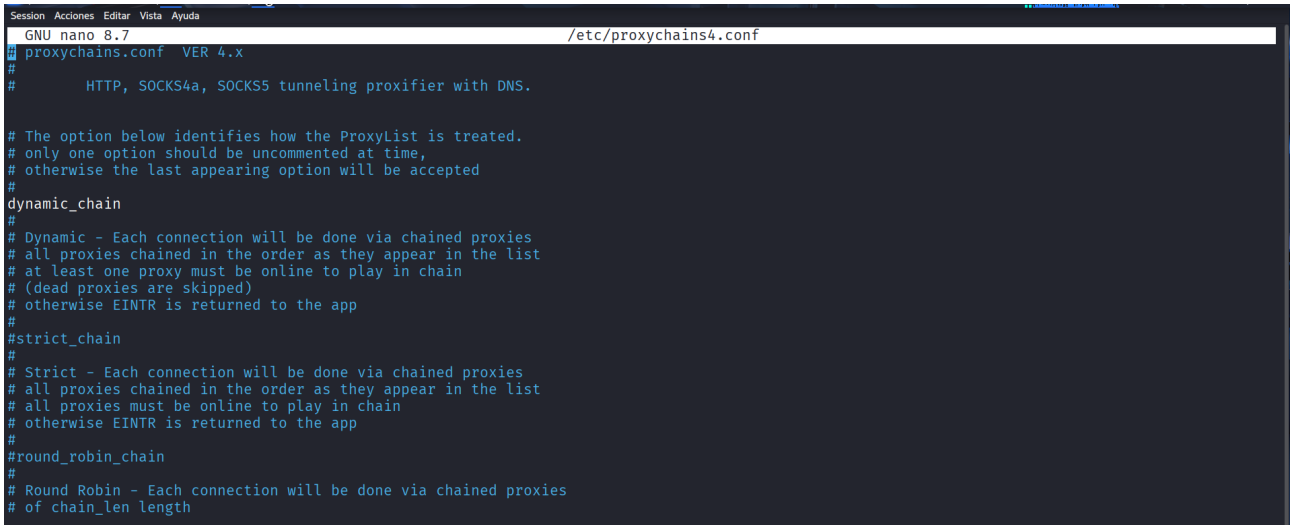
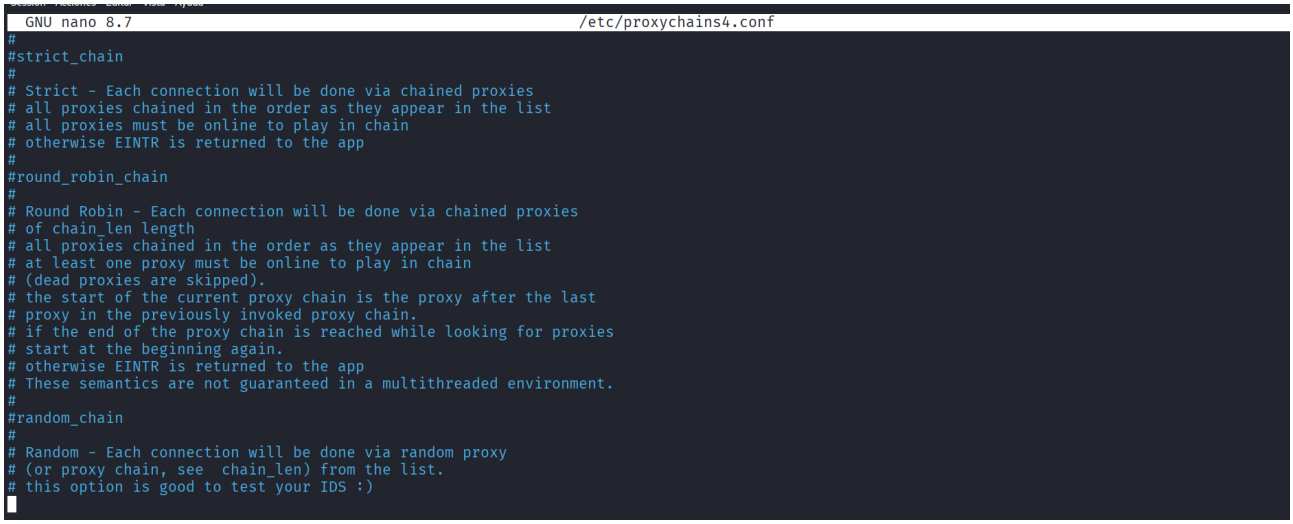
Martin
Dalla Pozza

Ejercicio Proxychains Tor

Se utiliza nano para editar y modificar los archivos de configuracion

nano /etc/proxychains4.conf





Es el archivo de configuración principal de ProxyChains v4, una herramienta que

fuerza a las aplicaciones a usar proxies (SOCKS4, SOCKS5, HTTP) incluso si dichas aplicaciones no fueron diseñadas para hacerlo.

En conjunto, el comando abre el archivo de configuracion de ProxyChains para su edicion.

¿Para que sirve ProxyChains?

ProxyChains se utiliza para redirigir el trafico de red de aplicaciones a traves de uno o varios servidores proxy.

