Module 6: Case Study: System Hacking

Problem Statement:

In a corporate environment, an organization has experienced a breach of confidential information due to lax security practices. The organization needs a comprehensive assessment and improvement of its security posture, including identifying vulnerabilities, assessing password strength, examining potential data exfiltration techniques, and ensuring user privacy through secure data erasure. Your task is to perform a series of security assessments and provide recommendations for enhancing the organization's cybersecurity measures.

Objective:

The objective of this assignment is to explore various tools and techniques commonly used in system hacking and security assessments. Students will learn how to identify vulnerabilities, perform system enumeration, extract sensitive information, and execute ethical hacking activities in a controlled lab environment.

Tasks to be Performed:

1. Demonstrate how Responder can be used to perform SMB, HTTP, and other service poisoning attacks. Capture NTLMv2 hashes and clear-text passwords from network traffic.

2. Use the reverse_tcp module to exploit a known vulnerability in a target system. Show how to create a payload, deliver it, and establish a reverse shell session.

3. Perform password auditing and cracking using L0phtCrack to assess the strength of passwords. Emphasize the importance of strong password policies.

4. Explore steganography by hiding data within image files using Openstego and Steghide. Demonstrate how this technique can be used to exfiltrate sensitive information covertly.

5. Show how Privacy Eraser can be used to securely erase traces of online and offline activities to maintain privacy.

Note: Ensure that you have proper authorization to perform network enumeration on the chosen target. Always follow ethical and legal guidelines when conducting security assessments. The target could be any authorized domain or any of the domains from the below list:

1. www.certifiedhacker.com
2. www.moviescope.com (Accessible only in Lab Setup)
3. www.goodshopping.com (Accessible only in Lab Setup)
4. Testphp.vulnweb.com
5. Machine IP from your Lab Setup