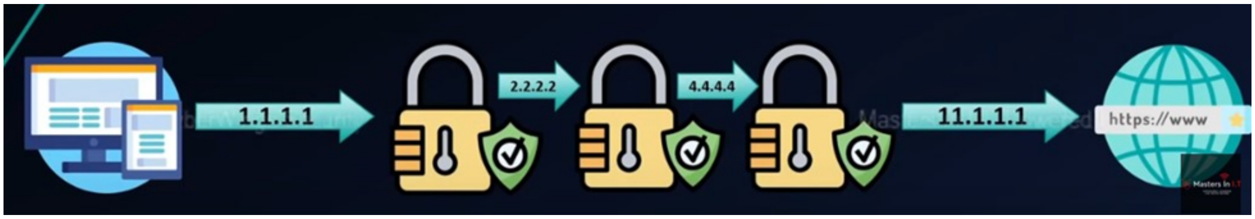
R V COLLEGE OF ENGINEERING

Name: ANKIT KUMAR **USN:** 1RV18IS007 **Dept/Lab:** ISE/CSDF **Expt No.:** 05 b
Date: 13/12/2021 **Title:** EXPLOITATION TOOLS

b. **PROXYCHAIN**

INTRODUCTION

Proxychains is a tool that forces every TCP communication coming out of your system to go through different or multiple proxies, you can chain multiple proxies with proxychain and your connection will go through these different proxies.



Some features of Proxychains include:

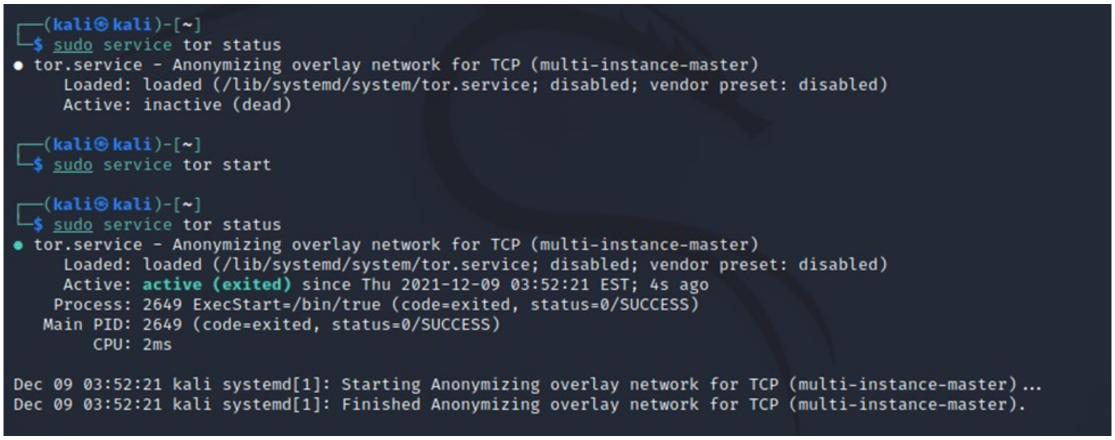
- It can be used with the server like squid, sendmail, etc
- Support SOCKS5, SOCKS4, and HTTP CONNECT proxy servers.
- It can be mixed up with different proxy type in the list.
- It supports different chaining option methods like:
    - **Random Chain**: Each connection made through proxychains will be done via a random combo of proxies in the proxy list.
    - **Dynamic Chain**: It is same as strict chain, but the dead proxies are excluded from the proxy list.
    - **Strict Chain**: All the proxies in the list will be used and they will be chained in the order.

Objectives - To illustrate the working of proxychains in order to hack anonymously into the system.

EXECUTION STEPS

1. **Installing Proxychains from a package**
   Command - *sudo apt-get install proxychains*

2. **Installing and Starting Tor Services**
   Proxychains by-default uses the Tor services, if it's not there in your system install it using the following command:
   Command - *sudo apt-get install tor*
   Now check the status of your tor service, if it is not active, then activate using the following command mentioned in the image below.

