

Martin

Dalla Pozza

Ejercicio Proxychains

```

(kali@kali)-[~]
└─$ sudo nano /etc/proxychains4.conf
[sudo] contraseña para kali:

(kali@kali)-[~]
└─$ proxychains4 curl ifconfig.me
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... ifconfig.me:80 ... OK

<html><head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<title>403 Forbidden</title>
</head>
<body text=#000000 bgcolor=#ffffff>
<h1>Error: Forbidden</h1>
<h2>Your client does not have permission to get URL <code></code> from this server.</h2>
<h2></h2>
</body></html>

(kali@kali)-[~]
└─$

(kali@kali)-[~]
└─$ proxychains4 curl ifconfig.co
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... ifconfig.co:80 ... OK
128.127.180.156

```

```

(kali@kali)-[~]
└─$ proxychains4 curl ifconfig.co
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... ifconfig.co:80 ... OK
128.127.180.156

(kali@kali)-[~]
└─$ curl ifconfig.co
212.63.124.33

(kali@kali)-[~]
└─$ proxychains firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17

(kali@kali)-[~]
└─$ proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17

```

```

(kali@kali)-[~]
└─$ systemctl status tor
● 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 Thu 2025-12-11 19:38:54 CET; 10min ago
 Invocation: f2799a0482944a9faec1a92d6f00a9a7
   Process: 2980 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 2980 (code=exited, status=0/SUCCESS)
     Mem peak: 2M
        CPU: 12ms

dic 11 19:38:54 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master)...
dic 11 19:38:54 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).

```

A continuacion tienes una explicacion clara, formal y completa de todos los comandos que ejecutaste, incluyendo lo que significan los resultados y por qué ves ciertos mensajes como el 403 Forbidden o el comportamiento de proxychains + firefox.

sudo nano /etc/proxychains4.conf:

Este comando abre el archivo de configuración principal de Proxychains con privilegios de administrador.

En este archivo defines:

El modo de encadenamiento (dynamic, strict, random).

Los proxies que usará (por defecto 127.0.0.1:9050 = Tor SOCKS5).

Opciones como proxy_dns.

proxychains4 curl ifconfig.me

Este comando envia curl a traves de Proxychains para consultar tu IP externa usando Tor.

Resultado:

403 Forbidden

Interpretacion:

El servicio ifconfig.me bloquea muchas peticiones provenientes de nodos Tor.

Por eso responde con 403 aunque el túnel Tor funciona correctamente.

El log muestra:

Dynamic chain ... 127.0.0.1:9050 ... OK

Esto confirma que Proxychains si esta enviando el tráfico a Tor.

proxychains4 curl ifconfig.co

Este servidor si acepta trafico desde Tor.

Resultado:

128.127.180.156

Esa IP no es tuya: es la IP de salida del nodo Tor.

Esto confirma que Proxychains + Tor funciona correctamente.

curl ifconfig.co (sin proxychains)

Resultado:

212.63.124.33

Esta sí es tu IP real (la del ISP, red local o VPS).

Esto te permite comparar:

Con proxychains Usas Tor Sale una IP distinta.

Sin proxychains Sale tu IP real.

proxychains firefox / proxychains4 firefox

El comando funciona, pero:

Firefox no imprime nada en terminal, solo muestra estos mensajes:

[proxychains] DLL init: proxychains-ng 4.17

Esto indica:

Proxychains está enganchando correctamente las bibliotecas de Firefox.

Firefox se abre, pero no ves logs de conexión en la terminal.

Para confirmar que Firefox está usando Tor, debes visitar:

<https://ifconfig.co>

<https://check.torproject.org>

Verificación del servicio Tor

Comando:

systemctl status tor

Salida:

Active: active (exited)

ExecStart=/bin/true

Esto es importante

Significa que:

El servicio principal tor.service no ejecuta Tor directamente.

Debian/Kali usan instancias por usuario llamadas:

tor@default.service

Por eso ves:

Main PID: 2980 (exited)

El servicio padre está activo pero no ejecuta Tor.

El Tor real está gestionado por instancias específicas.

Comprueballo:

systemctl status tor@default

Probablemente veras:

active (running)

Resumen:

Proxychains esta funcionando correctamente.

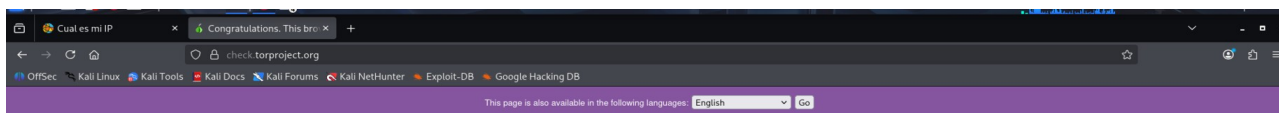
Tor esta funcionando, pero gestionado por tor@default

El error 403 es normal: ifconfig.me bloquea el trafico Tor.

