Anonymity and DOS

S2Day7Anon.md

Recalling

LAST TIME TOPICS

Topics

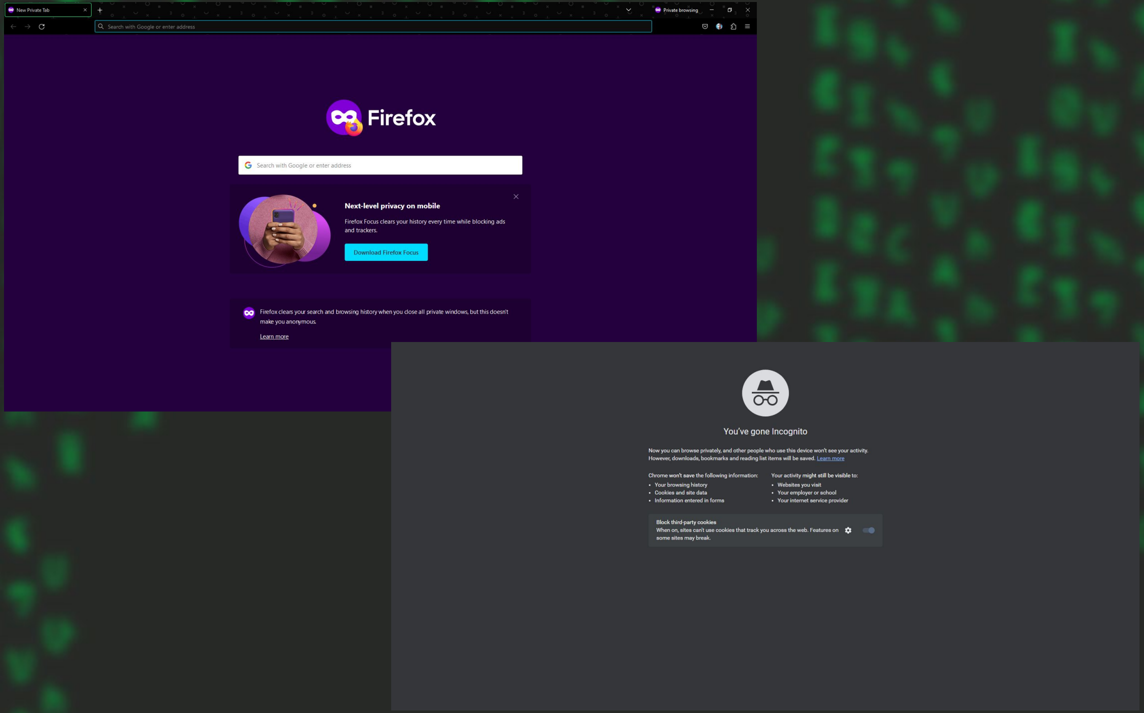
- Anonymity
- Methods of Anonymity
- IP and MAC
- DarkWeb
- DOS and DDOS
- How to do

Anonymity

- Anony/unknown in amharic is የማይታወቅ
- When Black Hat Hackers do Security tests on some target, They will be unknown
- This is because they are doing illegal things so they try to be anonymous/የማይታወቅ ሰው
- Keeping your identity private, but not your actions.
  - For example, using a fake name to post messages to a social media platform.
- Anonymity is Simply using a fake Profile/Location/Identity/personality

Online Privacy

- What do you think about incognito/privacy tabs?
- Do they give as privacy?
- These Programs are simply not logging what we are doing(aka history,cache,cookie) but still the site we visit with this program will have our ip and other informations also our ISP/internet service provider/ will know.
- Therefore, they dont give as real privacy. So how can we get that?



Next-level privacy on mobile

Firefox Focus clears your history every time while blocking ads and trackers.

Firefox clears your search and browsing history when you close all private windows, but this doesn't make you anonymous.

You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved.

