Becoming Anonymous and secure in internet
(Kali Linux+TOR+Proxy)

Before we become **Anonymous** and **secure** on the **internet** we need to know how the internet tracked our **IP Address**.

1.Every time we visit a website, our network sends out an information packet containing our **IP address**. The server that hosts the website we are trying to access, accepts that information packet, learns what network is asking for access, and knows where to send its response in the form of all the files that make up the site.Now both the website and the server that hosts it know our IP address.

- our device gets assigned a unique identifier called an IP address
- Every time we visit a website, ip address is sent along with our request
- Websites and servers record this information to know where to send data back to
- our device sends "information packets" containing our IP address
- These packets help websites identify who's requesting access
- Servers use this information to deliver content back to our device.

How can we prevent our IP address from being tracked

1.TOR (The Onion Router)

Tor is a privacy-preserving network designed to hide where your internet traffic comes from and where it's going.
Tor sends our connection through a few random computers/routers first, so websites can't see our real location.Tor hides us by mixing our internet traffic with many other people's traffic so no one can tell which traffic is ours.Tor provide: **IP address** anonymity, Protection from network-level tracking, Access to .onion hidden services.

TOR Browser install in **kali linux**

- sudo apt update (firstly update kali linux)

Install **torbrowser**

- sudo apt install tor torbrowser-launcher

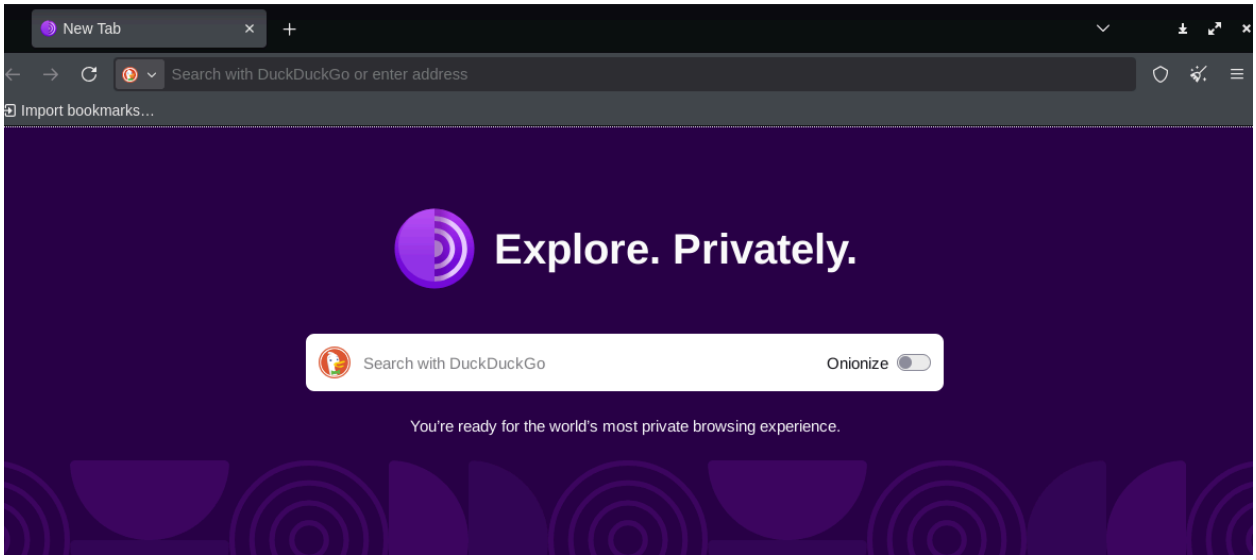
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install tor torbrowser-launcher
[sudo] password for kali:
Installing:
  tor  torbrowser-launcher
```

Launcher the **tor browser**

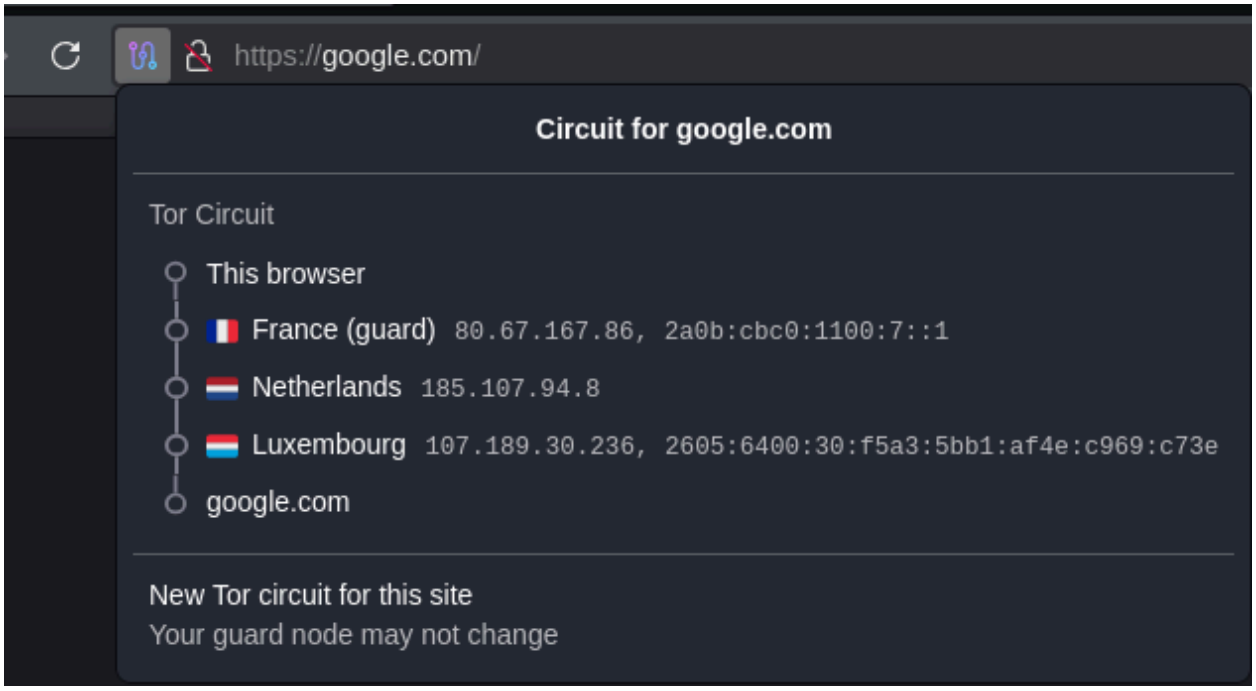
- torbrowser-launcher