Firefox no muestra logs, pero Proxychains está enganchado.

La diferencia entre IPs confirma que el tráfico pasa por Tor.

The screenshot shows a web browser window with the URL www.cualesmiip.com. The browser's address bar and tabs are visible at the top. The website's header includes a navigation menu with links like 'Cual es mi IP', 'Actualidad', 'Test de Velocidad', 'Localizar IP', 'Ocultar IP', 'Rastrear IP', 'Cambiar IP', and 'Comparar Online'. The main content area displays the IP address '128.127.180.156' in large blue text, with a 'Localizar IP' button next to it. Below the IP address, the domain 'balooga.behostings.net' is shown. A warning message states 'Tu seguridad está en riesgo, aprende a ocultar la IP de tu conexión'. The left sidebar contains a 'Ver más' section with links to 'Cursos ciberseguridad', 'Routers seguros', 'Software de privacidad', 'Dirección IP privada', 'VPN', 'Computadora', 'Conexión a internet', 'Antivirus software', 'Cambiar IP', and 'Operadores de redes'. The right sidebar features a 'Search for' section with a list of tools: 'CHECK MY PUBLIC IP', 'CHECK YOUR INTERNET SPEED', 'WHAT IS MY IP', 'CHECK MY INTERNET SPEED', 'VER TU ÁRBOL GENEALÓGICO', 'CHECK MY PHONE CARRIER', and 'FIND PERSON'. At the bottom, there are several advertisements for products like 'Nieuwe Laptop', 'Mode & Maison', and 'Terug naar School'.



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: 128.127.180.156

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Relay Search](#).

[Donate to Support Tor](#)

[Tor Forum](#) | [Volunteer](#) | [Run a Relay](#) | [Stay Anonymous](#)

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn More >](#)

JavaScript is enabled.

```
Session Acciones Editor Vista Ayuda
(kali@kali)-[~]
└─$ proxychains curl ifconfig.co
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... ifconfig.co:80 ... OK
128.127.180.156

(kali@kali)-[~]
└─$ curl ifconfig.co
212.63.124.33

(kali@kali)-[~]
└─$ sudo proxychains /usr/local/bin/noip2 -u -c /usr/local/etc/no-ip2.conf
[sudo] contraseña para kali:
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17

USAGE: noip2 [ -C [ -F ] [ -V ] [ -U #min ]
           [ -u username ] [ -p password ] [ -x progname ]
           [ -c file ] [ -d ] [ -D pid ] [ -i addr ] [ -S ] [ -M ] [ -h ]

Version Linux-2.1.9
Options: -C          create configuration data
          -F          force NAI off
          -Y          select all hosts/groups
          -U #minutes set update interval
          -u username use supplied username
          -p password use supplied password
          -x executable use supplied executable
          -c config_file use alternate data path
          -d          increase debug verbosity
          -D processID toggle debug flag for PID
          -i IPaddress use supplied address
          -I interface use supplied interface
          -S          show configuration data
          -M          permit multiple instances
          -K processID terminate instance PID
          -Z          activate sha dump code
          -h          help (this text)

(kali@kali)-[~]
└─$ nslookup midominio2022.ddns.net
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:   midominio2022.ddns.net
Address: 212.63.124.33
```

New customers get 15% off Enhanced or Pro Dynamic DNS, but hurry - this offer expires in 7 days! Use code **NEW15** at checkout!

noip

Dashboard

DDNS & Remote Access

DNS Records

DDNS Keys

Dynamic Update Client

Update Clients

Device Configuration Assistant

Managed DNS

Domains

Email

Server Monitoring

SSL Certificates

Team Login

Records

My No-IP / Records

Create Hostname

Free Dynamic DNS: 1/1

Upgrade to Enhanced Dynamic DNS

Free Dynamic DNS accounts are limited to 1 Hostname, currently there is 1 Hostname in your account.

Upgrade Now

ddns.net 1 record

No-IP Owned

Name	Type	Content	TTL	Last Update
midominio2022	A	212.63.124.33	60	Dec 11, 2025 09:00:30

Feedback

my@5eaf42e29-2025-12-10T21:31:05Z web03

Pasos del ejercicio:

Verificar que TOR esta funcionando

systemctl status tor Debe indicar active (running) si no, poner ***systemctl start tor***.

Comando ejecutado:

proxychains4 curl ifconfig.co

Que hace cada parte:

proxychains4

Es la herramienta que obliga al programa que ejecutes (en este caso, curl) a usar los proxys definidos en /etc/proxychains4.conf.

