

What is Proxychian?

Is the methodology of using multiple machines while browsing the internet to hide the identity of the original machine.

Why should I be anonymous while ethically hacking?

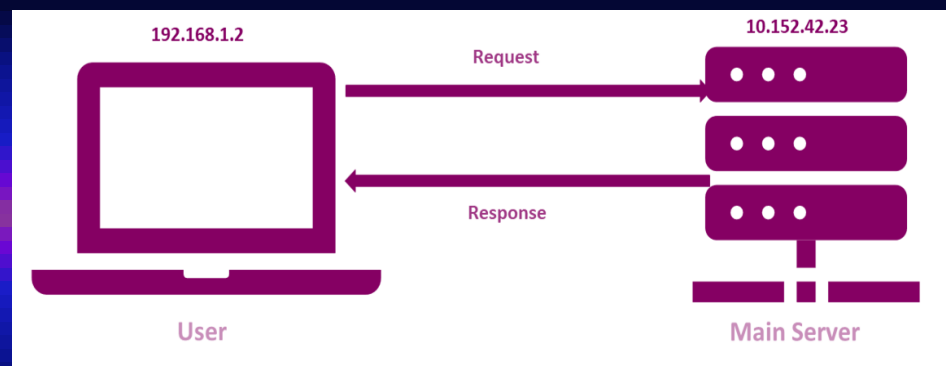
Because you are not alone...

Let me explain this in brief If you are an Ethical Hacker, then the organization has given you permission and due to this, you might think that you are not in trouble. But keep in mind that while you are trying to find a **vulnerability**, there might be some **other hacker** in the network. And to protect yourself from that hacker, you need to be Anonymous.

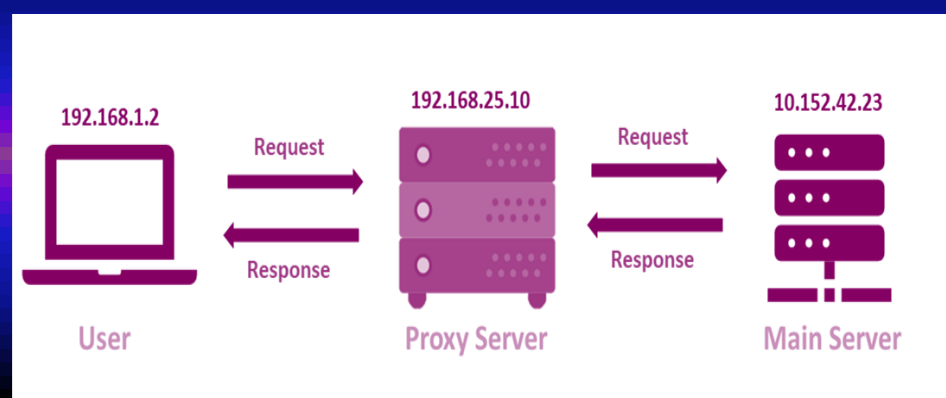
Proxychian for Anonymity

Do you know what happens when you request a server for some web page? The request is sent from your system to the server. The server processes the request and responds with the data that you requested for. And then, this response is sent to your system.

Well, how do you think the server identifies your system? Through your IP address!



The IP address can be used to identify the hacker's system and proxy is a way to avoid this. A proxy redirects the requests from your system to the main server through the proxy server. Using this, the IP address of your system is hidden because the request made to the main server is through the proxy server.



When you use Proxychain for ethical hacking, instead of one proxy server, your request gets redirected through multiple proxy servers. This makes tracing back the IP difficult. Now that you know what Proxychains are, let's see how to use Proxychain for ethical hacking.

