**Cybersecurity Fundamentals (CCF1C03)**

**Project Report Submission**

**Practical Class:** P05

**Submitted by**: 2403878H Rosemol Saju Mulakkal

**Date:** 26/07/2024

* **I am the originator of this work and I have appropriately acknowledged all other original sources used as my reference for this work.**
* **I understand that Plagiarism is the act of taking and using the whole or any part of another person’s work, including work generated by AI, and presenting it as my own.**
* **I understand that Plagiarism is an academic offence and if I am found to have committed or abetted the offence of plagiarism in relation to this submitted work, disciplinary action will be enforced.**



# School of Informatics & IT School

**Cybersecurity Fundamentals (CYFUN)**

**[Subject Code – CCF1C03]**

**PROJECT REPORT**

**Table of Contents**

Task A. LinkedIn Profile (5%)

Task B. Complete Week 11 & 12 Windows Lab (5%)

1. Creating and using group
2. Using Bit Locker Bit Locked Drive E
3. Using EFS encrypt <your name>.txt file
4. Firewall and Network protection
5. Using Group Policy to audit actions in Windows

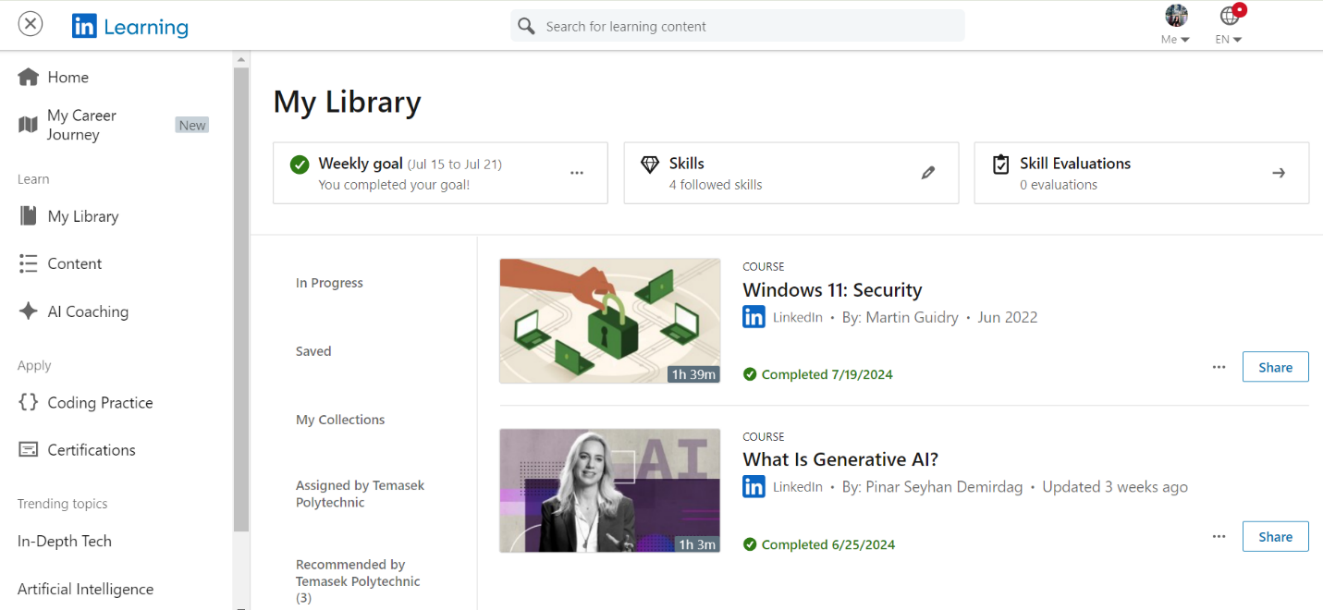
Task C. Network Services (10%)

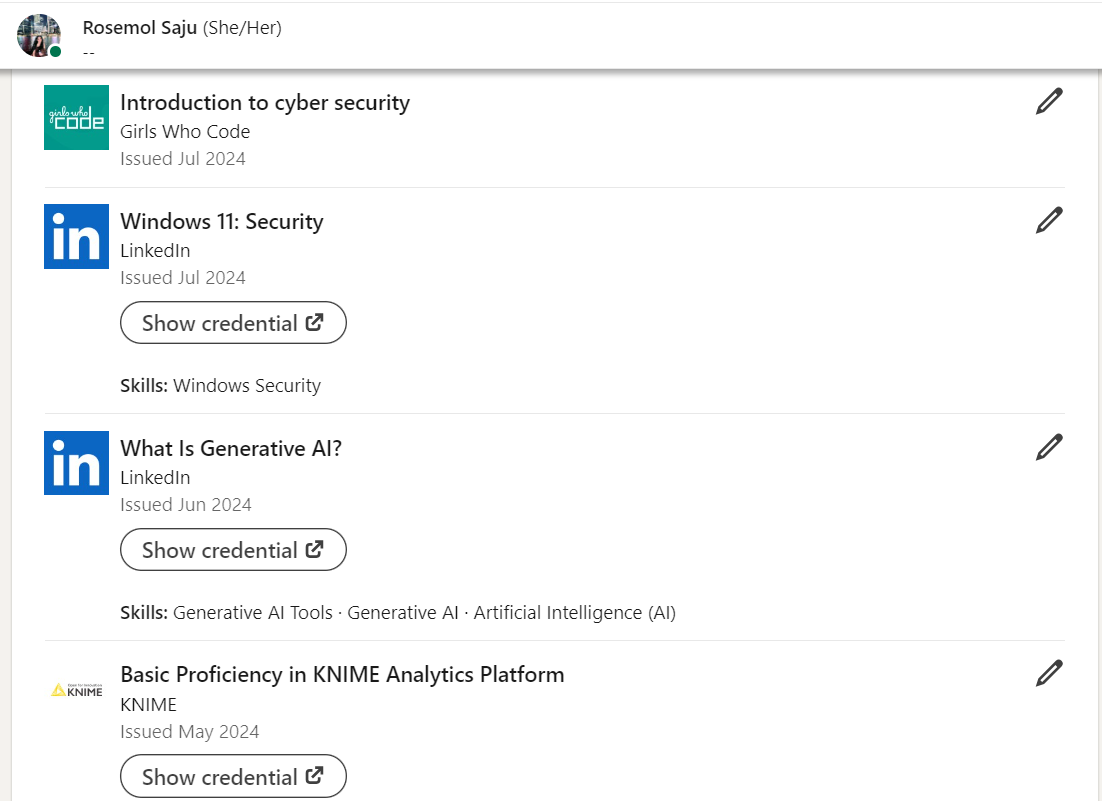
Task D. CIS Benchmark (5%)

Conclusion

Appendix and References

**Task A LinkedIn profile**



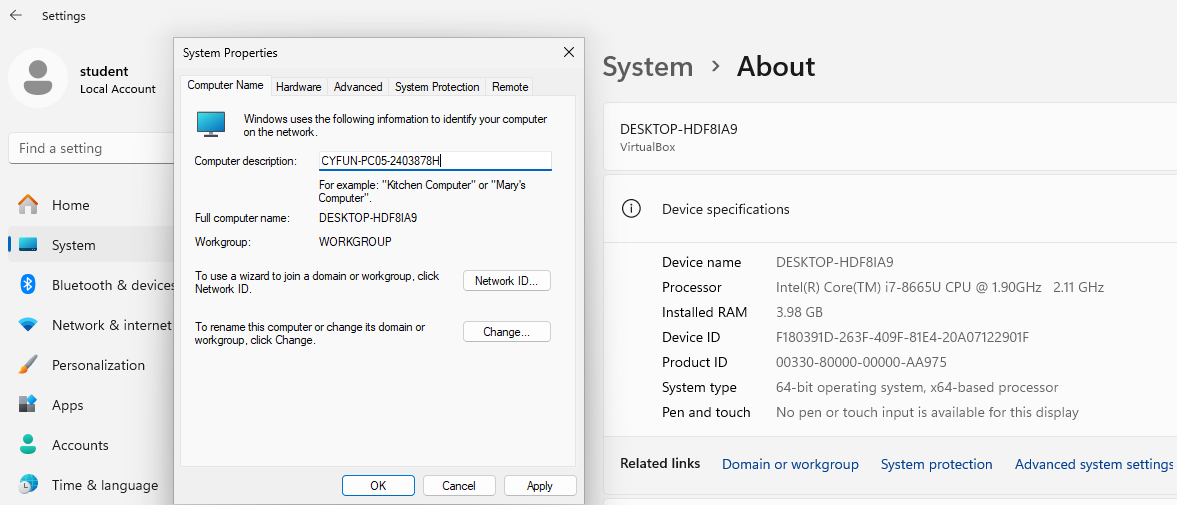




LINKEDIN PROFILE URL: [www.linkedin.com/in/rosemol-saju-67a9262ab](http://www.linkedin.com/in/rosemol-saju-67a9262ab)

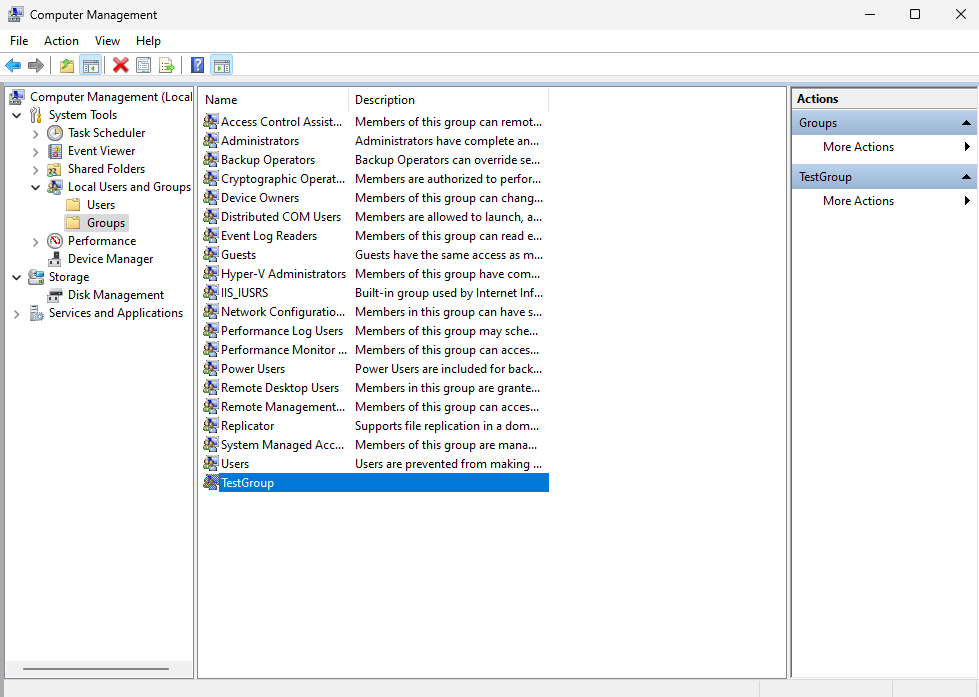
**Task B. Complete Week 11 & 12 Windows Lab (5%)**