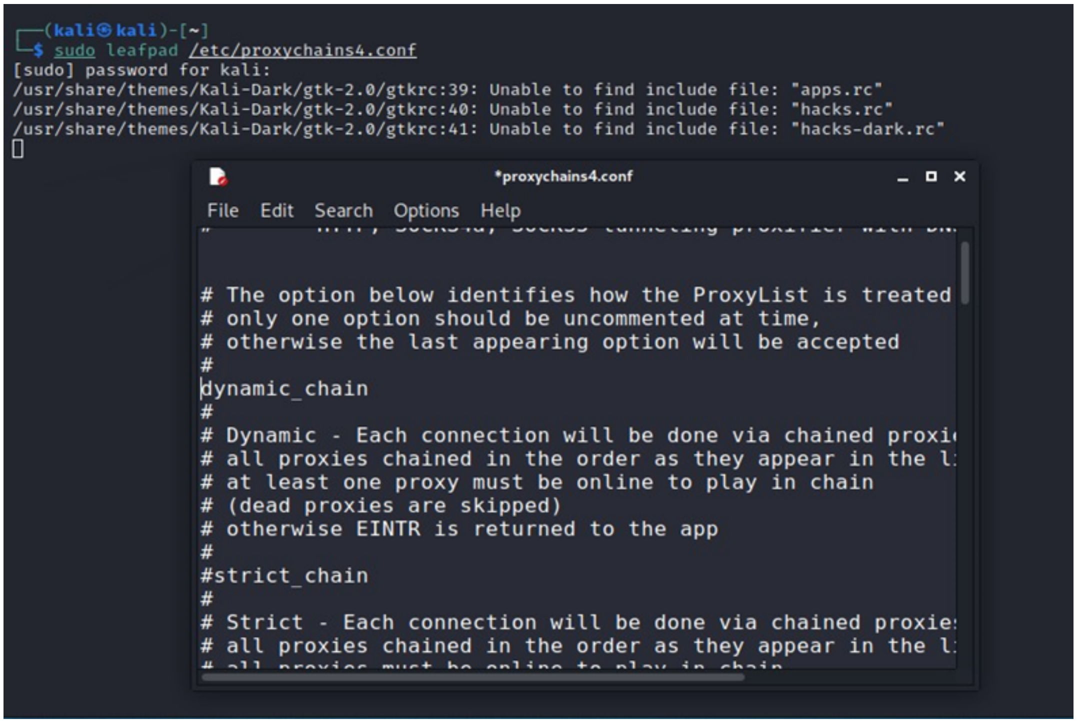


```
┌──(kali㉿kali)-[~]
└─$ sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
     Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
     Active: inactive (dead)

┌──(kali㉿kali)-[~]
└─$ sudo service tor start

┌──(kali㉿kali)-[~]
└─$ sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
     Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
     Active: active (exited) since Thu 2021-12-09 03:52:21 EST; 4s ago
    Process: 2649 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 2649 (code=exited, status=0/SUCCESS)
        CPU: 2ms

Dec 09 03:52:21 kali systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance-master)...
Dec 09 03:52:21 kali systemd[1]: Finished Anonymizing overlay network for TCP (multi-instance-master).
```

3. **Changing the default configuration**
   We will have to change the configurations of the proxychain tool, this can be done using any linux based editor.

   In the default case, Strict mode is enabled in the proxychains, so we will have to change this to Dynamic mode by commenting Strict mode and uncommenting Dynamic Mode.

   Also uncomment proxy_dns to increase our anonymity and add socks5 IP at the last as shown in the image below. Save the changes and proceed.

