School of Computing & Information Technology

CSCI262 System Security
SIM-2025-S4

Assignment 2 (12 marks, worth 12%)

Due date: November 13, 2025 9:00 pm Singapore time.

Make sure you include referencing for answers where it would obviously be needed.

1. You have two puzzles with parameters as follows:

   Puzzle A: One sub–puzzles. $k = 8$.

   Puzzle B: Eight sub-puzzles. $k = 4$.

   You should provide, for both cases other than part (b), the following:

   (a) The distribution of the number of cases that require each number of hashes. **(1.0 Mark)**

   (b) Explain the method you used to obtain your distributions. Don't go into too many details or show working, it's more "I wrote a C++ program to ... and then using ... I ...". **(0.5 Mark)**

   (c) A graph of the distribution of the data above. **(0.5 Mark)**

   (d) The average number of hashes needed. **(0.5 Mark)**

   (e) The standard deviation for the distribution of the number of hashes needed. **(0.5 Mark)**

   You should assume that if there are N possible solutions you check the N^{th} by hashing even if all others have failed and there has to be a solution.

2. Both Intrusion Detection Systems (IDS) and Deception Technologies (like honeypots) aim to identify malicious activity, but they operate on fundamentally different principles.

   - **Part A:** Compare the primary operational paradigm of a signature-based Network IDS (NIDS) with that of a low-interaction honeypot. How does each one "wait" for and then detect an attacker? **(1.0 Mark)**

   - **Part B:** A system administrator argues, "A well-configured IDS is all you need; honeypots are a waste of resources." Critique this statement. Under what scenarios would a honeypot provide intelligence that an IDS fundamentally cannot? (Discuss at least two distinct scenarios). **(1.0 Mark)**

   - **Part C:** Explain the concept of a "honeytoken." Provide a specific, concrete example of a honeytoken that could be deployed on a corporate network and describe what a "hit" on this token would reveal about an insider threat. **(1.0 Mark)**

3. This exercise explores how artificial intelligence can enable malware to adapt its behavior dynamically and how AI-driven defense systems counteract such threats. Students are expected to model, explain, and discuss the propagation and counteraction of an AI-enhanced malware (M) and its AI-based defender (D).

   Part A: Modelling the Spread of AI Malware M

   At $t = 0$, one system is infected by malware M. Every hour, each infected system uses reinforcement learning to improve its spreading strategy. Consequently, its infection rate grows by 10% every two hours. Construct a table for $t = 0\ to\ 12$ showing the number of infected systems each hour.

   (1.0 Mark)

   Part B: Deployment of Adaptive Defense D

   At $t = 6$, the defender AI D is deployed. D initially neutralizes one infected system per hour but learns to double its neutralization rate every 3 hours ($t = 9,\ t = 12,$ etc.). Construct a table showing both M and D populations from $t = 6\ to\ t = 15$ and identify when (if ever) D fully neutralizes M.

   (1.0 Mark)

   Part C: Pattern Analysis and Discussion

   Discuss how the presence of adaptive learning on both sides (M and D) affects the overall dynamics of cyber defense. How might AI escalation cycles occur in real-world cybersecurity?

   (0.6 Mark)

Part D: Visual Representation

Create a line graph showing both the infection and neutralization trends. Clearly label where M growth slows and where D surpasses M.

(0.4 Mark)

4. A core challenge in security is defining and enforcing "who can access what." Discretionary Access Control (DAC) and Mandatory Access Control (MAC) represent two classic models for solving this problem.

   Part A: Explain the fundamental difference between DAC and MAC, focusing on who or what is the ultimate authority that grants access to an object.

   (1.0 Mark)

   Part B: Describe a specific real-world scenario (e.g., in military, healthcare, or corporate R&D) where a DAC model like Unix file permissions would be insufficient or dangerous. Justify why MAC is necessary in this case.

   (1.0 Mark)

   Part C: The "Principle of Least Privilege" is a universal security goal. Compare how this principle is typically implemented and enforced in a DAC system versus a MAC system like SELinux or Windows Mandatory Integrity Control.

   (1.0 Mark)

Notes on submission

1. Submission is via Moodle.
2. Late submissions will be marked with a 25% deduction for each day, including days over the weekend.
3. Submissions more than three days late will not be marked unless an extension has been granted.
4. If you need an extension, apply through SOLS before the assignment deadline.
5. Plagiarism is treated seriously. Students involved will receive zero.