Nanyang Polytechnic

School of Information Technology

Operating Systems and Administration

Practical 4 – Windows Security Analysis and Configuration Assignment (35%)

2023 / 2024 Semester 2

This group practical submission is designed to enable the following learning objectives:

To improve the understanding of the desktop security configuration in Windows through actual implementation.

To acquire techniques in analyzing, developing and implementing security controls through referencing real-world and common desktop scenarios. The self-selected scenarios may be open ended. Students are expected to make appropriate assumptions, think of possible security issues and implement their solutions **using the knowledge and skills learnt in the earlier labs or by own research**.

Windows Security Analysis and Configuration (35%)

In this exercise, students will form into groups (teams). Each group comprises of **3 or max 4** students. Each project group team shall elect a leader. The team should discuss and allocate fair and equal share of tasks to each team member.

Each group is to present to the tutor their results of their implementation **during Week 5 practical**.

For this exercise, you will use the pre-installed Windows VMware image (herein termed as VM). You can copy the VM to your notebook or an external hard disk during practical classes. Do not modify directly on the common Windows VMware image in the lab PCs.

To execute the VMs, you need to have the VMware Workstation Player/Pro or any equivalent. MacOS users would need to get or loan a Wintel machine for this assignment.

You can use and install any appropriate tools in the VMs to help you in your security analysis and configurations, but do not uninstall any existing software in it.

Implementation

The teams are required to complete the following in practical submission:

To analyze and identify the security issues based on Microsoft Baseline Security Checklist (**Appendix B**) in the existing configurations of the Windows VMware image. Modify the appropriate configurations to address the security issues identified.

Deliverables

To identify, present and submit a checklist of baseline security issues in the existing VMware image. For each baseline security issue identified, modify the settings of the VMware image to correct and strengthen the security configurations of the system. Be prepared to demonstrate your implementation in the presentation.

You may consolidate all your implementations is a single VM or in separate VMs. Additional bonus shall be awarded to the former, where extra effort and teamwork is needed to accomplish.

Presentation

Present and demonstrate your implementations during the Week 5 practical. Each team is given **15 – 20 minutes** to present the results of your implementations. **Every member must present his/her own completed tasks**.

As your modified Windows VM is too big to be submitted, you will present it in class and only submit your **Powerpoint** slides to **Brightspace**. Your Powerpoint slides may list, in point form, any assumptions or scenarios you have adopted, all the security configurations you have implemented and include all relevant and final screenshots for each setting.

Use a consolidated team slides for pacing and as a guide during presentation.

Rubrics

		Group	Individual
1	Technical Competence		10%
2	Presentation		10%
3	Teamwork	15%	

	Excellent	Very Good	Good	Satisfactory	Unsatisfactory
Technical Competence	Demonstrate strong technical skills and creativity	Demonstrate strong technical skills	Demonstrate some technical skills	Somewhat lack in technical skills	Unable to demonstrate or demonstrate minimal technical skills
Presentation Stucture and Content	Presentation is concise with clearly stated focus.	Presentation is mostly concise with clearly stated focus.	Presentation is somewhat concise and has some clarity in focus.	Presentation is not concise and lack clarity in focus	Presentation does not have a focus
Teamwork	Team members work very well together and greatly shared knowledge and skills	Team members work well and able to share some knowledge and skills	Team members able to work and support one another and share some knowledge and skills	Team members has some difficulty working together and sharing knowledge and skills	Team members unable to work together and tend to work individually.

APPENDIX A - TEAM ORGANISATION

Module Group :_____

Team No : _____ (To be assigned by the tutor)

Scenario : A / B (to be allocated by tutor)

Team leader and members:

S/No	Admin No.	Name	Role
1.			
2.			
3.			
4.			

Note:

(i) All members must be from the same Module Group.
(ii) Each group to submit one form to the tutor.

APPENDIX B - Windows Baseline Security Checklists (Abridged)

1) Verify that all disk partitions are formatted with NTFS
2) Make sure the Guest account is disabled
3) Disable or delete unnecessary accounts
4) Use account passwords
5) Set stronger password policies
6) Set account lockout policy
7) Disable Internet Connection Sharing
8) Protect file sharing and shared folders
9) Enable Internet Connection Firewall
10) Use software restriction policies
11) Disable unnecessary services
12) Disable USB, or Disable Autorun and Boot from USB (preferred)
13) Install antivirus software and updates
14) Keep up-to-date on the latest security updates
15) Disable Remote Access
16) Secure system from Powershell exploits
17) Enable Auto Updates
18) App Management - Only allow the installation of approved applications from controlled software repositories or application marketplaces
19) Application Control - Whitelisting and blacklisting of executables or apps
20) Maximise or Enhance Windows Defender Features
    a) Antivirus
    b) Exploit Guard
    c) Device Guard
    d) Application Guard
    e) Credential Guard
21) Enable Microsoft SmartScreen
22) Enable Windows Hello
23) Enable Windows Sandbox
24) Enable Windows Secure Boot
    a) Enable TPM if available
    b) Create personal security certificates if necessary
25) Enable Windows BitLocker Encryption
    a) Otherwise, use Encrypted Folders, or both
26) Enable File Backups
27) Enable Restore Points
28) Install Host-Based Intrusion Prevention System
29) Etc.