

Forum:[Hack Forums](#)

Thread: [\[TUT\] Setting up Proxychains to improve opsec. \[Kali Linux\]](#)

The Amazing Sinner - August 24, 2020, 10:54 pm

Another tutorial by me, in this short tutorial I will be explaining setting up Proxychains with TOR =)

We'll be setting up Proxychains on our Kali OS.

Installing Tor:

First we have to make sure Tor is installed:

Open your terminal and type the following:

Code `sudo apt-get install tor proxychains`

If the package is installed check if Tor is running:

Code `sudo service tor status`

You can use `sudo "service tor start"` and `"sudo service tor stop"` to start or stop the service.

Set up Proxychains:

Now we need to configure our Proxychains config file, first let's locate the proxychains directory:

Code `locate proxychains`

You should see that the proxychains config file is in `/etc/`.

We can use Kali's "leafpad" to edit the file. Type:

Code `leafpad /etc/proxychains.conf`

Here's the content of the config file:

Code `# proxychains.conf VER 4`

`#`

`# HTTP, SOCKS4, 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
We can use three processes of chaining with proxychains.

Strict Chain: Allows proxies to be chained in a certain order.

Random Chain: Proxies are chosen at random in your proxy list.

Dynamic Chain: Dynamic chain works in the same way as strict chain but skips non working proxies. This is what we will be using in this guide.

Add a "#" in front of Strict chain and uncomment Dynamic Chain.

Go to the bottom of the file and change "socks4 127.0.0.1 9050" to "socks5 127.0.0.1 9050".

Testing Proxychains

We are ready to go ! Let's check our current IP adress on <https://www.whatismyip.com>. Remember it, then close firefox.

Now in your terminal write:

```
Code proxychains firefox whatismyip.com
```

Your IP should have changed and you are now browsing through a tor tunnel.

You can start any program with proxychains by typing "proxychains" before your program's name:

```
Code proxychains nmap
```

```
proxychains sqlmap
```

That's it ! If you have any question shoot me a PM or post here I'll get back to you =)

Argonaut.exe - August 24, 2020, 11:05 pm

I've read a book about anonymity recently this was explained, but you have been a lot more clear and schematic!

Excellent tutorial!

The Amazing Sinner - August 24, 2020, 11:05 pm

(Aug 24, 2020 11:05 PM)Argonaut.exe Wrote: [\[CITE\]](#) I've read a book about anonymity recently this was explained, but you have been a lot more clear and schematic!

Excellent tutorial!

Thank you!

Raikou - August 26, 2020, 3:50 pm

Hey nice tut looks super similiar to a youtube tutorial I saw but why are you not using a VPN? since you need to make sure to type that keyword "proxychains" before running every program is kinda annoying and it seems like you need to set it up again after a reboot (I dont know shit about this these are just the questions I have)

The Amazing Sinner - August 26, 2020, 3:57 pm

(Aug 26, 2020 03:50 PM)Raikou Wrote: [\[CITE\]](#) Hey nice tut looks super similiar to a youtube tutorial I saw but why are you not using a VPN? since you need to make sure to type that keyword "proxychains" before running every program is kinda annoying and it seems like you need to set it up again after a reboot (I dont know shit about this these are just the questions I have)

This is all done in Kali Linux, mostly used for penetration testing purposes. A lot of VPN's have a bunch of flaws as well.

Even when you're "successfully" connected to a VPN, some of your traffic may not be routed

through that connection. This is called a leak, and it undermines the entire point of using a VPN for privacy. Proxychains are a great way to route your traffic in kali. If you have any other questions, let me know.

Raikou - August 26, 2020, 4:10 pm

(Aug 26, 2020 03:57 PM)The Amazing Sinner Wrote: [\[CITE\]](#) This is all done in Kali Linux, mostly used for penetration testing purposes. A lot of VPN's have a bunch of flaws as well.

Even when you're "successfully" connected to a VPN, some of your traffic may not be routed through that connection. This is called a leak, and it undermines the entire point of using a VPN for privacy. Proxychains are a great way to route your traffic in kali. If you have any other questions, let me know.

Yea I know this is done in Kali but thanks for answering my question makes more sense now.

The Amazing Sinner - October 1, 2020, 6:55 pm

Should I post more tutorials? Let me know!