**Set the computer name to CYFUN-PCXX\_Admin No Eg: CYFUN-PCO1-1234567A**

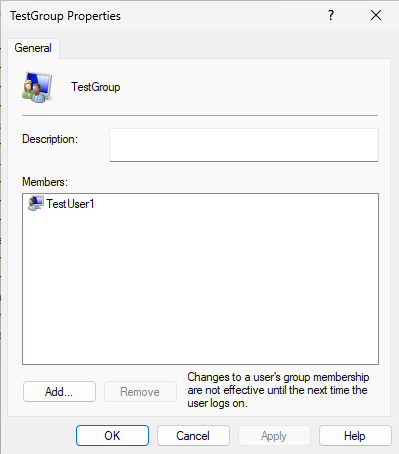
****

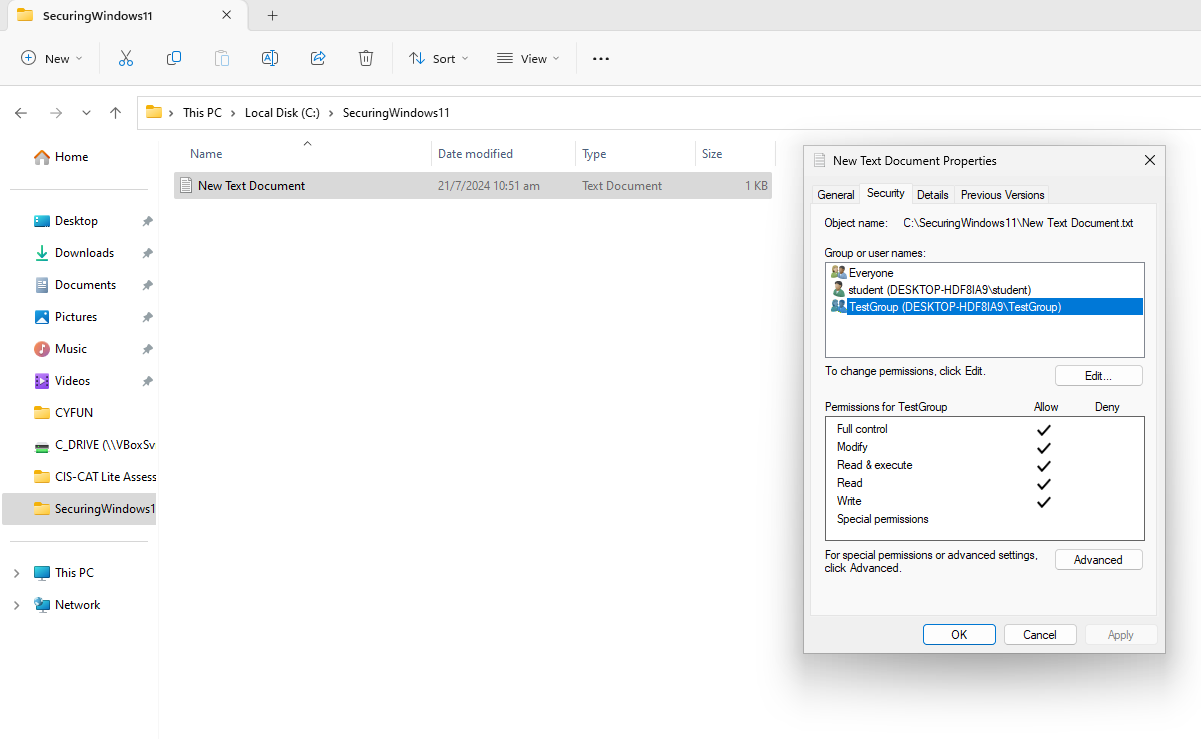
I set the computer name to CYFUN-PCO5-2403878H

**Creating and using group**



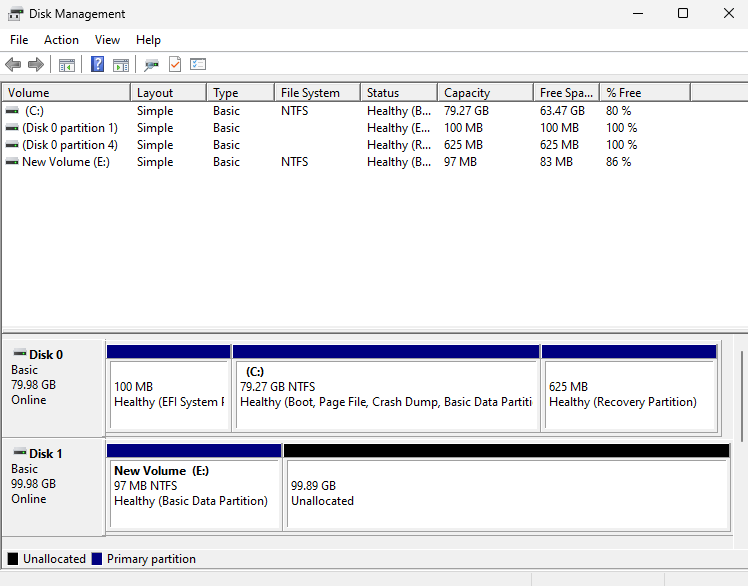
\*Created a Test group with TestUser1 as its member\*



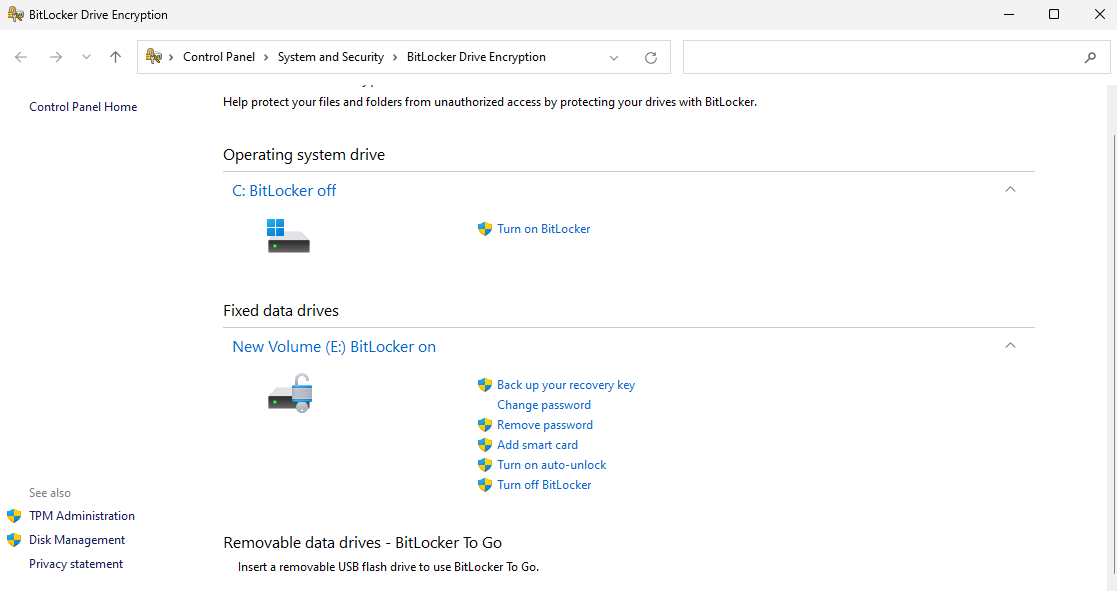
****

Assigned TestGroup the access for full control to the text document. This allows everyone in the group for full control to the document. In this instance TestUser1 will have full control for this document.

**Using Bit Locker Bit Locked Drive E**

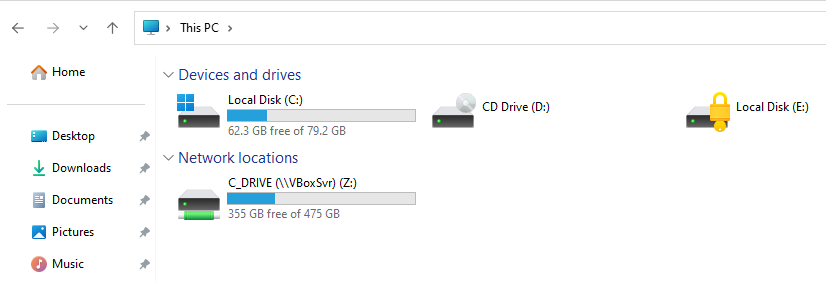
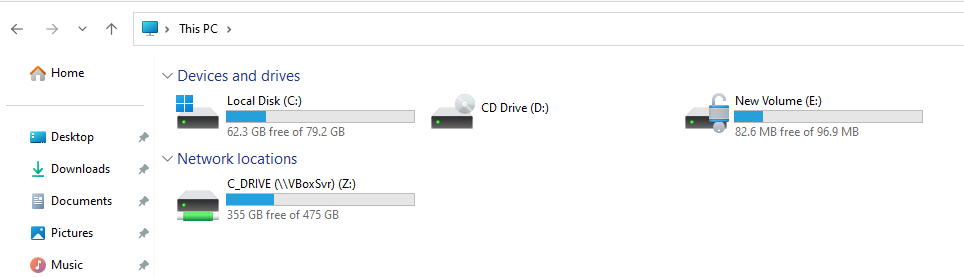


\*Created the E Drive\*



\*Turned on bitlocker for the E Drive\*

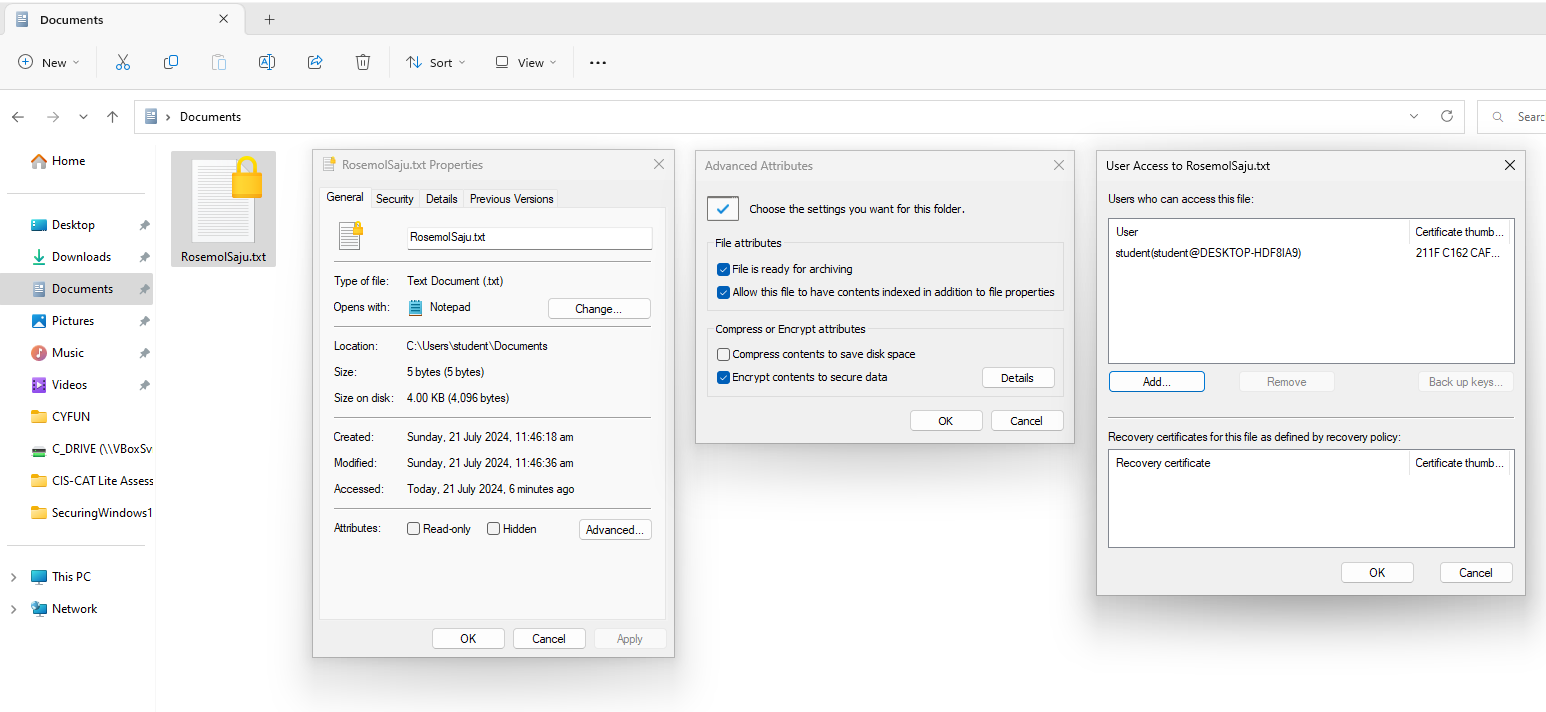
To unlock E Drive, need to enter password which we had set earlier.