Chrome won't save the following information:
- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:
- Websites you visit
- Your employer or school
- Your internet service provider

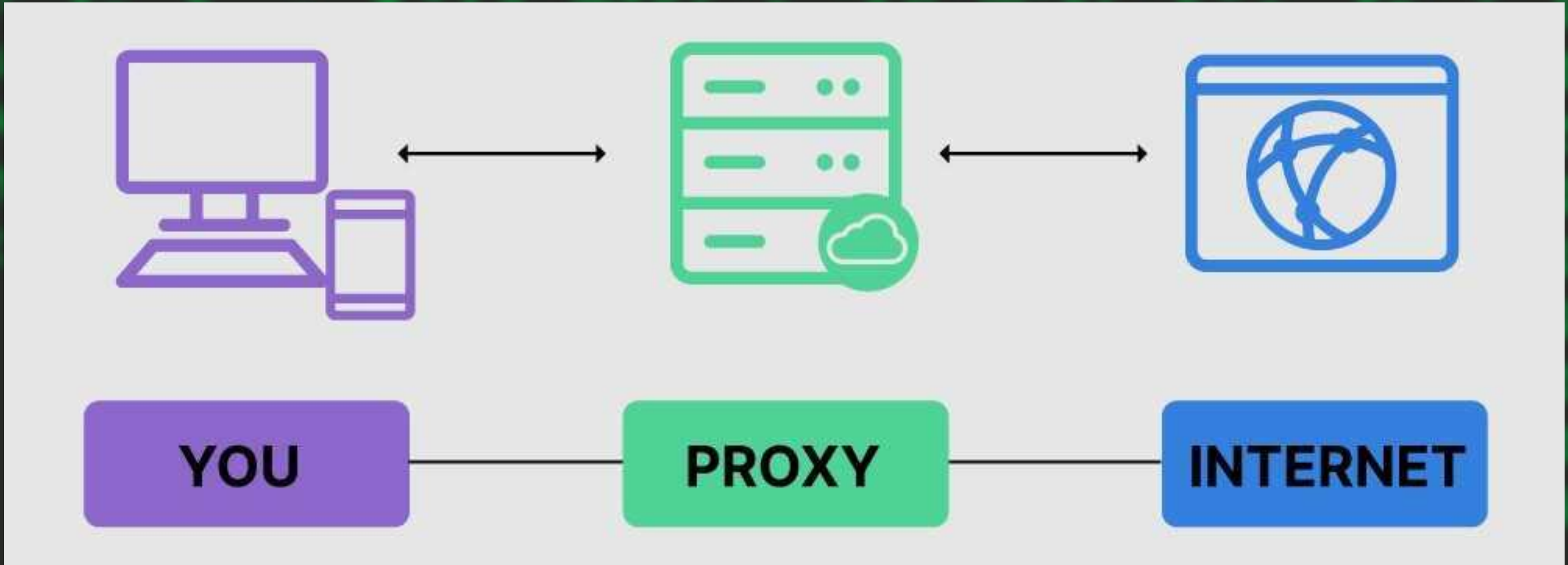
Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

Methods of Anonymity

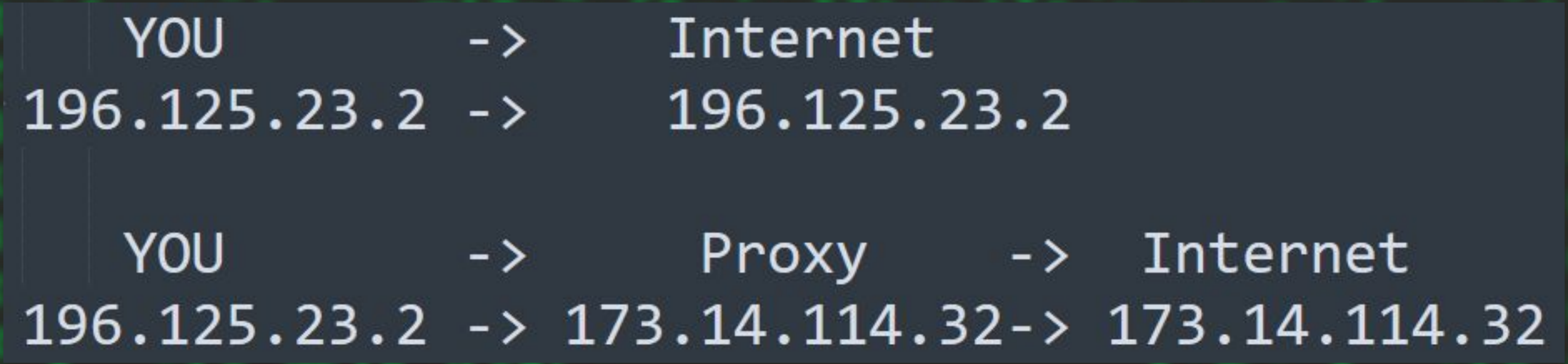
- There are several ways to be protected or to be Anonymous on the internet.
- These methods can change our identity,location or personality.
  1. Proxychains
  2. Tor Network
  3. VPN
  4. Mac change
  5. Incognito
  6. Secured OS
  7. Temp mail
  8. Temp number

