Javen Lai Le Yu

2202934B

P17

Appendix: Page

A) Certifications

LinkedIn:
https://www.linkedin.com/learning/certificates/306c3b06ea62eb2eb2608edfcdb5ce55c3b24bcb875178374da2bff961fdbbb0?u=76881922

Linux Course:

Dear JAVEN LAI LE YU JAVEN LAI LE YU,

Congratulations on completing the NDG Linux Unhatched course in the Cisco Networking Academy. This letter documents you have successfully completed the NDG Linux Unhatched course, which provides an introduction to the Linux command line. Linux is everywhere! As the reach of Linux continues to grow, knowledge of Linux is a core skill for all IT professionals. By completing this course, you have gained a better understanding of Linux.

If you decide to pursue additional knowledge of Linux consider:

NDG LINUX ESSENTIALS

This course is the perfect next step for beginners looking to expand their skills and knowledge of Linux. This full-semester course can be delivered as instructor-led training or as a self-paced learning experience. The NDG Linux Essentials course is designed to prepare you for the Linux Professional Institute Linux Essentials Professional Development Certificate.

NDG LINUX SERIES

This certification level series offers beginners more rigorous in-depth coverage. The NDG Introduction to Linux I and NDG Introduction to Linux II courses focus on the basic Linux system administration skills needed in preparation for the Linux Professional Institute LPIC-1 certification.

Again, congratulations and we wish you continued success!

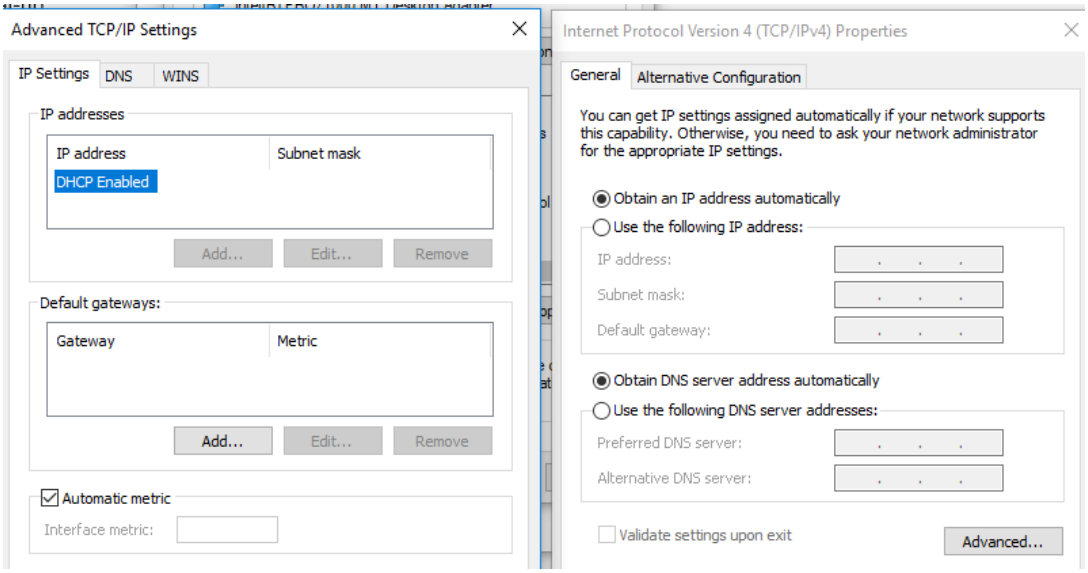
Sincerely,
The NDG Team

Date 27 Oct 2022

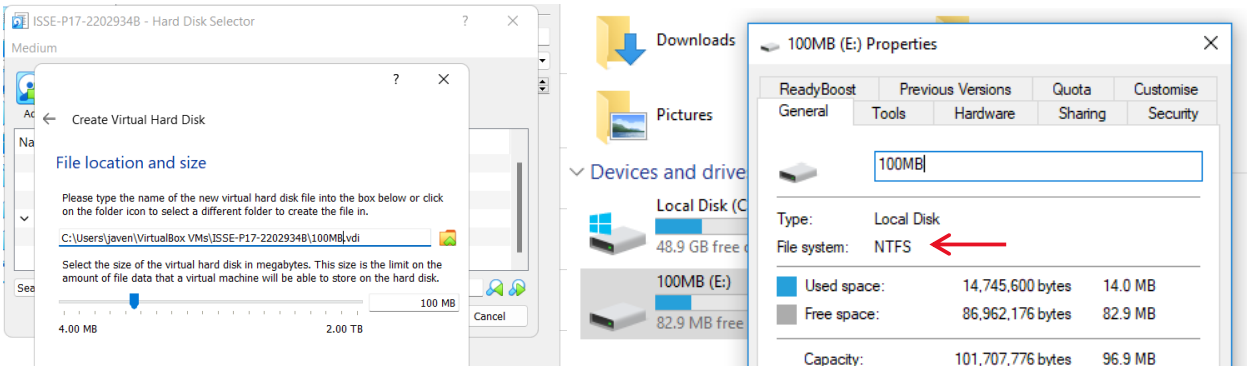
Part A

This section is not fully documented as it's the same as LMS Lab Materials.

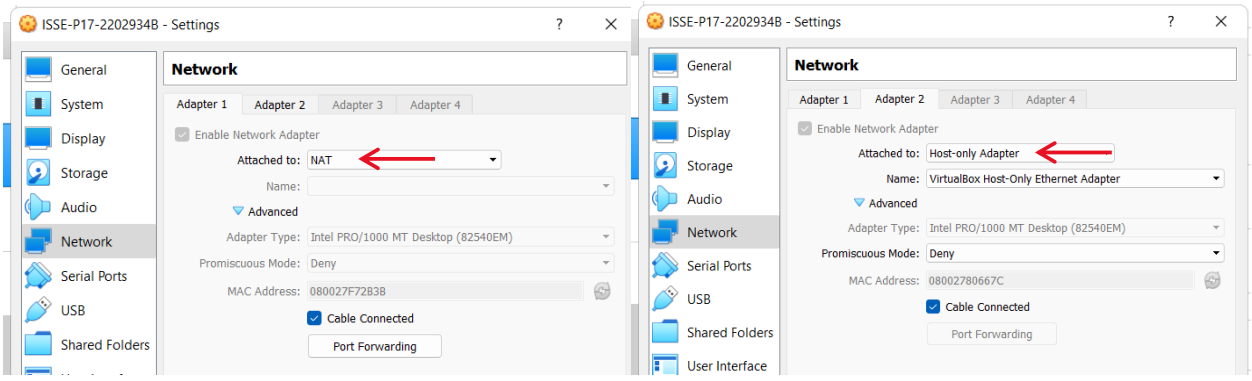
1. Following through Week 1 and 2, the Virtual Machine is setup with the configurations:



Check to ensure DHCP enabled.

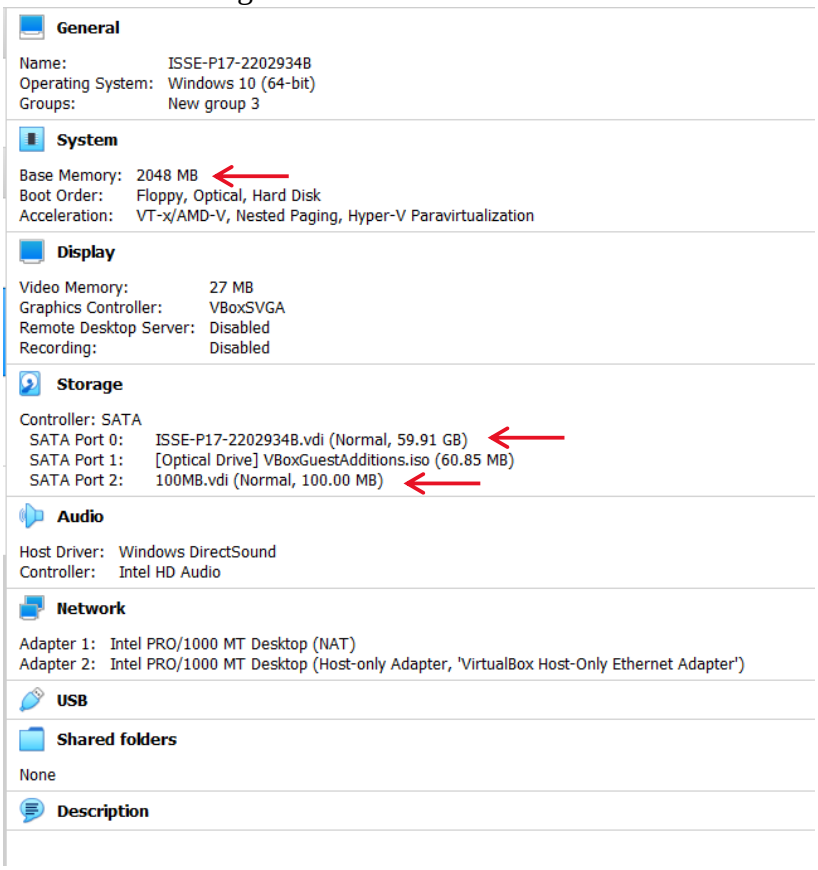


Left: Creation of Virtual Hard Disk (Week 2), Right: Check if file system is NTFS.



Setting up NAT and Host-only ethernet Adapters. Left: Adapter 1, Right: Adapter 2.

Overview of configurations of VM.

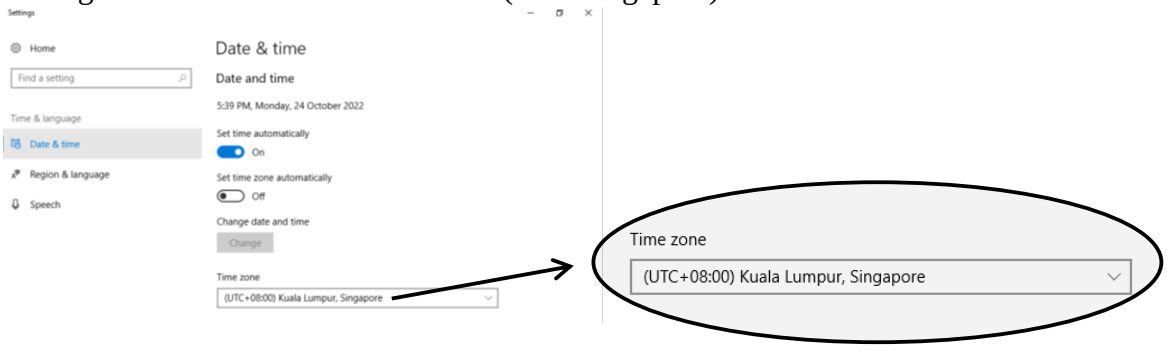


Meets requirements as stipulated on Specifications.