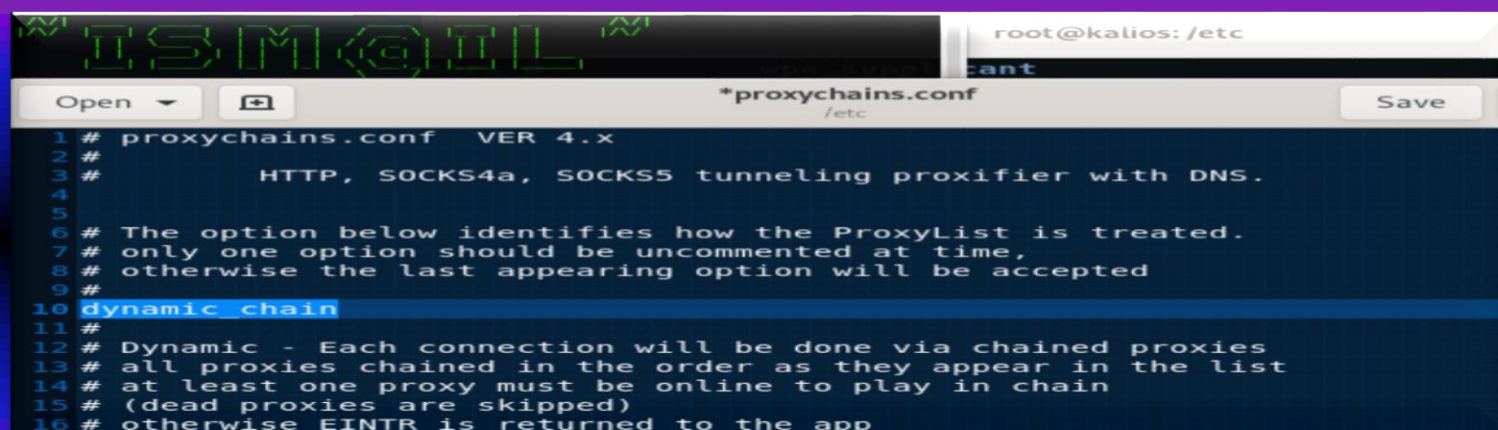
To install Proxychain, Open the terminal and run the following command

```
$ sudo apt-get install proxychains
```

Next, you need to make some changes in the configuration file. Open the proxychains.conf file.

```
$ sudo nano /etc/proxychains.conf
```

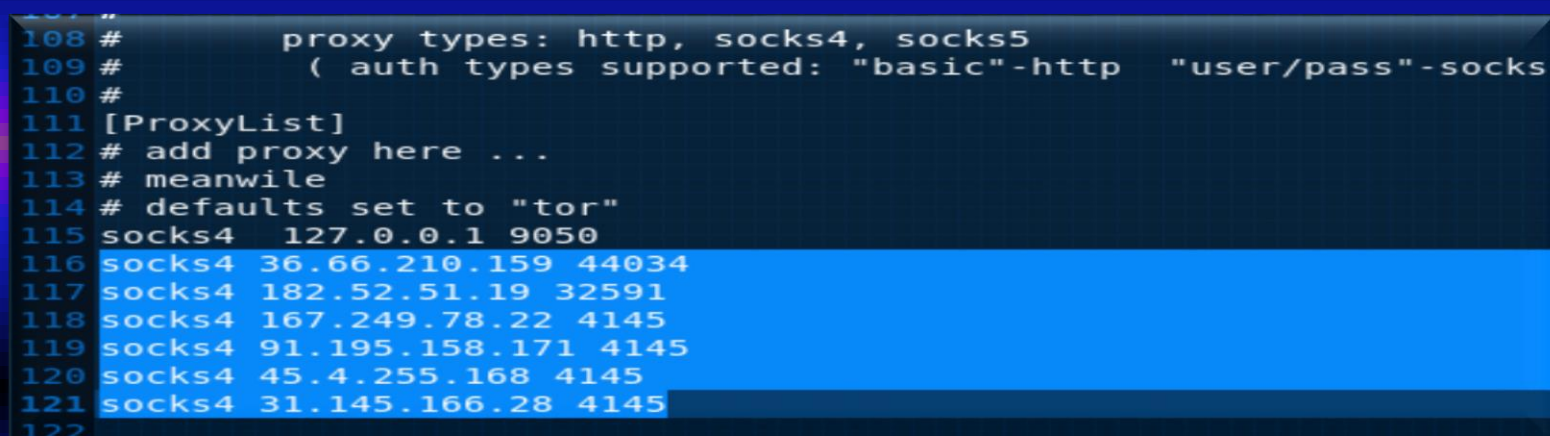
In this file, by default, the line `dynamic_chain` is commented and the line `strict_chain` is not commented. Remove the comment from `dynamic_chain` and comment out `strict_chain`. This is to make Proxychain work even if few proxy servers are not online.



```
1 # proxychains.conf  VER 4.x
2 #
3 #      HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.
4 #
5 #
6 # The option below identifies how the ProxyList is treated.
7 # only one option should be uncommented at time,
8 # otherwise the last appearing option will be accepted
9 #
10 dynamic_chain
11 #
12 # Dynamic - Each connection will be done via chained proxies
13 # all proxies chained in the order as they appear in the list
14 # at least one proxy must be online to play in chain
15 # (dead proxies are skipped)
16 # otherwise EINTR is returned to the app
```