```
┌──(kali㉿kali)-[~]
└─$ torbrowser-launcher
Tor Browser Launcher
```

This is **TOR Browser**

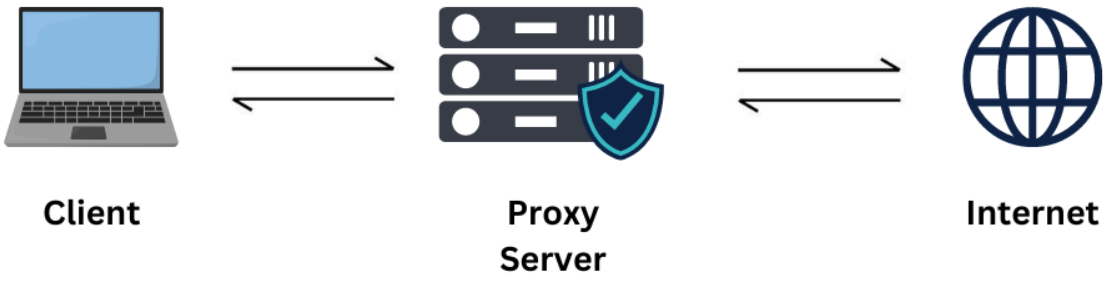


TOR encrypts the data , destination and IP address . If someone intercepts the traffic they can see only the IP address of the previous hop and the website owner can see only the IP address of the last router that sent the traffic. In that case (picture) owner see the last IP address which is **107.189.30.236**



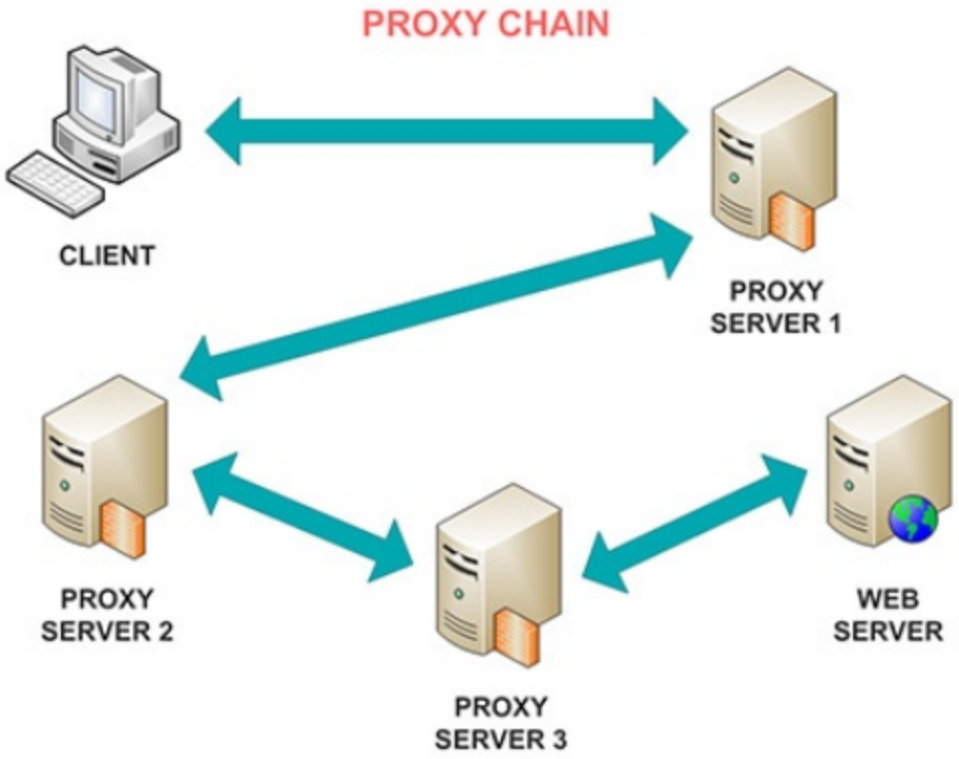
Note:
The U.S. and other nations view Tor as a national security threat because it lets governments and terrorists communicate anonymously. Intelligence agencies, like the NSA, have previously broken Tor's anonymity and likely can again use methods like traffic correlation and running Tor routers. While Tor still hides your identity from services like Google, it may not fully protect you from spy agencies.

2.Proxychains
Before knowing **proxychains** , we need to know about **proxy** .
A proxy is a server that sits between you and the internet.A proxy forwards your request to a website so the website cannot see your real identity (IP address).



Proxychains

Now, **Proxychains** is a Linux tool that forces any program to use a proxy (like TOR, SOCKS, or HTTP proxies).Proxychains makes your tools (like Nmap, Curl, Nikto, Burp, etc.) connect to the internet through a proxy, even if the tool itself does not support proxies.

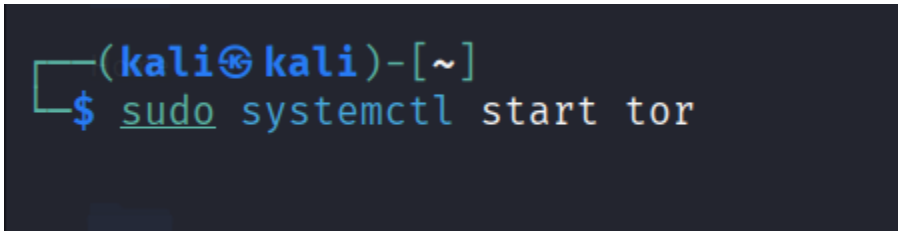


We use **proxychains** in **2** ways.**with TOR** and **without TOR**. If you want to do **Anonymous pentesting** then use **Proxychains with TOR**. Or if you want just to do fast browsing use just Proxychains. In that case, since we are working on **cybersecurity** and **ethical hacking**, we will use **Proxychains with TOR**.

Installing Proxychains
Proxychains is already **pre-install** in **kali linux** . Before starting proxychains you need to install **TOR.**

Start TOR service

- sudo systemctl start tor



Verify TOR is working or not working

- sudo service tor status