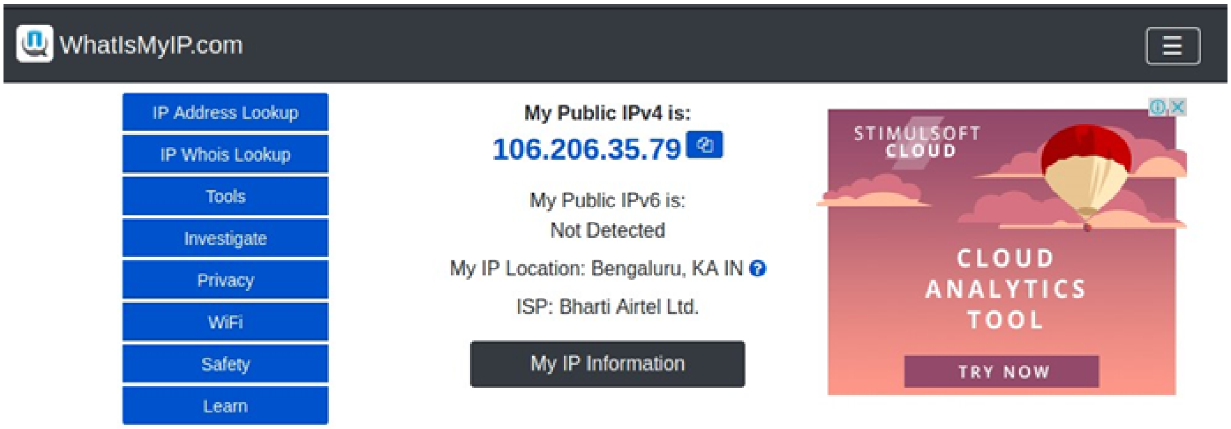


```
┌──(kali㉿kali)-[~]
└─$ sudo leafpad /etc/proxychains4.conf
[sudo] password for kali:
/usr/share/themes/Kali-Dark/gtk-2.0/gtkrc:39: Unable to find include file: "apps.rc"
/usr/share/themes/Kali-Dark/gtk-2.0/gtkrc:40: Unable to find include file: "hacks.rc"
/usr/share/themes/Kali-Dark/gtk-2.0/gtkrc:41: Unable to find include file: "hacks-dark.rc"
▯
```

```
#        HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DN

# 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 proxi
# all proxies chained in the order as they appear in the l
# 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 proxie
# all proxies chained in the order as they appear in the l
# all proxies must be online to play in chain
```

4. Now, to change the IP address, use the following commands shown in the image. Specify the name of the browser and the search engine to use. In my case, my IP changed from Bengaluru to San Angelo. The images show my initial IP, which was later

changed. Note that your internet speed will be reduced to a certain extent as proxychains uses many intermediate proxies to transfer the network traffic.