After entering the password which we had set the E Drive is now unlocked.

Bitlocker is now working after restarting the computer by simply using command promt instead of hard restarting.

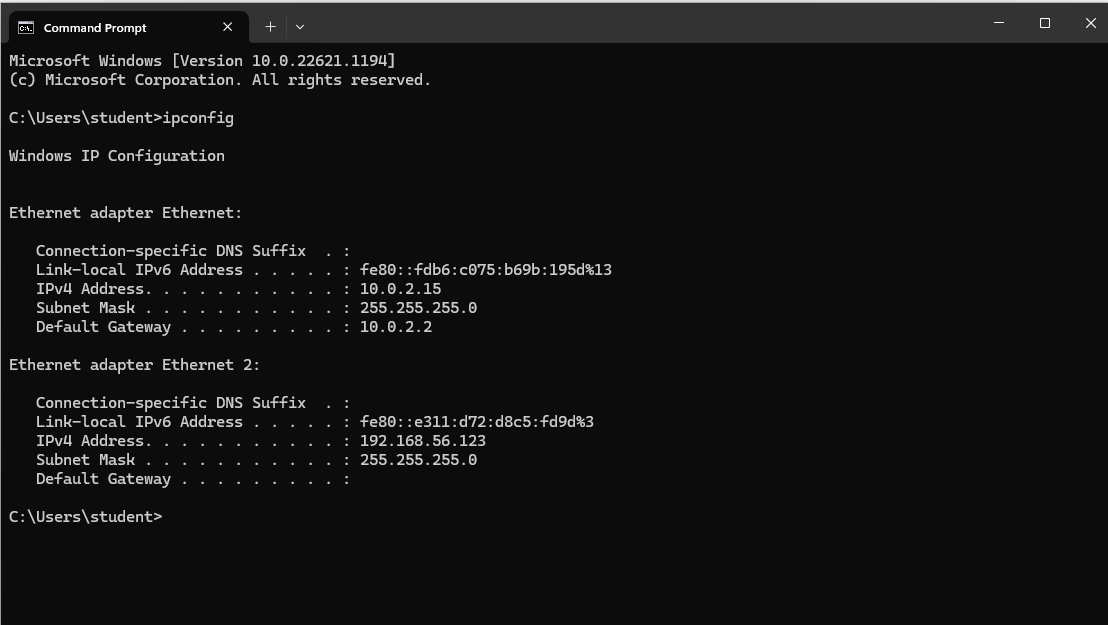
**Using EFS encrypt <your name>.txt file**



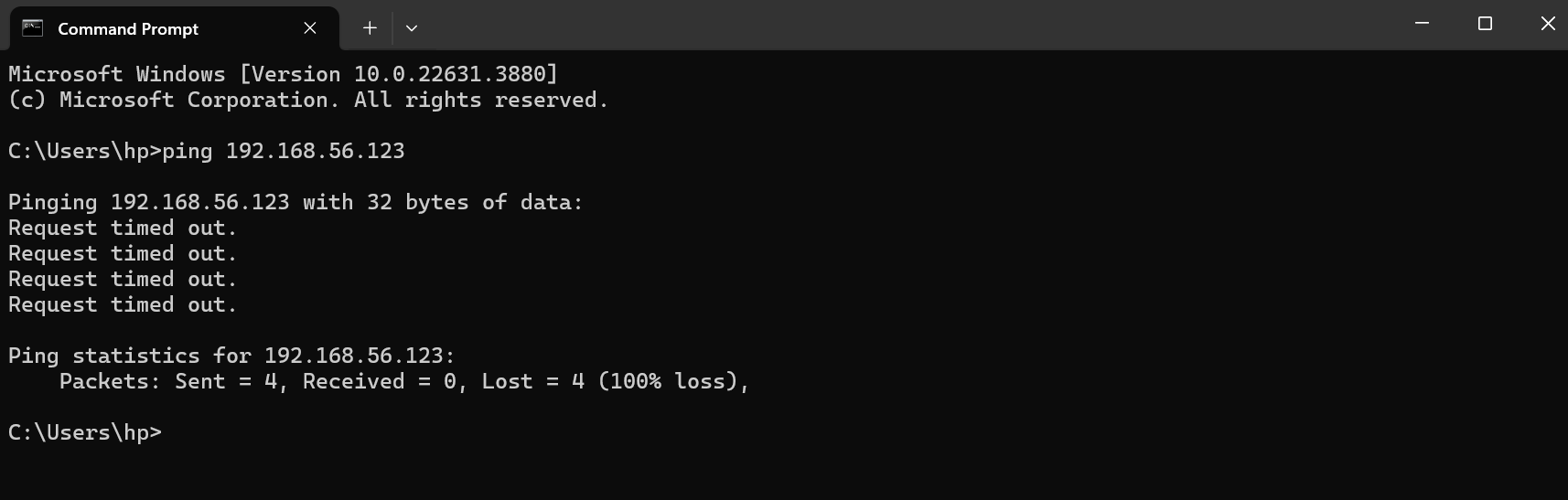
Using BitLocker encrypted **<your name>.txt file** in my case, RosemolSaju.txt is the file name.

This shows the users that are allowed to access the RosemolSaju.txt file. In this case, the user, student, is allowed to view the file.

**Firewall and Network protection / successful ping from laptop to VM**

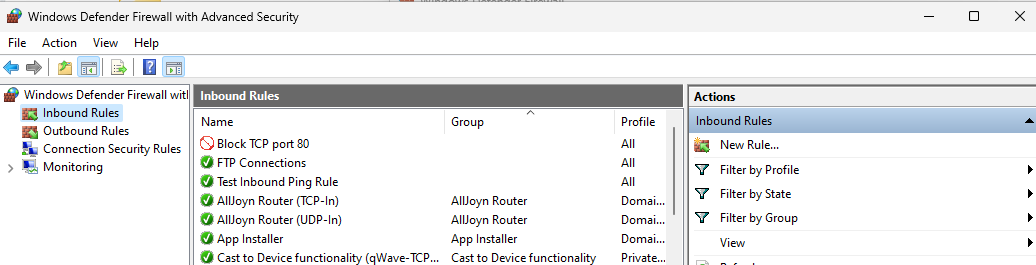
****

\*This is the ip address of the virtual machine desktop\*

****

\*Unsuccessful ping from the desktop to the VM\*

Created a new firewall rule (Test Inbound Ping Rule) that allows inbound ICMPv4 protocol traffic for both local and remote IP addresses on all network profiles.This allows pings to be successful.

****

Inpound Ping Rules

Rule type: Custom

Program: All program

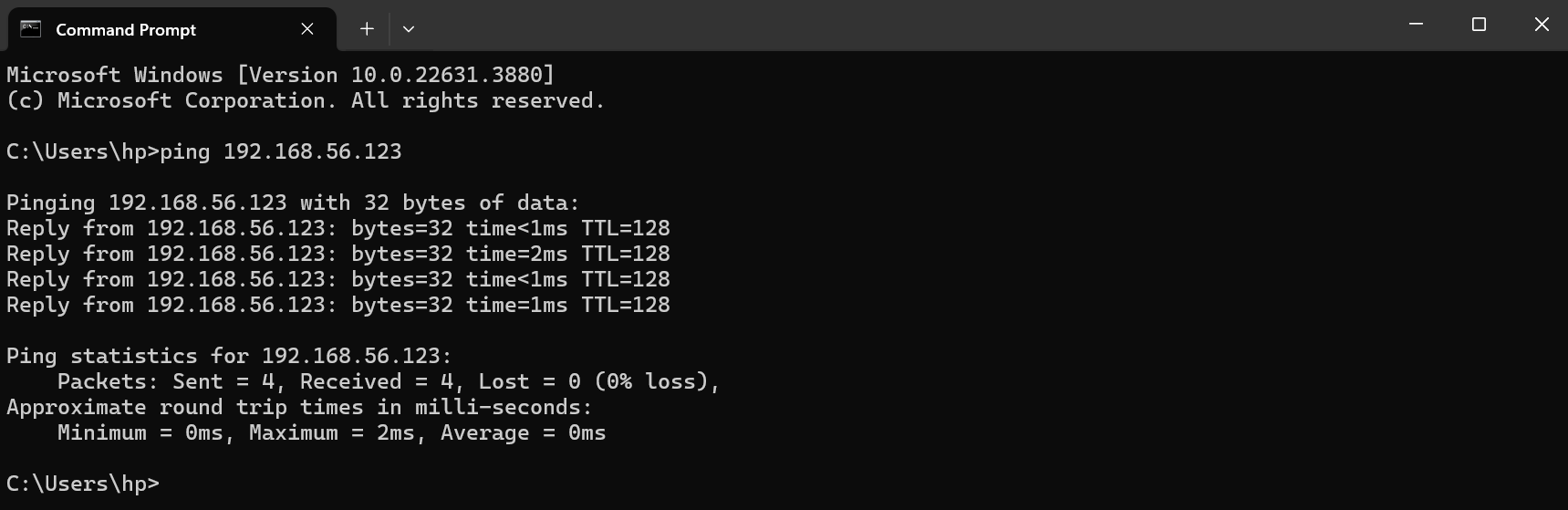
Protocol:ICMPv4

Scope: Any IP address

Action: Allow the connection

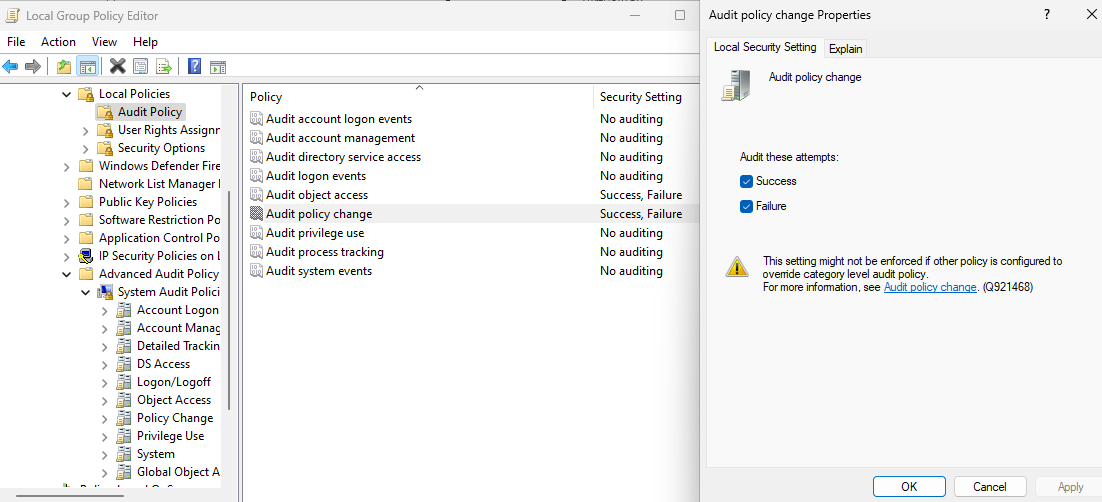
Profile: Domain, Private, Pubic

Name: Test Inbound Ping Rule

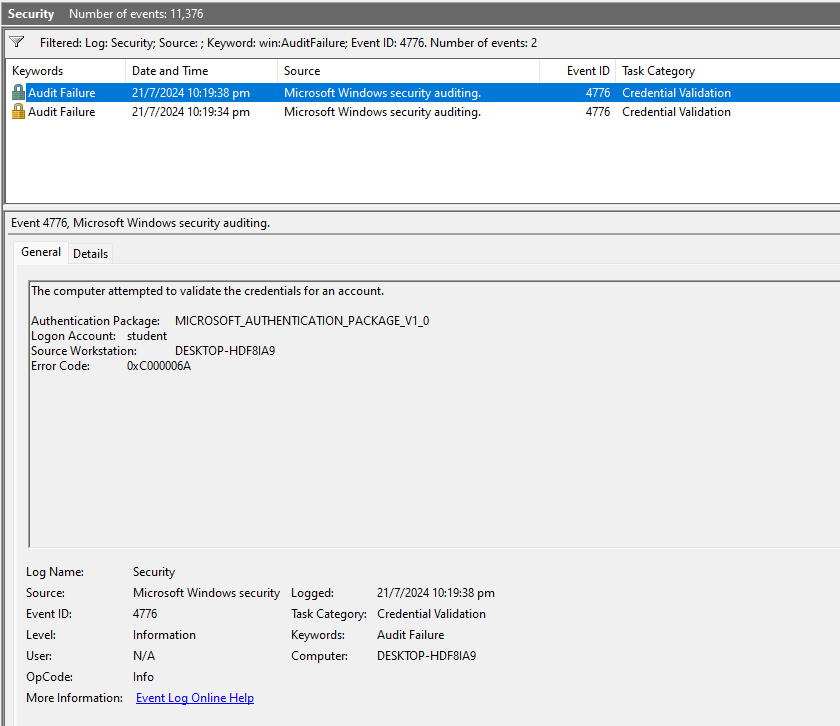
****

\*Successful ping from desktop to VM after adding an inbound rule to allow pings to come through\*