```
┌──(kali㉿kali)-[~]
└─$ sudo 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 Tue 2025-11-18 11:13:41 EST; 36s ago
 Invocation: 2c1f1486666f47b0995ed7dcbb0303ef
    Process: 198227 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 198227 (code=exited, status=0/SUCCESS)
   Mem peak: 1.7M
        CPU: 54ms
```

Setting up Before using proxychains, you will need to set it up to hide your IP.The first step is to add your proxies to the proxychains configuration.Open the proxychains configuration file using a text editor. We will use nano.

- sudo nano /etc/proxychains4.conf

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/proxychains4.conf
```

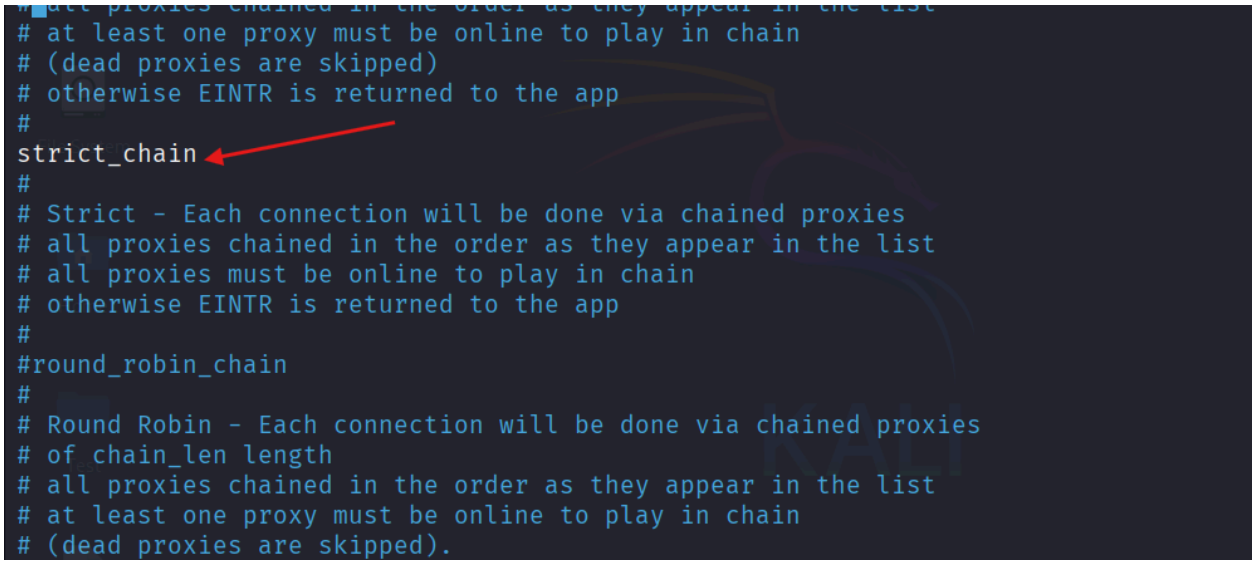
In proxychains , there are three kinds of changes (Dynamic,Strict,Random)

Dynamic: in dynamic chaining if one of the proxies down or not responding, it automatically goes to the next proxy.If one proxy is dead, Proxychains will skip it and use the next one.uncommand dynamic chain..**disable or cut #.**

