Asia Pacific University of Technology and Innovation
Master Level
Security Operation Center and Incident Response
CT111-3-M-SOC
Assignment 2 (Individual) – 50%

Course Learning Outcome:

CLO 3: Perform an advanced cyber-attack using any appropriate tools and complete the incident response procedures based on the given scenario (A5, PLO6)

Cyber-attack simulations are crucial for enhancing cybersecurity measures by replicating real-world attack scenarios to test and improve defense mechanisms. Indicators of Compromise (IoCs) are essential in identifying and responding to cyber incidents, as they provide key data points that reveal signs of malicious activity. This assignment aims to simulate a cyber-attack to collect relevant IoCs and utilize this data to develop and refine automated response strategies, thereby improving overall incident management and response capabilities.

Task: Individual (18.10.2024):

1. **Select and Research a Cyber-Attack Type:**
   - Choose a specific type of cyber-attack and conduct studies on the methodologies and tools associated with it.

2. **Simulate the Cyber-Attack:**
   - Based on your research, choose one tool to perform the simulation (e.g., Metasploit, Burpsuite, Hydra, etc.). The steps for setting up and executing the simulation should be accompanied by clear and detailed screenshots for each stage. Include brief descriptions explaining the content and relevance of each screenshot.

3. **Capture and Analyze Forensic Evidence:**
   - Document and capture the Indicators of Compromise (IoCs) generated during or after the simulation. You can use any tool, utilities or methods such as Event Viewer for windows logs or Wireshark for network traffic analysis. The steps for capturing and analyzing the IOCs should be accompanied by clear and detailed screenshots.

4. **Develop an Incident Response Plan (IRP):**
   - Formulate a comprehensive Incident Response Plan tailored to the specific attack type you simulated. Include strategies for detection, containment, eradication, and recovery to effectively respond to and manage the attack.

Instructions:

This individual assignment carries **50%** of your total assignment assessment marks. No marks will be awarded for the entire assignment if any part of it is found to be copied directly from printed materials or from another sources. All submissions should be made on or before the due date. Any late submissions after the deadline will not be entertained. **A zero (0)** mark will be awarded for late submission unless extenuating circumstances are upheld. The expected length is approximately 1,500 words plus diagrams and with all references clearly indicated and provided using APA Referencing Convention.

Assessment Criteria:

Guidelines for the Report:

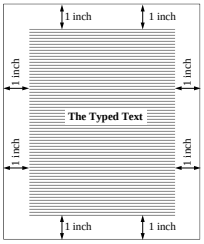
Document the results of your work in a **professional and systematic** manner, in the form of a **computerized report**. **Your completed report is to be submitted through the Online Submission Platform (Moodle)**.

Your completed documentation should meet the following requirements:

1. Table of contents for every detailed chapter/section.
2. Introduction
3. Chapters / sections (according to the Tasks)
4. Documentation of the configured device(s) (optional)
5. Conclusion
6. Appendices (optional)
7. Bibliography or References

In your document the report is to be written in a professional manner, paying due regard to the following aspects:

- The report should have a consistent layout and be divided into enumerated sections, sub-sections, sub-sub sections etc.
- The report should be fully referenced using the University standard.
- Your report must be typed using Microsoft Word with Times New Roman font and size 12 and it should be in 1.5 spaces.
- The report should have a one (1") margin all around the page as illustrated below:



- Every report must have a front cover. The front cover should have the following details:
  - Name
  - Intake code.
  - Subject.
  - Project Title.
  - Date Assigned (the date the report was handed out).
  - Date Completed (the date the report is due to be handed in).

Assessment Criteria:

- Research and Investigation 20%
- Demonstration of Selected tool 30%
- Forensic Evidence/Logs of Events 30%
- Incident Response Plan 20%

Marking Rubrics:

	1 to 5 (Fail)	**6 to 10 (Pass)**	**11 to 17 (Merit)**	**18 to 20 (Distinction)**
Research and Investigation (20)	Poor research and investigation of the problem and tools. Poor or unable to perform evaluation of the requirement.	Satisfactory research and investigation is done. Satisfactory evaluation of the problem and tools.	Good analysis and investigation of the problem and tools. Provided good evaluation of the requirements with proper reasoning.	Outstanding research and investigation has been performed. Provided excellent evaluation of the requirements with good reasoning.
	1 to 5 (Fail)	**6 to 15 (Pass)**	**16 to 25 (Merit)**	**26 to 30 (Distinction)**
Demonstration (30)	Very poor or minimal demonstration of the selected tool/no tool selected.	Demonstration done with lack of explanation on the selected tool. Insufficient descriptions on the use of the tool to launch the attack	Demonstration done with satisfactory explanation. Good descriptions on the use of the tool to launch the attack with screenshots of command	Excellent analysis of the problem and selected tool. Proper usage and demonstration of tool in launching the attack and testing the accuracy of the solution
	1 to 5 (Fail)	**6 to 15 (Pass)**	**16 to 25 (Merit)**	**26 to 30 (Distinction)**

Forensic Evidence (30)	Very poor or minimal demonstration of forensic evidence/no evidence demonstrated.	Forensic evidence provided with minimal explanation on the results gathered from the logs.	Good forensic evidence provided with satisfactory explanation on the results gathered from the logs. Good descriptions and presentation of proofs on the discovery of evidence.	Excellent forensic evidence provided with good explanation on the results gathered from the logs. Excellent descriptions on the logs with excellent presentation of proofs on the discovery of evidence.
	1 to 5 (Fail)	**6 to 10 (Pass)**	**11 to 15 (Merit)**	**16 to 20 (Distinction)**
Incident Response Plan (20)	No incident response plan was provided and did not follow any standard. Missing major details on the proof of the evidence.	Acceptable incident response plan provided but did not really follow the standard. Missing few details on the proof of the evidence.	Good incident response plan provided and following the standard without proper justification to solve the discussed issue	Exceptional incident response plan provided following the standard with justification provided to solve the discussed issue