CACHE

Comienzo comprobando que la máquina está activa y tengo conectividad, después enumero los puertos abiertos:

```
ping -c1 10.10.10.188
nmap -Pn -p- --open -T5 -v -n 10.10.10.188 -oG allPorts
```

```
[x@XmaXinE ~/SEC/htb/cache]$ ping -c1 10.10.10.188
PING 10.10.10.188 (10.10.10.188) 56(84) bytes of data.
64 bytes from 10.10.10.188: icmp_seq=1 ttl=63 time=53.5 ms

--- 10.10.10.188 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 53.548/53.548/53.548/0.000 ms
[x@XmaXinE ~/SEC/htb/cache]$ nmap -Pn -p- --open -T5 -v -n 10.10.10.188 -oG allPorts
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-07 04:03 CEST
Initiating Connect Scan at 04:03
Scanning 10.10.10.188 [65535 ports]
Discovered open port 80/tcp on 10.10.10.188
Discovered open port 22/tcp on 10.10.10.188
Completed Connect Scan at 04:04, 28.46s elapsed (65535 total ports)
Nmap scan report for 10.10.10.188
Host is up (0.056s latency).
Not shown: 45282 filtered ports, 20251 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 28.50 seconds
```

Con la función extractPorts copio los puertos abiertos para detectar versiones de los servicios:

```
extractPorts allPorts
nmap -Pn -sC -sV -p 22,80 10.10.10.188 -oN targeted
```

```
[x@XmaXinE ~/SEC/htb/cache]$ extractPorts allPorts

[*] Extracting information...

        [*] IP Address: 10.10.10.188
        [*] Open ports: 22,80

[*] Ports copied to clipboard

'extractPorts.tmp' borrado
[x@XmaXinE ~/SEC/htb/cache]$ nmap -Pn -sC -sV -p 22,80 10.10.10.188 -oN targeted
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-07 04:26 CEST
Nmap scan report for 10.10.10.188
Host is up (0.053s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a9:2d:b2:a0:c4:57:e7:7c:35:2d:45:4d:db:80:8c:f1 (RSA)
|   256 bc:e4:16:3d:2a:59:a1:3a:6a:09:28:dd:36:10:38:08 (ECDSA)
|_  256 57:d5:47:ee:07:ca:3a:c0:fd:9b:a8:7f:6b:4c:9d:7c (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Cache
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 8.61 seconds
```

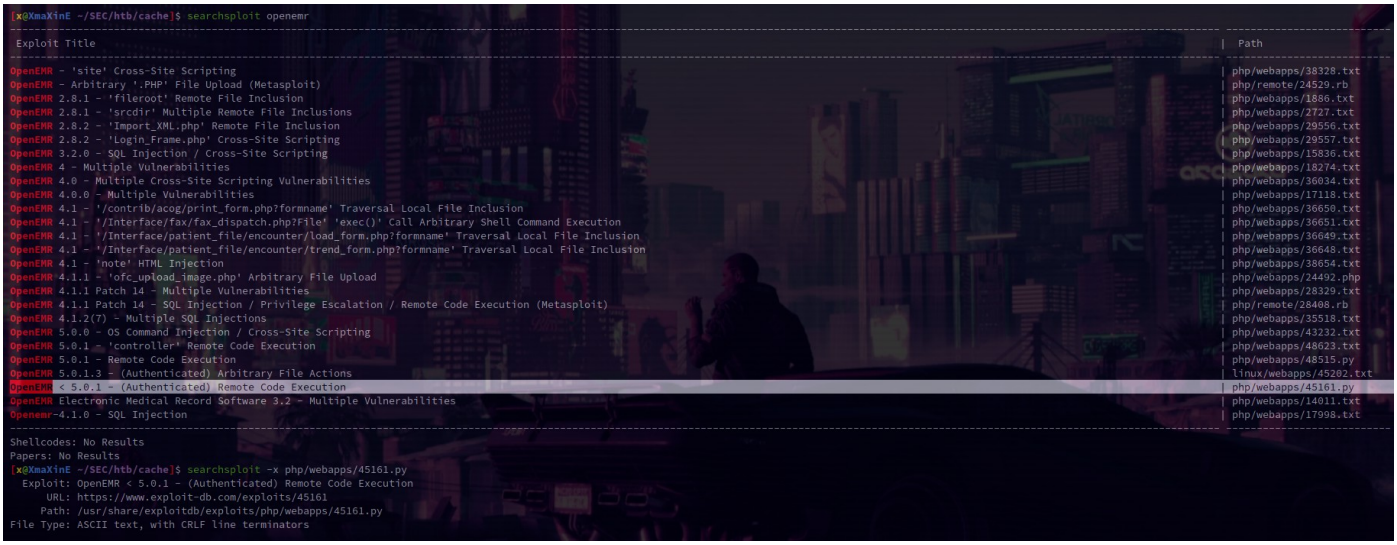
Navego por el servicio web y no encuentro nada sospechoso, lanzo un fuzeo rápido y tres páginas me llaman la atención:

```
ffuf -c -w /home/x/.local/src/SecLists/Discovery/Web-Content/common.txt -e .txt,.html,.php -u http://10.10.10.188
/FUZZ
```