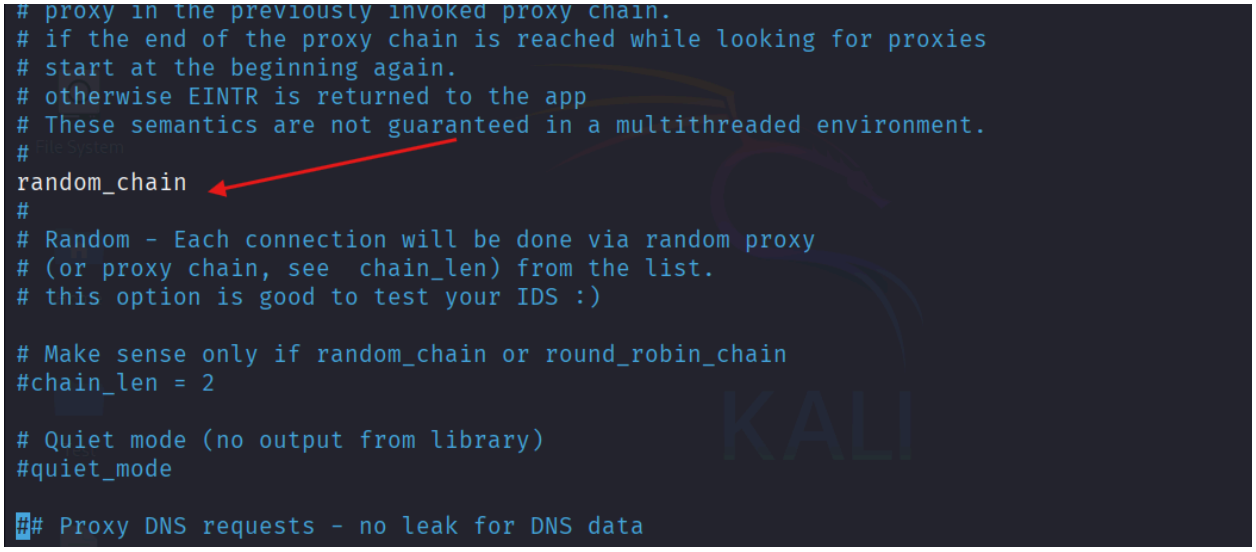
```
# proxychains.conf  VER 4.x
#
#        HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.


# 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: in strict chaining If a proxy fails, the connection fails all together.Proxychains will use proxies in the exact order you write them.If any proxy fails the whole chain fails.uncommand strict chains..**disable or cut #.**



Random: in random chaining a random chain selects proxies for each connection in random ways.This means that each time we use proxychains, the proxy will look different to the target, making it harder to track our traffic from its source.uncommand random chain.**disable or cut #.**



For this test, comment out the already existing **socks4** proxy and add as many proxies as you want.Here, sock proxy is set on the **9050 port** which is the default port for **Tor**. and also here i

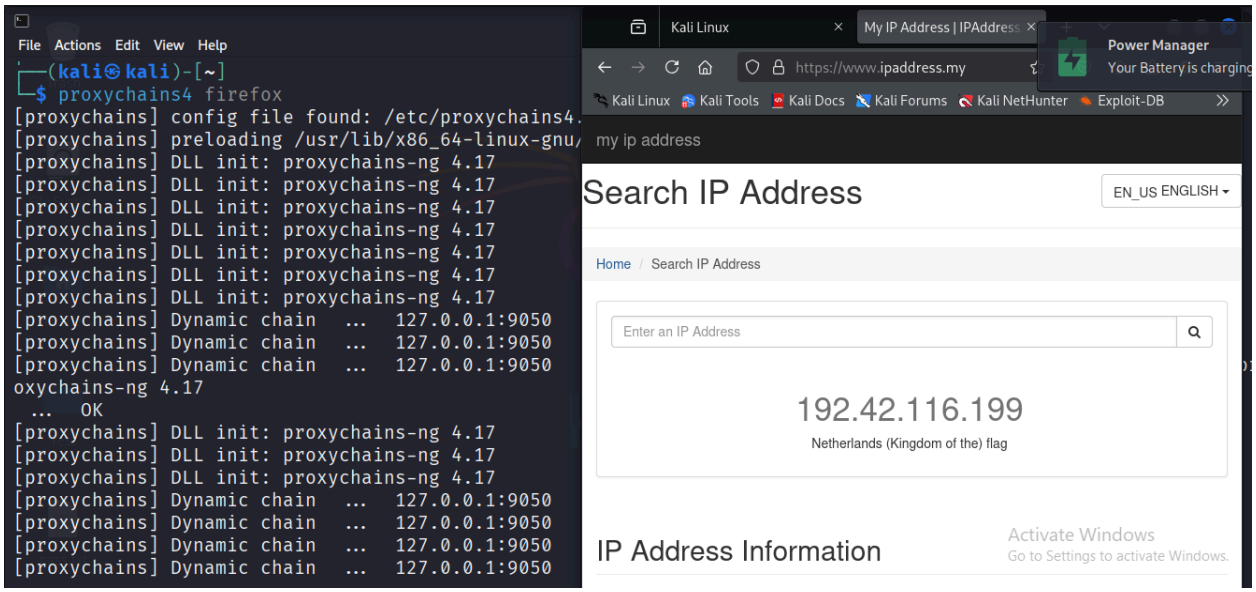
set proxy **sock5 127.0.0.1 9050**. You can also configure how **proxychains** use the list of proxies you have provided. These can be dynamic, strict, circular or random chains.