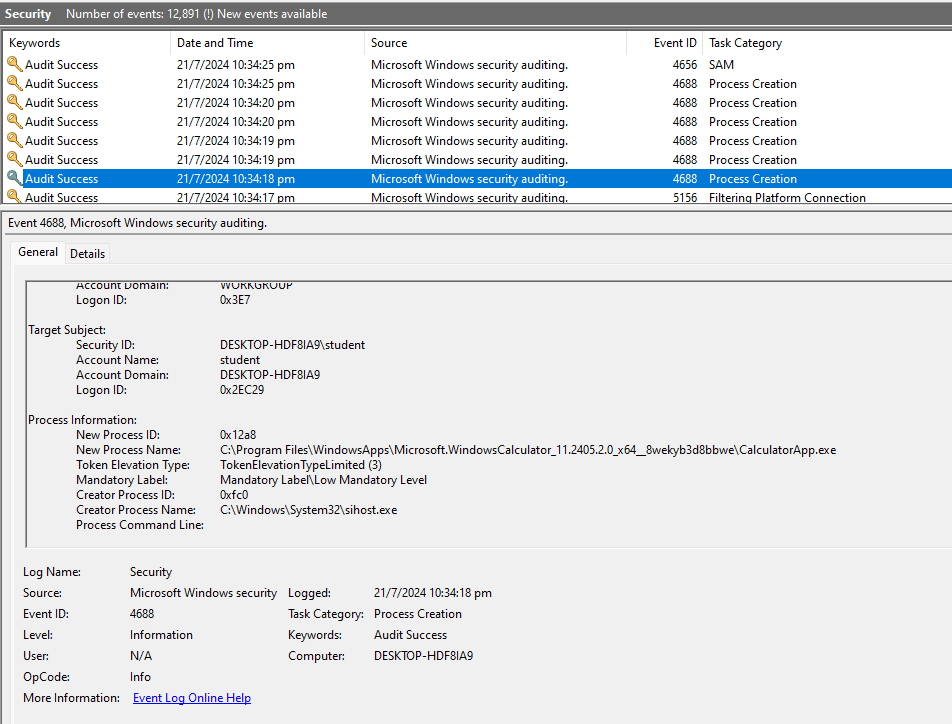
**Using Group Policy to audit actions in Windows**

****

Audit Failure

****

After using group policy to audit actions, I logined in with the incorrect password and it is seen recorded in the security audits.This shows the audit failure which the event id is 4776.

Audit Success

Launched the calculator app to check the windows security event logs. Since I was able to run the calculator app it showed audit success.

**Task C. Network Services (10%)**

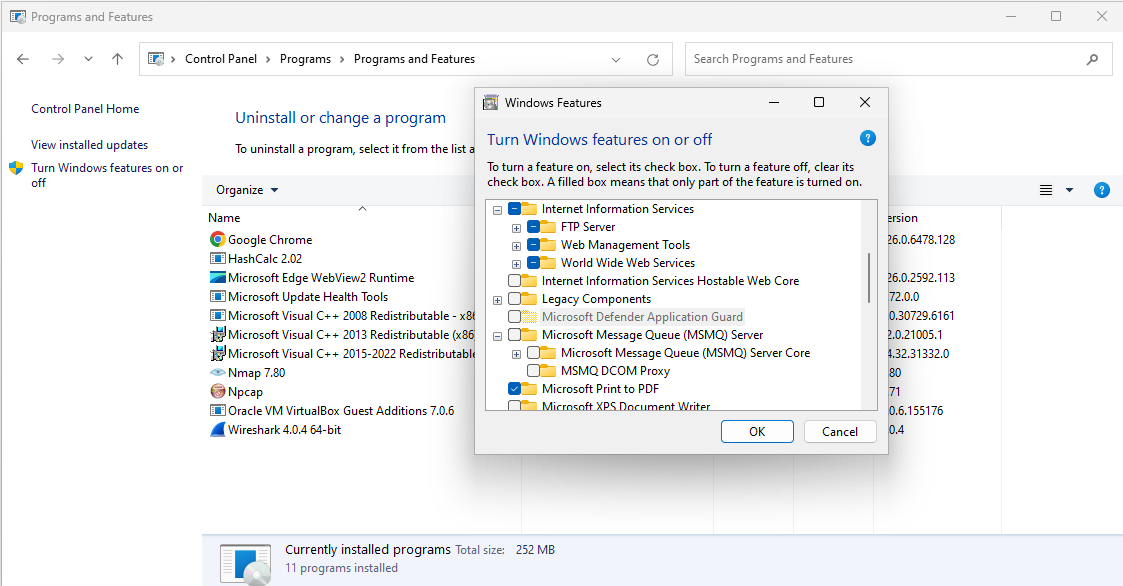
### VirtualBox Host-Only Adapter

### A VirtualBox Host-Only Adapter creates a private network for the VM and the host laptop. It allows them to communicate securely without connecting to external networks, and this is useful for isolated development or testing environments.

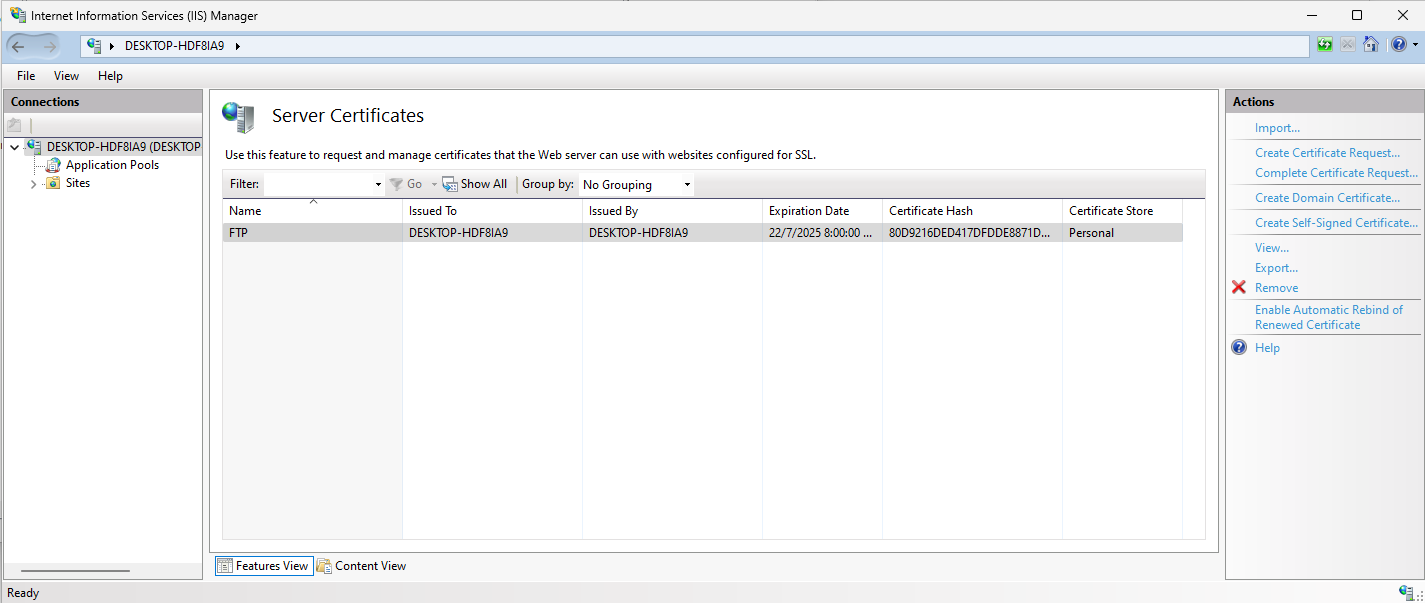
### SSL/TLS and how they work

### SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are the protocols that encrypt data sent over the internet. They ensure that information like passwords and credit card numbers remain private and secure between the web server and a browser or application.

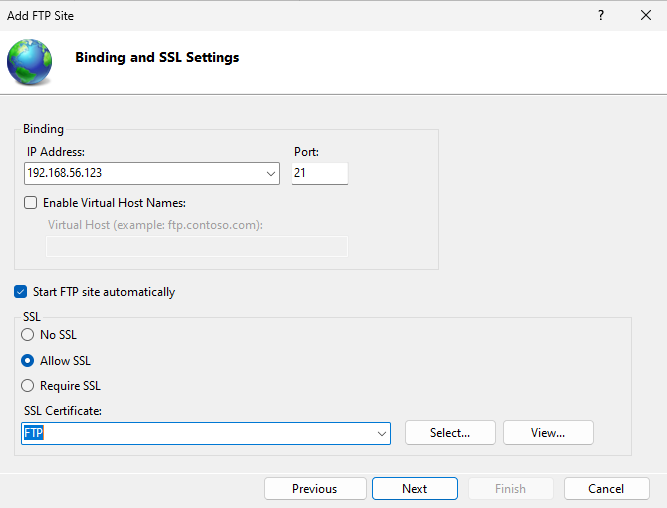
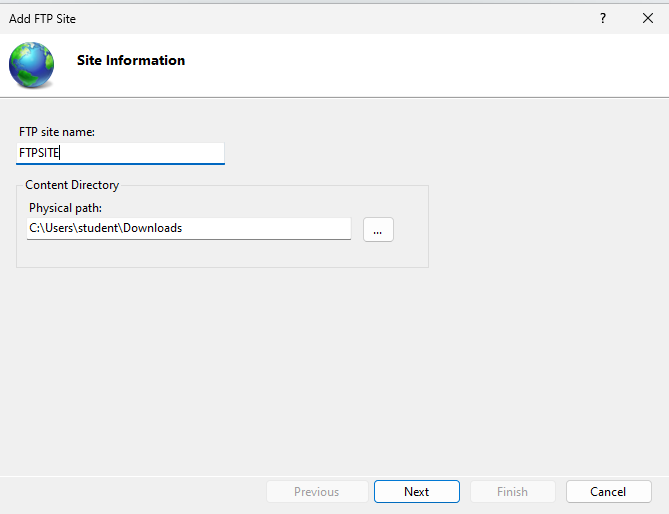
**i. Set up secure IIS FTP service with SSL/TLS using self-signed certificate.**

****

These are few steps are important to set up IIS FTP services with SSL using self-signed certificate on my VM. Under Windows we enable IIS Then select both sub options under FTP server and the IIS Management Console under Web Management tools. Then we press ok button which will install these features.



