In-course Assignment Information Sheet

CT112-3-M-Advanced Ethical Hacking

Intakes: APUMF2406CYS(PR), APUMF2406CYS, APDMF2406CYS

Date Assigned: 25th November 2024

Date Due: TBA

Lecturer: Ts Dr Vinesha Selvarajah

Assignment Overview: This assignment is graded at **100%** and will contribute 70% towards the in-course marks. It consists of one group component and consists of one individual practical task as follows:

Section A (Group) CLO2:

This section is a GROUP component of the vulnerability assessment. However, risk analysis and policy formulation must be conducted individually for description. Section A carries **60%** of total assessment marks.

Task 1: Vulnerability Scanning and Assessment (CL02) (Group)

This section is an individual task focusing on vulnerability scanning and assessment and carries **30% out of the 60% of this section.**

Case Study: Indonesia – E-commerce in the Crosshairs

In the first quarter of 2023, Indonesia saw a steep rise in cyberattacks, with an estimated 100 million attacks recorded daily. One of the largest e-commerce platforms, ShopEase Indonesia, was among the affected. The company confirmed a significant data breach involving sensitive customer information, including usernames, encrypted passwords, email addresses, and transaction histories.

The breach resulted from a vulnerability in the platform's third-party payment gateway integration. While no financial data was directly exposed, the incident raised concerns about user privacy and the risk of phishing attacks targeting customers. This was not the first security lapse for ShopEase Indonesia; two years prior, they faced a similar breach but implemented security measures aligned with PCI DSS standards to safeguard payment processes.

The recurring nature of these breaches' points to gaps in the company's overall cybersecurity architecture. In response, the company's CTO, Ms. Maya Suhendra, has approached your cybersecurity consultancy to conduct a comprehensive security audit of their systems. You are tasked with performing penetration testing on their web application, evaluating the network architecture, and presenting a detailed report. The report must include:

1. **Findings**: A summary of vulnerabilities discovered during the testing process.
2. **Mitigation Plan**: Specific technical measures to address these vulnerabilities.
3. **Policy Recommendation**: A long-term strategy and a cybersecurity policy that ShopEase Indonesia should adopt to minimize risks.

Vulnerability assessment is the way to find weaknesses in a system that helps security professionals plan their protection and attack countermeasure strategies. It needs to be carefully managed for its resources, to ensure the highest performance and operational efficiency. In this assignment, you are required to do a ***vulnerability assessment*** on a given operating system in a virtual environment. You must design the standard procedure for scanning along with the use of a proper tool to identify the vulnerabilities of the given operating system.

Deliverables for Task 1:

You are required to work on the given ***VMware*** file to plan the strategies in the group and scan the file to identify the current vulnerabilities in the file. **After the scanning, you are supposed to take this section individually**. Your tasks are defined as follows:

1- Proposed scanning method (vulnerability assessment methodology) and justify on a selected tool for Vulnerability Scanning for victim machine ***(Windows Server 2008.vm)***.

2- Identify any **THREE (3)** vulnerabilities and briefly explain them. (Each member only **ONE** Vulnerability)

Task 2: Risk Analysis and Policy Formulation (Individual)

This section carries **30%** of the total in course marks. Based on your findings in Part 1, you are now required to design a risk assessment plan and formulate policies to prevent such attack from happening in the future. For the risk assessment plan, you should **design a Risk Assessment Process** by following but **not limited** to the steps below:

Subsequently, **formulate a policy** to prevent such incident/attack from taking place. Your policy could include prevention, mitigation and necessary measures to be taken into consideration when such an incident occurs.

Deliverables for Task 2:

1. Justify and perform the Risk assessment methodology on the selected vulnerability.
2. Formulation of policy in mitigating/preventing the selected vulnerability.

Section B Lab Portfolio (CLO3)

This section is a lab practical portfolio on the following areas below which carries **40%** of the assignment. Each student should **attempt all 4 areas** using the virtual machines given in launching the following attacks following a **proper methodology**. You are free to chose any tools to perform the following and should be launched in a contained environment.

1. Password / Rainbow Table Attacks in Depth
2. Web Application Attack (**Not** to be launched on an actual site)
3. SQL Injection
4. Microsoft Windows Post Exploitation

***WARNING*: DO NOT try the aforementioned tools or techniques on real systems! You should test and create your tutorials by using Isolated/Testbed environments such as VMWare, Metasploitable, DVWA, etc.)**

Guidelines for the Report

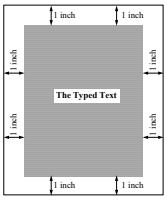
Document the results of your work professionally and systematically, in the form of a **computerized report**. **One (1**) softcopy and hardcopy of your documentation are to be submitted.

Your completed documentation should meet the following requirements:

1. Table of contents for every detailed chapter/section.
2. Introduction
3. Group Section
4. Individual Section 1
5. Individual Section 2
6. Individual Section 3
7. Conclusion
8. References
9. Appendices
10. Workload matrix

Submission requirements

1. Your report must be typed using Microsoft Word with Times New Roman font. You need use to **include a word count** at the end of the report (excluding title, source code of program & contents pages) Report should be in 1.5 spaces.
2. APA Referencing style should be used at all times adhering to the university policy.
3. The report has to be well presented and should be *typed*. Submission of reports that are *unprofessional* in its outlook (dirty, disorganized, inconsistent look, varying coloured paper and size) will not fair well when marks are allocated.
4. Ensure that the report is printed on standard A4 (210 X 297 mm) sized paper. Paperweight of 80 grams and above is highly recommended.
5. The report should have a one (1") margin all around the page as illustrated below:



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

7. **All** information, figures and diagrams obtained from external sources **must** be referenced using the APA referencing system accordingly.

MARKING SCHEME

42%	**Section A (Group / Individual** CLO2: Propose the implementation of vulnerability assessment and risk analysis for Digital Assets (A5,PLO9)		
7%	Introduction and Method (10)		
10.5%	Vulnerability Identification and Justification and Assessment of Selected Vulnerabilities (15)		
10.5%	Risk Assessment (15)		
10.5%	Policy Formulation (15)		
3.5%	Formatting and Referencing (5)		
	Total (60)		
28%	**Section B Lab Practical / Portfolio** CLO 3: Demonstrate ethical hacking and penetration testing activities using suitable tools and methodologies. (P5,PLO3)		
	Criteria	**Name:** **TP:**	**Name:** **TP:**
7%	Password/Rainbow Table Attacks in Depth (10)		
7%	Web Application Manipulation Tools (10)		
7%	SQL Injection (10)		
7%	Microsoft Windows Post Exploitation (10)		
	Total (40)		