Server & Cloud Security Diploma in CSF/IT Oct 2022	Week 5-17 **Assignment (40%)**
Assignment	

Introduction

The final assignment of SCS module has the following components:

Components	Deliverables	Scope	Weightage	Deadline
Part 1: Group Component	Group Report & Demo	Hardening Linux OS	20%	05 Feb 2023
Part 2: Individual Component	Individual Report	Securing a Windows File Server	20%	05 Feb 2023

Part 1-Group (20%): Hardening Linux OS

Scenario

Linux is an open-source operating system (OS) and IT infrastructure platform allowing various distributions such as Ubuntu, Fedora, and CentOS. One of the main considerations of choosing Linux over Windows is 'free of charge'. Enterprise would have no license cost of deploying a Linux server.

Task Requirements

Form a team of 3-4 members.

Your team are tasked to research and select one Linux distribution, install it in your virtual environment and make your best efforts to secure it.

Your team may need to research and self-learn some basic Linux commands in order to complete this task.

Task Details

Develop your own guidelines / best practices to secure the Linux server. The areas / approaches can be but not limited to the following functions:

- User / Account Management
- SSH Keys for Authentication
- Disk Encryption for Linux
- Linux Firewall
- Monitoring and Auditing

Deliverables

- Your team should produce a detailed **report** to explain your suggested guidelines / best practices to secure the Linux OS.
- Prepare a **team demo** of your work during Week 16 or 17 class hours.

Part 2 - Individual (20%): Securing a Windows File Server

Scenario

A file server is a necessary but also critical component in an enterprise. It provides a centralized location for storing and sharing work related files, but at the same time, if the file server is compromised, there may be a big data breach to the company.

Task Requirements

- Task 1: Setup and harden a file server
- Task 2: Secure the file server with additional security tools.

Task Details

Task 1: Setup and Harden a File Server

You can consider to setup a new Windows Server VM and add the **File and Storage Services** role to it to promote it into a file server. (**Alternatively**, you can add the role to your **MS1** VM to save your host computer's RAM and CPU. Do note that this is only an alternative to this assignment, but it is not a good choice in real practice to have multiple server roles in one server.)

Make sure your file server is successfully setup, and the share folders can be accessed from the client computer.

To harden the file server, refer to the LinkedIn Learning contents that you have learnt in Week 2 & 3. You may consider to implement but not limited to the following approaches:

- Encrypting File System (EFS)
- IPSec
- File Server Resource Manager
- Password Policies, Account Lockout Policies
- Audit Policies

Task 2: Secure the File Server with Additional Security Tools

Search and propose additional security tool(s) to secure the file server. You must install the tool(s) to your file server, configure it and test it to prove that your tool is a good solution to improve the security of the file server. The tool(s) can be but not limited to the following functions:

- Anti-Malware
- Host Firewall
- Host IDS/IPS
- Data Loss Prevention
- Full Disk Encryption
- Vulnerability Scanning

Deliverables

You should demonstrate that the file server and security tools configured are functioning and produce a detailed **report** with the following details and necessary screenshots:

- Procedures of setting up a file server with connection testing results;
- File server hardening approaches and implementation results;
- Explain the key functions / features of the proposed security tool(s);
- Install, configure the tool(s), prepare test cases, and perform testing & evaluation of the tools;
- Any other good practices implemented to secure the file server (if applicable).

--End of Assignment--