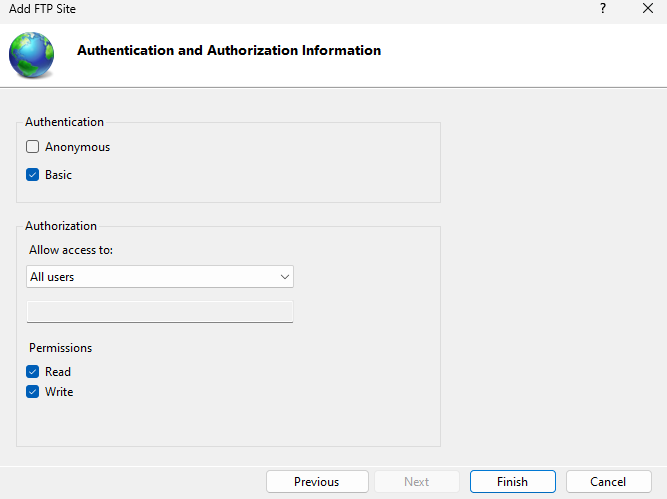
In Internet Information Services (IIS) I first created a Server certificate more specifically, Self-Signed Certificate which I named to FTP



The following 4 steps are to add a FTP site which is done on IIS.

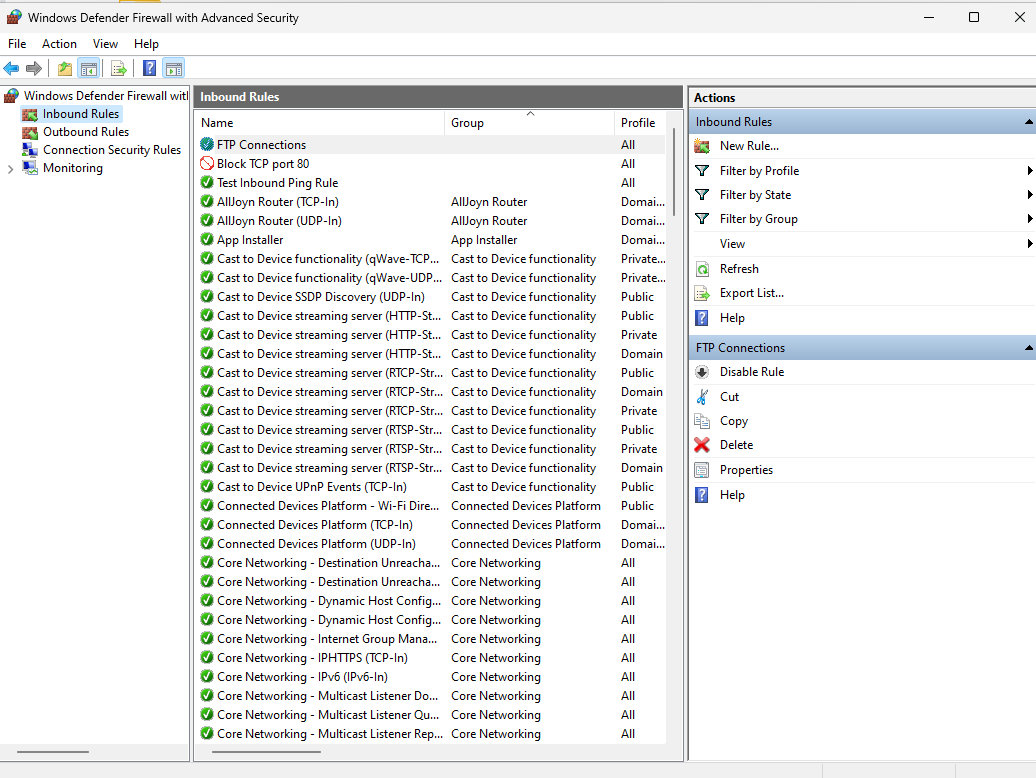
The ip address is the VMs one which is 192.168.56.123 and port is 21. The SSL is the one we created, FTP

I named my site as FTPSITE and its path is in the downloaded folder in my VM.



I set to basic authentication and allowed access to all users which allows all users permission to read and write.

Inbound rule



Then I created an inbound rule which allows the FTP connections to come through so that the FTP connections will come through.

Inpound Ping Rules

Rule type: Port

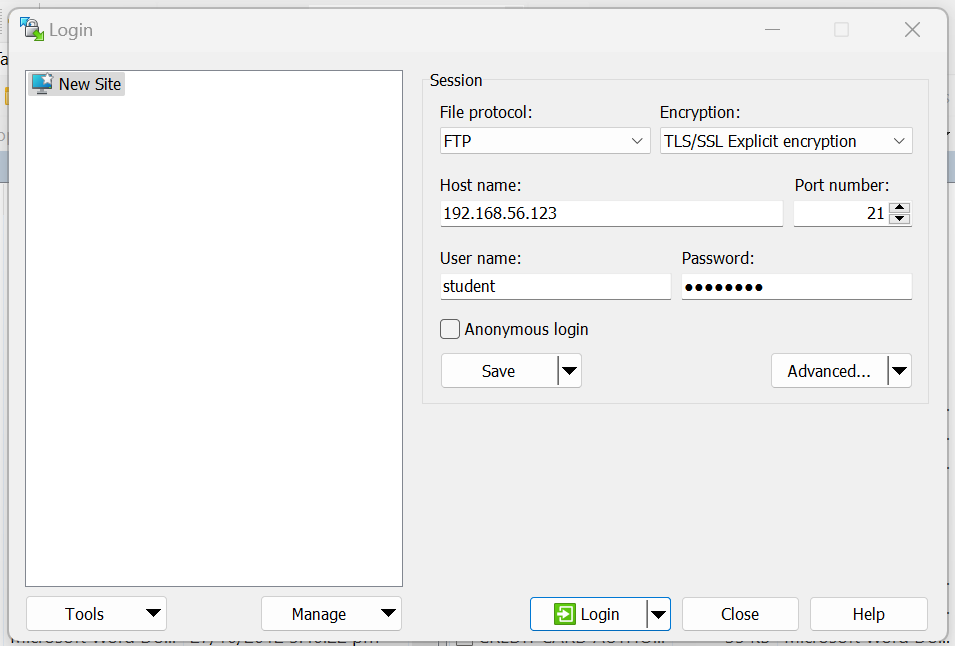
Protocol: Applies to TCP and specific local port 20-21

Action: Allow the connection

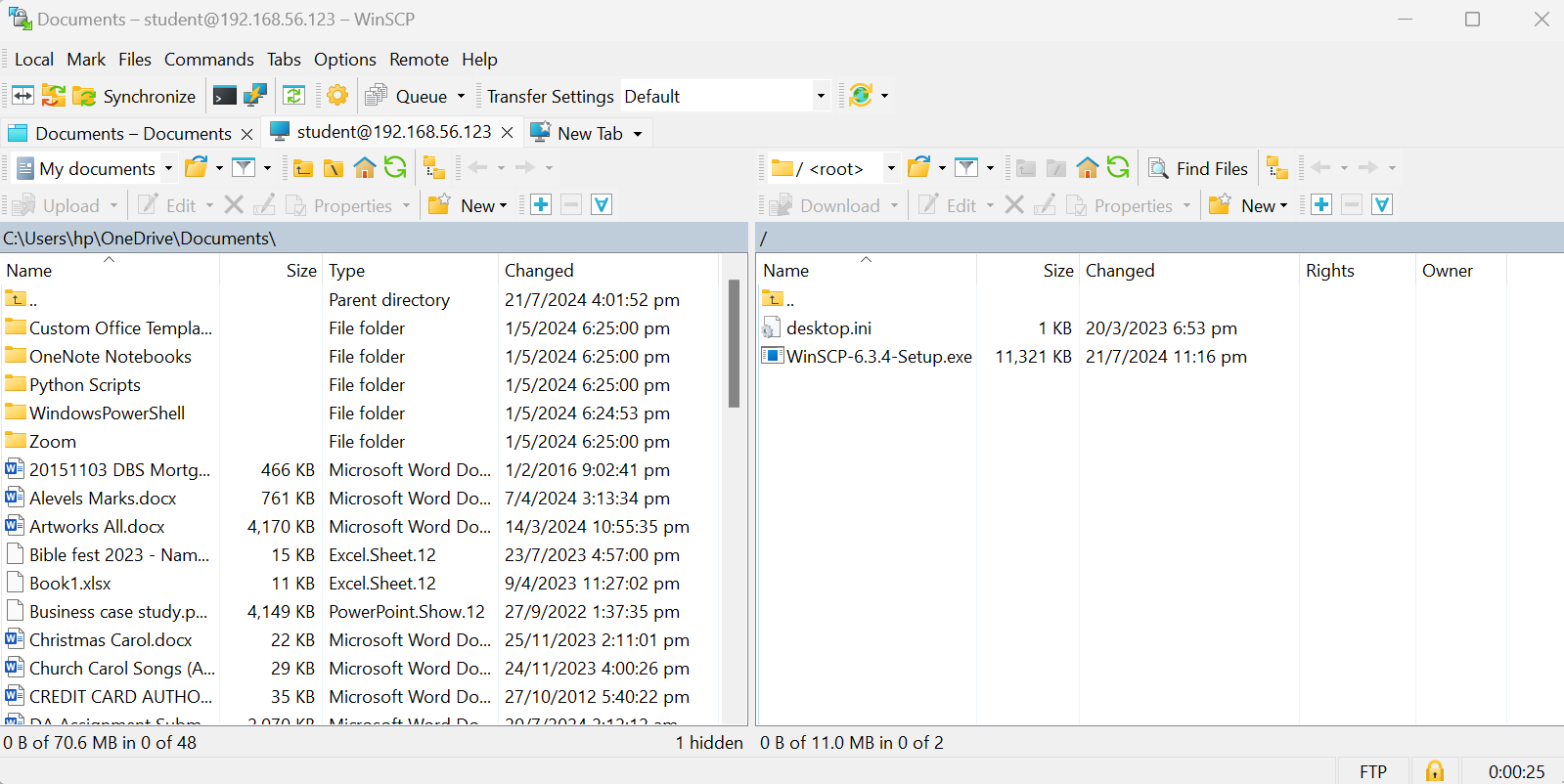
Profile: Domain, Private, Pubic

Name: FTP Connections

WINSCP Software



In WINSCP I tried to connect it to my secure FTP server



Successful connection from the WINSCP software to the secure FTP server.

