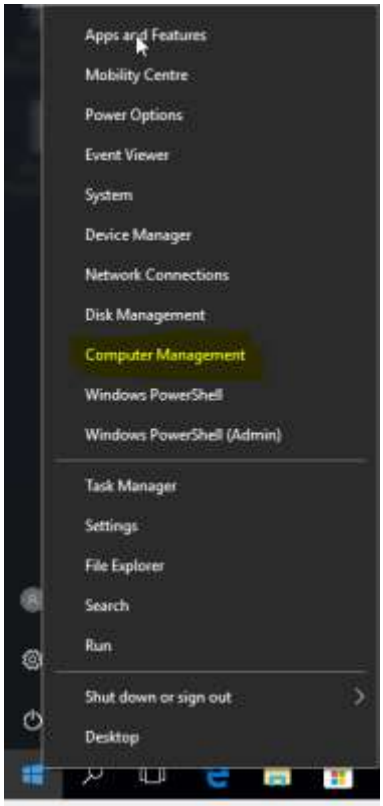
Watch the video.

https://www.linkedin.com/learning/windows-10-security/working-with-local-accounts-in-windows-10?u=76881922


LEARNING
Browse
Search for skills, subjects or software
Home
In Progress
Saved
Me
Watching: Working with local accounts in Windows 10
From the course: Windows 10: Security
Overview
Contents
Q&A
New
Working with local accounts in Windows 10
1m 39s

Create a "TestUser**" Local** account as follow.

a.



b.

2. Authorization

Watch the video and fill in the table.

https://www.linkedin.com/learning/windows-10-security/overview-of-authorization?u=76881922

Fill in the table below with the correct definitions.

a. All the above and allow to change the file permission
b. Read file content without file execution
c. Read, Execute, Write and Delete file
d. Make file content changes but cannot delete file
e. Read file content and ability to execute the file

Permissions	**Definition**
Read	b
Read and Execute	d
Write	d
Modify	c
Full Control	a

2.1 Inheritance of permissions

Watch the video

https://www.linkedin.com/learning/windows-10-security/understanding-inheritance-of-permissions?u=76881922

When the inheritance permission of a parent folder is disabled, will the files permission under the parent folder remains as before or will their inherited permission be removed?

Removed

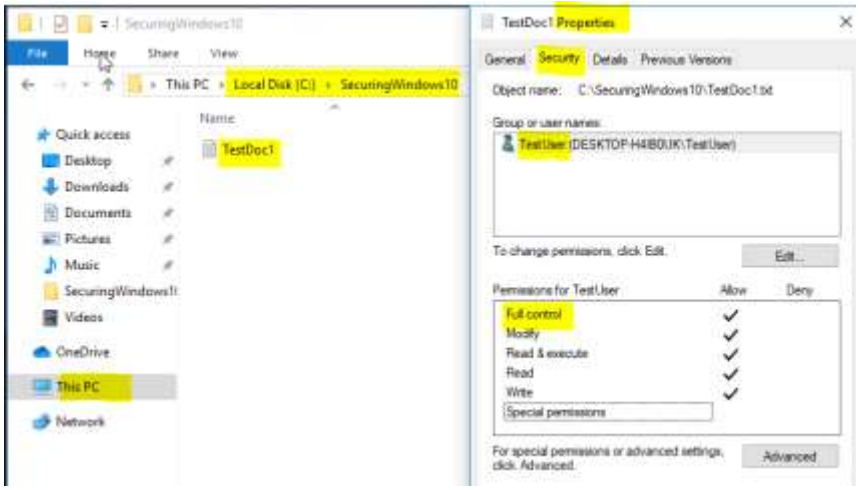
2.2 Disable permission inheritance

Create a new folder “SecuringWindows10” in C: drive

In the new folder, create a text file “TestDoc1.txt” with the content “Hello World”

Remove all inherited permission for TestDoc1.txt and only give the account “TestUser” Full control of the file.

If done correctly, the file properties should look as follow:



2.3 Assigning permissions

Watch the video

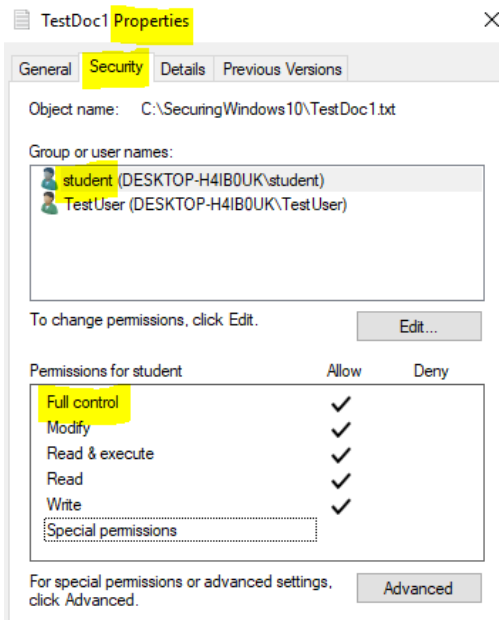
https://www.linkedin.com/learning/windows-10-security/assigning-permissions?u=76881922

Assign the account “student” with Full control permission to the file TestDoc1.txt

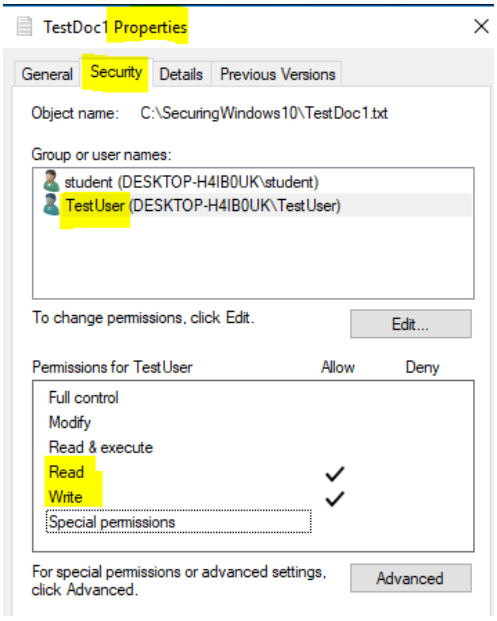
“TestUser” account should only have Read and Write permission to this file.

If done correctly, the file properties should look as follow:

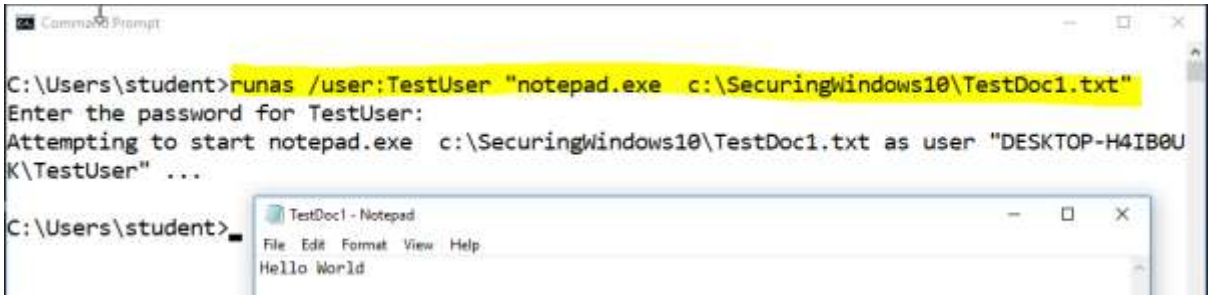
a.



b.