Part B

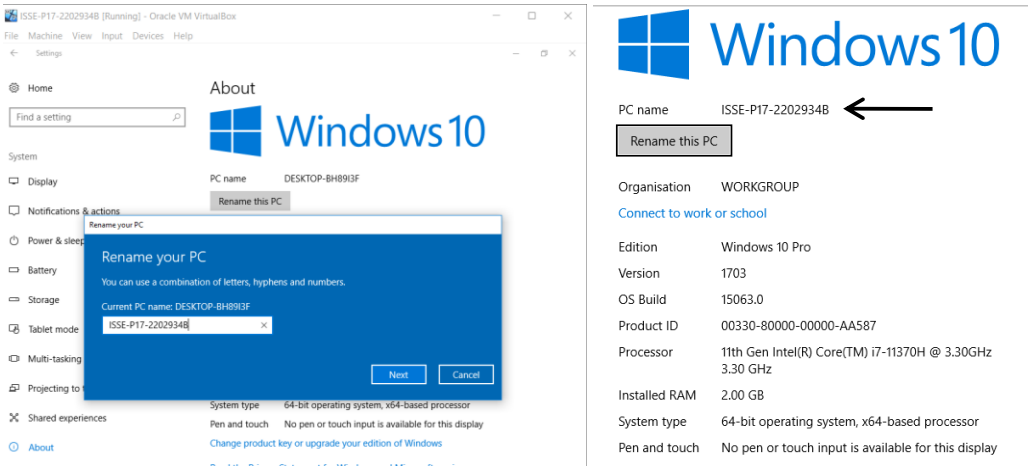
1.2) Changing PC **date**:

Settings > Date & time > Time zone > (Find Singapore):



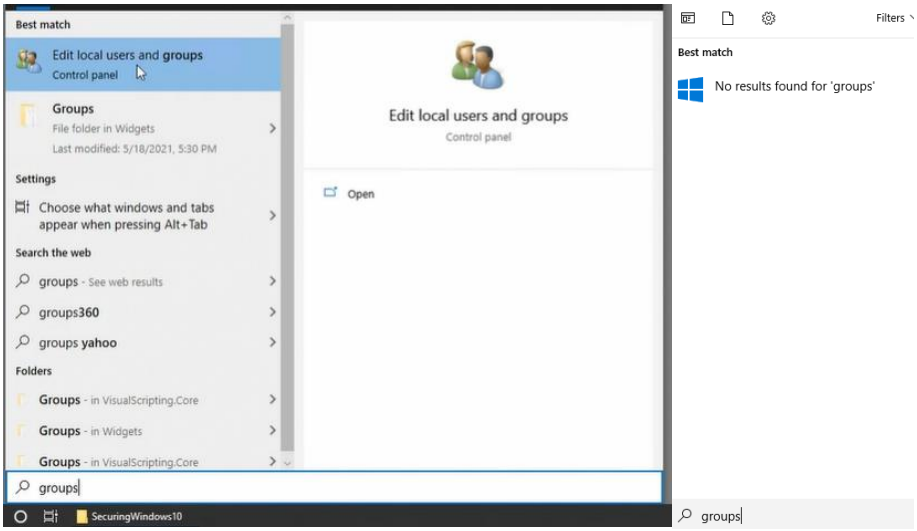
1.3) Changing PC **name**:

Settings > About > Rename this PC > 'ISSE-P17-2202934B'



2. **Edit User and Group**, after going through LinkedIn Learning Course: Windows 10: Security > 2. Authorization > Working with built-in groups.

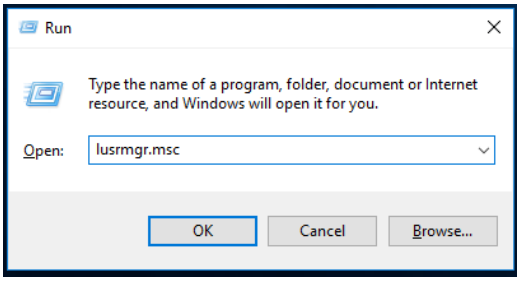
2.1) Problem: My VM's Search is unable to access 'Edit local users and groups'.



(left is LinkedIn, Right is my VM)

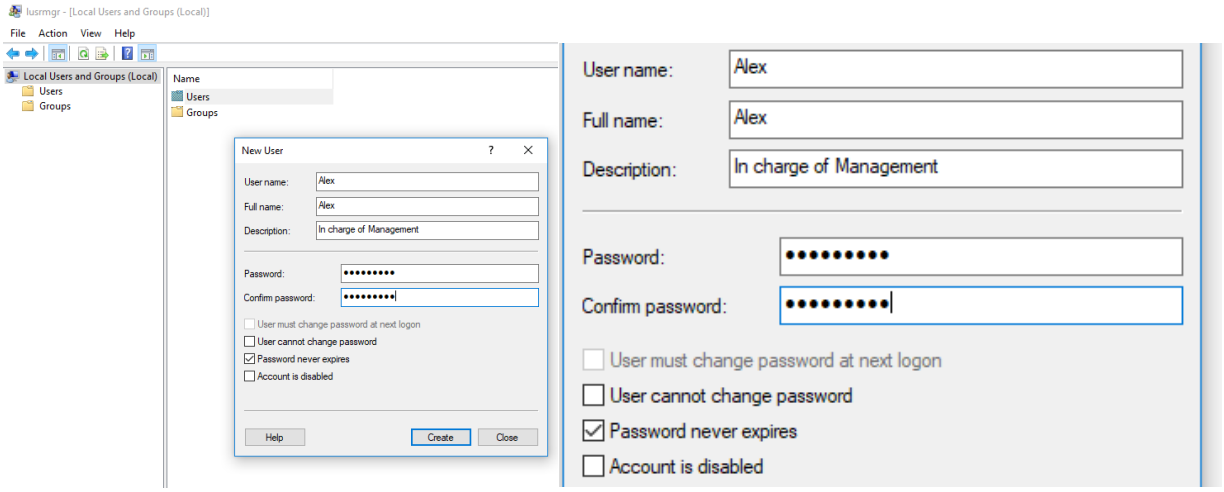
Solution: https://www.thewindowsclub.com/open-local-users-and-groups-on-windows-10

Open Run (Windows Key + R) > 'lusrmgr.msc'



2.2) **Creating the specified Users**

Users > (Right Click) > New User… >



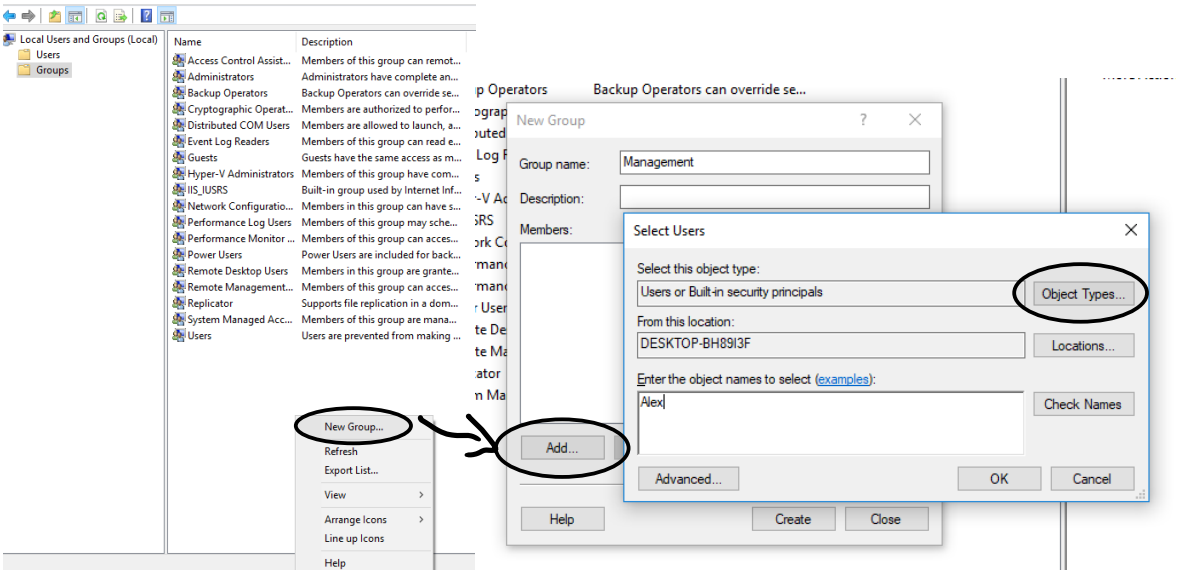
This process is repeated for the remaining Users to be created, with the same configuration: 'Password never expires' – *as we do not want to force them to change a password when the assigned password is already a strong secret.* Each User will get a distinctive password.

'student' was created as the default account for the VM; no changes were made for this User.

