Computer Security - Assignment 5

Malware Deep Dive Research (30 Points)

Choose **one** type of malware from the following list: Virus, Worm, Trojan Horse, Rootkit, Backdoor, Botnet, Privacy-invasive software (spyware/adware), or Ransomware. Conduct an in-depth independent study of the selected malware type and write a tiny technical report that explains its internal working mechanisms, including how it typically infects a system, how it executes or persists once inside, and how it achieves its malicious goals such as data theft, disruption, control, or monetization. You are also required to include **at least one** real-world example of this malware type, describing how it was used in practice and what impact it caused, as well as discuss common defense techniques used to detect or mitigate it in modern operating systems or networked environments. You should write in your own words. Your answer should be approximately 300–500 words.

Reflection on the Future of Cybersecurity (20 Points)

As this course is coming to an end, we have studied many foundational concepts in computer security. Many of these ideas have remained relevant for decades and continue to form the basis of modern cybersecurity practice. Looking forward, the field of security is likely to undergo significant transformation. While quantum computing is often discussed as a long-term disruptive force, we are already witnessing a different and more immediate shift with the rapid rise of AI systems.

This raises important questions about the future of cybersecurity: How will AI change the way we defend systems and the way attackers operate? Can traditional security principles still hold in AI-driven environments? And perhaps more importantly, how should we rethink “security” when systems themselves begin to learn, generate, and adapt?

In this assignment, you are asked to reflect deeply on these questions. You may focus on a specific topic (for example, AI-assisted vulnerability discovery, malware generation using LLMs, AI-based intrusion detection), or you may take a broader perspective on the relationship between AI and cybersecurity.

There is no single correct answer. You are encouraged to express your own thoughts, doubts, or even uncertainties. However, your reflection should demonstrate genuine reasoning based on what you have learned in this course. **Superficial or fully AI-generated responses that do not reflect personal thinking will receive no credit for this section.** Your answer should be approximately 200–500 words.

SQL Injection Attack Lab (50 points)

This assignment is based on the **SQL Injection Attack Lab** (https://seedsecuritylabs.org/Labs_20.04/Web/Web_SQL_Injection/) .

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

Required Tasks

You must complete the following tasks:

Task 0: Lab Environment Set Up

Follow the official SEED Lab instructions to start the containerized web application and familiarize yourself with it.

Task 1: Get Familiar with SQL Statements

This step is very simple; you just need to run the instructions provided.

Task 2: SQL Injection Attack on SELECT Statement

- Task 2.1: Consider how the input is inserted into the SQL statement, inject a payload that changes SQL logic.
- Task 2.1: The instructions already indicate how to encode special characters; continue using the code you injected in the previous step, but apply the encoded format.
- Task 2.3: For this step, you just need to follow the instructions. However, you need to think about your findings.

Task 3: SQL Injection Attack on SELECT Statement

- Task 3.1: Now you need to attempt an injection on the Edit Profile page; you already know that the salary attribute name in SQL is `salary`.
- Task 3.2: The method is similar to that in Section 3.1, but you need to take into account an additional attribute value `Boby`.
- Task 3.3: In the database, the hash of password is stored, so if you have to modify the database with new generated hash value.

Additional Tips for Setting Up the Web Application

1. **Do NOT unzip `Labsetup.zip` inside a shared folder.**
   This can cause unexpected permission issues that may lead to hard-to-debug errors.
2. **Check MySQL status after building the container.**
   After running `dcbuild`, carefully inspect the logs to see whether MySQL starts correctly. In particular, look for any errors or messages containing *"denied"* or *"failed"*. If such issues exist, the client will not be able to connect properly.

   To fix permission-related problems, run the following commands:

   ```
   cd Labsetup
   sudo chmod -R 755 .
   ```

   Then restart the database with:

   ```
   dcdown
   sudo rm -rf mysql_data
   dcbuild
   dcup
   ```

3. **Don't forget to update your `/etc/hosts` file.**
   Add the following mapping as instructed:

   ```
   10.9.0.5    www.seed-server.com
   ```

Important Note

This is the last 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.