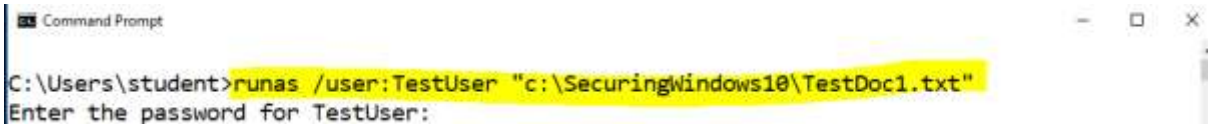


Run the following command. Are you able make changes and save to the file?



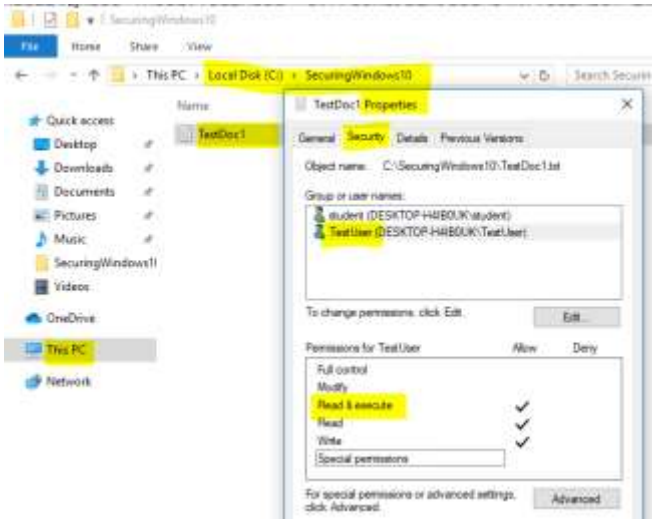
Yes. Can make changes and save to the file.

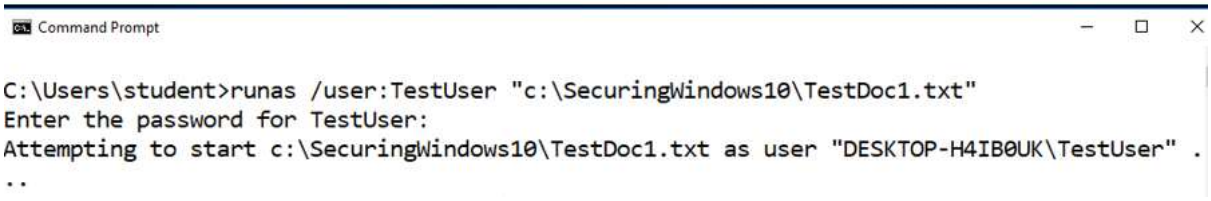
Run the following command. Are you able to execute the file? If not, why?



No, .txt file cannot be exeuted as no execute rights.

Grant TestUser Read and Execute permission, can the file be executed? If not, why?





No, bec .txt file cannot be directly executed. even though read, execute and write access is granted.

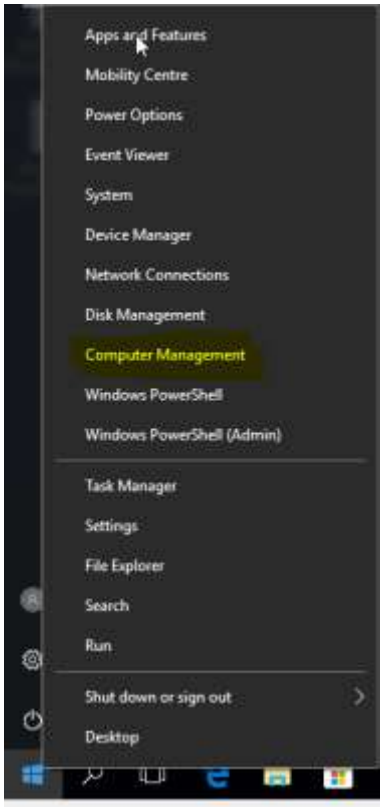
2.4 Creating and using groups

Watch the video

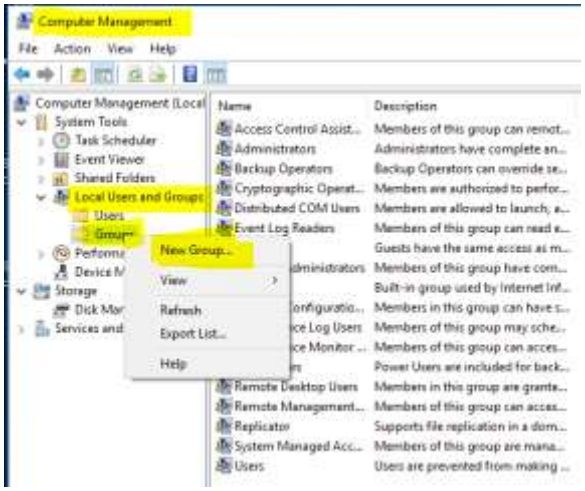
https://www.linkedin.com/learning/windows-10-security/creating-and-using-groups?u=76881922

Right click Window start bar and use Computer Management to add new group.

a.

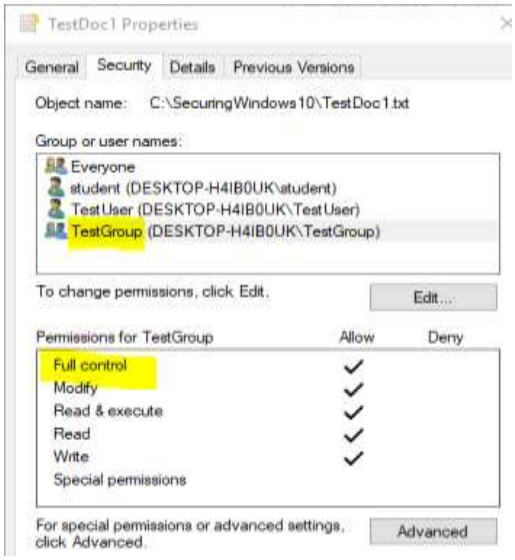


b.

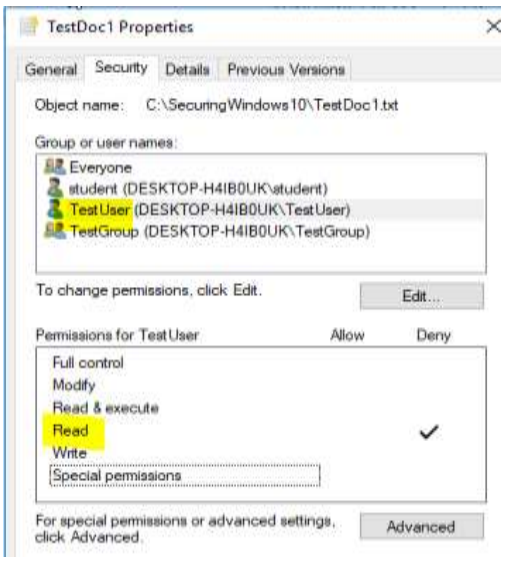


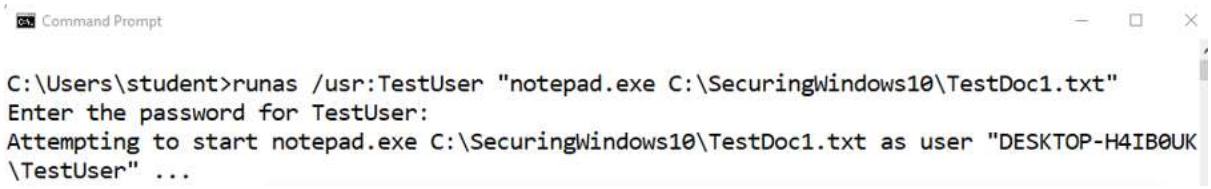
a. Add “TestGroup” as a new group.
b. Assign “TestUser” to this new group.
c. Grant “TestGroup” Full control to “TestDoc1.txt”
d. Remove all permissions of TestUser from TestDoc1.txt and Deny read access for TestUser to the file.
e. TestUser is a member of TestGroup which has Full control of the file.
f. Try reading the file as TestUser. is TestUser able to read the file?

a.



b.





