How To Use Proxychains Kali Linux

Proxychains

Proxychains is open source software for Linux systems and comes pre installed with Kali Linux, the tool redirect TCP connections through proxies like TOR, SOCKS and HTTP (S) and it allows us to chain proxy servers.

With proxychains we can hide the IP address of the source traffic and evade IDS and firewalls. We can use use proxychains in alto of situations, like when we want to avoid giving up our IP address or when scanning a target or visiting a website.

Furthermore chaining multiple proxies makes it difficult to track down the source IP address of the TCP connection, the application gives us a way to hide ourselves and stay anonymous. However proxy servers are likely to log your traffic and have to obey local law and jurisdiction.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step:1 Upgrade/Update & Install Tor

1.1 Upgrade and update the OS.

```
sudo apt-get update
sudo apt-get upgrade
```

1.2 Install the tor service.

```
sudo apt-get install tor
```

1.3 Start Tor service.

```
sudo service tor start
```

1.4 Display Tor service status.

```
sudo service tor status
```

NOTE: Tor service needs to run for proxychains to work.

Step2: Configure Proxychains

2.1 The proxychains configuration file is located in the “/etc/” directory edit the configuration file.

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

There is three methods we can run proxychains.

1. strict_chain
2. dynamic_chain
3. random_chain

strict_chain: is the default option in proxychains, every connection goes through the proxies in order that is listed in the configuration file. Strict chaining is best used when you want the source traffic appear from a particular locations.

dynamic_chain: works like the strict chain but it does not require all the proxies in the configuration file to work. If a proxy is down then the connection will jump to the next proxy server in the list.

random_chain: randomnesses proxy connections from the list on the configuration file, the chain of proxy will look different to the target.

Uncomment out the “dynamic_chains” line, it will enable dynamic chaining.

```
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
#
#random_chain
```

NOTE: Uncomment "*chain_len*" if you are using random_chain , the parameter establishes the number of IP addresses in the chain which are utilized in generating your randomized chain of proxies.

2.2 By default proxychains sends traffic through the host at 127.0.0.1 on port 9050. This is the default Tor configuration, *if you are planing to use Tor leave the "defaults set to "tor" as it is. If you are not using Tor, you will need to comment out this line.*

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

2.3 Add proxy servers to the proxychains configuration file, there are free proxy servers on the Internet, i am using free proxy in this lab, you can find them here, another good site with free proxies is spys.one.

Before adding custom proxies add Tor socks5 support, and "socks5 127.0.0.1 9050"

```
# meanwile
# defaults set to "tor"
socks4         127.0.0.1 9050
```

```
SOCKS5          103.21.161.105 6667
HTTPS           156.202.174.101 8080
HTTPS           183.76.154.184 8080
HTTP            142.93.130.169 8118
SOCKS5          178.62.59.71 23187
SOCKS5          50.63.26.13 43001
```

2.4 Prevent DNS leaks, uncomment “Proxy DNS requests – no leak for DNS data”.

```
# Quiet mode (no output from library)
#quiet_mode

 Proxy DNS requests - no leak for DNS data
proxy_dns
```

Exit & Save

Step 3: Proxychains Syntax

3.1 Verify that the proxychains is working.

```
proxychains firefox www.whatsmyip.org
```

3.2 Use Proxychains with nmap.

```
proxychains nmap 1.1.1.1
```

```
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-14 22:00 CEST
Nmap scan report for one.one.one.one (1.1.1.1)
Host is up (0.013s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 57.22 seconds
root@iPhone:~#
```

Summit

We have covered how to run proxychains and hide the identity of our source traffic and stay anonymous without being detected.

Check out the Ethical Hacking notes for more Kali Linux quick guides.

DISCLAIMER: This software/tutorial is for educational purposes only.

The tutorial should not be used for illegal activity and the author is not responsible for its use or the users action.