**ii. Set up secure IIS web service with SSL using self-signed certificate**

### Network Address Translation (NAT)

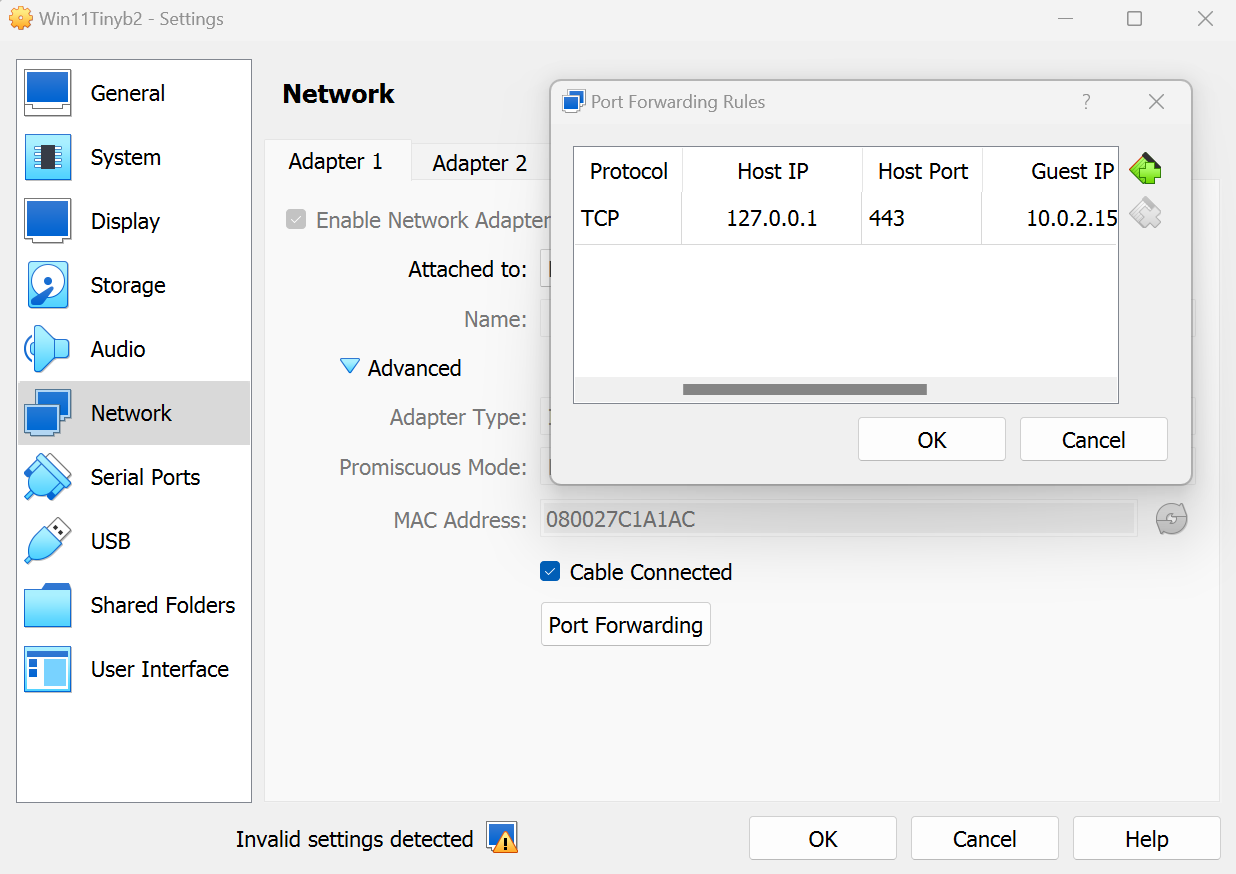
Network Address Translation (NAT) modifies IP addresses in packet headers, allowing multiple devices in a local network to share a single external IP address for internet access which enhances security.

### Localhost 127.0.0.1

Localhost 127.0.0.1 is the loopback IP address of a device, enabling it to communicate with itself. It is commonly used for testing and troubleshooting applications locally without needing an external network connection.

### Port Forwarding

Port Forwarding redirects communication requests from one IP address and port to another, enabling remote access to services or devices within a private network from external networks. It's essential for allowing external users to access specific services hosted behind the router or firewall configured with NAT.



\*Port 443 is the secure port (https) while port 80 is the unsecure one (http)\*

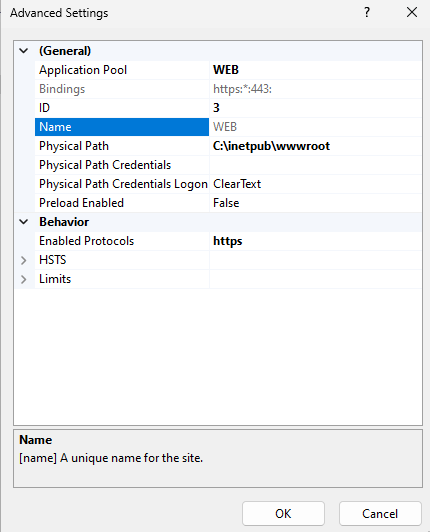
Protocol:TCP

Host Ip: 443

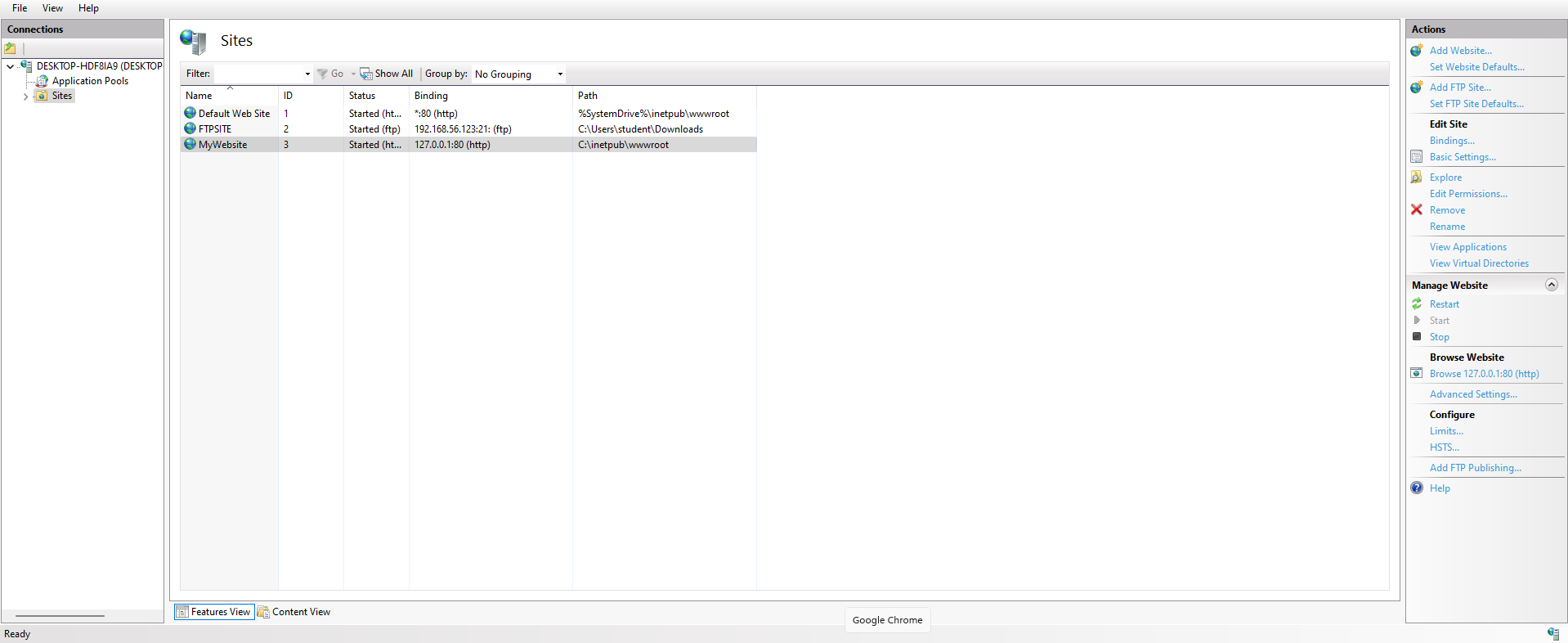
Guest Ip: 10.0.2.15

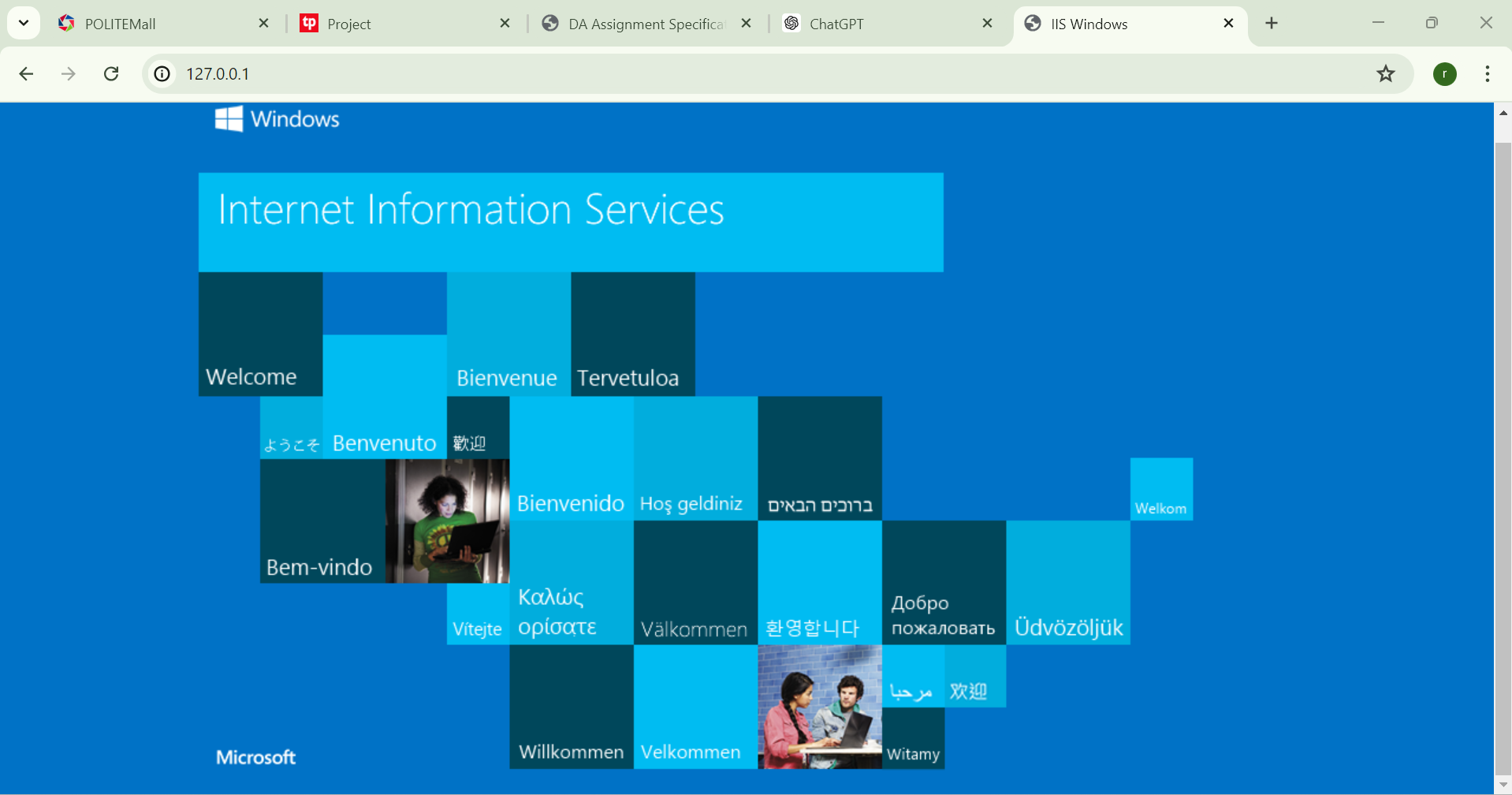
Guest Port:443

I set my network to allow for port forwarding



This shows the properties of the site and that it is https and that the site is secure





\*However we are unable to have the site as https as the certificate we used is self signed and hence not a legitamate/valid certificate. Eg. https site have valid certificates example could be like from microsoft \*

The website is now connected and this means that when the IP address 120.0.0.1 in the VM and the IP address in the laptop are connected, they are communicating with the same network.