Yes, testUser is under TestUsers group, which has full control rights

2.5 Built in Groups

https://www.linkedin.com/learning/windows-10-security/working-with-built-in-groups?u=76881922

Is the group “Everyone” visible under Computer Management Local Group folder?

Alas, "Everyone" is not visible

Try granting the “Everyone” group to access “TestDoc1.txt”. Can it be done?

Yes, it can be done.

Fill in the table below with the following correctly matched.

a. Interactive
b. Anyone who can be authenticated with a password
c. All locally logon users excluding remote users
d. Everyone
e. All users including guest account without password
f. Authenticated Users

Implicit Groups	Definition Text
a	c
d	e
f	b

Why should you be aware of implicit groups?

You can accidently give everyone permission to a file.

3. Encryption - Bit Locker

Watch the video and encrypt the drive using bit locker.

https://www.linkedin.com/learning/windows-10-security/using-bitlocker?u=76881922

Turn on bit locker for C: drive. Can you? If not, why?

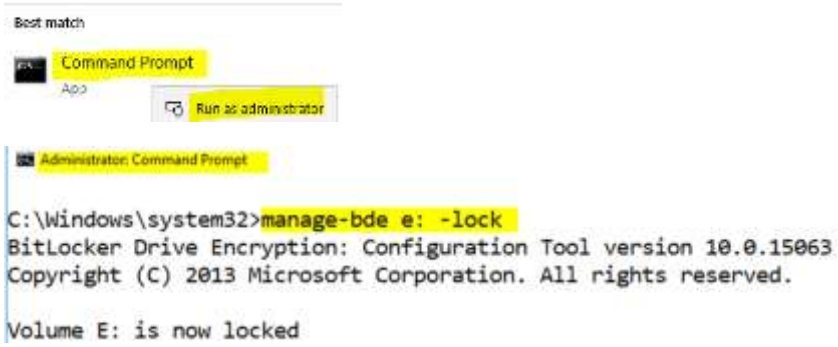
Cannot. It shows this drive can't use a "trusted platform module."

Enable Bit Locker for E: drive where it is an additional 100M virtual disk added to the Win10 VM.

Open an Administrator Command Prompt shell.

Bit Lock E: drive using the following command “manage-bde”.

The command must be run using administrator command prompt, else it would fail.



Unlock E: drive using the following command line. Fill in the blank.

https://www.top-password.com/blog/decrypt-bitlocker-encrypted-drive-from-command-line/

If you can remember your BitLocker user password, type the following command. After pressing Enter, you’ll be prompted to enter the user password. manage-bde -unlock D: -Password

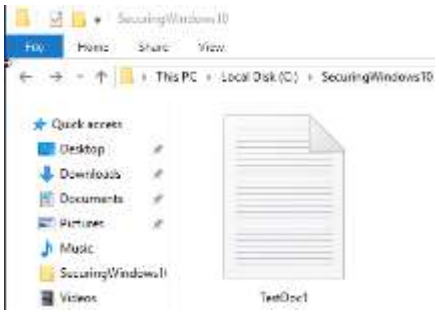
3.1 Encrypted File System (EFS)

Watch the video.

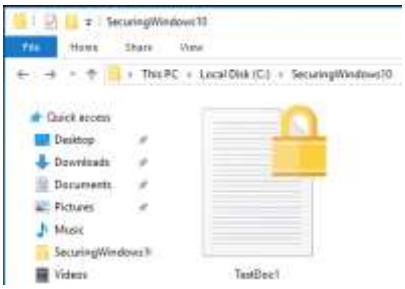
https://www.linkedin.com/learning/windows-10-security/using-efs?u=76881922

Using EFS, create a **self-sign** certificate to encrypt "TestDoc1.txt". You see a Lock icon on the file if done successfully.

a. Before EFS



b. After EFS



What is the difference between Bit Locker and EFS? Fill in the table below.

https://www.howtogeek.com/236719/whats-the-difference-between-bitlocker-and-efs-encrypting-file-system-on-windows/

a. Encrypt by individual user
b. Encrypt using individual generated certificate
c. Encrypt the entire drive
d. Encrypt individual files selectively
e. Encrypt by password
f. Encrypt by administrator

Bit Locker	**EFS**
a	b
c	d
e	f

4. Virus and Malware

Watch the video.

https://www.linkedin.com/learning/windows-10-security/virus-and-malware-overview?u=76881922

Fill in the table below with the correct definitions.

a. Perform interactive human action such as sending email without human intervention
b. Need not attached to a host program to spread itself
c. Need to attached to a host program to spread itself
d. Malicious program that disguise as legitimate program

Virus	c
Worm	b
Trojan	d
Bot	a

4.1 Window Defender

Watch the video.

https://www.linkedin.com/learning/windows-10-security/windows-defender-virus-and-threat-protection?u=76881922

What does the “Controlled folder access” feature do? Is it available in your Window VM?

It protects specified folders or files from unauthorized changes or apps.
Yes, its available in my Windows VM.

4.2 Firewall and network

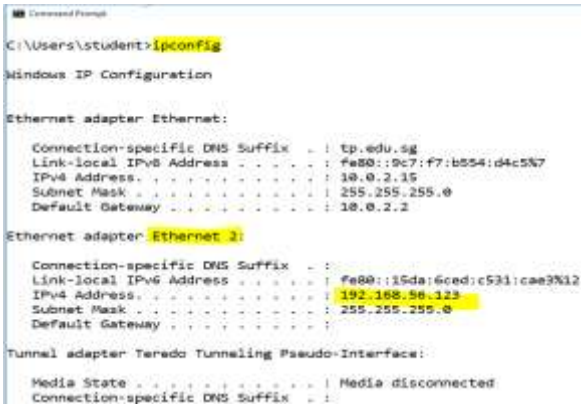
Watch the video.

https://www.linkedin.com/learning/windows-10-security/windows-defender-firewall-and-network-protection?u=76881922

Verify that the VM Network Adapter 2 is Enabled and the Cable connected. Check that the Win10 VM Ethernet 2 Host-only adapter has an IP address. Otherwise please check the Window Ethernet 2 TCP/IP v4 network setting is correct.

a.

b.