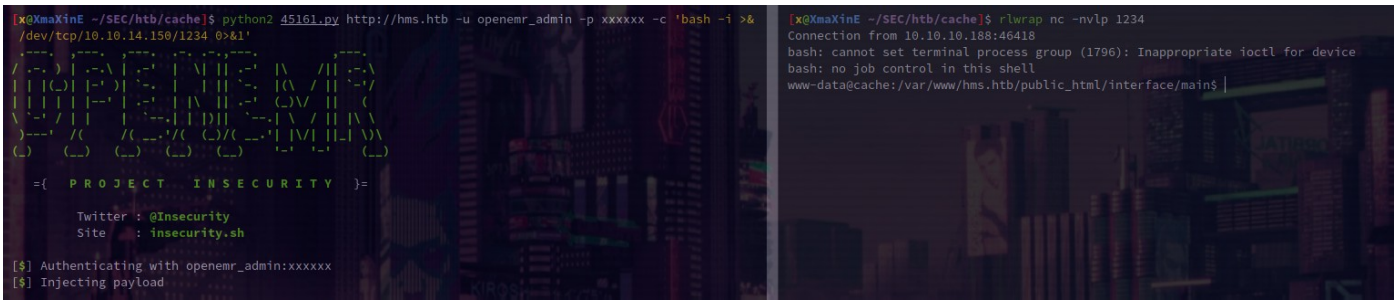
```
[x@XmaXinE ~/SEC/htb/cache]$ ffuf -c -w /home/x/.local/src/SecLists/Discovery/Web-Content/common.txt -e .txt,.html,.php -u http://10.10.10.188/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.1.0-git
------------------------------------------------

 :: Method           : GET
 :: URL              : http://10.10.10.188/FUZZ
 :: Wordlist         : FUZZ: /home/x/.local/src/SecLists/Discovery/Web-Content/common.txt
 :: Extensions       : .txt .html .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
------------------------------------------------

.hta.php                [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta.html               [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta.txt                [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.html          [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.txt           [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.txt           [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd.html          [Status: 403, Size: 277, Words: 20, Lines: 10]
author.html             [Status: 200, Size: 1522, Words: 180, Lines: 68]
contactus.html          [Status: 200, Size: 2539, Words: 283, Lines: 148]
index.html              [Status: 200, Size: 8193, Words: 902, Lines: 339]
index.html              [Status: 200, Size: 8193, Words: 902, Lines: 339]
javascript              [Status: 301, Size: 317, Words: 20, Lines: 10]
jquery                  [Status: 301, Size: 313, Words: 20, Lines: 10]
login.html              [Status: 200, Size: 2421, Words: 389, Lines: 106]
net.html                [Status: 200, Size: 290, Words: 23, Lines: 19]
news.html               [Status: 200, Size: 7231, Words: 948, Lines: 100]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10]
:: Progress: [18608/18608] :: Job [1/1] :: 715 req/sec :: Duration: [0:00:26] :: Errors: 0 ::
```

javascript/ me devuelve 301, jquery/ tiene el archivo "functionality.js" que contiene las credenciales "ash - H@v3_fun". Me logueo en login.html pero no consigo nada. Haciendo un diccionario con cewl de una página del servidor y escaneando virtual hosts se da con el dominio hms.htb (lol). Añado el nombre a /etc/hosts y al acceder me encuentro con una página de login de openEMR, pruebo las credenciales anteriores sin suerte.

Busco exploits para este servicio y uno me llama la atención:



El exploit para la versión más alta es un RCE, en el exploit hay un enlace a un vídeo , siguiendo los pasos ya tengo shell como www-data:



Enumerando encuentro un servicio escuchando en el puerto 11211, parece ser memcrashed, investigando encuentro esta página[1] que explica cómo dumpear los datos del servicio, con esto conseguimos las credenciales "luffy - 0n3_p1ec3".

Sigo enumerando y veo que luffy pertenece al grupo docker, tengo algo de experiencia con docker y sé que esto es lo mismo que ser root

```
groups
docker run -v /:/mnt --rm -it ubuntu chroot /mnt sh
```

[1] https://www.hackingarticles.in/penetration-testing-on-memcached-server/