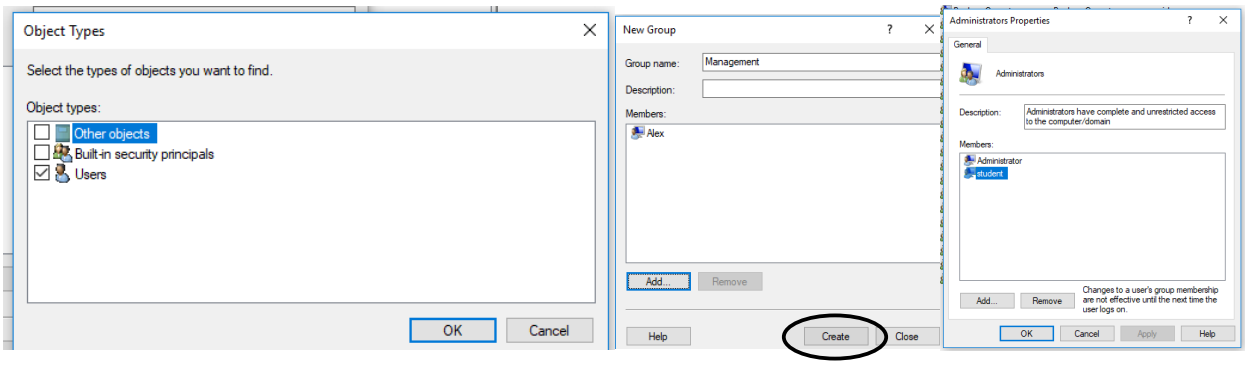
2.3) **Creating the Groups** as required:

Groups > (Right Click) > New Group…

Similarly,



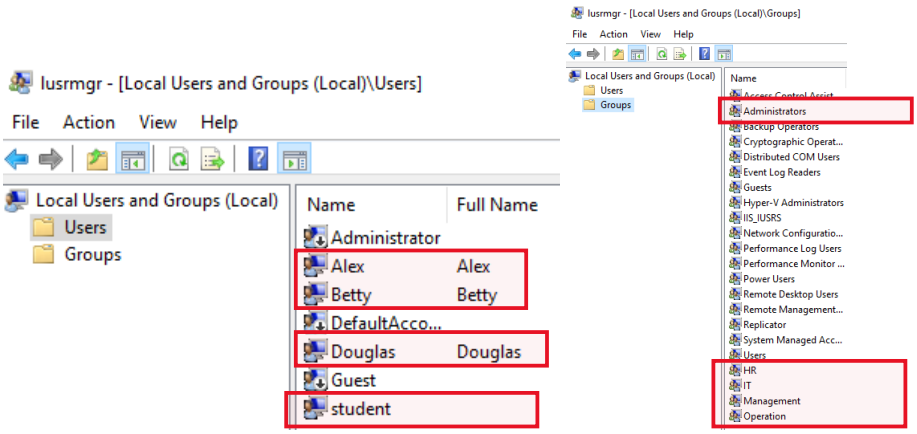
Also changed the object type to ONLY Users:



Lastly, click on create. This process is replicated for the subsequent Groups.

By default, student is already in ‘Administrators’ Group. (Last pic on right)

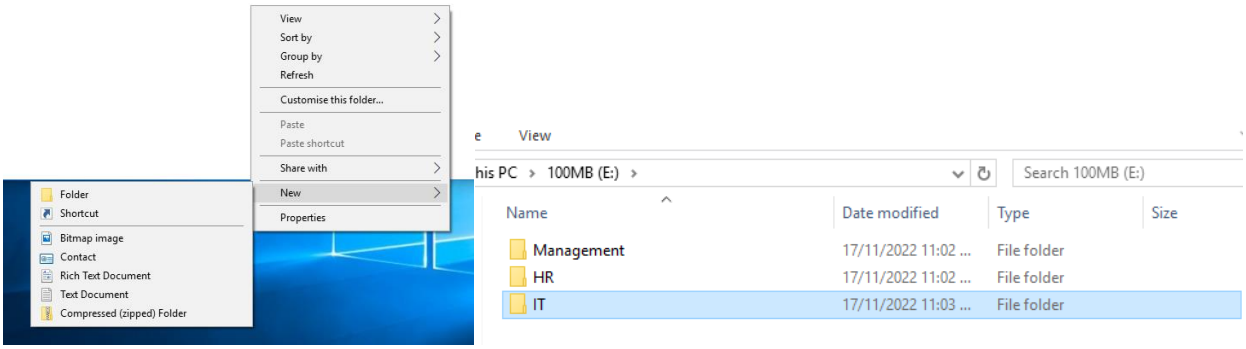
Overview of Users and Groups:



2.4) **Making Folder for each department**:

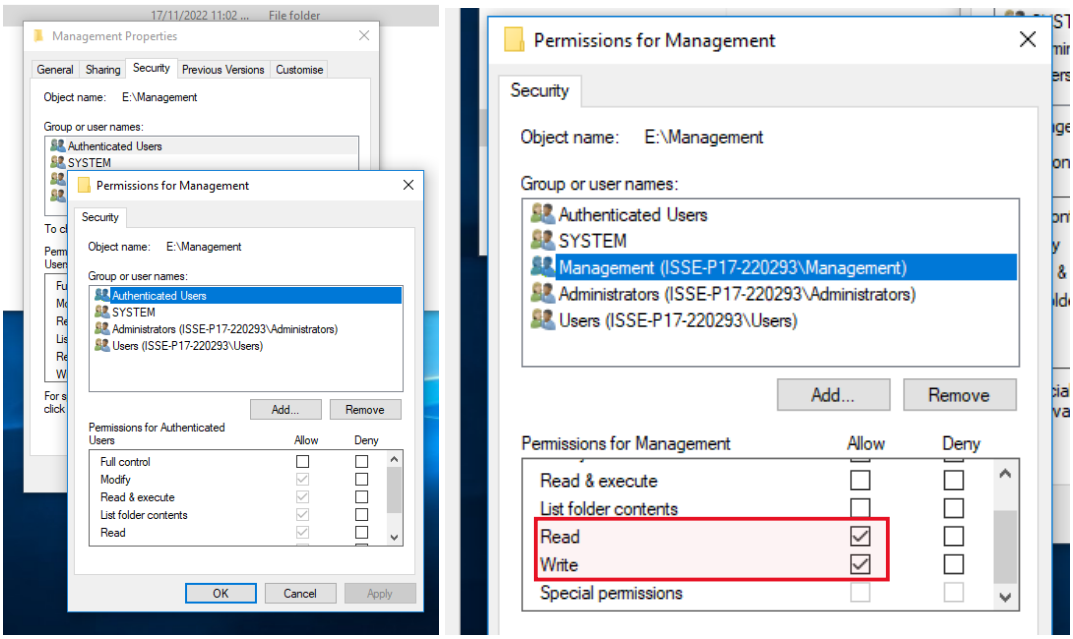
This PC > E:Drive > (Right Click) > New > Folder x3

Rename Files accordingly:

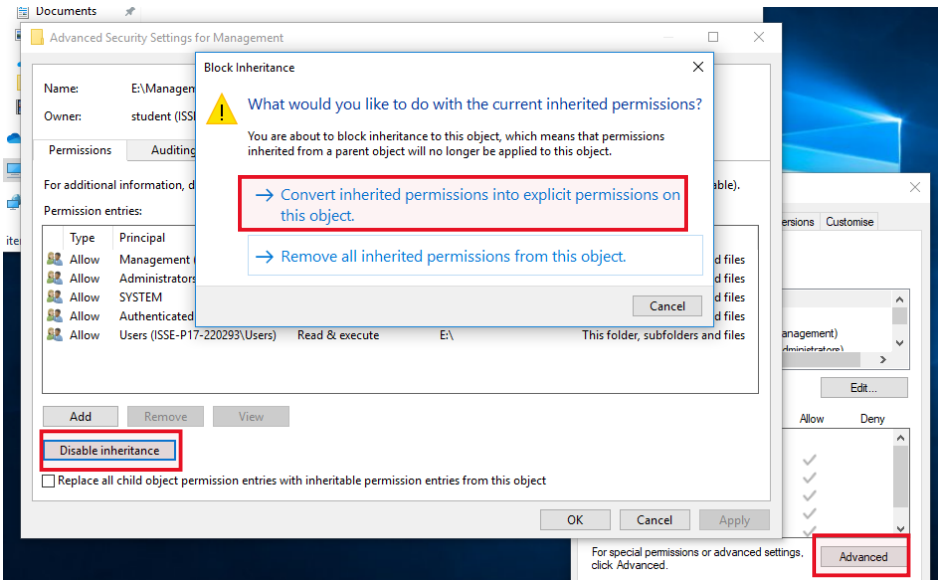


(Right Click on selected file) > Properties > Security > Edit

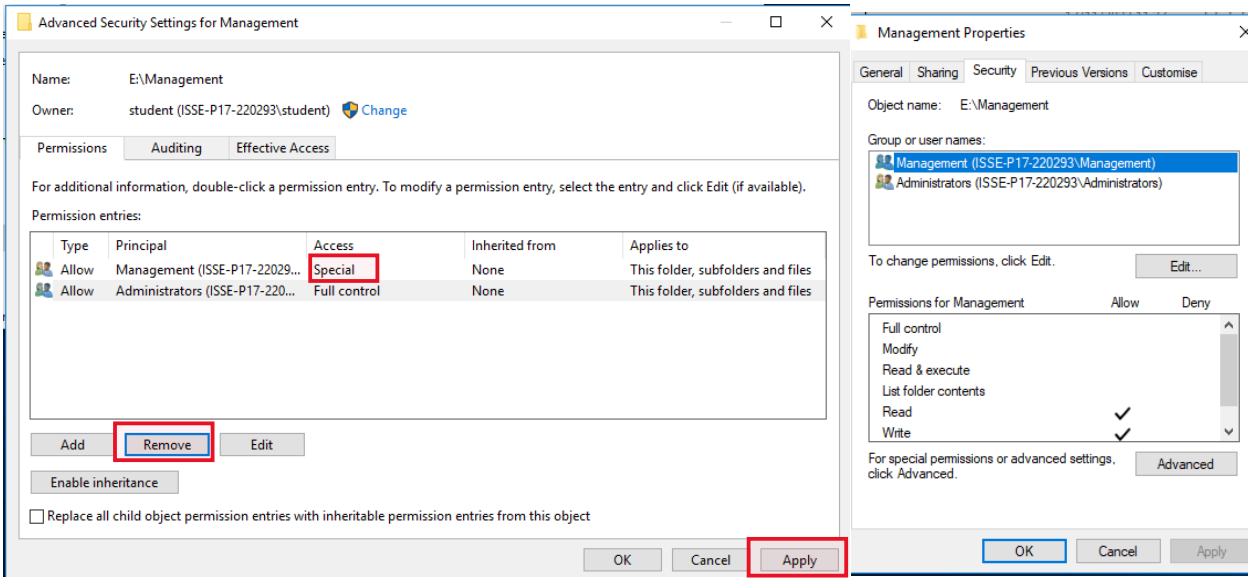
Add groups specified by requirements, **edit permissions**,



Disable Inheritance:

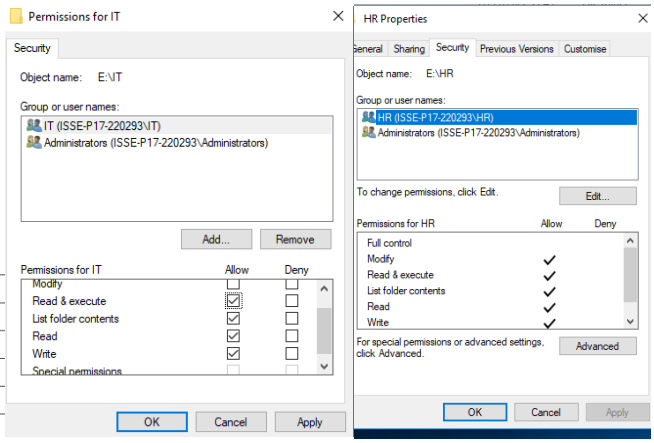


Remove all Groups not specified in requirements and Apply:

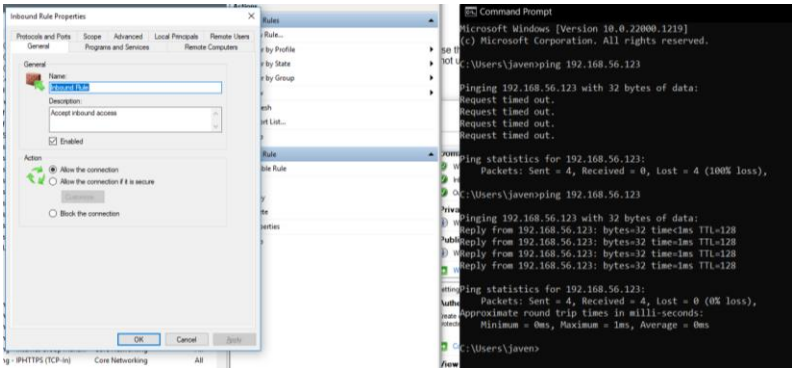


Result: (Right Photo). Repeat this process for subsequent 2 folders, only changing the permissions specified in requirements:

Folder	Group Owner	Permission
Management	Management	Read, Write (Special)
	Administrators	*Full control*
HR	HR	Modify
	Administrators	*Full control*
IT	IT	Read, Write, Execute
	Administrators	*Full control*

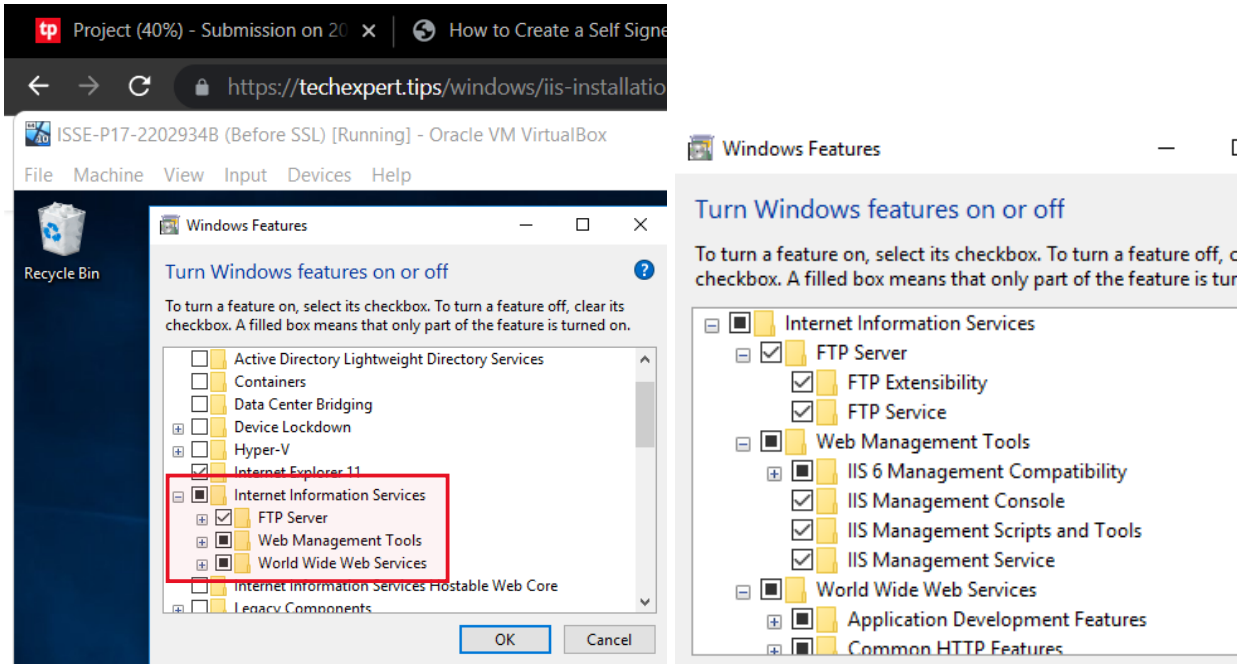


To Allow for Host Laptop to interact with my VM, an Inbound Rule using ICMPv4 Protocol was created. To test if VM accepts inbound requests, my laptop ping to VM.



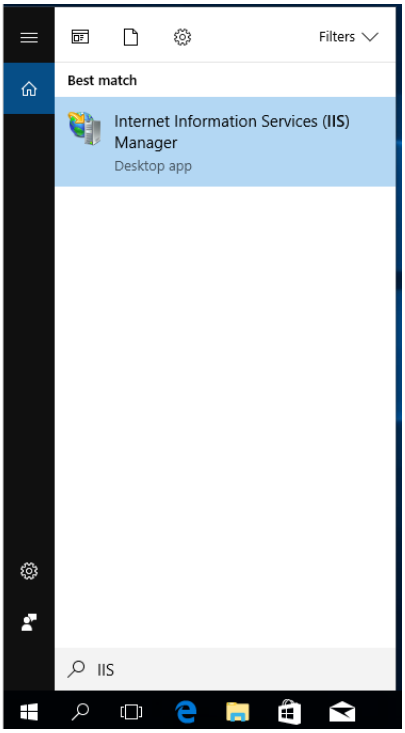
IIS FTP with SSL Certification

1) Enable IIS and FTP Feature



All Subfolders within Features are turn on.

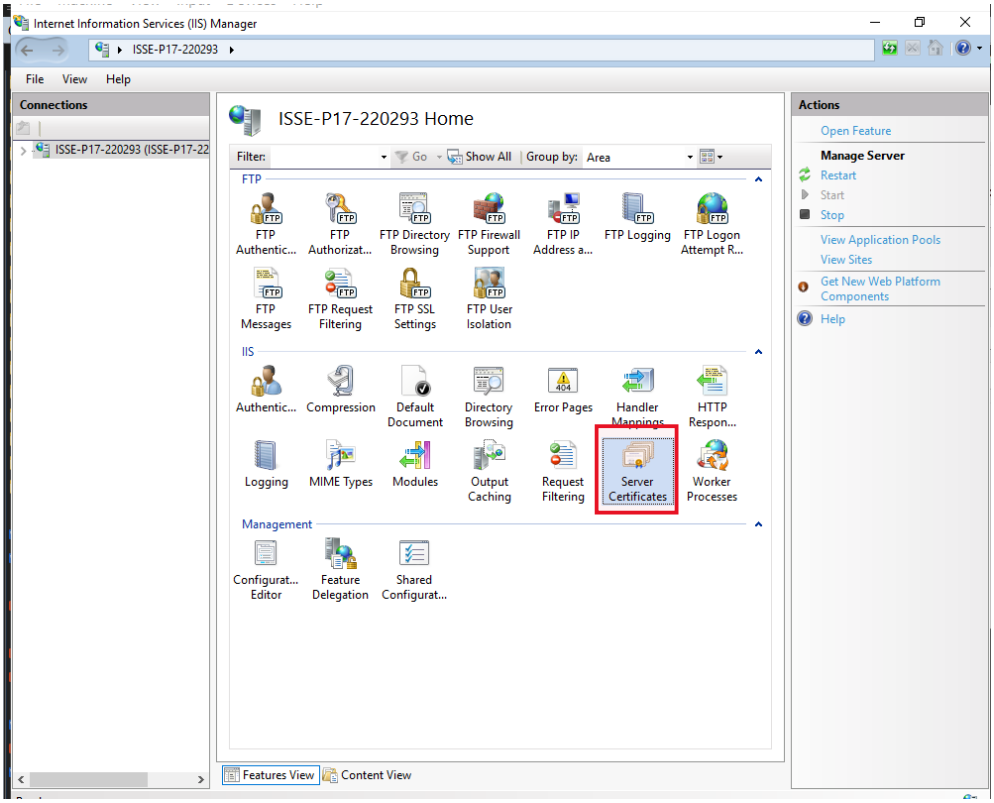
2) Once IIS activated, use taskbar and search for 'IIS'.

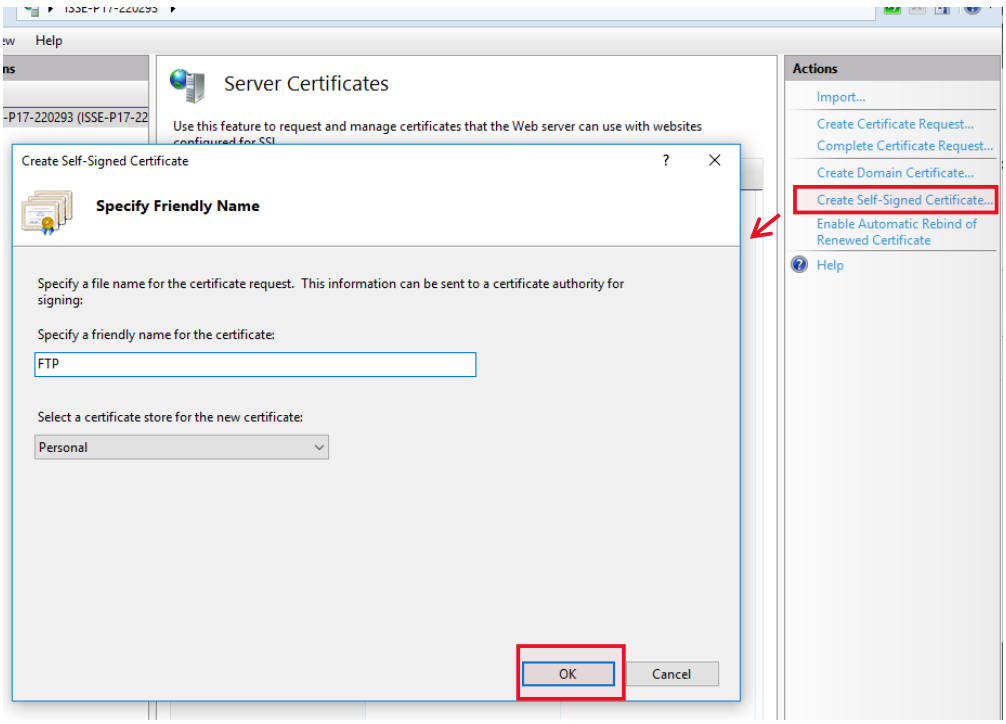


If 1st step isn't done accordingly, there will be no results for 'IIS' in taskbar.