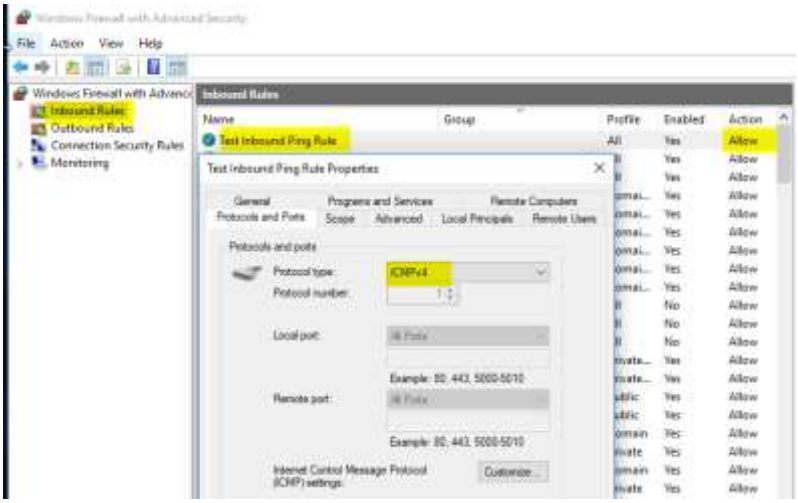
Run the ping command from your laptop. Can you ping from your laptop to the Win10 VM?

Configure the Win10 VM firewall to allow other machine to ping to it.

Use Windows Firewall with Advanced Security settings, create a firewall rule name “Test Inbound Ping Rule” to allow inbound ICMPv4 ping traffic for all Network profiles.

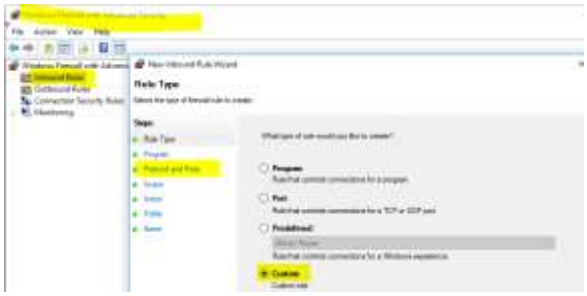
a.

b.

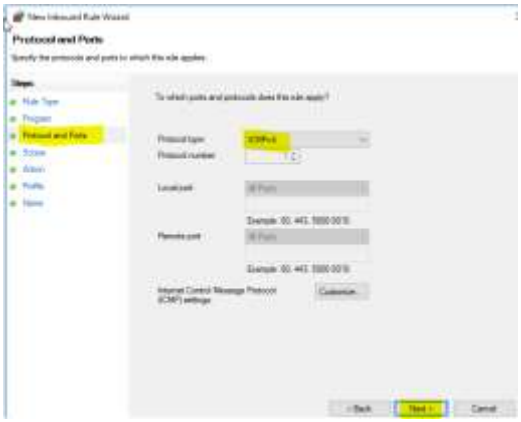


Create a custom firewall rule name “Test Inbound Ping Rule” to allow inbound ICMPv4 protocol traffic for both local and remote IP addresses on all Network profiles.

a.



b.

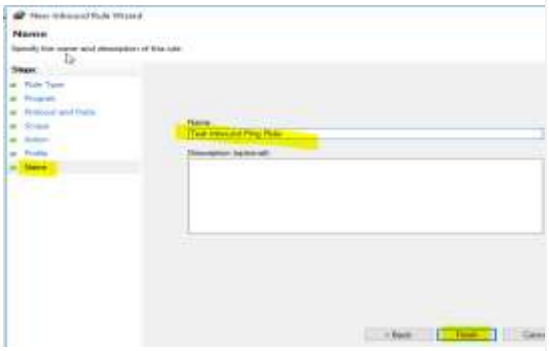


c.

d.

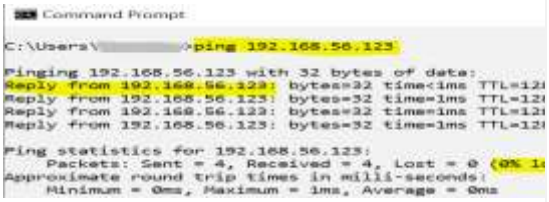
e.

f.



g.

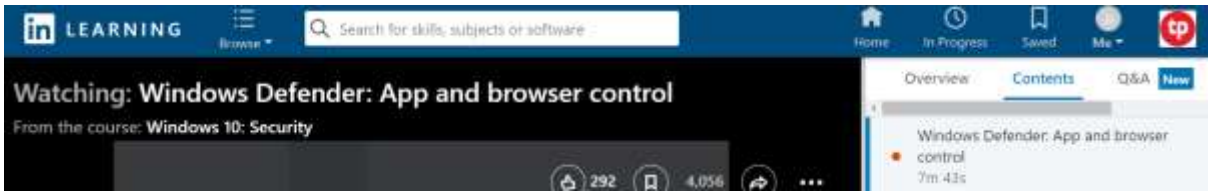
h.



4.3 App and bowser control

Watch the video.

https://www.linkedin.com/learning/windows-10-security/windows-defender-app-and-browser-control?u=76881922



What does the feature “Exploit protection” under App and browser control that was discussed in the video protect against?

5. Network Security - Securing network traffic using IPSec

Watch the video.

https://www.linkedin.com/learning/windows-10-security/securing-network-traffic-by-using-ipsec?u=76881922

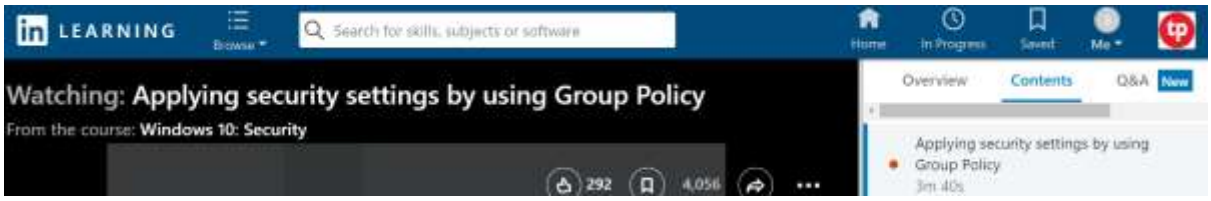
What is the different between IPSec Request and Require mode?

Watch the video and create a custom IPSec rule name “IPSecRequest” in the firewall under Connection Security Rules. You need not test the connection.

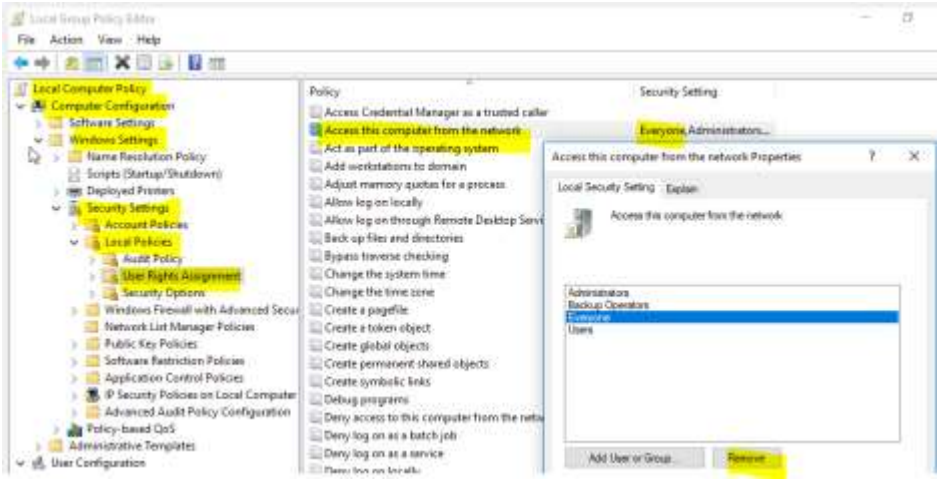
6. Group Policy

Watch the video.