What is Proxy Server?

- A **proxy server** is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network.
- Proxy means intermediary/መካከለኛ



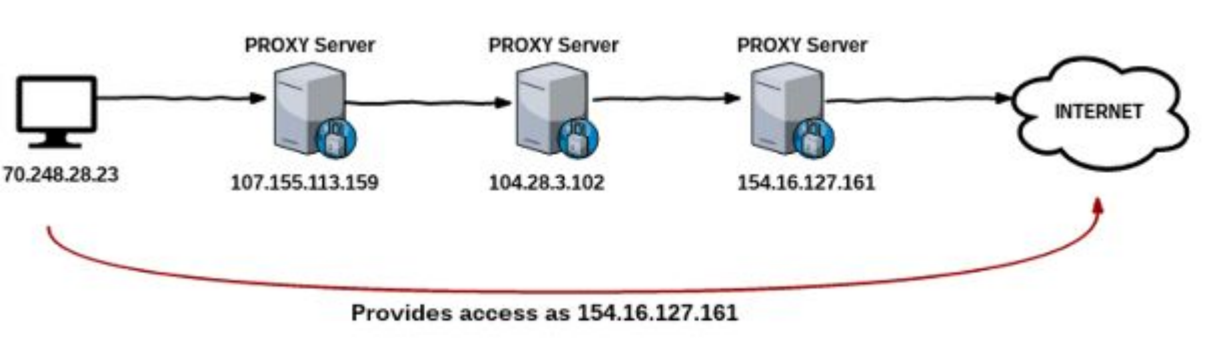
…means



```
   YOU       ->    Internet
196.125.23.2 ->    196.125.23.2

   YOU       ->     Proxy    ->  Internet
196.125.23.2 -> 173.14.114.32-> 173.14.114.32
```

ProxyChains

- We have seen what proxy is so lets see what Proxy chains are.
- Proxy chain is simply a chain of proxys.
- We have a lot of proxy lists so our request will pass through lot of proxys.
- This will hide our IP.



- Here our 1st IP was 70.248.28.23 but the Internet(webserver,...) know as 154.16.127.161

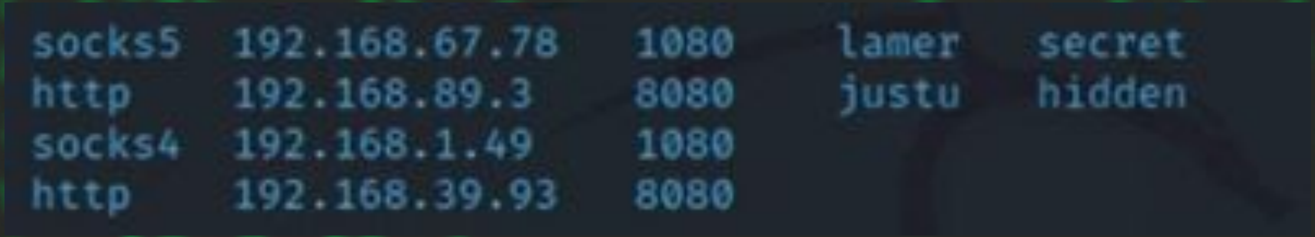
Types of ProxyChains

Based on the path we follow There are 4 Types of proxychains.