**Task D. CIS Benchmark (5%)**

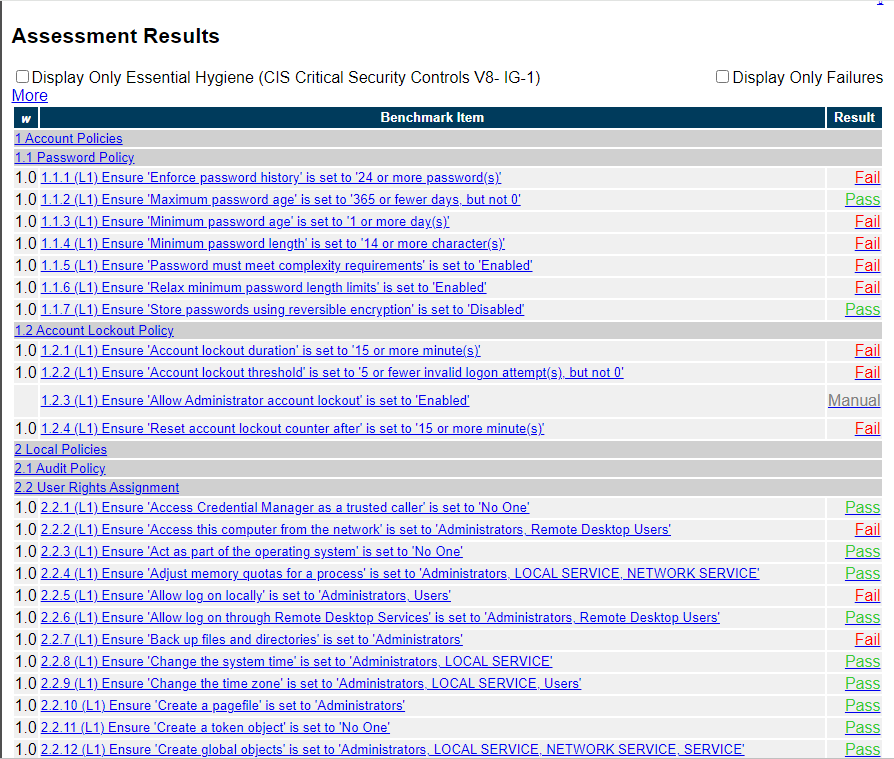
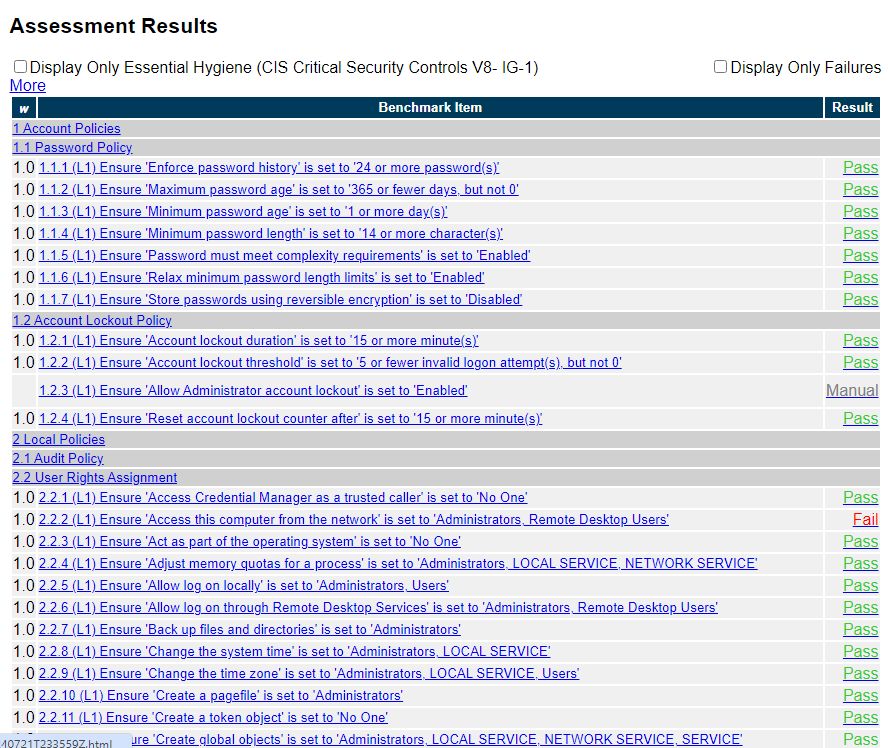
**Account Policy**

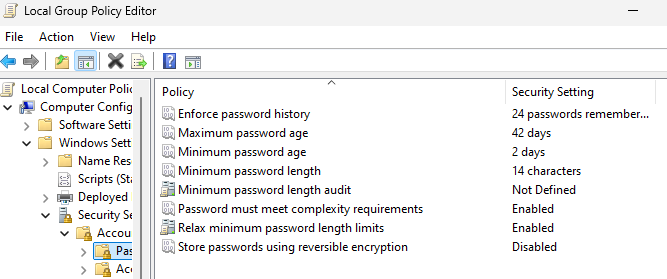
Before rectification



After rectification

****

 ****

****

I went to edit group policy and then selected security settings and under there there is password settings and there I edited the max password age to 42 days and the min password length to 14 characters

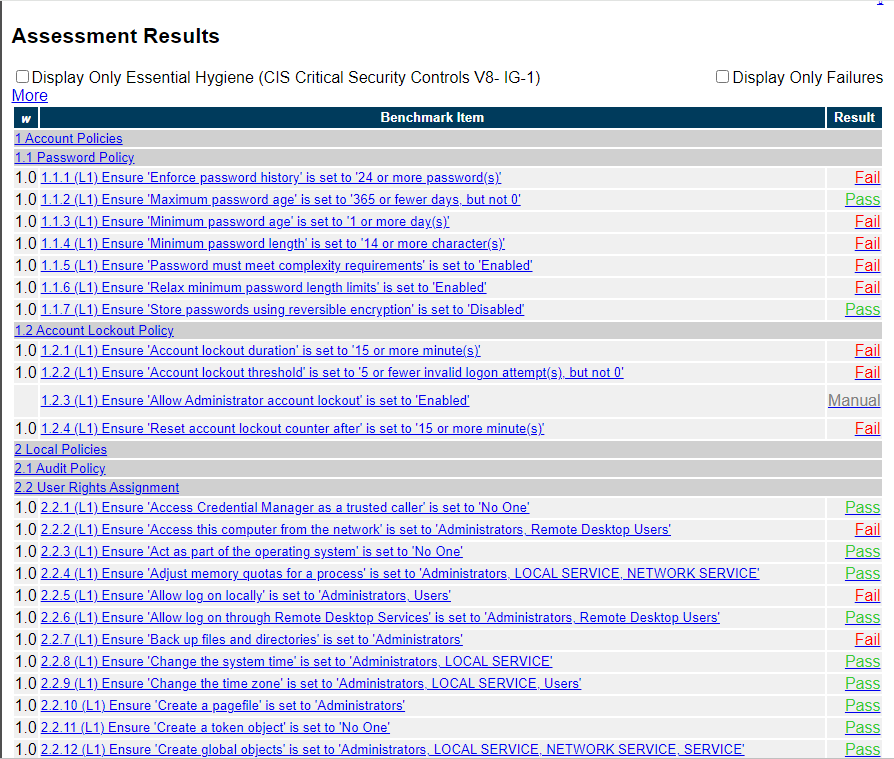
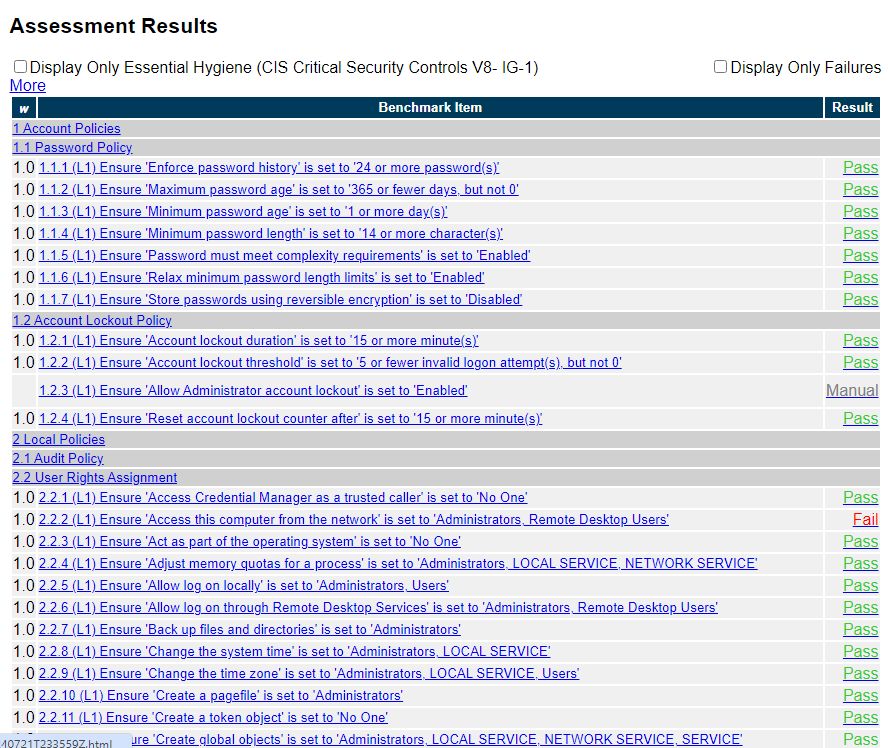
**Local Policy**

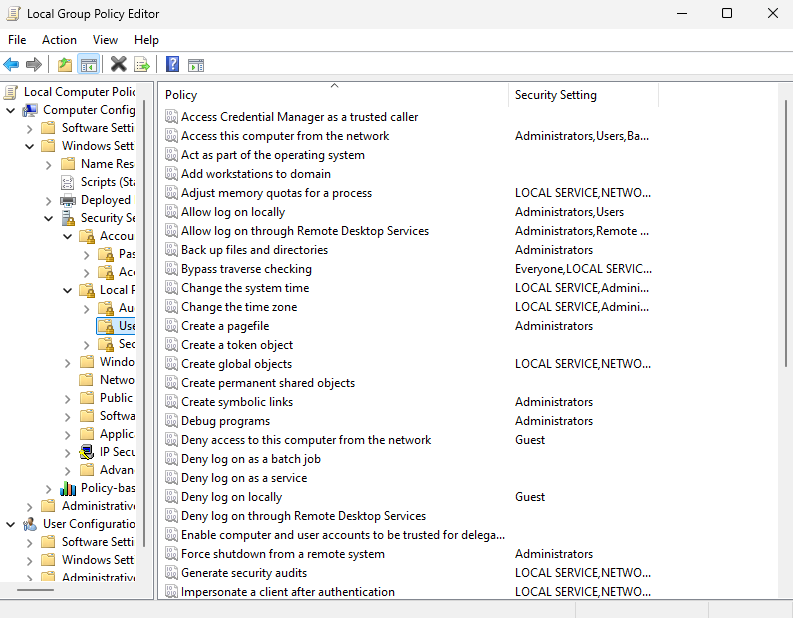
Before rectification

****

After rectification

****

****

****

I went to edit group policy and changed the user rights for allow log on locally to administrator and users and backup files to administrator.

**System Services**

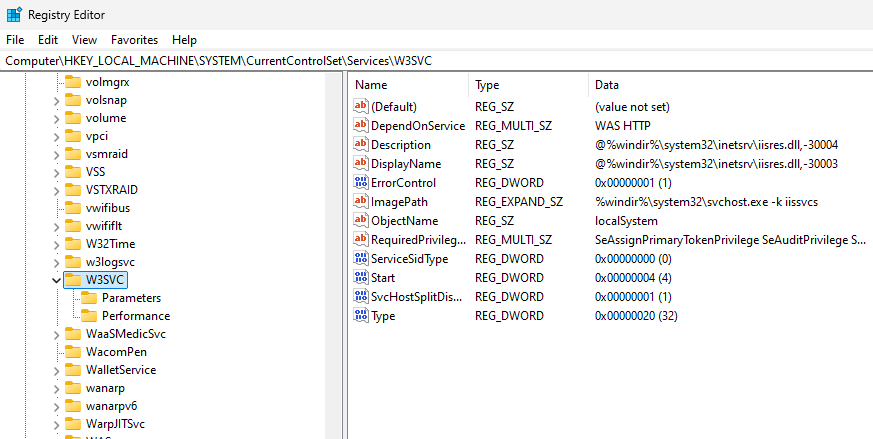
Before rectification

****

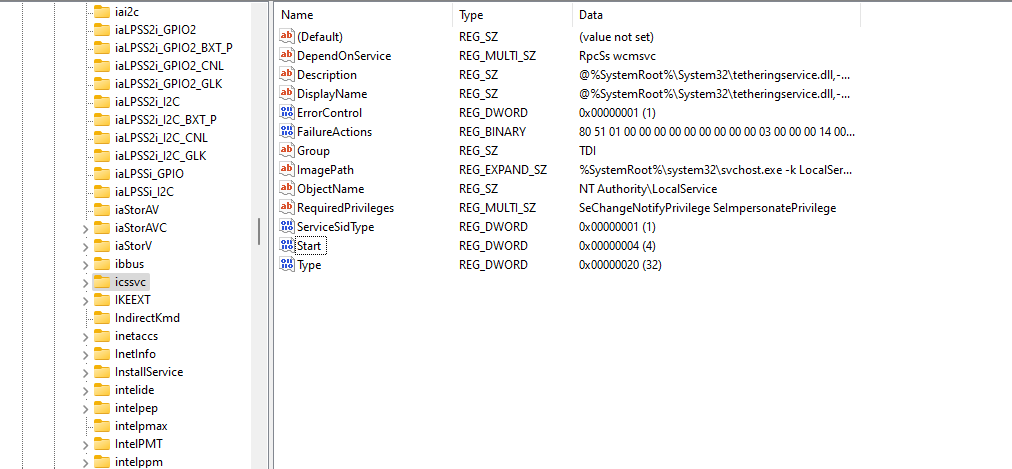
**After rectification**

****

****

****

Since I did not have system services in the edit group policy, I went to registry editor and fixed the registry value to 4.