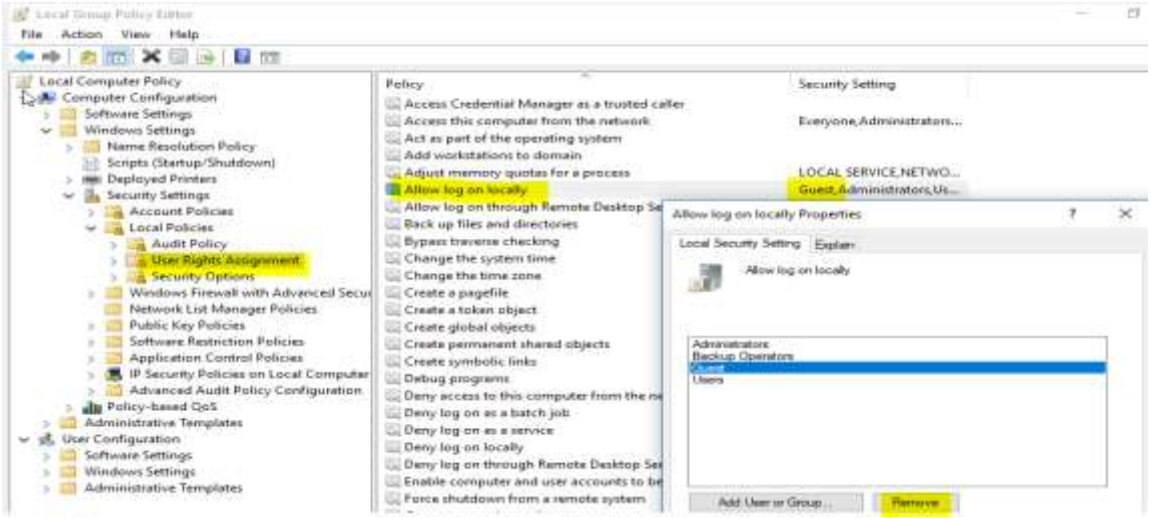
https://www.linkedin.com/learning/windows-10-security/applying-security-settings-by-using-group-policy?u=76881922



Remove the Everyone group from “Access this computer from the network”



Remove the Guest group from “Allow log on locally”

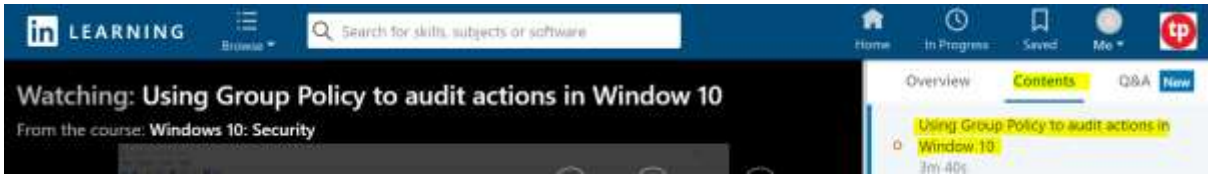


Set the same password policy as below

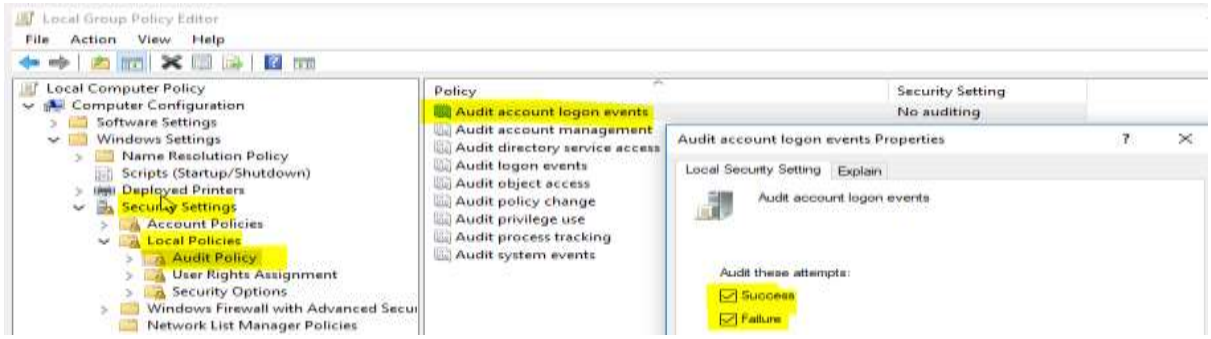
6.1 Audit account logon events

Watch the video.

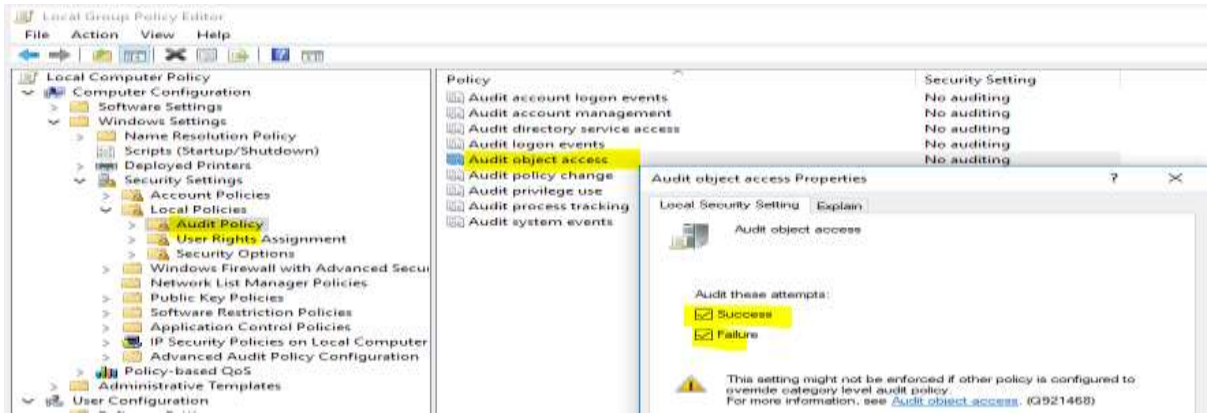
https://www.linkedin.com/learning/windows-10-security/using-group-policy-to-audit-actions-in-window-10?u=76881922



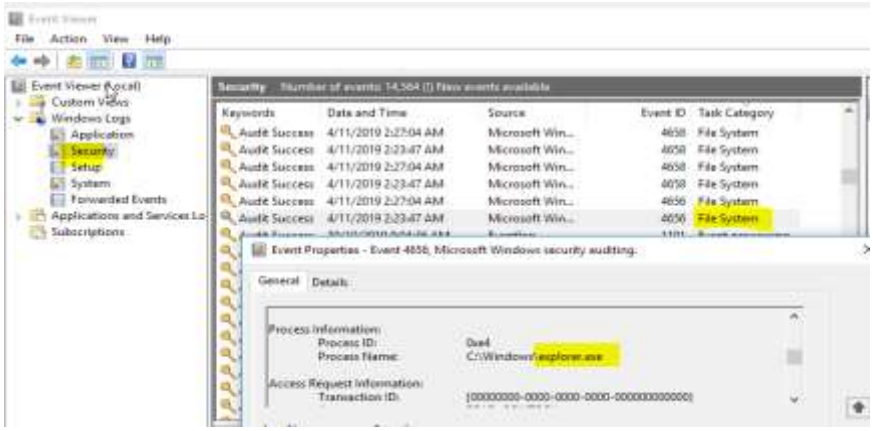
Enable Audit account logon events for both success and failure



Enable Audit object access for both success and failure



Try accessing some files. Investigate the Window Security Event logs for File System events.



