Computer Security - Assignment 1

1. Question 1 (25 Points)

Select a **security incident from January 2025** in which a malicious actor was involved (there are many to choose from). Your task is to **summarize what happened in** the incident and analyze it through the lens of core security principles.

Your write-up should include the following elements:

1. **A clear description of the incident** — what occurred, who was targeted, and what impact the event had.
2. For each of the **three primary security goals** — **confidentiality**, **integrity**, and **availability** — include:
    - A statement about whether that goal was violated in this incident.
    - A brief explanation of how the violation occurred if it was indeed violated.
3. **An assessment of the attacker**:
    - What type of attacker you believe was responsible.
    - A reasonable **speculation about the attacker's motive**, supported by evidence or logical reasoning.
4. **Cite your information sources** — include at least one reliable reference where you found the details of the incident.

2. Question 2 (25 Points)

In this question, you will explore the **National Vulnerability Database (NVD)** to see how often security problems are discovered and how they are described: https://nvd.nist.gov/

Step 1: How Many Vulnerabilities?

1. Go to the NVD website and open the list of **CVE vulnerabilities**.
2. Choose **one month from 2025** (you can use your birthday month if you like).
3. Find:
    - The **total number of vulnerabilities reported** in that month.
    - The **average number of vulnerabilities reported per day**.
4. Assume you spend **5 minutes reading each CVE**.
    - About **how many hours per week** would you spend reviewing vulnerabilities? Show your basic calculation.

Step 2: Looking at Individual CVEs

1. Click on **2–3 CVE entries** from your chosen month.
2. Briefly describe:
    - What kind of information a CVE page contains.
3. Do any of these CVEs involve **software you recognize or use** (such as Windows, macOS, Chrome,

Github, etc.)?

- If yes, give one example.
- If no, say so.

Step 3: Security Impact (Big Three)

1. For **one CVE you looked at**, answer:
   - Which of the **three security goals** might be affected? Explain your answer in **1–2 sentences**.
2. Finally, in your own words:
   - What is the **most important piece of information** on a CVE page that helps you decide whether it matters to you?

3. Question 3 (25 Points)

Consider the following **subjects** and **objects** in the **Bell–LaPadula security model**. Each subject has a security **clearance**, and each object has a security **classification**. The levels **C**, **S**, and **TS** represent **Classified**, **Secret**, and **Top Secret**, respectively, in increasing order of sensitivity.

Subject Clearances

- **Alice Chen**: (C, {RESEARCH})
- **Bob Martinez**: (S, {OPERATIONS})
- **Carol Nguyen**: (S, {RESEARCH})
- **Dr. Evelyn Park**: (TS, {RESEARCH, OPERATIONS})

Object Classifications

- **ResearchNotes**: (C, {RESEARCH})
- **ProjectPlans**: (S, {RESEARCH, OPERATIONS})
- **IncidentReports**: (TS, {OPERATIONS})

Questions

1. Using the Bell–LaPadula access control rules, construct an **access control matrix** showing which subjects are allowed to **read** and/or **write** each object.
   - Use **R** for read permission and **W** for write permission.
   - Include all subjects and all objects.
2. What **classification label** (security level and category set) could an object have so that **Dr. Park** is able to **write to it without restriction** under the Bell–LaPadula model?
3. Suppose Dr. Park wants to update the **ResearchNotes** object, which requires **write access**, but her current clearance does not allow this action.
   - Is there a way to enable this update **while still following Bell–LaPadula rules**?
   - Briefly explain how or why not.

4. Question 4 (25 Points)

The following questions relate to the **Secure Design Principles** discussed in class.

1. In the **Bell–LaPadula model**, access control can be refined using **compartments** and **need-to-know labels**.
    - Which **secure design principle** does this idea most closely relate to?
    - Briefly explain how compartments and need-to-know enforcement reflect this design principle.
2. In the 1800s, **Auguste Kerckhoffs** stated that the security of a cryptographic system should **not depend on keeping the algorithm secret**, but only on keeping the **key** secret. This idea is now known as **Kerckhoffs's Principle**.
    - Which **secure design principle** is this most closely related to?
    - Explain the connection between Kerckhoffs's Principle and that design principle in your own words.

5. SEEDLABS Setup

We will assign **2–4 experiments from the SEED Labs in later assignments**, so it is necessary to **set up the lab environment in advance**.
Although this is part of the Assignment 1, **it will not be graded**. However, **if you do not complete it, you will not be able to proceed with the subsequent assignments**, so it is strongly recommended that you complete it carefully.

For detailed setup instructions, please refer to
https://seedsecuritylabs.org/labsetup.html and https://github.com/seed-labs/seed-labs/blob/master/manuals/vm/seedvm-manual.md,
where comprehensive guidance is provided.

Please note the following:

- Although the platform provides a **cloud-based lab environment**, I strongly recommend that you **install VirtualBox locally** and **import the pre-built SEED Ubuntu 20.04 image** provided by the platform. Becoming proficient in configuring and using virtual machines is an essential skill for anyone studying security. In practice, **all security attacks should be learned and conducted in a virtual environment**.
- After installing and configuring the new virtual machine, please make sure that **file transfer between the host machine and the VM works properly**.
    - Click **Devices → Insert Guest Additions CD Image…**
    - Configure **Devices → Shared Folders** to enable folder sharing with the host machine.
    - You may encounter **permission issues when accessing the shared folder**. If so, use the following command to modify the folder permissions:

      ```
      sudo usermod -aG vboxsf $USER
      ```

      Then reset VM for the changes to take effect.