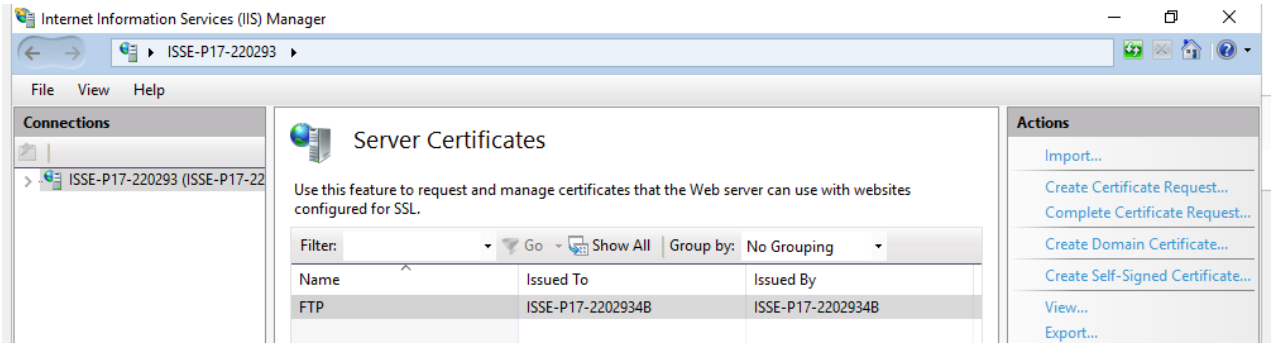
3) Create SSL Certificate

Follow red squares to know where to click





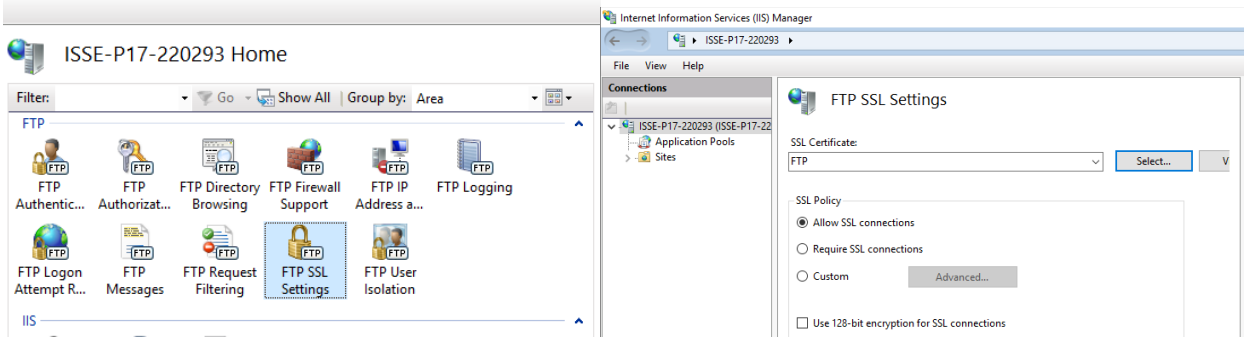
4) SSL Certificate created:



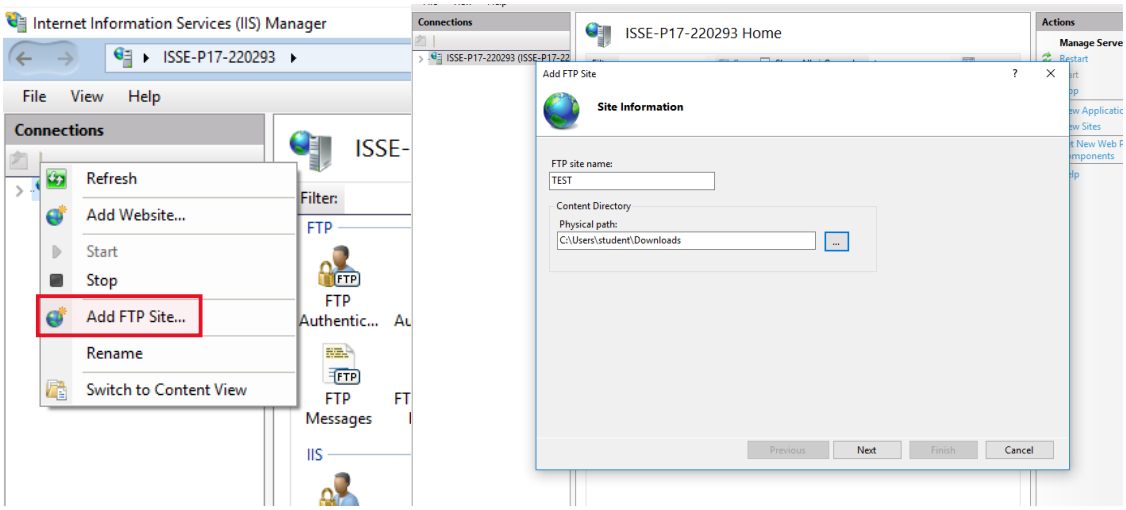
Full details - Expand VM to full screen:

Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
FTP	ISSE-P17-2202934B	ISSE-P17-2202934B	15/12/2023 8:00:00 AM	7D7169726443E273A9C0FFA46...	Personal

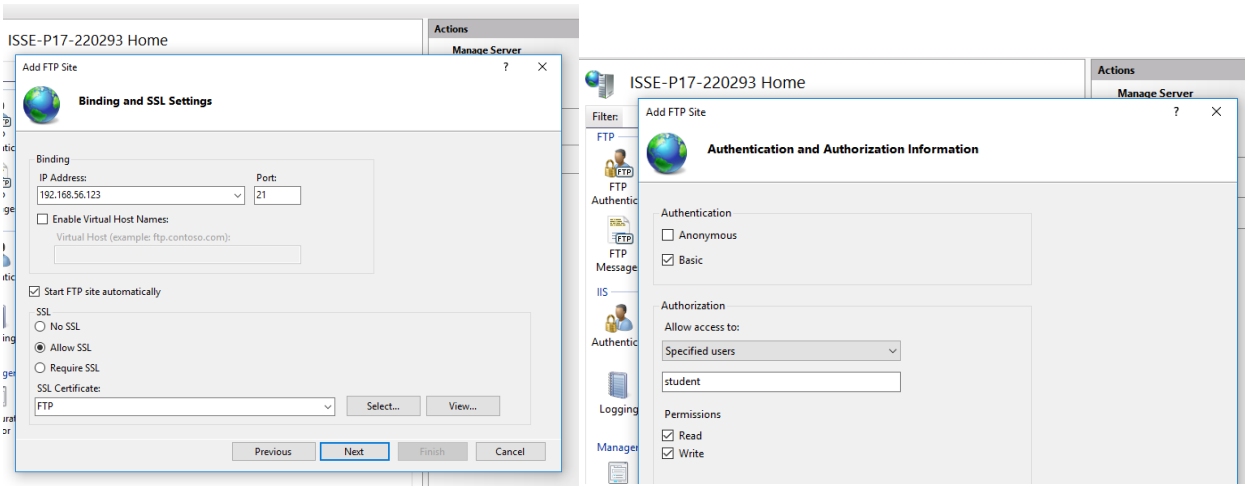
5) Using the Certificate created:



6) Add FTP Site

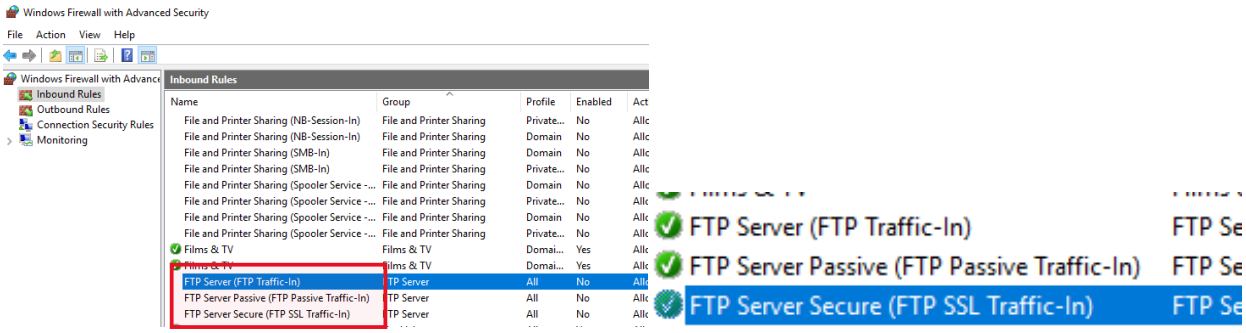


Physical path is where the Files Transferred through FTP will end up at.



'FTP' Certificate is used for this FTP site. FTP can only be accessed using student.

7) Enable Firewall



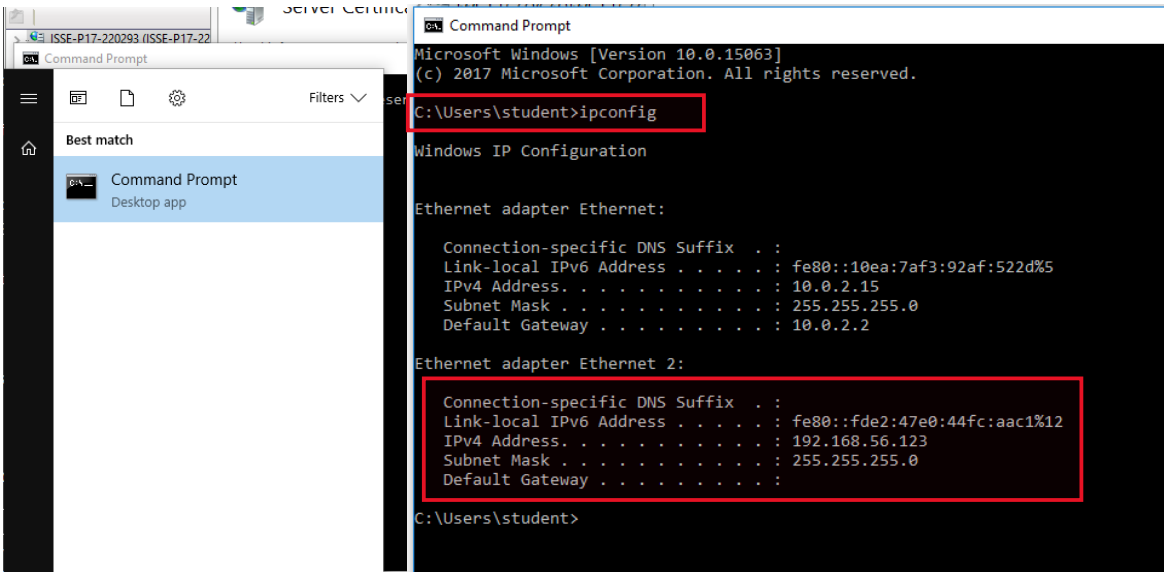
Enable all 3 Rules, to allow FTP Connection.