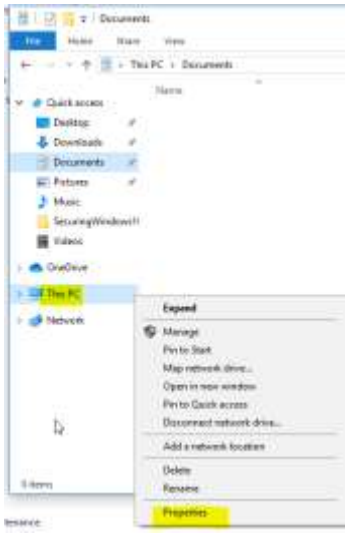
7. Remote Desktop

Watch the video.

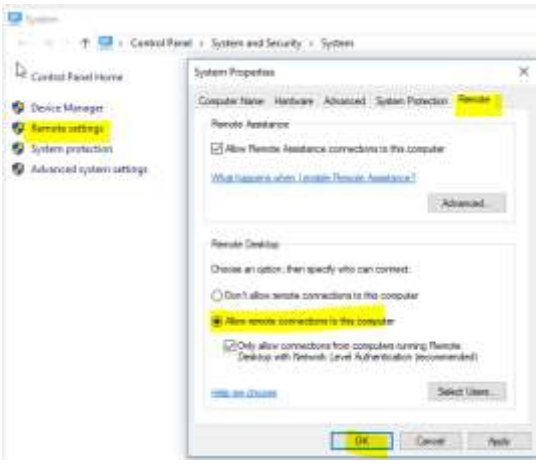
https://www.linkedin.com/learning/windows-10-security/basic-configuration-of-remote-desktop-2?u=76881922

Allow remote connections to the computer.

a.

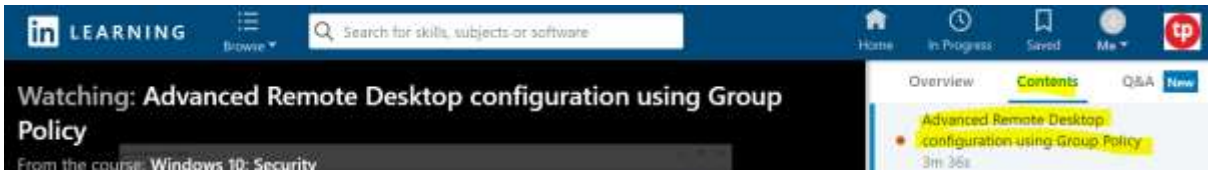


b.

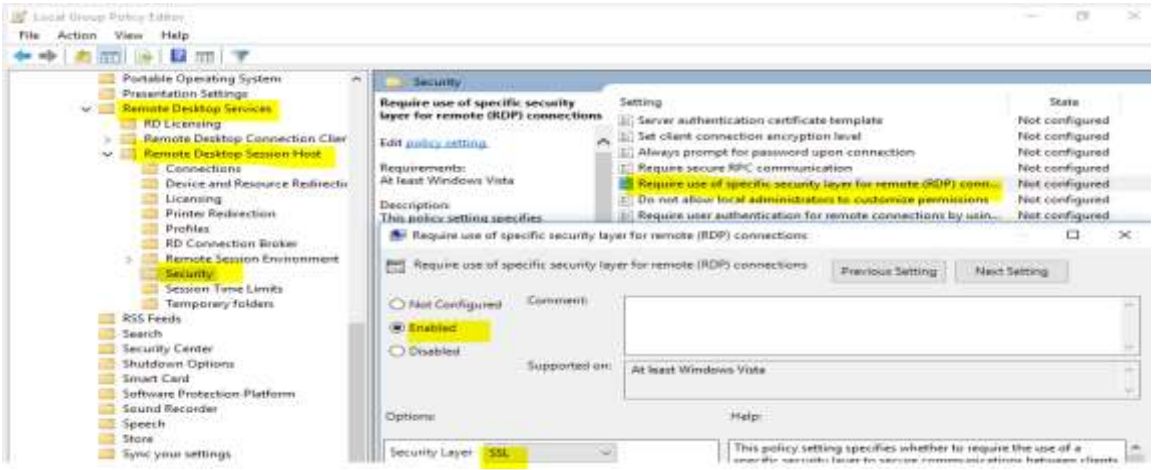


7.1 Advance Remote Desktop using Local Group Policy

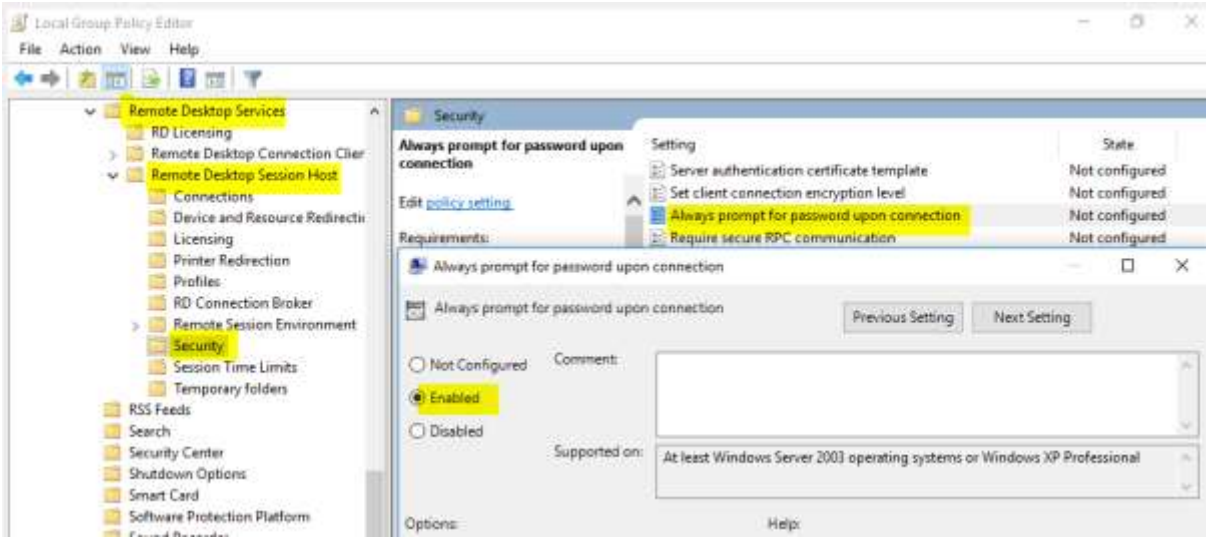
https://www.linkedin.com/learning/windows-10-security/advanced-remote-desktop-configuration-using-group-policy?u=76881922



