FIT5003 Software Security Assignment 3 (S2 2024)

Total Marks 100

Please Check Moodle for the Due Date

1 Overview

The learning objective [illegible] you to perform penetration testing, thread modelling, and write ethics for hackin[illegible]oyed in Lab10 (Penetration Testing) can be utilized for this assignment.

2 Submission

You need to submit a report (one single PDF file) to describe what you have done and what you have observed with **screen shots** whenever necessary. Please follow the template of report wherever provided. Typeset your report into .pdf format (make sure it can be opened with Adobe Reader) and name it as the format: **[Your Name]-[Student ID]-FIT5003-Assignment.pdf**. Please do not submit any extra files, all screenshots or code (if applicable) should be embedded in the report.

Late submission penalty: Late submissions incur a 5-point deduction per day. For example, if you submit 2 days and 1 hour late, that incurs 15-point deduction. Submissions more than 7 days late will receive a zero mark. If you require extension or special consideration, refer to **special consideration form**. Kindly note that no member of the teaching team is authorized to grant extensions or special considerations. Therefore, refrain from seeking assistance on this matter from any teaching team member. Please adhere to the guidelines provided in the link mentioned.

Zero tolerance on plagiarism: If you are found cheating, penalties will be applied, i.e., a zero grade for the unit. University policies can be found at `https://www.monash.edu/students/academic/policies/academic-integrity`

For each question (Q1, Q2, and Section 5), a Generative AI statement must be included to indicate the extent of its use. This statement must specify whether Generative AI tools were employed in the response. If no AI tools were used, the statement should explicitly state that. Ensure a total of three statements, one for each designated section.

3 Penetration Testing [50 Marks]

The learning objective of this part is to learn the process of conducting a standard penetration test and subsequently compose a formal report detailing the identified vulnerabilities. The examination will be executed on virtual machines deliberately designed to be vulnerable, publicly accessible for educational purposes. You may leverage walkthroughs created by other testers as reference material; however, direct replication of text or screenshots from these walkthroughs is strictly prohibited. While utilizing a walkthrough for guidance is permitted, the report should be an original composition. External resources, beyond the provided walkthrough, can be consulted and referenced appropriately. It is important to note that the penetration test report will be checked for plagiarism through Turnitin.

Download one of the below Virtual Machines (VMs) and perform penetration test on it. The goal of the test is to make an attempt to compromise the VM.

- **HACKINOS: 1** (https://www.vulnhub.com/entry/hackinos-1,295/)
- **CENGBOX: 1** (https://www.vulnhub.com/entry/cengbox-1,475/)
- **BASIC PENTESTING: 1** (https://www.vulnhub.com/entry/basic-pentesting-1,216/)
- **DEATHNOTE:** .com/entry/deathnote-1,739/)

Q1 (50 marks): Ide bilities in the selected Virtual Machine and write a report. The report should b at:

Executive Summa 0 Marks)
{Briefly explain the penetration testing results, e.g. was the goal achieved? if yes, how? you can also provide high-level recommendations here. }

Vulnerability List (Max 200 Words) - 14 Marks)
{Create a table with columns: Vulnerability Name, Severity and Page No.} (Utilize CVSS3.0 calculator for calculating the severity of the issue)

Details of Vulnerabilities
Chosen three vulnerabilities should be written in the following format - (36 Marks)

{Severity} (e.g. High)	{Vulnerability Name e.g. SQL Injection}
Vulnerability	{Describe the vulnerability, exploit it and write step by step guide on how to reproduce the exploitation with screenshots} (Max 400 Words)
References	{add references here, for further reading, e.g. Heap Overflow}
Risk	{Explain risk here} (Max 200 Workds)
Recommendation	{Make theoratical recommendations here} (Max 200 Words)

4 Threat Modelling [36 Marks]

A pharmaceutical company has developed a system to diagnose an illness using a wearable device and machine learning (ML) models. Diagnosis tests are performed by clinicians using a mobile application and the patients are asked to do certain activities while wearing the devices. The motions captured from the wearable devices are sent to a mobile app via Bluetooth and then sent to a cloud API for processing over internet.

The cloud API collect the data and process them using ML models. The result reports processed by ML models are saved in a database in the cloud. The clinicians can pull the reports from the cloud API and view them using the same mobile app.

Q2 (30 Marks): To complete threat modelling of above scenario, perform the following:

- Draw a DFD (it can be second or a third level DFD) for the above system and identify the trust boundaries. (10 Marks)
- Identify at-lea an Information Disclosure threat, and suggest mitigation strategies for 2 Marks)
- Add the mitig D. (8 Marks)

5 Ethics in Hac

Developing an Ethical Hacking Policy is essential. Your task is to communicate guidelines to ethical hackers in your company (fictitious) regarding appropriate hacking conduct, prohibited activities, and behaviors classified as unethical. List a minimum of five policy directives. Kindly ensure your response falls within the 150 to 500 word limit.

6 Report Completion and Quality of Presentation [10 Marks]

The remaining 10 marks are allocated to the quality and clarity of the report.