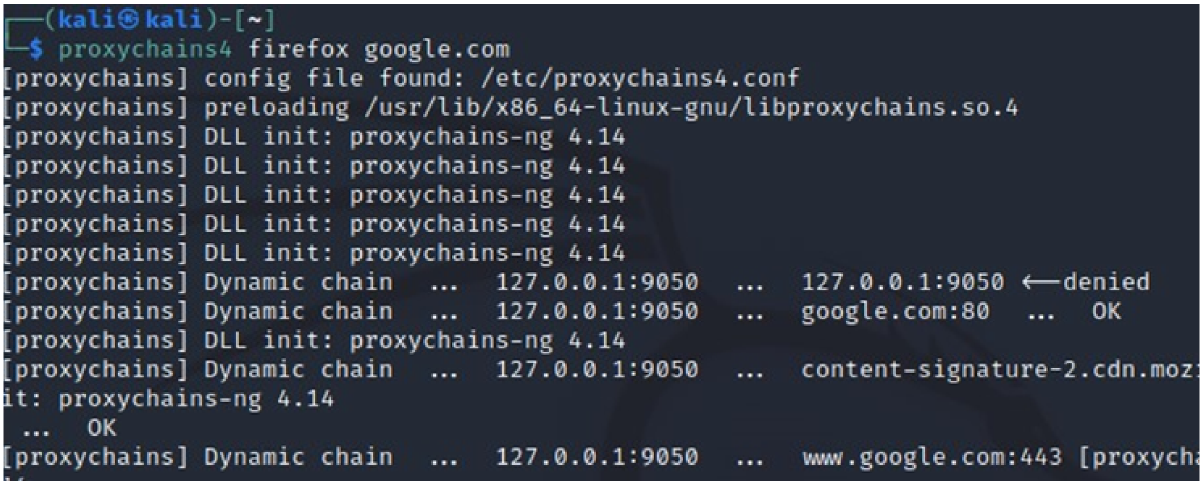


My Public IPv4 is:
106.206.35.79

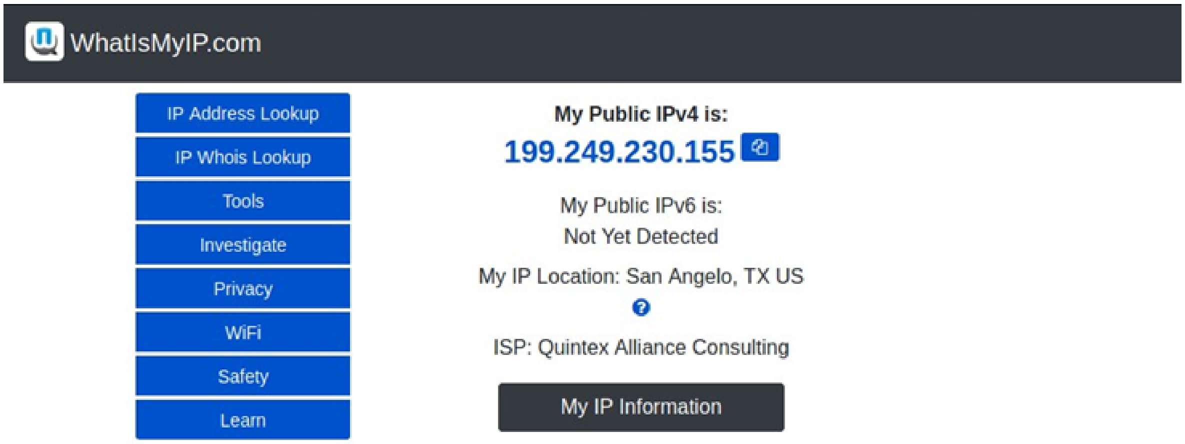
My Public IPv6 is:
Not Detected

My IP Location: Bengaluru, KA IN

ISP: Bharti Airtel Ltd.



```
┌──(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 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  127.0.0.1:9050 ←—denied
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  google.com:80  ...  OK
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  content-signature-2.cdn.moz
it: proxychains-ng 4.14
 ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  www.google.com:443 [proxycha
```



My Public IPv4 is:
199.249.230.155

My Public IPv6 is:
Not Yet Detected

My IP Location: San Angelo, TX US

ISP: Quintex Alliance Consulting

5. We can also combine the use of proxychains with other tools like nmap for port scanning, if we simply use nmap, then while port scanning the other person can detect our real IP address, but when used with proxychains, proxy servers will be used to hide our real IP while port scanning.for example:
   Command - *proxychains nmap 192.168.1.1/24*
   - proxychains : tell our machine to run proxychains service
   - nmap : what job proxychains to be covered
   - 192.168.1.1/24 or any arguments needed by a certain job or tool, in this case is our scan range needed by Nmap to run the scan.

CONCLUSION

1. In order to hack anonymously with the least chance of detection, we need to use an intermediary machine whose IP address will be left on the target system. This can be done by using proxies.
2. If we string multiple proxies in a chain, we make it harder and harder to detect our original IP address. If one of those proxies is outside the jurisdiction of the victim, it makes it very unlikely that any traffic can be attributed to our IP address.

REFERENCES

1. Proxychains - https://linuxhint.com/proxychains-tutorial/
2. Proxychains - https://www.geeksforgeeks.org/how-to-setup-proxychains-in-linux-without-any-errors/