There are questions that we can use our own created proxy IP! Yes — we can use our own created proxy IP address in Proxychains, as long as your proxy server is correctly running.To use our own created proxy, the proxy must be:Running,Accessible (public or LAN), Correct port open,Correct type (SOCKS4 / SOCKS5 / HTTP)
If it meets these requirements, Proxychains will work perfectly.

Note: SOCKS is a proxy protocol that sends your internet traffic through another server, hiding your real IP. SOCKS4 Older version and SOCKS5 Advanced version.

Now the proxychains are set up.Whenever you want to use an app or tool, just add the command proxychains4 before the app command to route the connection through your proxies.

For example, to open **Firefox**, simply type the following command. You saw proxy firefox ip address

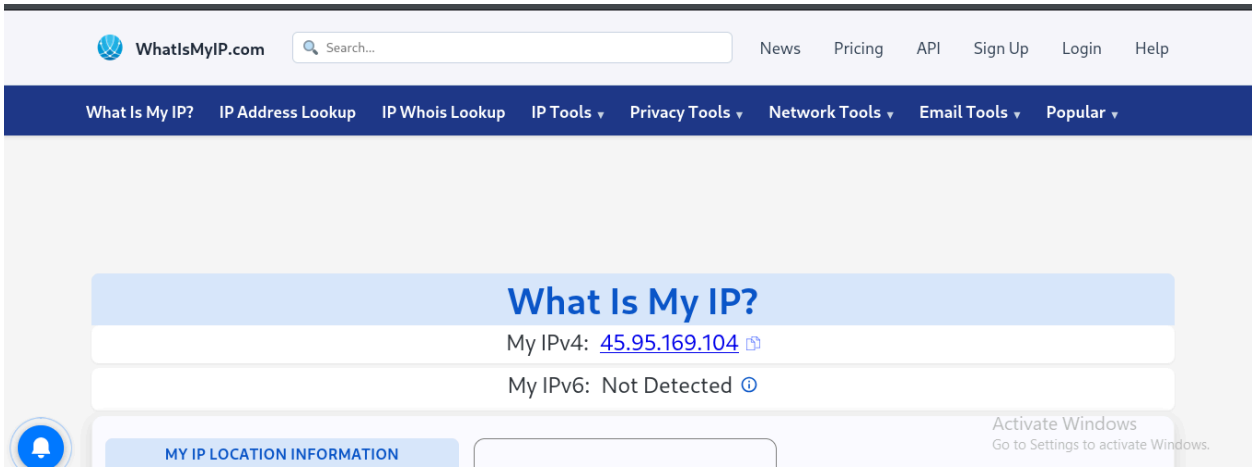
- Proxychains4 firefox



When i open **Firefox** and go to **google** , my ip address showings different