To make Proxychain for ethical hacking more effective, let us add some more proxy servers. Scroll down to the end of the file and you will see a default proxy server. Add the following lines at the end of the file:

```
socks4 36.66.210.159 44034
socks4 182.52.51.19 32591
socks4 167.249.78.22 4145
socks4 91.195.158.171 4145
socks4 45.4.255.168 4145
socks4 31.145.166.28 4145
```



```
107 #
108 #      proxy types: http, socks4, socks5
109 #      ( auth types supported: "basic"-http  "user/pass"-socks
110 #
111 [ProxyList]
112 # add proxy here ...
113 # meanwhile
114 # defaults set to "tor"
115 socks4 127.0.0.1 9050
116 socks4 36.66.210.159 44034
117 socks4 182.52.51.19 32591
118 socks4 167.249.78.22 4145
119 socks4 91.195.158.171 4145
120 socks4 45.4.255.168 4145
121 socks4 31.145.166.28 4145
122
```

I suggest you add more such proxy servers. You'll find the details of proxy servers with a simple "**proxy server list**" search on the internet.

Save (Ctrl+O) and exit (Ctrl+X) the file.

Before using Proxychain, check if your IP address is traceable. To check this, open any Internet Browser and open the following URL: <https://www.dnsleaktest.com>. This website will display your IP address. Close the browser. Now let's try Proxychain.

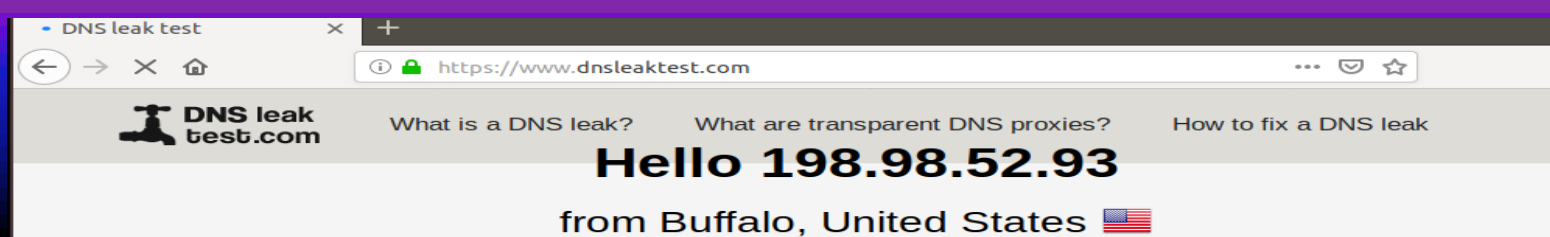
The syntax to run proxychain is:

```
$ proxychains <application/command>
```

Let's run Proxychain and see if it works. Open the terminal and run the following command:

```
$ proxychains firefox www.dnsleaktest.com
```

You can now see that the IP address has changed!



Conclusion

If you're going to be testing the vulnerabilities of popular websites without permission, Proxychains or something similar is definitely necessary. Proxychains can also be configured with Tor for maximum security when browsing.