

Report on

TOR TO PROTECT YOUR SYSTEM



AICTE APPROVED SUMMER INTERNSHIP PROGRAM

NAME: Shaurya Damathia

COLLEGE: Thapar Institute of Engineering and Technology, Patiala

COURSE: Cyber Security and Ethical Hacking

INTRODUCTION:

In today's digital age, protecting our system from various cyber threats is paramount. This report explores how TOR (The Onion Router) can be utilized to enhance your system's security and anonymity online. TOR is a powerful tool designed to anonymise internet traffic and protect user's privacy. Tor Browser prevents someone watching your connection from knowing what websites we visit. Anyone monitoring your browsing habits can see is that we're using Tor.

WORKING OF TOR AND ITS BENEFITS:

TOR functions by routing internet traffic through a global network of volunteer-operated servers. This onion routing process involves multiple layers of encryption, ensuring that no single point in the network can link the origin and destination of the data.

The primary advantage of TOR is the anonymity it provides. By masking a user's IP address and routing traffic through multiple nodes, TOR prevents surveillance and tracking. It also enables access to censored content, making it a vital tool in oppressive regimes.

INSTALLATION AND CONFIGURATION OF TOR:

- The command “sudo apt install tor” installs the Tor package from the default repositories.

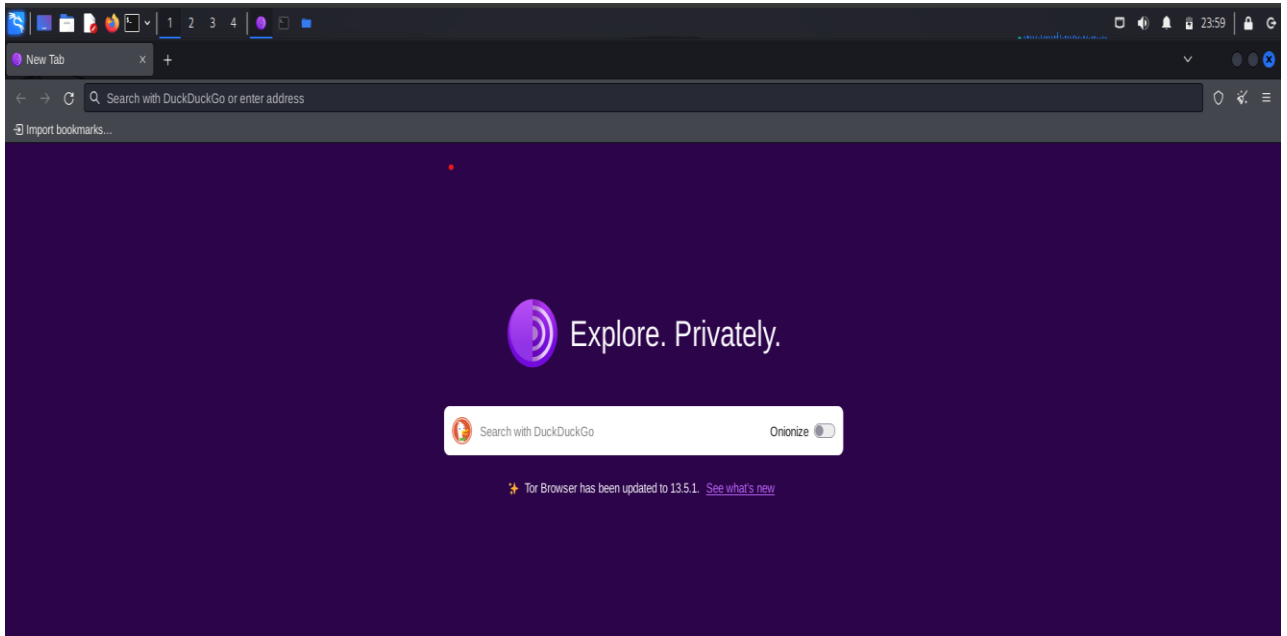
```
(user1@kali)-[~]  
$ sudo apt install tor  
tor is already the newest version (0.4.8.12-1).  
Summary:  
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 475
```

Before installing, we can also update our package lists to ensure we get the latest version of Tor available in the repositories using the command:

“sudo apt update”

- Browse for <https://www.torproject.org/download/> on any browser in Kali Linux. Scroll down and click on “Download for Linux” to set up for Tor to protect the system.

- Once downloaded, extract all the files from the folder named “tor-browser-linux64-11.0.9_en-US” and save on the desktop.
- Launch the Tor Browser and wait for it to connect to the Tor network.



Search for “hidden wiki” website on the browser. The Hidden Wiki is a well-known directory of links to various hidden services on the Tor network. It's often used as a starting point for navigating the .onion sites that are only accessible through the Tor Browser.