****

**Windows Firewall with Advanced Security**

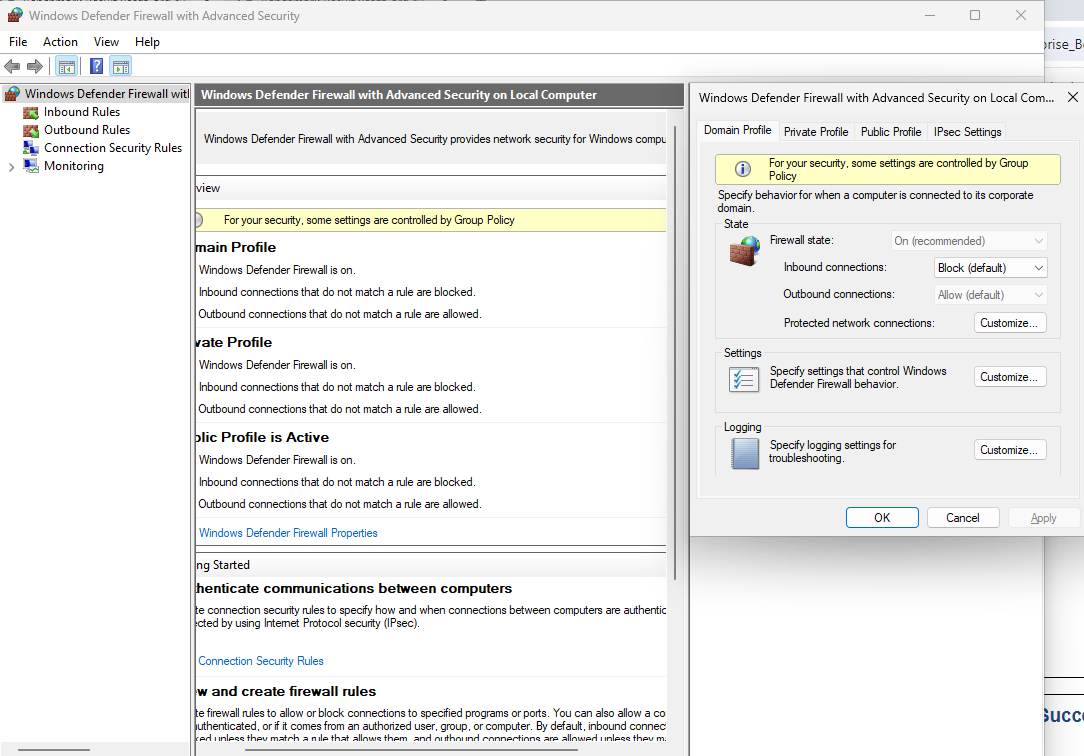
Before rectification

****

**After rectification**

****

**** ****

****

In windows defender firewall I changed the firewall state and inbound rules

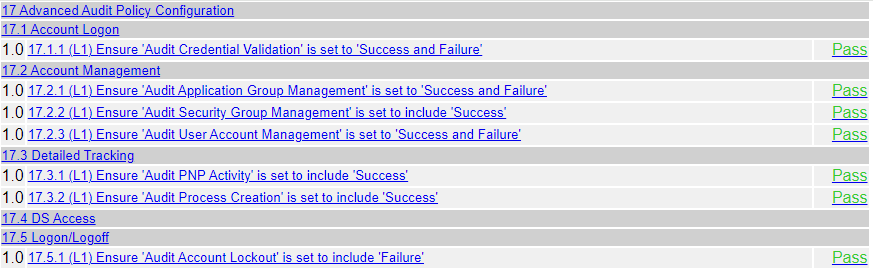
**Advance Audit Policy Configuration**

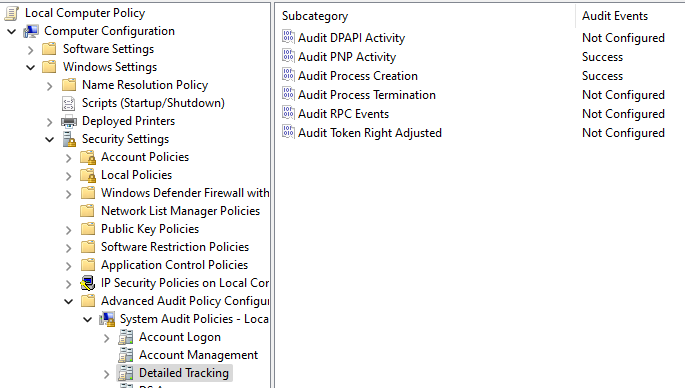
Before rectification

****

**After rectification**

****

****

****

In edit group policy I amended the detailed tracking to success.

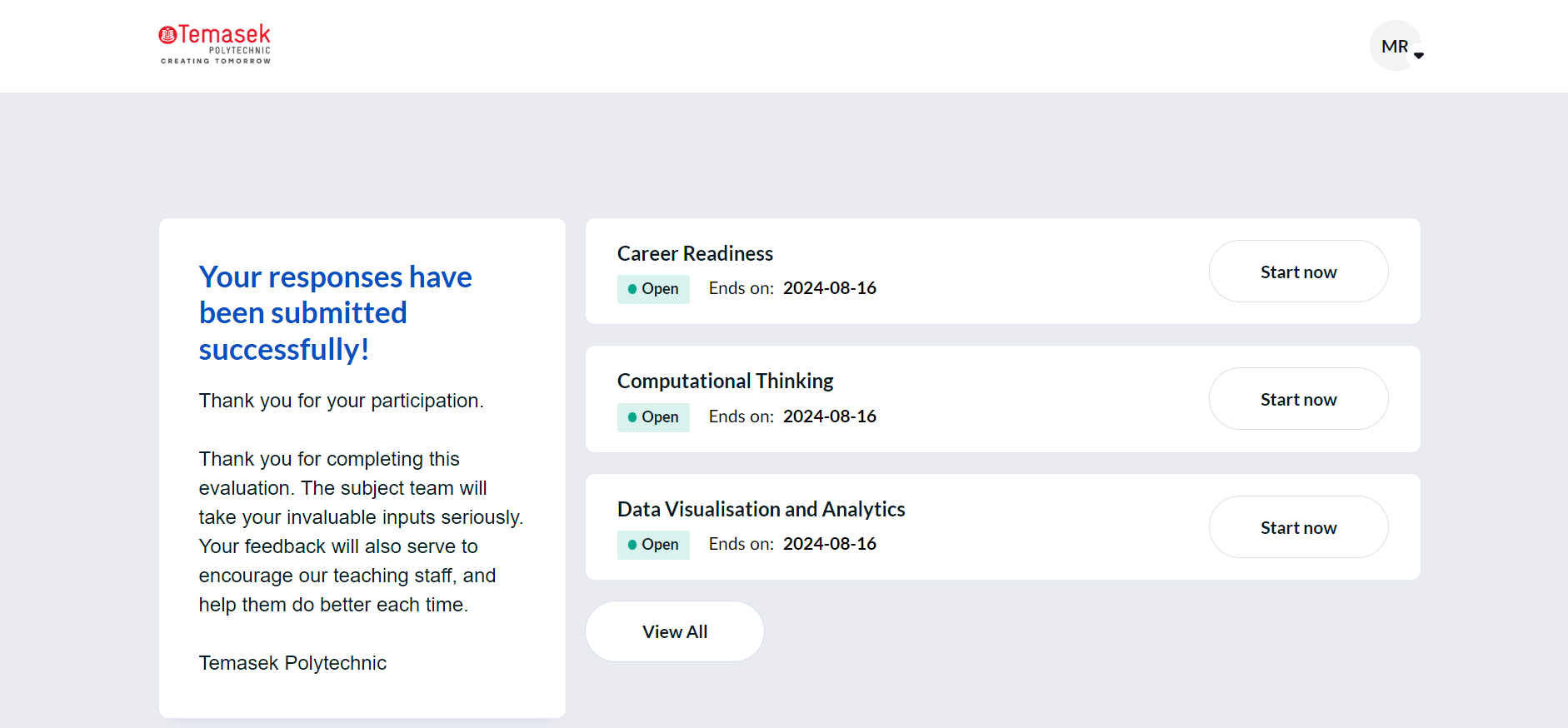
**Conclusion**

Throughout this project, I have significantly enhanced my technical skills in Windows security and network services. Under the guidance of my knowledgeable tutor and by completing the Windows 11 Security course on LinkedIn Learning, I developed a strong foundation in securing Windows systems and implementing essential practices to defend against potential threats. This online learning experience was invaluable, providing theoretical knowledge that I could directly apply to practical tasks. Setting up secure FTP and web services with SSL/TLS was a challenging yet rewarding experience, requiring me to learn about network protocols and the nuances of secure communications and system hardening. By actually implementing these configurations on my Virtual Box machine, I gained a deeper and more practical understanding of these concepts. Running the CIS-CAT Lite tool and addressing identified vulnerabilities provided hands-on experience in adhering to industry benchmarks and improving system security. This process underscored the importance of proactive measures in maintaining a robust security posture, especially in remote work environments. Overall, this project not only honed my technical skills but also reinforced the critical role of cybersecurity in safeguarding organizational data and operations. I enjoyed doing this project and learnt a lot from doing this assignment. Thank you. (199 words)

**Appendix and References**

1. [**https://winscp.net/eng/docs/guide\_windows\_ftps\_server#on\_windows\_desktop\_windows\_11\_windows\_10\_windows\_8\_windows\_7\_and\_windows\_vista**](https://winscp.net/eng/docs/guide_windows_ftps_server#on_windows_desktop_windows_11_windows_10_windows_8_windows_7_and_windows_vista) **(To add FTP self-signed certificate)**
2. [**https://www.itechguides.com/how-to-install-iis-in-windows-11/#:~:text=How%20Do%20I%20Enable%20IIS,Then%20click%20the%20OK%20button**](https://www.itechguides.com/how-to-install-iis-in-windows-11/#:~:text=How%20Do%20I%20Enable%20IIS,Then%20click%20the%20OK%20button) **(To enable IIS)**
3. [**https://www.linkedin.com/learning/windows-11-security/introducing-windows-11-security?resume=false&u=76881922**](https://www.linkedin.com/learning/windows-11-security/introducing-windows-11-security?resume=false&u=76881922) **(Overall task B)**
4. [**https://www.ionos.com/digitalguide/server/know-how/localhost/**](https://www.ionos.com/digitalguide/server/know-how/localhost/) **(To create local host)**

**Tessy Survey**



Tessy Survey for The Cybersecurity Module

**END**