Computer Security - Assignment 4

Real-World Physical Security Breach Analysis (30 points)

The goal of this assignment is to help you understand how physical security failures occur in real-world scenarios, and how such failures can lead to serious consequences. You are required to research and analyze **at least three** real-world physical security breach incidents. Examples include (but are not limited to): Data center intrusion, ATM physical attacks, Office tailgating. For each case, you must clearly describe:

- Attack Process
  - How the attack was carried out
  - What vulnerabilities were exploited
  - Whether social engineering or insider access was involved
- Consequences
  - What damage or impact was caused, e.g., Financial loss, Data leakage, Service disruption.
  - Who was affected
- Propose practical and realistic countermeasures. Your suggestions should address:
  - Preventive controls
  - Detective controls
  - Deterrent controls

Please notice that focus on real-world cases, not hypothetical scenarios. Clear explanation and logical reasoning are expected.

Vulnerabilities in Operating System (20 points)

Choose **one operating system** (e.g., Windows, Linux, or macOS), and investigate **two CVE vulnerabilities published** on https://www.cvedetails.com/top-50-products.php. For each vulnerability, briefly describe what the vulnerability is, how it works, and what potential damage or impact it may cause if exploited. You should base your analysis on information from the CVE database or other reliable sources. Please use your own words (no copy-paste) and include links or references to the CVE entries.

MD5 Collision Attack Lab (50 points)

This assignment is based on the **SEED Labs MD5 Collision Attack Lab** (https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_MD5_Collision/) .

You are required to carefully read the official lab instructions and complete the assigned tasks.

Required Tasks

You must complete the following tasks:

Task 1: Generate MD5 Collisions

- Use the provided tool (`md5collgen`) to generate two different files with the same MD5 hash
- Verify:
    - The files are different
    - The MD5 hashes are identical
- Analyze the differences between the two files

Task 2: Understand MD5 Properties

- Study how MD5 processes data in 64-byte blocks
- Explain:
    - How MD5 computes hash values iteratively
    - Why collision can be extended with additional data (suffix)

Task 3: Create Colliding Programs

- Construct two executable programs
    - Same MD5 hash
    - Different behaviors/output
- Demonstrate and explain how the attack works

Submission Requirements

Your report must include:

1. **Screenshots**

- Screenshots must include: Your terminal output and key steps of the experiment.
- Each screenshot must contain a watermark, handwritten note, or unique identifier. This is required to prove that the work is your own.

2. **Analysis and Explanation**

You must clearly explain: How each task is performed; Key commands and their purposes; Observations and insights.

Important Note

This is the third time a SEED Lab assignment has been given. **No excuses will be accepted** for issues such as: Virtual machine not working; Environment setup problems; Computer crashes. You must submit whole assignment together. Partial submissions are NOT allowed. **Late submission of any part will be treated as late submission of the entire assignment.** If screenshots **do not meet verification requirements** (e.g., missing watermark/identifier), **50% of the total grade will be deducted**. If your report **lacks clear explanations, 50% of the total grade will be deducted**. This assignment will be subject to **plagiarism detection**. Any form of academic dishonesty will be handled according to course policies.