Según tu salida, está usando un SOCKS5 proxy Tor en la dirección 127.0.0.1:9050.

Significa: todo el tráfico de curl pasa a través de Tor.

curl:

Es un cliente que permite hacer peticiones HTTP/HTTPS desde la linea de comandos.

ifconfig.co:

Es un servicio web que responde con tu IP publica tal como la ve el servidor.

Si usas Tor, mostrara una IP de salida de la red Tor, no la tuya real.

Explicacion de la salida que ves

[proxychains] Dynamic chain ... 127.0.0.1:9050 ... ifconfig.co:80 ... OK

128.127.180.156

Dynamic chain: la cadena de proxys de Proxychains esta en modo dinámico (usa los que estén disponibles).

127.0.0.1:9050: Proxychains conectó a través del proxy Tor local.

ifconfig.co:80 la petición al servidor web se realizó correctamente.

128.127.180.156 esta es la IP de salida que el servidor detecto.

Esta NO es tu IP real. Es una IP de un nodo de salida de Tor.

En resumen comando:

Fuerza a curl a usar Tor (via Proxychains).

Consulta un servicio que devuelve tu IP publica.

Te muestra la IP de salida de Tor, confirmando que el trafico esta siendo anonimizado.

Comando ejecutado:

```
proxychains4 /usr/local/bin/noip2 -U -c /usr/local/etc/no-ip2.conf
```

Este comando intenta ejecutar el cliente No-IP (noip2) a traves de Proxychains, usando Tor u otros proxys definidos en /etc/proxychains4.conf.

Que hace cada parte del comando:

proxychains4

Obliga a que cualquier aplicación que ejecutes después pase TODO su trafico a traves de los proxys configurados.

En tu caso, Proxychains está configurado para usar 127.0.0.1:9050, que es el proxy SOCKS de Tor.

/usr/local/bin/noip2

Es el ejecutable del cliente dinamico de No-IP, el que actualiza tu dirección IP publica en el DNS dinámico.

-U

Este parámetro indica a noip2 que actualice inmediatamente tu IP ("force update").

-c /usr/local/etc/no-ip2.conf

Indica qué archivo de configuración debe usar.

Explicacion de la salida mostrada:

```
[proxychains] config file found: /etc/proxychains4.conf
```

```
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
```

```
[proxychains] DLL init: proxychains-ng 4.17
```

Esta salida significa:

Proxychains encontro su archivo de configuracion
/etc/proxychains4.conf

Preload del modulo dinamico

Esta cargando libproxychains.so.4 para interceptar todas las llamadas del programa que vas a ejecutar (en este caso, noip2).

DLL init

Proxychains ya esta funcionando y redirigira todas las conexiones de noip2 hacia los proxys que tenga configurados.

No ves mas output porque noip2 no muestra informacion detallada al ejecutarse asi, a menos que este mal configurado o tenga errores.

Comando ejecutado:

nslookup midominio2022.ddns.net

Este comando consulta al servidor DNS que usa tu sistema (en tu caso 192.168.1.1, el router) para saber qué dirección IP tiene asociado el dominio midominio2022.ddns.net.

Interpretacion de la salida:

Server: 192.168.1.1

El DNS que respondio es tu router (usa DNS del ISP o los que tengas configurados).

Non-authoritative answer:

Significa que el router no es el servidor propietario del dominio, pero te está devolviendo la información que obtuvo de los DNS de No-IP.

Name: midominio2022.ddns.net

Dominio consultado

Address: 212.63.124.33:

Esta es la IP publica que No-IP tiene actualmente registrada para tu dominio.

Esto confirma que:

El dominio existe.

El DNS esta funcionando.

Tu dominio apunta a la IP pública 212.63.124.33.

Es la IP que No-IP considera como tu ubicación actual.

Pregunta clave: ¿Es esta IP tuya?

Depende de si:

¿Estas usando tu red normal sin Tor, VPN, Proxychains?

Si esa IP debería ser tu IP pública real del ISP.

¿Estas usando Tor, Proxychains, VPN u otra salida anonimizada?

Entonces NO es tu IP real:

Es la IP del nodo de salida o de la VPN.

¿noip2 o ddclient actualizaron la IP mientras estabas en Tor o usando Proxychains?

En ese caso, tu dominio NO apunta a tu red real, sino a una IP equivocada.

Como comprobar si 212.63.124.33 es tu IP real

Ejecuta:

curl ifconfig.me

Si coincide con 212.63.124.33, entonces es tu IP real.

Si no coincide, significa que No-IP se actualizó con una IP incorrecta.