1. Dynamic chain
2. Strict Chain
3. Round Robin Chain
4. Random Chain

Dynamic Chain

- Dynamic Chaining is That way the proxy Servers are chained is as the proxy list given.
- If there is any server that is not working it will be skipped.
- If any of them doesn't work it will be broken and display errors.



```
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
```

Strict Chain

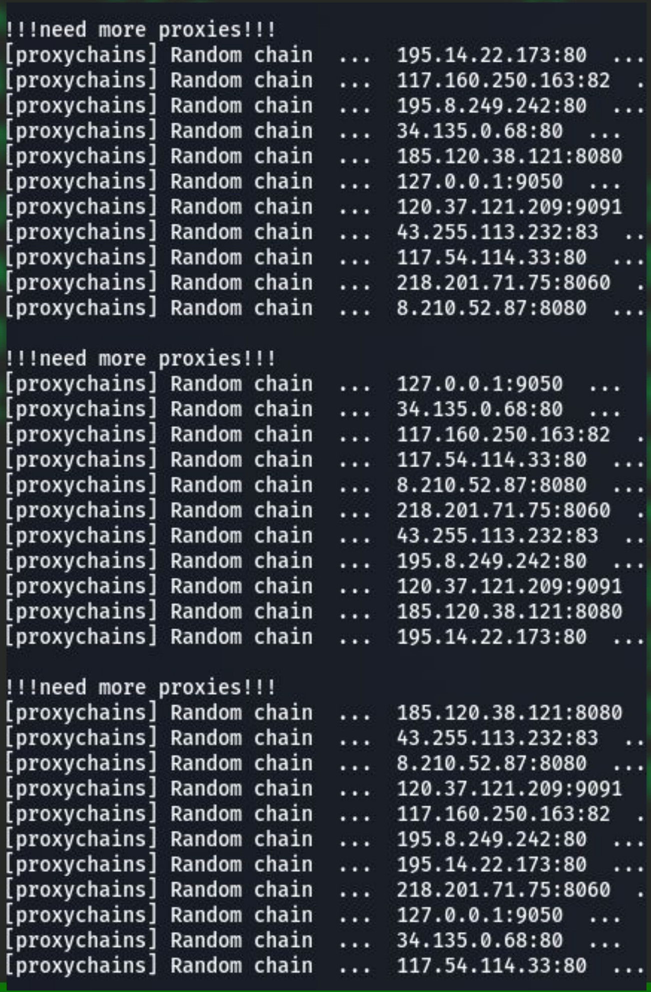
- All Proxies chained in the order as the are listed.
- All proxies Have to be up and working, if one server is not working it will display error

Round Robin chain

- It follows the order of the proxy list
- It will skip if 1 proxy is not working
- If all the proxies not working it will start again and check them.
  - This makes it different from Dynamic chain