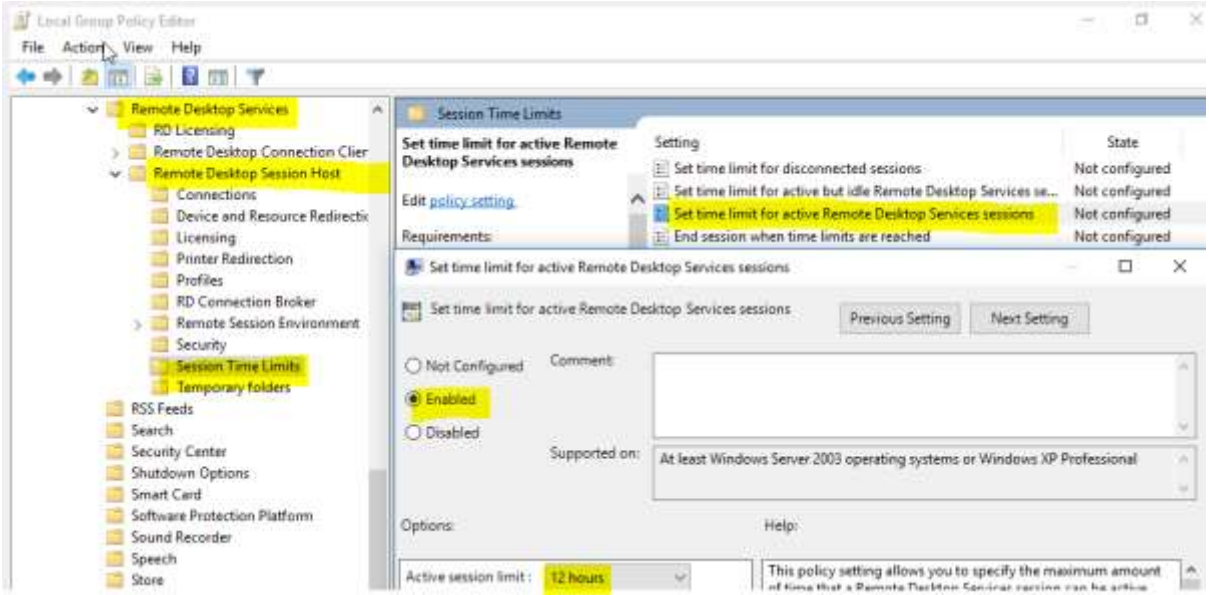
Enable SSL for RDP require use pf specific security layer.



Enable “Always prompt for password upon connection”

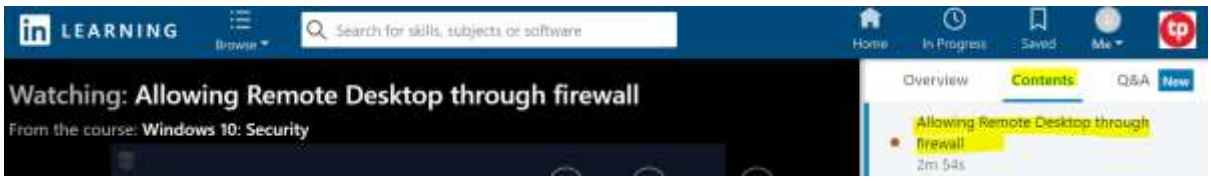


Session Time Limits for active Remote Desktop Services sessions to 12hrs

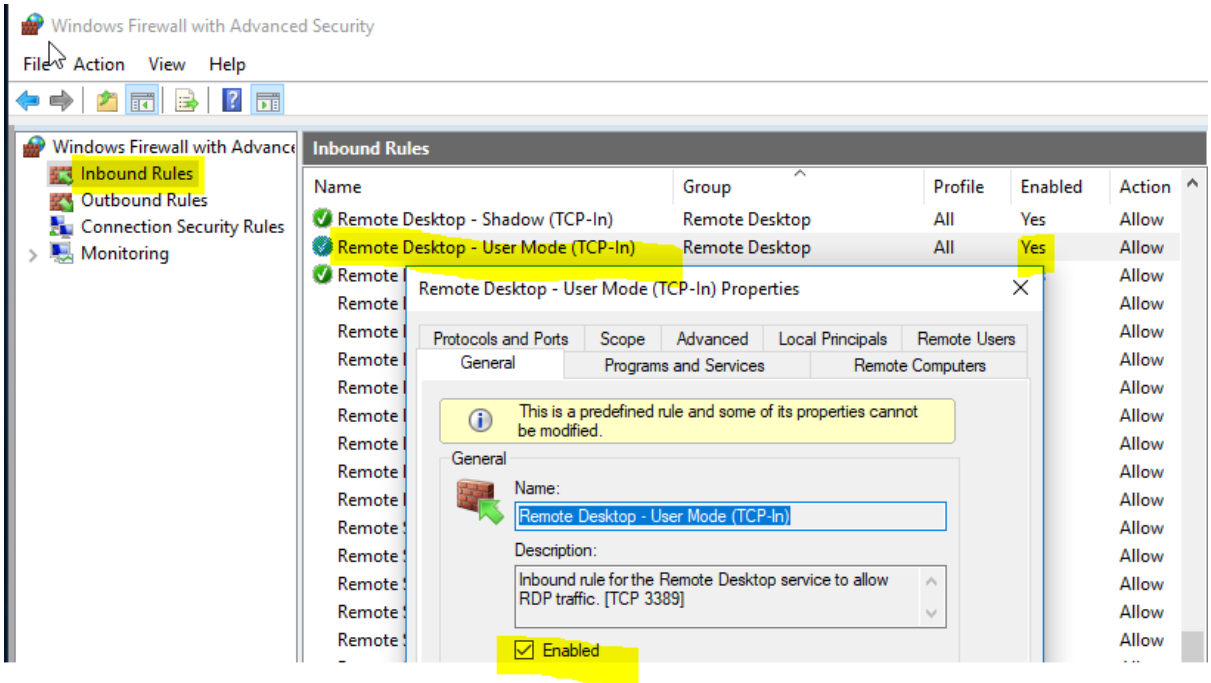


7.2 Allowing RDP through firewall

https://www.linkedin.com/learning/windows-10-security/allowing-remote-desktop-through-firewall?u=76881922



Verify Inbound Rules, Remote Desktop – User Mode (TCP-In) is Enabled on the firewall

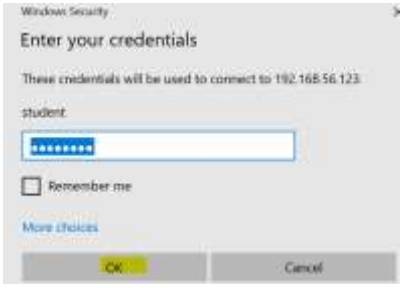


Remote into the Win10 VM from your laptop. Run these command on your laptop.

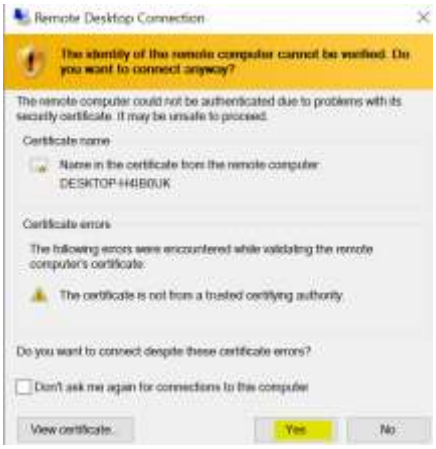
a.

b.

c.