Es comun en:

Anonimato y privacidad

Pruebas de penetración (pentesting)

Bypass de restricciones de red

Enrutamiento del tráfico a traves de Tor

¿Que se configura dentro de proxychains4.conf?

El archivo contiene varias secciones importantes:

Modo de encadenamiento de proxies

Define como se usan los proxies:

dynamic_chain
Usa los proxies disponibles en orden; si uno falla, continúa con el siguiente.

strict_chain
Obliga a usar todos los proxies en el orden definido. Si uno falla, la conexión falla.

random_chain
Selecciona proxies aleatoriamente.

Solo uno debe estar activo (sin # al inicio).

Resolucion DNS a traves del proxy:

Opciones clave:

proxy_dns
Evita fugas DNS resolviendo nombres de dominio a través del proxy.

remote_dns_subnet
Define el rango IP usado internamente para DNS remoto.

Esto es critico para anonimato.

Listados de Proxy

Vamos utilizar socks5

SOCKS5 es la versión moderna y ampliamente utilizada.

[ProxyList]
add proxy here ...

meanwile

defaults set to "tor"

socks5 127.0.0.1 9050

Ejemplo comun para Tor:

127.0.0.1:9050 corresponde al servicio Tor local.

¿Cuando es necesario editar este archivo?

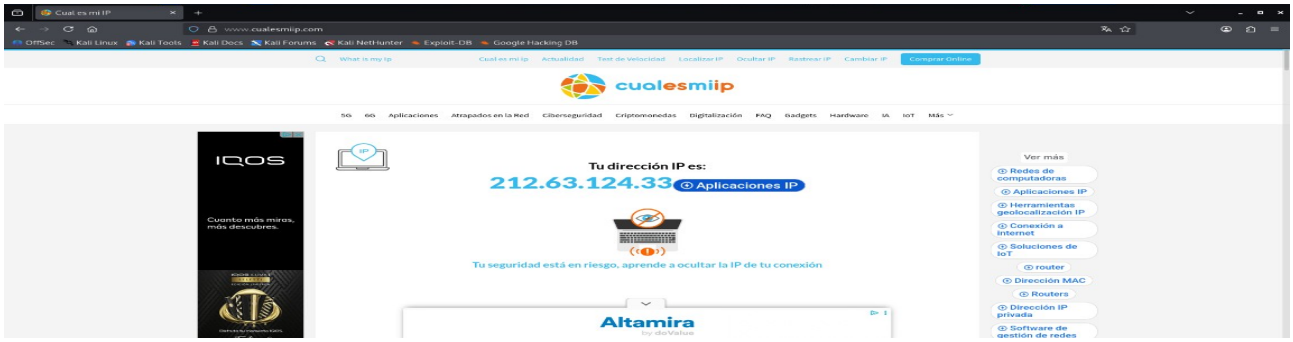
Se edita cuando:

Se agregan o cambian proxies

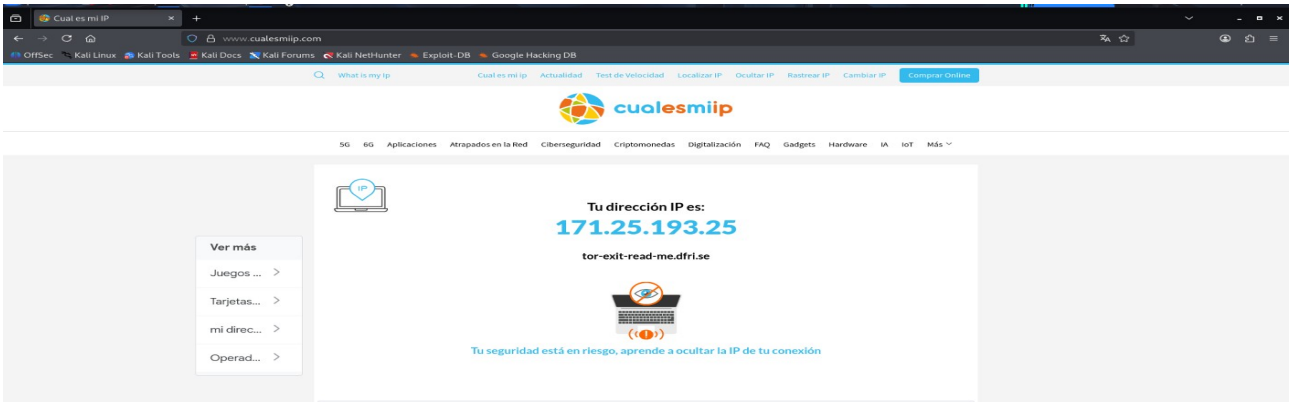
Se configura Tor

Se ajusta el comportamiento del encadenamiento

Se mejora la privacidad (DNS, timeouts)




```
┌──(kali㉿kali)-[~]
└─$ service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
     Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)
     Active: active (exited) since Mon 2025-12-15 13:38:19 CET; 15s ago
 Invocation: 7b4ed5b1a56345d3ba6a9df463ca321c
    Process: 53255 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 53255 (code=exited, status=0/SUCCESS)
   Mem peak: 2M
        CPU: 23ms
```



Si ejecutamos Firefox la IP es 212.63.124.33
Si ejecutamos Proxychains Firefox la IP es 171.25.193.25
Tener en cuenta que el estado del Servicio de Tor debe estar activo