

**Martin**

**Dalla Pozza**

**Ejercicio Proxychains Tor**

Se utiliza nano para editar y modificar los archivos de configuracion

***nano /etc/proxychains4.conf***

```
Session Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ nano /etc/proxychains4.conf
```

```
Session Acciones Editar Vista Ayuda
GNU nano 8.7 /etc/proxychains4.conf
# proxychains.conf  VER 4.x
#
# HTTP, SOCKS4a, SOCKS5 tunneling proxyifier with DNS.
#
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#round_robin_chain
#
# Round Robin - Each connection will be done via chained proxies
# of chain_len length
```

```
Session Acciones Editar Vista Ayuda
GNU nano 8.7 /etc/proxychains4.conf
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#round_robin_chain
#
# Round Robin - Each connection will be done via chained proxies
# of chain_len length
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped).
# the start of the current proxy chain is the proxy after the last
# proxy in the previously invoked proxy chain.
# if the end of the proxy chain is reached while looking for proxies
# start at the beginning again.
# otherwise EINTR is returned to the app
# These semantics are not guaranteed in a multithreaded environment.
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see chain_len) from the list.
# this option is good to test your IDS :)
```

```

GNU nano 8.7 /etc/proxychains4.conf
# dnat 1.1.1.1 1.1.1.2

# ProxyList format
#   type ip port [user pass]
#   (values separated by 'tab' or 'blank')
#
#   only numeric ipv4 addresses are valid
#
#   Examples:
#
#       socks5 192.168.67.78 1080 lamer secret
#       http 192.168.89.3 8080 justu hidden
#       socks4 192.168.1.49 1080
#       http 192.168.39.93 8080
#
#   proxy types: http, socks4, socks5, raw
#   * raw: The traffic is simply forwarded to the proxy without modification.
#   ( auth types supported: "basic"-http "user/pass"-socks )
#
# [ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 9050

```

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 configuración de ProxyChains para su edición.

### ***¿Para que sirve ProxyChains?***

**ProxyChains** se utiliza para redirigir el tráfico de red de aplicaciones a través de uno o varios servidores proxy.

### ***Es común en:***

Anonimato y privacidad

Pruebas de penetración (pentesting)

Bypass de restricciones de red

Enrutamiento del tráfico a través 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 ...

# meanwhile

# 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

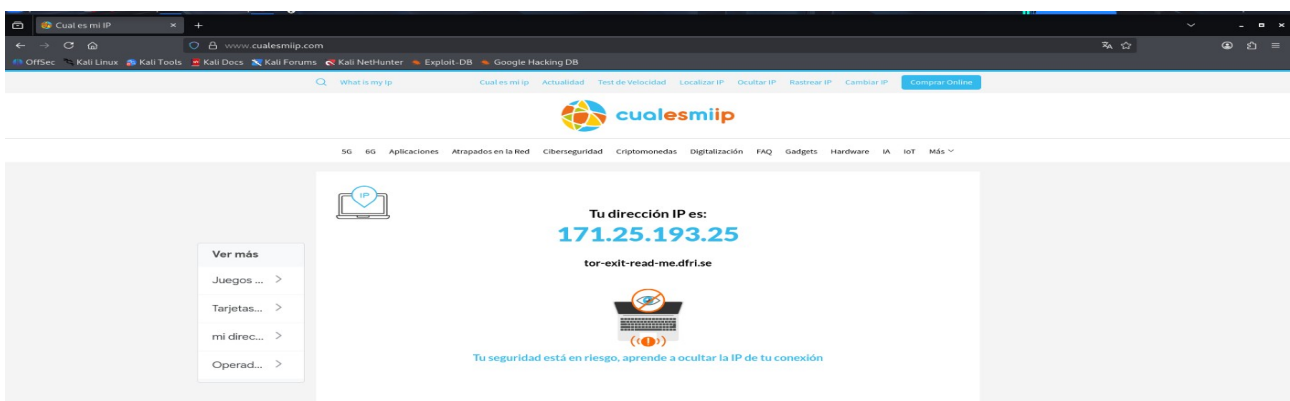
Se configura Tor

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**