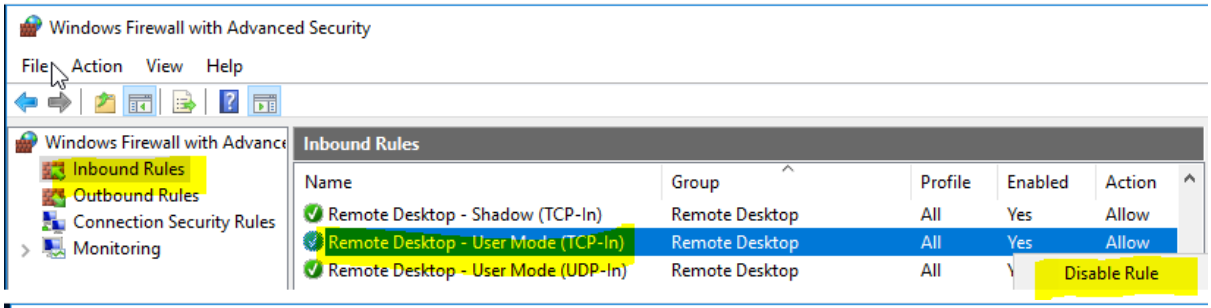


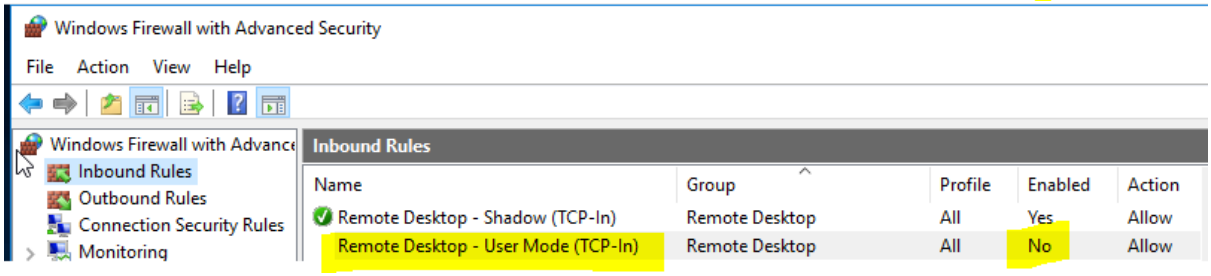
d.



e.

Disable Inbound Rules, Remote Desktop – User Mode (TCP-In) on the firewall.





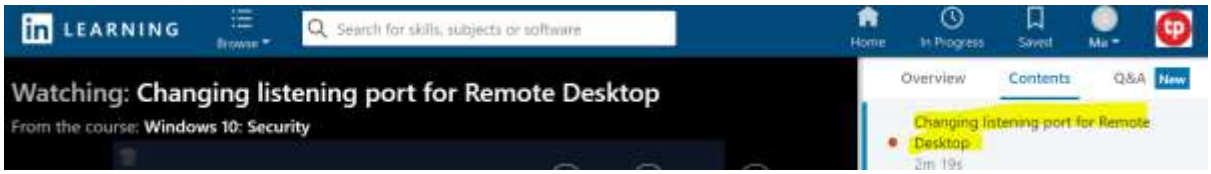
Try to remote access to the Win10 VM from your laptop again.

Are you able to do remote access?

7.3 Changing Listening Port for RDP (Challenge Lab)

Watch the video.

https://www.linkedin.com/learning/windows-10-security/changing-listening-port-for-remote-desktop?u=76881922



Change the Win10 VM RDP service to listen on port 4567. Try to remote desktop into the Win10 VM from your laptop using the new RDP port 4567 as below. (hint: You may need to configure additional inbound firewall rule on the Win10 VM)

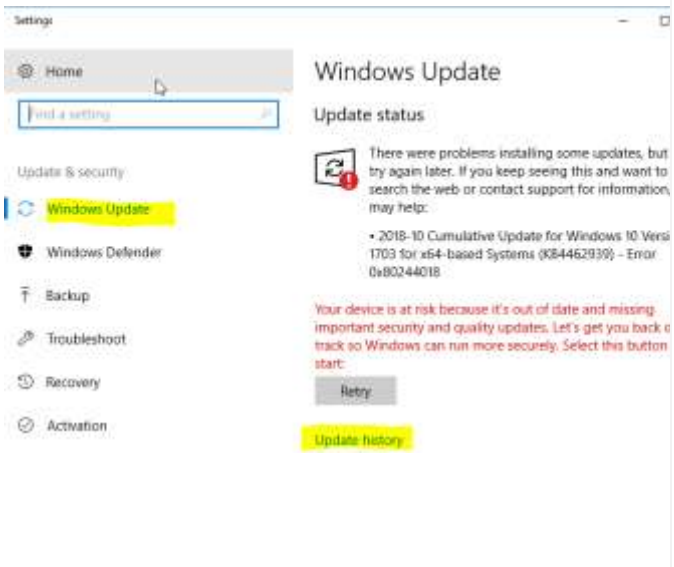
8. Miscellaneous

8.1 Window Update

Explore window update features. Try to perform an update and uninstall one of the updates.

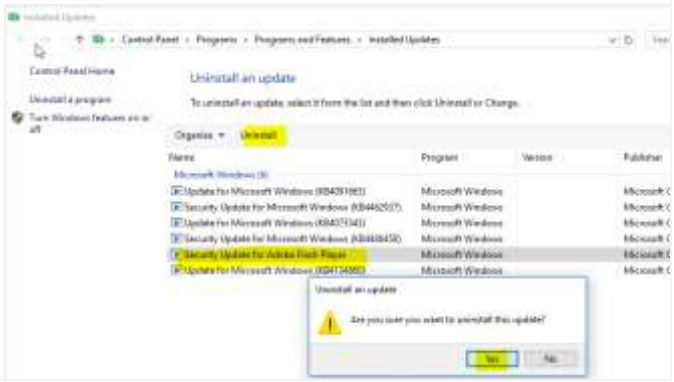
a.

b.



c.

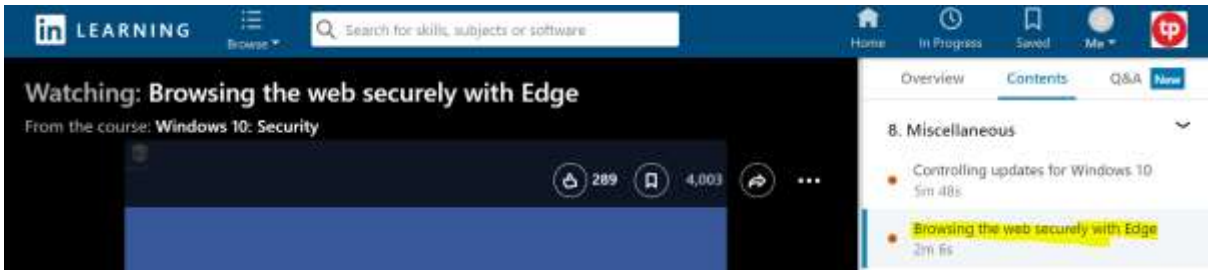
d.



8.2 Browsing securely

Watch the video.

https://www.linkedin.com/learning/windows-10-security/browsing-the-web-securely-with-edge?u=76881922



Perform the following on the browser settings.

a. Block pop-ups
b. Disable Adobe Flash Player
c. Disable save password
d. Block only third party cookies
e. Enable help protect from malicious sites

8.3 Secure Boot

Watch the video.

https://www.linkedin.com/learning/windows-10-security/secure-boot?u=76881922

Given the following, arrange them in the correct boot sequence and definitions in the table below.

a. UEFI verify firmware signature
b. Secure Boot
c. Check device drivers for malware before loading the devices
d. Load OS kernel with verified certificate
e. Early Launch Anti Malware
f. Trusted Boot

Boot Sequence	Boot Definition
b	a
f	d
e	c

END