However, many links on the Hidden Wiki lead to content or services that may be illegal or harmful. Always exercise caution when exploring the Dark Web. We must be aware of the legal implications and potential risks involved.

The links can cover a wide range of content and services, including:

Information and News Sites:

- Sites that offer news, articles, and information on various topics, often from alternative or underground perspectives.

Privacy and Security Tools:

- Sites offering tools and resources related to privacy, security, and anonymity.

Educational Resources:

- Sites providing educational content on various topics, including technology, science, and more.

Cultural and Entertainment Sites:

- Sites related to entertainment, such as music, videos, and other forms of media.

ANONYMIZING USING TOR AND PROXYCHAINS:

Proxychains is a tool used to force network connections made by applications to go through a proxy server or a chain of proxies. It allows us to route traffic from any application through various types of proxies, such as SOCKS or HTTP proxies.

It is designed to tunnel network connections through one or more proxy servers. This can be useful for anonymity, bypassing censorship, or accessing services restricted to specific IP addresses.

Types of Proxies Supported:

- **SOCKS4/5:** Proxychains supports SOCKS4 and SOCKS5 proxies, which can handle a variety of protocols and provide good support for anonymity.
- **HTTP:** HTTP proxies can also be used, though they are generally less versatile compared to SOCKS proxies.

To use Tor with Proxychains, we need to configure Proxychains to use Tor's SOCKS5 proxy.

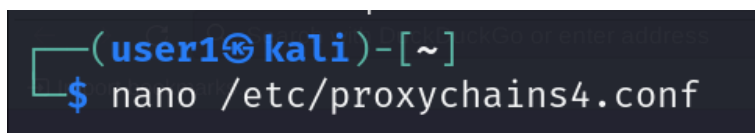
SOCKS PROXIES:

- SOCKS (Socket Secure) Proxy is a protocol for handling traffic between a client and a server through a proxy server. SOCKS proxies can tunnel any kind of traffic, making them useful for a variety of applications. Tor uses SOCKS5 proxies to route traffic.
- SOCKS5 is an enhanced version of SOCKS that supports various authentication methods and UDP (User Datagram Protocol) traffic, in

addition to TCP (Transmission Control Protocol). It is commonly used for its improved flexibility and security features.

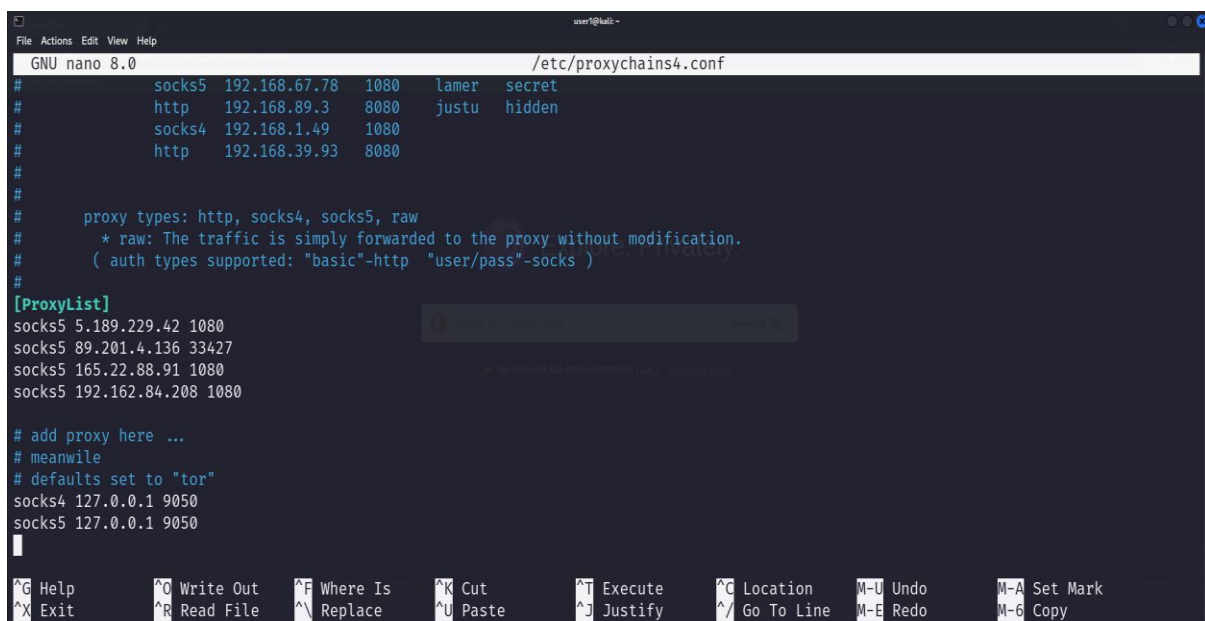
- SOCKS4 is an older version of the SOCKS protocol with fewer features compared to SOCKS5. It only supports TCP traffic and does not provide authentication support.
- Some of the IPs representing the configuration for SOCKS5 proxy server are:
 - socks5 5.189.229.42 1080
 - socks5 89.201.4.136 33427
 - socks5 165.22.88.91 1080
 - socks5 192.162.84.208 1080