Getting entry point for IIS

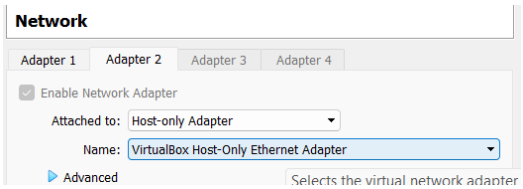
IP Address of VM must be obtained for WinSCP to FTP to VM.

To get IP Address:

1) Cmd > ipconfig



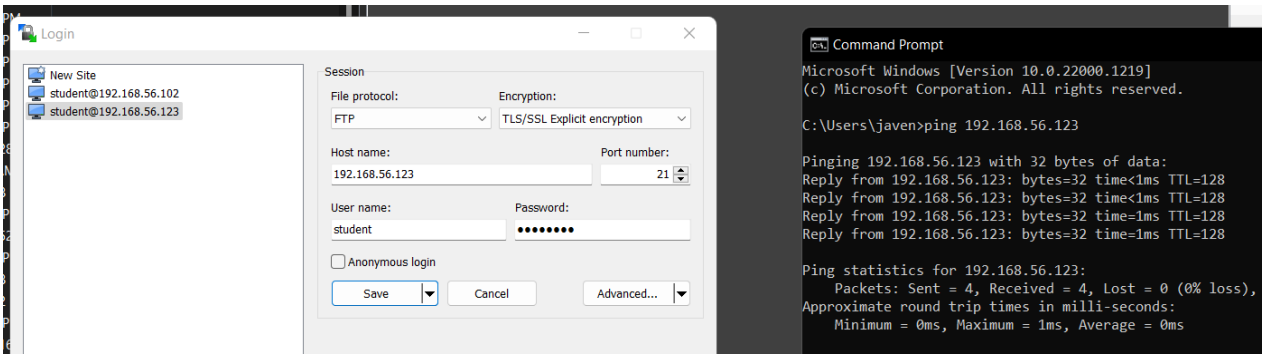
IPv4 Address is the IP Address.



Host-Only IP Address will be used as its unique to VM.

WinSCP Connection

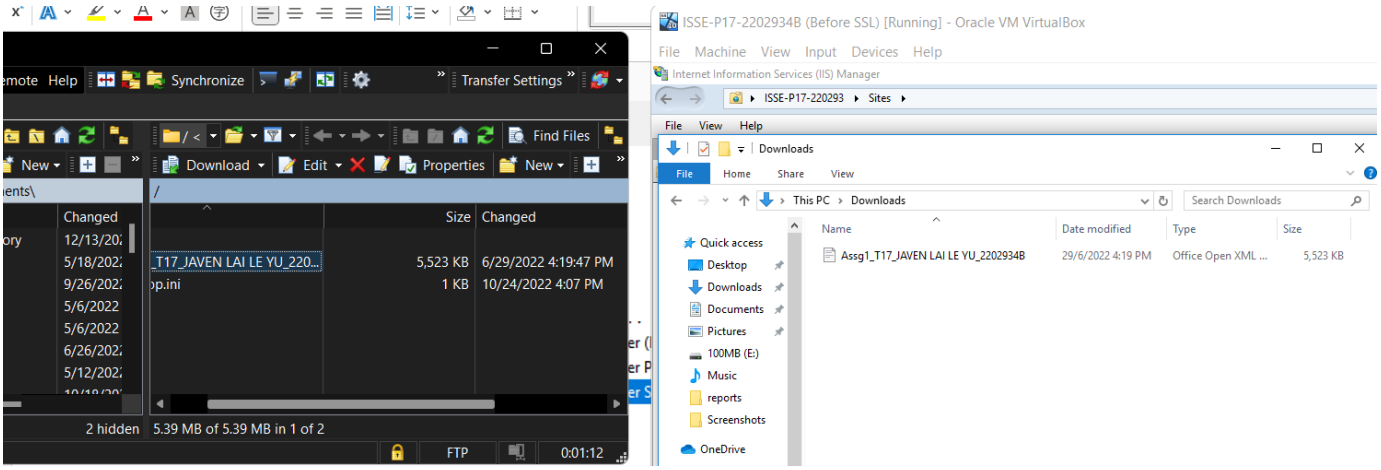
Using Host PC to test connection via ping before FTP.



Reflection of setting up FTP

Took me quite awhile to figure it out even with the references provided in the assignment specs. I also had to figure out that the Firewall Rules must be enabled for the connection to be successful.

Testing Connection: **Successful**

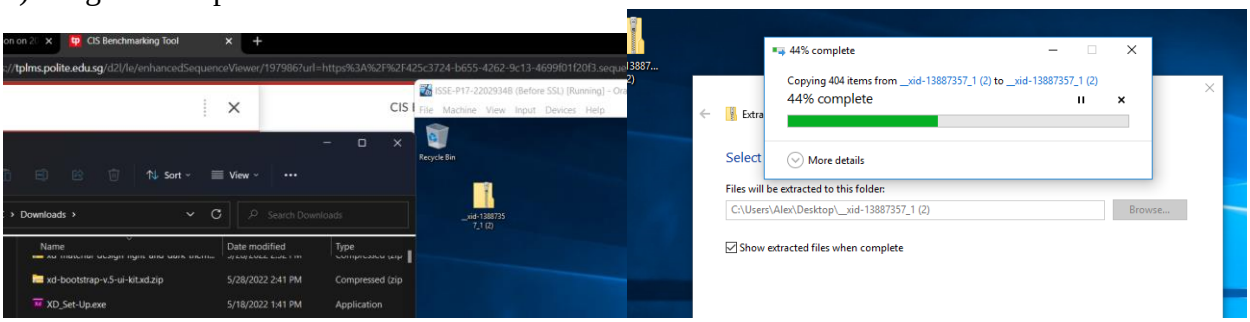


I was able to drag and drop a file from my Host PC to VM. Hence, FTP connection is successful.

CIS Benchmark Test

1) Enabled Drag and Drop (Devices > Drag and Drop > Bidirectional)

2) Drag and Drop CIS Benchmark ZIP file to VM.



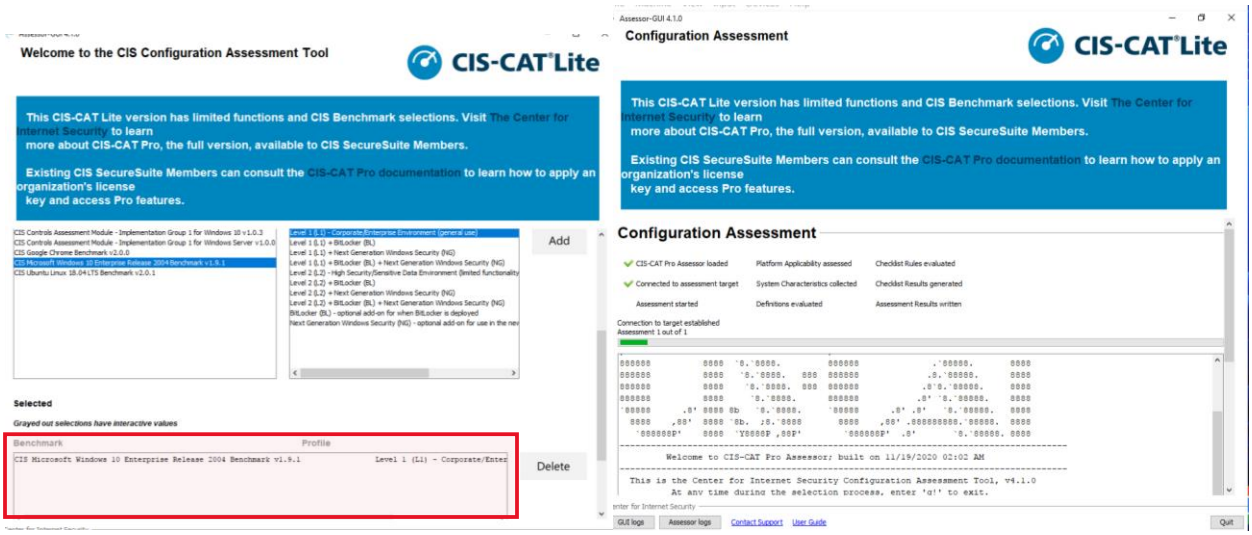
3) Extract All from Zip file before running Accessor CLI Gui (Need to Extract before using)

4) Snapshots of Scan Configurations:

Selected

Grayed out selections have interactive values

Benchmark	Profile
CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.1	Level 1 (L1) - Corporate/Ente



Benchmark **before Remediation**

Summary

Description	Tests					Scoring		
	Pass	Fail	Error	Unkn.	Man.	Score	Max	Percent
1 Account Policies	3	5	0	2	0	3.0	10.0	30%
1.1 Password Policy	1	4	0	2	0	1.0	7.0	14%
1.2 Account Lockout Policy	2	1	0	0	0	2.0	3.0	67%
2 Local Policies	59	38	0	1	1	59.0	98.0	60%
5 System Services	9	12	0	0	0	9.0	21.0	43%
6 Registry	0	0	0	0	0	0.0	0.0	0%
7 File System	0	0	0	0	0	0.0	0.0	0%
8 Wired Network (IEEE 802.3) Policies	0	0	0	0	0	0.0	0.0	0%
9 Windows Firewall with Advanced Security	0	26	0	0	0	0.0	26.0	0%
17 Advanced Audit Policy Configuration	8	19	0	0	0	8.0	27.0	30%
18 Administrative Templates (Computer)	4	138	0	0	0	4.0	142.0	3%
19 Administrative Templates (User)	0	10	0	0	0	0.0	10.0	0%

Upon analysis, I **shortlisted the following Policies** I deem as important **to be improved**:

Account Policies:

1.0	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	Fail
1.0	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	Fail
1.0	1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	Fail