```
┌──(kali㉿kali)-[~]
└─$ proxychains4 firefox google.com
[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
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
```

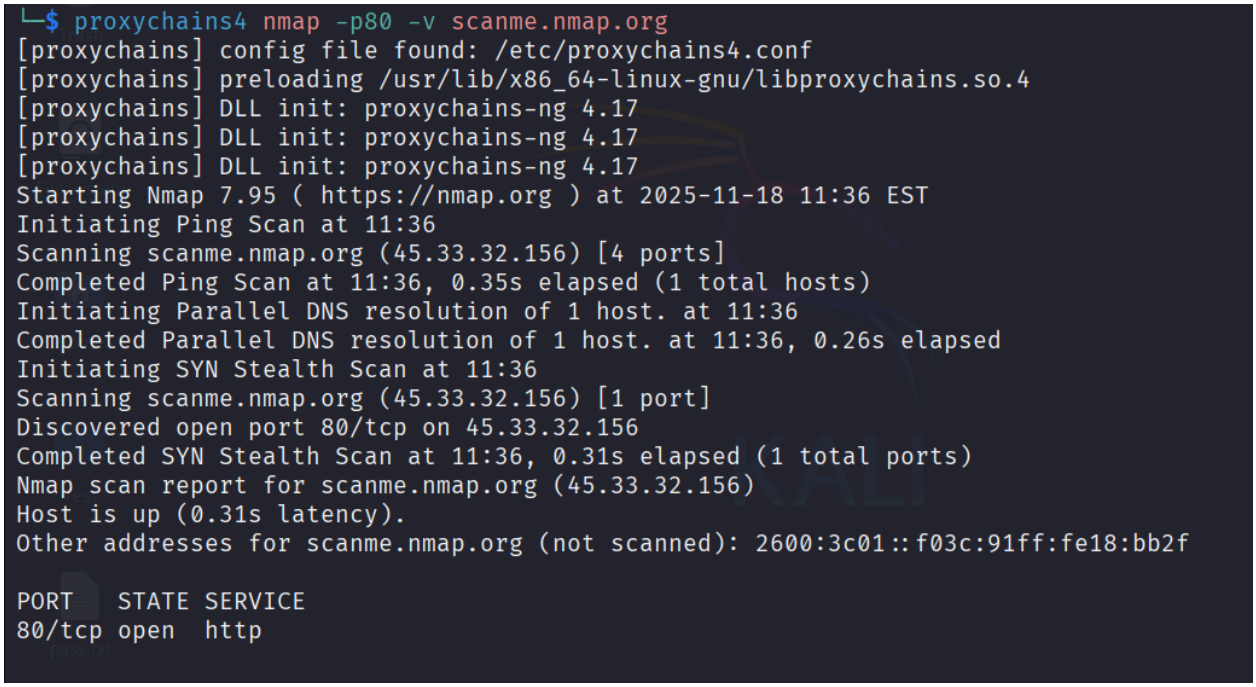
You can see my ip address



Use Tools

I am using **nmap** tools with proxychains

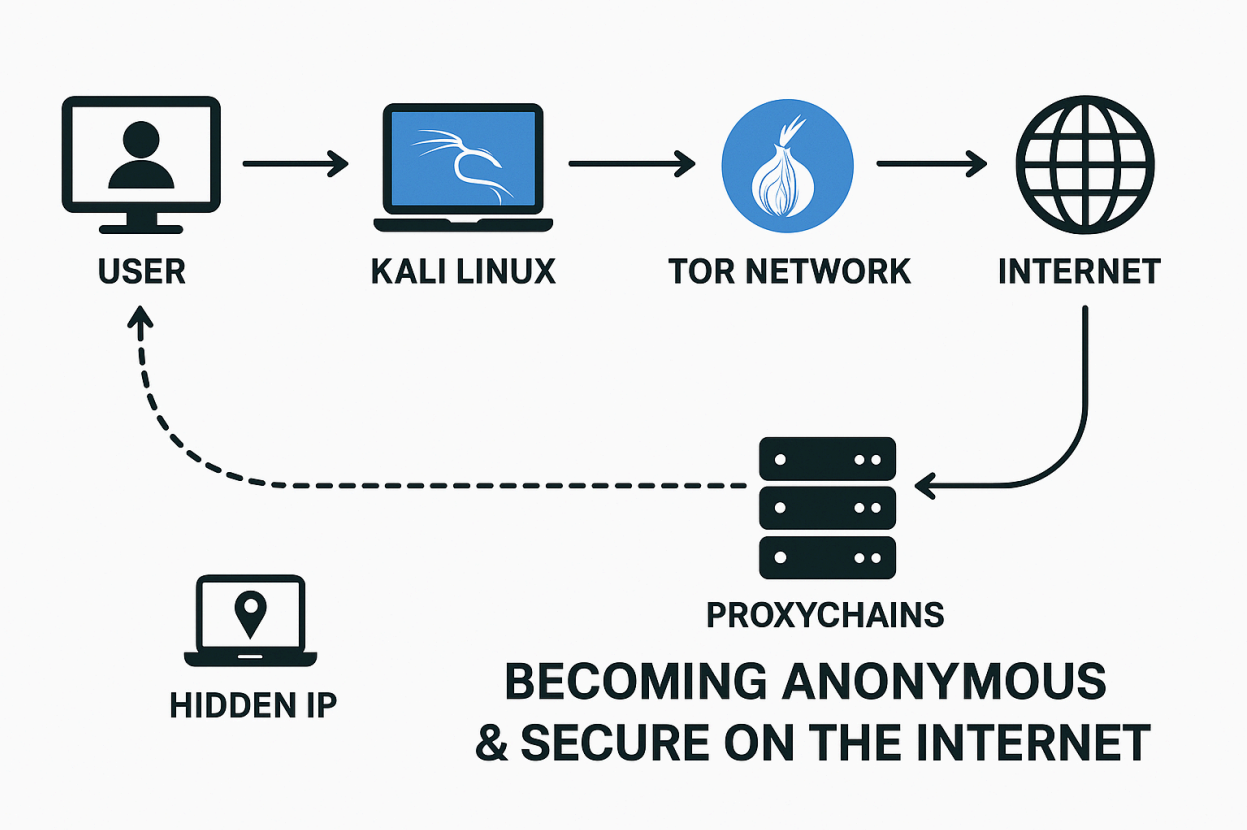
- proxychains4 nmap -p80 -v scanme.nmap.org



Conclusion:

Using **Kali Linux**, combined with **Tor** and **Proxychains**, gives you a strong layer of anonymity by hiding your **real IP address**, routing your traffic through multiple encrypted nodes, and forcing all tools to use anonymous proxy routes.

- **Kali Linux** provides the tools you need for secure and controlled penetration testing.
- **Tor** anonymizes your traffic by bouncing it through **three encrypted relays**, making tracking extremely difficult.
- **Proxychains** force any application (like Nmap, Curl, Firefox, Nikto, SQLMap) to run through **Tor or custom proxies**, giving you flexible multi-layer anonymity.
- Combining Tor + Proxychains adds **dynamic, chained proxies**, making your source IP unpredictable.
- This setup increases privacy but **does not guarantee 100% anonymity**—browser leaks, DNS leaks, misconfigurations, and human mistakes can still expose you.


USER
KALI LINUX
TOR NETWORK
INTERNET
PROXYCHAINS
HIDDEN IP
BECOMING ANONYMOUS
& SECURE ON THE INTERNET

END