AY2022/2023 S2

School of Computing
ST2612 Securing Microsoft Windows

Securing Active Directory Operations

1.0 INTRODUCTION

This assignment constitutes part of your in-course assessment (20%). Please spend some time to research materials outside your textbook to complete this assignment.

2.0 OBJECTIVES

The learning objectives of this assignment are to research the topics that relate to securing Windows Server and Active Directory and to make a 10 to 20 minutes demonstration of what you have accomplished to the tutor/class.

3.0 INSTRUCTIONS

3.1 You may work on this assignment either individually or in pairs.

3.2 The deliverables are:

- An Individual Report (for each member).
- A 10 to 20 minutes* demonstration.

*10 minutes per member

3.3 Written Report Submission.
To be submitted through Brightspace by Wednesday, 9pm, 8th Feb 2023 (Week 17).

3.4 Demonstrations will be done during the practical time on Week 17/18 **after** the written report submission.

3.5 Take note of the "SOC – Policy on Late Submission of Assignments". 50 marks will be deducted for every working day late submission. Assignments will not be accepted after more than 2 working days after the due date.

4.0 ASSIGNMENT REQUIREMENTS

4.1. The tasks

Each individual/pair may select and carry out **ONE** operational task from the following two choices:

4.1.1 Operational tasks for demonstration:

- Setting up a single site single Domain Network with High availability (HA) measure on the ADDS, DNS and DHCP services.
    - Your setup has to cater for security and availability issues / concerns.
    - Your setup may consist of, at the minimum, two Domain Controllers.
    - Each Domain Controller runs ADDS, DNS and DHCP services to support the Domain members.
    - Your setup should be able to operate continuously without failing for a designated period of time when one of the Domain Controllers is going offline (due to maintenance down time or hardware failure).

- Hardening the security measure of a single site single Domain Network with an in-house Intrusion Detection System (IDS) that based on audit logs.
    - The setup has to cater for file object access monitoring.
    - Your setup is required to implement a distributed file system (DFS) to host important and confidential files.
    - For the setup of DFS, at least two member servers should be setup to provide the DFS Services. (DC is not supposed to run DFS.)
    - Your IDS setup should monitor the following types of log entries:
        - The access log entries of the DFS namespaces shared folders.
            - To simplify the task, you are only required to monitor the file read accesses (Success and/or failure attempts) within a specific DFS folder.
    - This task may involve PowerShell and/or Python programming. (To extract the log entries and generate a formatted text report.
        - The text report, at the minimum, need to provide the following information:
            - Date/time, folder/file name, successes/failure, user id for each file assess attempts.
            - Please refer to a suggested text report in the Appendix A of this document.

4.1.2 The requirement of your demonstration:

You are **not expected/allowed** to carry out any installations nor configurations during the demonstration. You have to prepare your system for the operational demonstration only. (Creating testing user accounts, folders, files are not supposed to carry out during the demonstration. All these configurations should be well prepared beforehand.)

In the 10 to 20 minute demonstration, you have to show the key elements* of the operational tasks, you have implemented.

*key elements refer to the part of the task that have significant operational and/or security implications. Minimum of THREE key elements per member are expected to be shown during the demonstration.

For example, the following list shows one key element for each of the task.

- For the High Availability (HA) operations: As long as one DNS is online, the DNS Services remains available for all domain clients.

- For the IDS/DFS operations: As long as one DFS server is online, the clients can retrieve and update the files from the DFS folder(s). (To ensure availability)

4.1.3 The requirement of the written report:

- The basic report structure may consist (all/most) of the following:
  1. Title page.
  2. Summary.
  3. Table of contents.
  4. Introduction.
  5. Body of the report.
  6. Conclusions and recommendations.
  7. References and appendices.

  Reference for report structure:

  https://www.monash.edu/rlo/assignment-samples/engineering/eng-writing-technical-reports

- The body of the report is required to provide a step by step procedures (setup guide similar to the SMW lab exercises style.) for the operational task you have carried out. It may include the scripts/program source too.
- You need to list the sources of all the reference you have referred to for this assignment. (e.g. YouTube links, Internet Article links, textbook… etc.)
- In this report, you are required to provide a demo agenda for each of the members which outlines the plan/flow, testing data set, and/or any assumptions of your demonstrations. You have to base on this agenda to conduct your demonstration.

5.0 MARKING SCHEME

Written report (Group)	
Structure and Completeness (refer to 4.1.3)	20 %
Readability and Correctness	25 %
Relevant Reference	5%
Demonstration (Individual)	
Preparation and Presentation Flow (Based on the planned agenda)	10%
Correctness, Completeness and relevancy (For 3 Key elements)	30%
Q and A (During Demonstration)	10%
Total	100%

Warning: Plagiarism - anyone found plagiarising in this assignment would be penalised.

Appendix A - Sample IPS report

```
Report Generation Date/Time: 18/08/2022 - 13:35,28/7/2022 11:07:04 am
File Access Section:

Timestamp,Security ID,Account Name,Object Type,Object Name,Audit Type (Success/Failure)
28/7/2022 10:37:44 am,Kitty\Mgr1,Mgr1,File,C:\Shares\SF3\smw_srv2016.txt,Success
28/7/2022 10:38:01 am,Kitty\user1,user1,File,C:\Shares\SF3\smw_srv2016.txt,Failure
```

Note: The above is extract from a text file. It consists of two log entries. Each entry consists of multiple comma separated columns.
The sample depicts the minimum required information to be shown in the IPS report. You may provide additional useful information in your report.

~ The End ~