Local Policies:

1.0	2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	Fail
1.0	2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'	Fail
1.0	2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	Fail
1.0	2.3.7.5 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	Fail
1.0	2.3.7.6 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	Fail

System Services:

1.0	5.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'	Fail
1.0	5.41 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'	Fail
1.0	5.42 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled'	Fail
1.0	5.43 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled'	Fail
1.0	5.44 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled'	Fail

Was careful with which policies I chose as some policies could affect my VM's functionality

Windows Firewall with Advanced Security:

1.0	9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	Fail
1.0	9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	Fail
1.0	9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	Fail

+ all other Domains

Advanced Audit Policy Configurations:

17.5 Logon/Logoff		
1.0	17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'	Fail
1.0	17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'	Fail
1.0	17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success'	Pass
1.0	17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'	Fail
1.0	17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	Fail

Administrative Template (Computer):

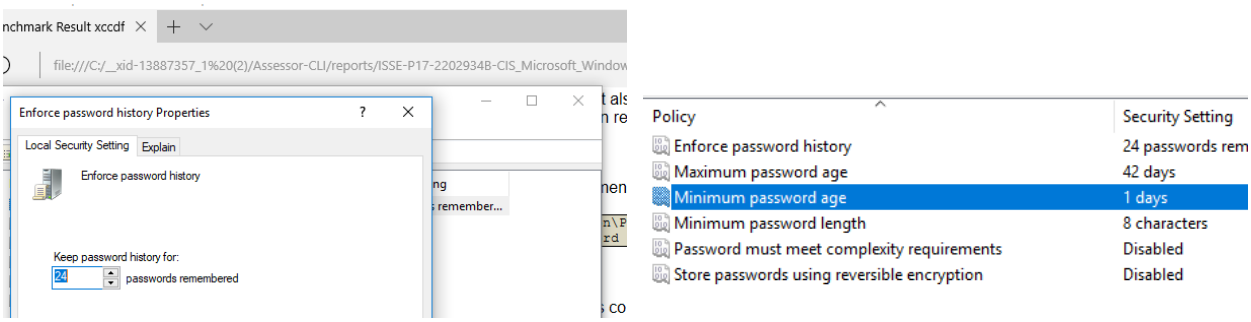
18.9.6 App runtime		
1.0	18.9.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	Fail
18.9.10.1 Facial Features		
1.0	18.9.10.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	Fail
1.0	18.9.102.2 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	Fail
1.0	18.9.102.3 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	Fail
1.0	18.9.102.4 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	Fail

Administrative Template (User):

1.0	19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled'	Fail
1.0	19.1.3.2 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled'	Fail
1.0	19.1.3.3 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'	Fail

Remediation of Policies as stipulated

1) Account Policies.



Enforce password history: ensure Users make NEW AND UNIQUE passwords *rather than reusing their old passwords* – to beef up security.

Minimum password age: accommodate the above feature, Users can **only change their Passwords once every day** – the long waiting time will convince them to just create a new password rather than removing the 24 passwords memory just to reuse their old password which would take 24 days.

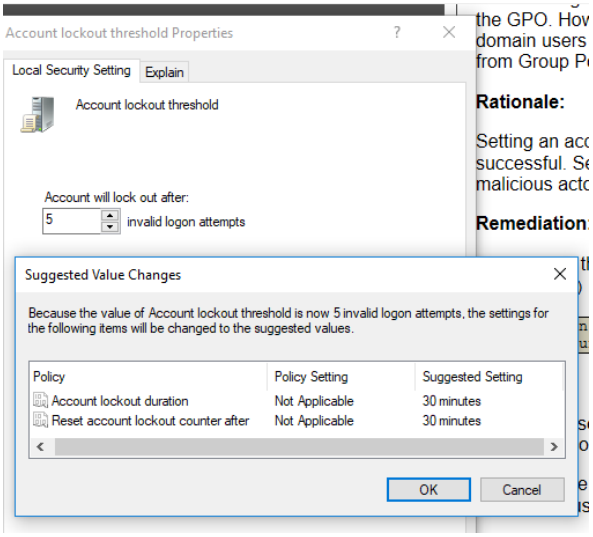
Minimum Password length should be 8 characters to avoid weak passwords:

- (Does not change Benchmark results, just for good practice)

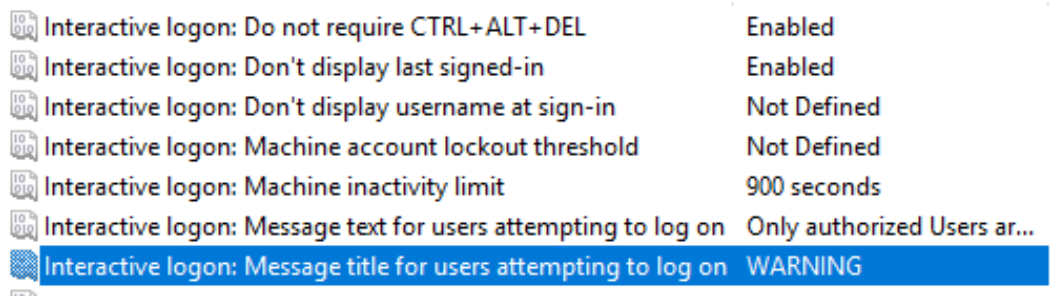
No requirement for complex password which requires special char – don't force User as they might struggle to memorize their password making it counter-intuitive.

Account lockout threshold:

- In hopes of mitigating Brute-Force and Dictionary Attacks, there will be a **cooldown to stop Hacker from spamming the login** system with bots.



2) Local Policies: Creating a stricter Interactive Login experience.

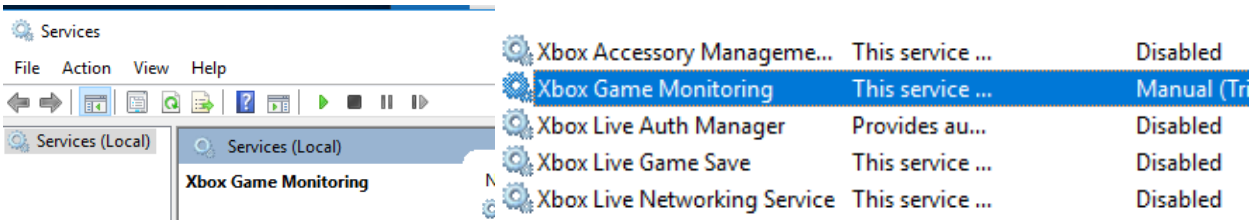


Don’t display last-signed in to prevent much information from being disclosed. Set an idle logout time to prevent an unintended User from accessing while the real User is away. Warning for hackers about legal consequences to deter unauthorized access.

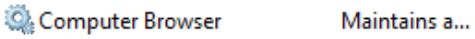
CTRL +ALT + DEL should not be enabled on VM as it will these keys will directly interfere with host Computer.

3) System Services

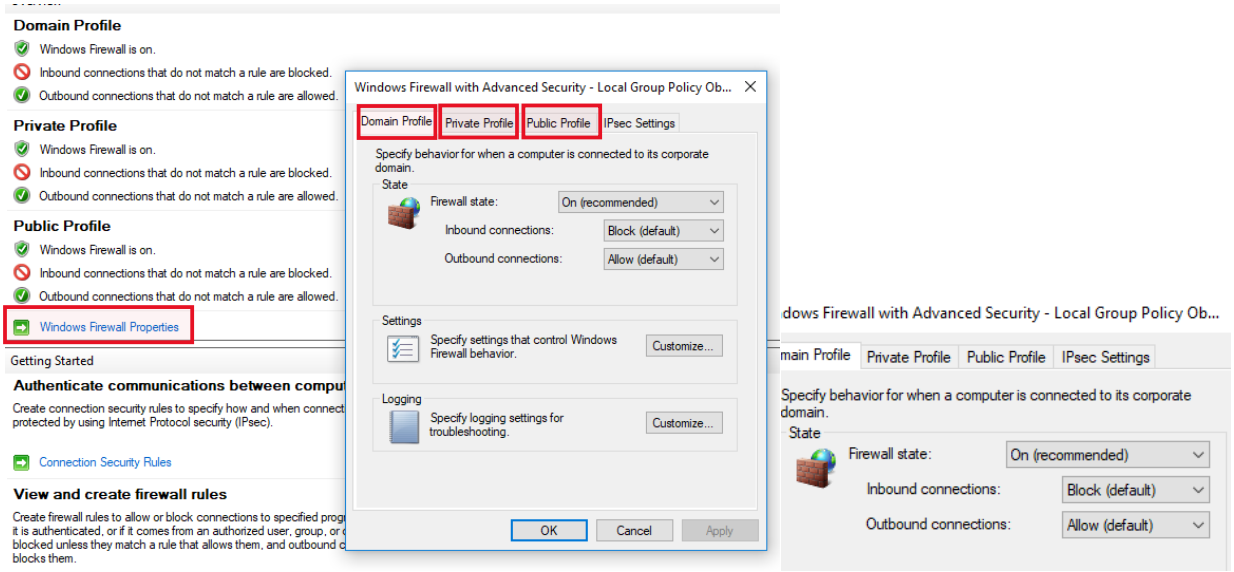
The system policies were risky as some could interfere with crucial services such as IIS FTP. Therefore, I disabled all XBOX policies as it will not affect VM’s functionality.



Disable Computer Browser as it’s a legacy feature which slows the VM down by producing unnecessary traffic.

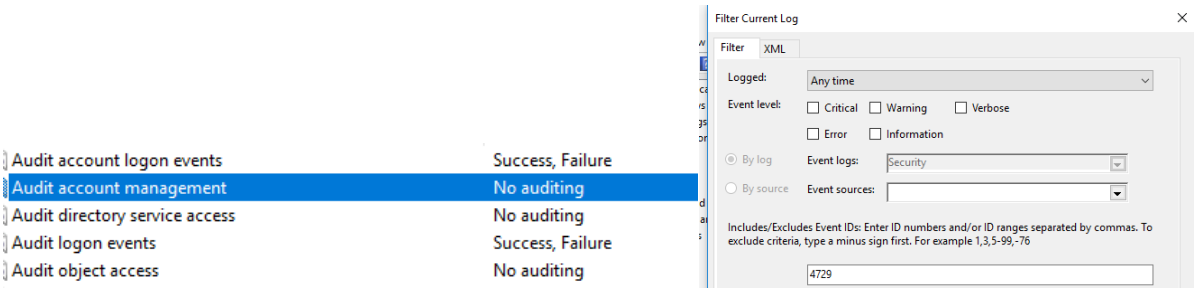


4) Firewall



Turn on Firewall for all profile to enhance security by preventing unwanted, unintended connections and access, to and from this VM.