- ❖ The command “nano /etc/proxychains4.conf” opens the Proxychains configuration file in the nano text editor. This file is where we configure the proxies that Proxychains will use to route network traffic.



```
(user1@kali)-[~]  
$ nano /etc/proxychains4.conf
```

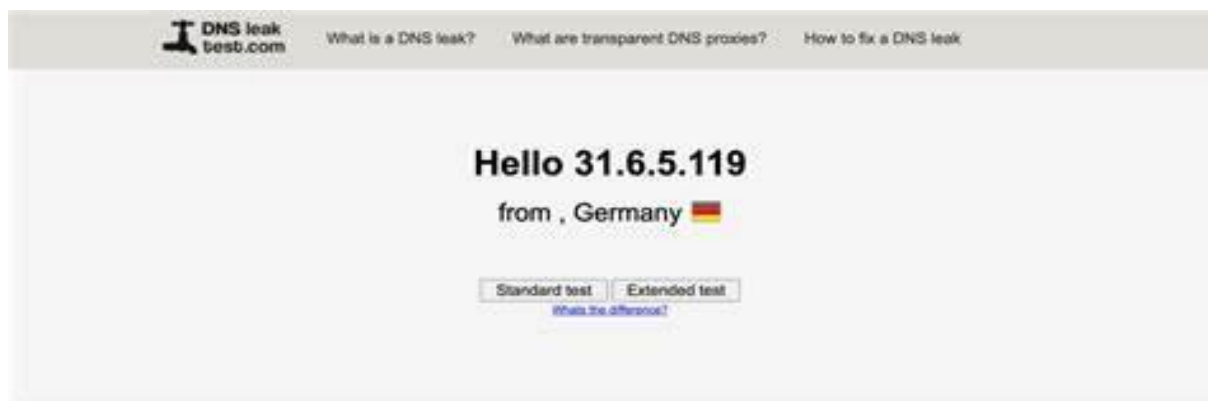
- ❖ To route traffic through SOCKS5 proxy server at above given IP addresses and corresponding ports, we added the lines under the “ProxyList” section as shown in figure.



```
GNU nano 8.0 /etc/proxychains4.conf  
# socks5 192.168.67.78 1080 lamer secret  
# http 192.168.89.3 8080 justu hidden  
# socks4 192.168.1.49 1080  
# http 192.168.39.93 8080  
#  
# proxy types: http, socks4, socks5, raw  
# * raw: The traffic is simply forwarded to the proxy without modification.  
# ( auth types supported: "basic"-http "user/pass"-socks )  
#  
[ProxyList]  
socks5 5.189.229.42 1080  
socks5 89.201.4.136 33427  
socks5 165.22.88.91 1080  
socks5 192.162.84.208 1080  
  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
socks4 127.0.0.1 9050  
socks5 127.0.0.1 9050
```

- ❖ Using “proxychains Firefox www.dnsleak.com” with Firefox browser allows us to route the browser’s traffic through the proxies specified in our Proxychains configuration file.

```
user1@kali: ~  
$ proxychains firefox www.dnsleak.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] Strict chain ... 5.189.229.42:1080 [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  
... timeout  
[proxychains] Strict chain ... 5.189.229.42:1080 ... timeout  
[proxychains] Strict chain ... 5.189.229.42:1080 ... timeout  
[proxychains] Strict chain ... 5.189.229.42:1080 ... timeout
```



When we run the command, Proxychains intercepts all network traffic from Firefox and routes it through the proxies defined in our `/etc/proxychains4.conf` file.

Visiting www.dnsleaktest.com helps us determine if our DNS queries are leaking outside of the proxy network (such as through our ISP) or if they are being routed properly through the proxy. This is important for ensuring our anonymity and privacy.

CONCLUSION:

By following these steps, you have successfully installed and configured Tor on Kali Linux. Tor and Proxychains together offer a robust solution for enhancing online anonymity and privacy. Tor routes traffic through multiple nodes to

anonymize users, while Proxychains allows applications to utilize Tor's SOCKS5 proxy, extending this anonymity to all network activity. Proper configuration of both tools is essential to ensure effective privacy protection, and users should remain cautious about their online practices. By leveraging Tor with Proxychains, individuals can significantly improve their online security and maintain a higher level of anonymity.