Mr. Robot CTF Write-Up

Introduction

The “Mr. Robot” CTF challenge on TryHackMe is inspired by the popular TV show "Mr. Robot" and involves a series of tasks to explore and exploit vulnerabilities in a simulated environment. The challenge is designed to test your skills in enumeration, exploitation, and privilege escalation.

Task 1: Enumeration

Objective

Discover open ports and services running on the target machine.

Solution

Port Scanning: I used nmap to perform a port scan on the target machine.

Command:

```
nmap -sC -sV -oN nmap_initial.txt <TARGET_IP>
```

-sC: Runs default scripts.
-sV: Detects service versions.
-oN: Saves the output to a file.

Results: The scan revealed the following open ports:

22/tcp - SSH
80/tcp - HTTP

Task 2: Web Application Enumeration

Objective

Find vulnerabilities in the web application running on port 80.

Solution

Web Directory Enumeration: Used gobuster to enumerate directories.

Command:

```
gobuster dir -u http://<TARGET_IP> -w /usr/share/wordlists/dirb/common.txt -o gobuster.txt
```

Discovered a directory /admin with restricted access.

Directory Analysis: Accessed http://<TARGET_IP>/admin and found a login page.

Task 3: Exploiting the Login Page

Objective

Bypass the login page to gain access.

Solution

SQL Injection: Attempted SQL injection on the login form. Using the classic ' OR '1'='1 payload to bypass authentication.

Successful Login: The payload allowed access to the admin panel, where additional information could be found.

Task 4: Privilege Escalation

Objective

Gain root access to the target machine.

Solution

SSH Access: From the admin panel, found SSH credentials (user:robot, pass:toor).

SSH into the Machine: Used the credentials to SSH into the machine.

Command:

```
ssh robot@<TARGET_IP>
```

Privilege Escalation: Once logged in as robot, found a sudo misconfiguration allowing robot to execute commands as root without a password.

Command:

```
sudo -l
```

Output indicated the ability to run /bin/bash as root.

Root Access: Escalated to root by running:

Command:

```
sudo /bin/bash
```

Successfully obtained root access.

Conclusion

The “Mr. Robot” CTF was successfully completed by following a structured approach to enumeration, exploitation, and privilege escalation. Key steps included port scanning, web directory enumeration, exploiting a SQL injection vulnerability, and leveraging a sudo misconfiguration for privilege escalation.