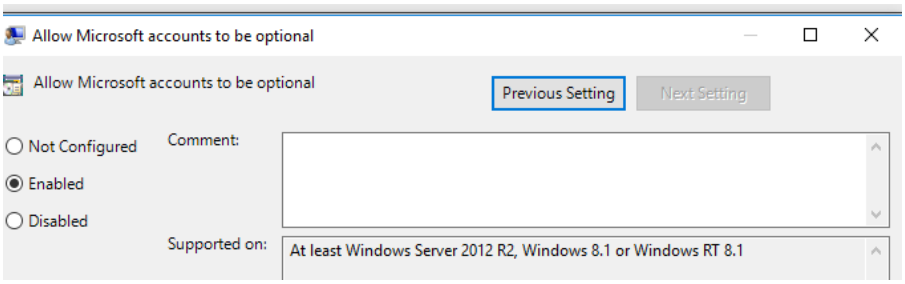
5) Audit policies



Audit: Record events for tracking, to find if there are any suspicious activities.

6) Administrative Template for Computer

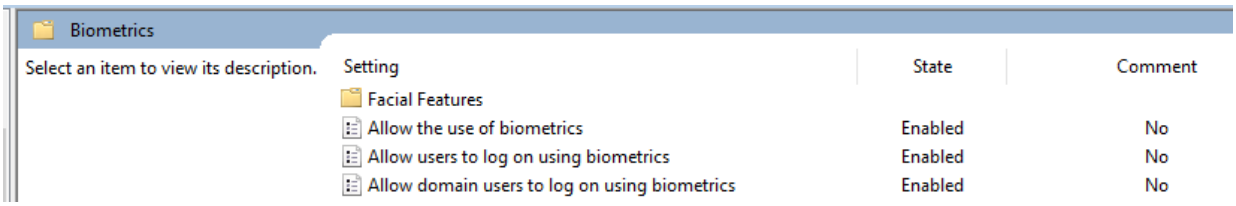
Allow Microsoft Accounts to be optional:



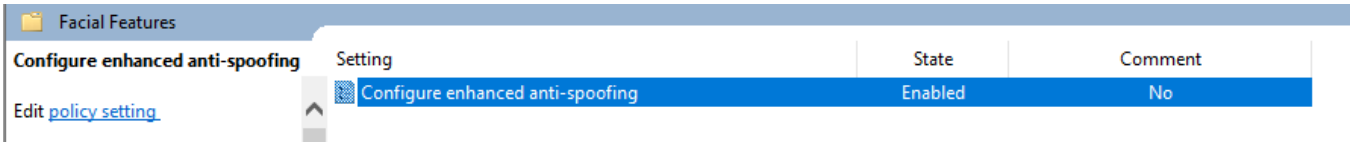
Allow more flexibility; Not forced to a Microsoft Account only.

Biometric (Face Recognition) is enabled if the computer has it.

Instead of going through the hassle of typing the password every time, which could cause the password to be eavesdropped and seen by others, Biometric is much more convenient and safer.

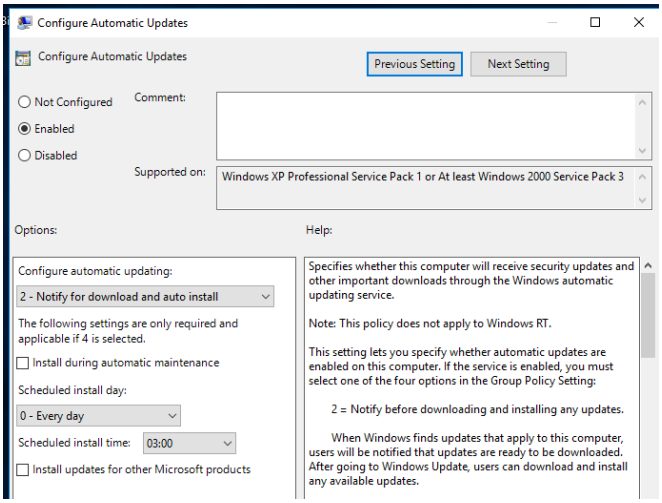


Facial Features > **Configure enhanced anti-spoofing**:



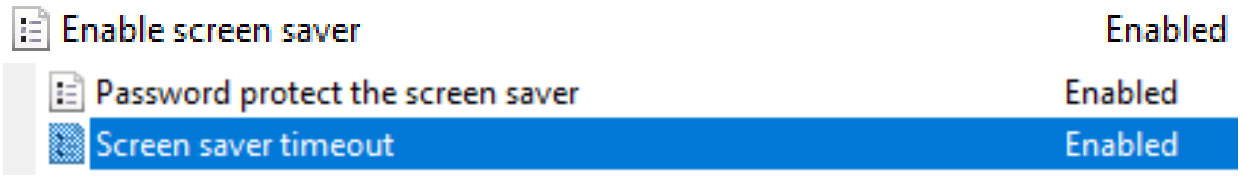
To beef up security of biometrics, enhance the facial recognition system if the computer can.

Enable Automatic Updates:



Check for new updates regularly to ensure system is the newest and most secured version.

7) Administrative Template for User



Turns off computer screen after 900 Seconds of inactivity. To protect computer screen from damage and prevent unwanted User from accessing the computer when the real User is away.

All New Passes:

1.0	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	Pass
1.0	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	Pass
1.0	1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	Pass
1.0	17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'	Pass
1.0	17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'	Pass
1.0	17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'	Pass
1.0	17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	Pass
1.0	18.9.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	Pass
1.0	18.9.10.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	Pass
1.0	18.9.102.2 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	Pass
1.0	18.9.102.3 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	Pass
1.0	18.9.102.4 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	Pass
1.0	2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'	Pass
1.0	2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	Pass
1.0	2.3.7.5 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	Pass
1.0	2.3.7.6 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	Pass
1.0	19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled'	Pass
1.0	19.1.3.2 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled'	Pass
1.0	19.1.3.3 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'	Pass
1.0	9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	Pass
1.0	9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	Pass
1.0	9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	Pass
1.0	9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	Pass
1.0	9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	Pass
1.0	9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	Pass
1.0	9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	Pass
1.0	9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	Pass
1.0	9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	Pass
5 System Services		
1.0	5.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'	Pass
1.0	5.41 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'	Pass
1.0	5.42 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled'	Pass
1.0	5.43 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled'	Pass
1.0	5.44 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled'	Pass

Benchmark **after remediations**

1 Account Policies	6	2	0	2	0	6.0	10.0	60%
1.1 Password Policy	3	2	0	2	0	3.0	7.0	43%
1.2 Account Lockout Policy	3	0	0	0	0	3.0	3.0	100%
2 Local Policies	62	35	0	1	1	62.0	98.0	63%
5 System Services	10	11	0	0	0	10.0	21.0	48%
6 Registry	0	0	0	0	0	0.0	0.0	0%
7 File System	0	0	0	0	0	0.0	0.0	0%
8 Wired Network (IEEE 802.3) Policies	0	0	0	0	0	0.0	0.0	0%
9 Windows Firewall with Advanced Security	9	17	0	0	0	9.0	26.0	35%
9.1 Domain Profile	3	5	0	0	0	3.0	8.0	38%
9.2 Private Profile	3	5	0	0	0	3.0	8.0	38%
9.3 Public Profile	3	7	0	0	0	3.0	10.0	30%
17 Advanced Audit Policy Configuration	13	14	0	0	0	13.0	27.0	48%
18 Administrative Templates (Computer)	9	133	0	0	0	9.0	142.0	6%
19 Administrative Templates (User)	3	7	0	0	0	3.0	10.0	30%

As I was completing this project, I realized that some of my previous Pass in turned to Fail after I made the amendments to fix the selected Failed Tests.

This could be due to the fact that IIS and FTP being enabled – My first Benchmark test was done before implementing IIS FTP.

Total Improvements:

3 (Account Policies) + 4 (Local Policies) + 5(System) + 4 (Audit) + 9 (Windows Firewall) + 5 (Administrative Templates Computer) + 3 (Administrative Template User) = 33 new Passes

Conclusion

Summary:

In this project, I configured a Windows OS from scratch, Setup Accounts and Groups on the Virtual Machine, restrict permissions of Groups to their respective files, configured a Virtual Machine Setup according to given specifications and edited several Local Group Policies and Rules.

I also configured the VM to interact with my Host Laptop, with Protocols like Inbound rules, Enabling/Disabled Firewall Restrictions and File Transfer Protocol with IIS.

Lastly, I ran CIS Benchmark test to discover previously unbeknownst vulnerabilities and patched them accordingly. Once policies were changed, a final test is run, and that concludes the end of this assignment.

Reflection:

ISSE was an eye-opening and insightful journey as I learnt how to configure and setup both a Windows and Linux OS from this module, along with other relevant Software and Hardware knowledge (e.g., How Traditional Servers and Modern Cloud Servers Work, Number System Conversions etc.).

BitLocker and EFS (Encrypted File Service) had intrigued me because I now know how to keep my files and documents confidential. I found the term ‘Interactive Users’ interesting as I didn’t know about the ability to remote desktop and how there is a User Group to classify Local Users (Users who are using the laptop physically) prior to ISSE. Configuring group policies were simpler than I expected too.

I always thought Firewall and Operating Systems were advanced technology that I would never understand - but ISSE really got me curious to start exploring and figuring out how things are done. I was pleasantly surprised upon understanding the concept of a Firewall and how it’s just a bunch of set Rules to allow and prevent certain actions.

After going through this project, along with my own research, I now understand how schools and parents manage to restrict or block access to certain tasks (e.g., Access Internet) on Laptops and Computers. Also, I’m now confident that I have the required knowledge and skills to protect my own devices as this module was something of a useful ‘computer literacy course’.

References

Access Local Groups and Users:

https://www.thewindowsclub.com/open-local-users-and-groups-on-windows-10

Disabling File inheritance:

https://winaero.com/enable-disable-inherited-permissions-windows-10/

Creating SSL Certification:

https://aboutssl.org/how-to-create-a-self-signed-certificate-in-iis/

Partial FTP:

https://www.freecodespot.com/blog/enable-iis-service/

General Overview:

https://www.linkedin.com/learning/windows-10-security-14135501/windows-10-security-overview?autoplay=true&u=76881922