Random Chain

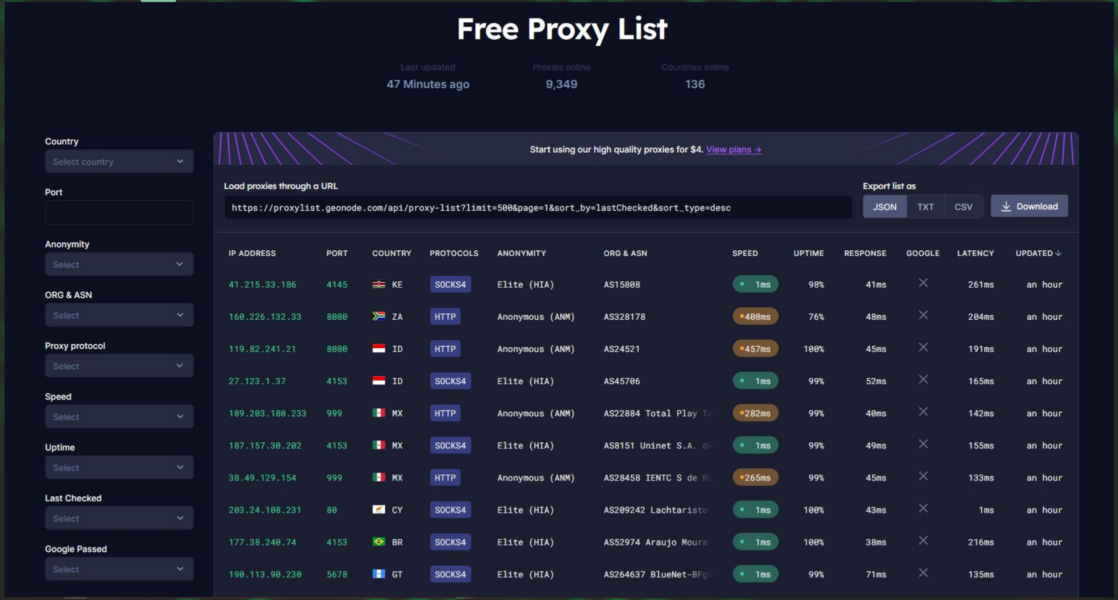
- It will choose some Proxy server Randomly and creates chain in random order.
- Not working will be Skipped!
- Each Request will be in random sequence of servers.



```
!!!need more proxies!!!
[proxychains] Random chain  ...  195.14.22.173:80  ...
[proxychains] Random chain  ...  117.160.250.163:82  .
[proxychains] Random chain  ...  195.8.249.242:80  ...
[proxychains] Random chain  ...  34.135.0.68:80  ...
[proxychains] Random chain  ...  185.120.38.121:8080
[proxychains] Random chain  ...  127.0.0.1:9050  ...
[proxychains] Random chain  ...  120.37.121.209:9091
[proxychains] Random chain  ...  43.255.113.232:83  ..
[proxychains] Random chain  ...  117.54.114.33:80  ...
[proxychains] Random chain  ...  218.201.71.75:8060  .
[proxychains] Random chain  ...  8.210.52.87:8080  ...

!!!need more proxies!!!
[proxychains] Random chain  ...  127.0.0.1:9050  ...
[proxychains] Random chain  ...  34.135.0.68:80  ...
[proxychains] Random chain  ...  117.160.250.163:82  .
[proxychains] Random chain  ...  117.54.114.33:80  ...
[proxychains] Random chain  ...  8.210.52.87:8080  ...
[proxychains] Random chain  ...  218.201.71.75:8060  .
[proxychains] Random chain  ...  43.255.113.232:83  ..
[proxychains] Random chain  ...  195.8.249.242:80  ...
[proxychains] Random chain  ...  120.37.121.209:9091
[proxychains] Random chain  ...  185.120.38.121:8080
[proxychains] Random chain  ...  195.14.22.173:80  ...

!!!need more proxies!!!
[proxychains] Random chain  ...  185.120.38.121:8080
[proxychains] Random chain  ...  43.255.113.232:83  ..
[proxychains] Random chain  ...  8.210.52.87:8080  ...
[proxychains] Random chain  ...  120.37.121.209:9091
[proxychains] Random chain  ...  117.160.250.163:82  .
[proxychains] Random chain  ...  195.8.249.242:80  ...
[proxychains] Random chain  ...  195.14.22.173:80  ...
[proxychains] Random chain  ...  218.201.71.75:8060  .
[proxychains] Random chain  ...  127.0.0.1:9050  ...
[proxychains] Random chain  ...  34.135.0.68:80  ...
[proxychains] Random chain  ...  117.54.114.33:80  ...
```

demo

Getting Working Free Proxy Server is hard, But Hackers Most of the time Buy Some VIP servers, so they can do anything what they want.



Free Proxy List

Last updated: 47 Minutes ago
Proxies online: 9,349
Countries online: 136

Country: Select country
Port:
Anonymity: Select
ORG & ASN: Select
Proxy protocol: Select
Speed: Select
Uptime: Select
Last Checked: Select
Google Passed: Select

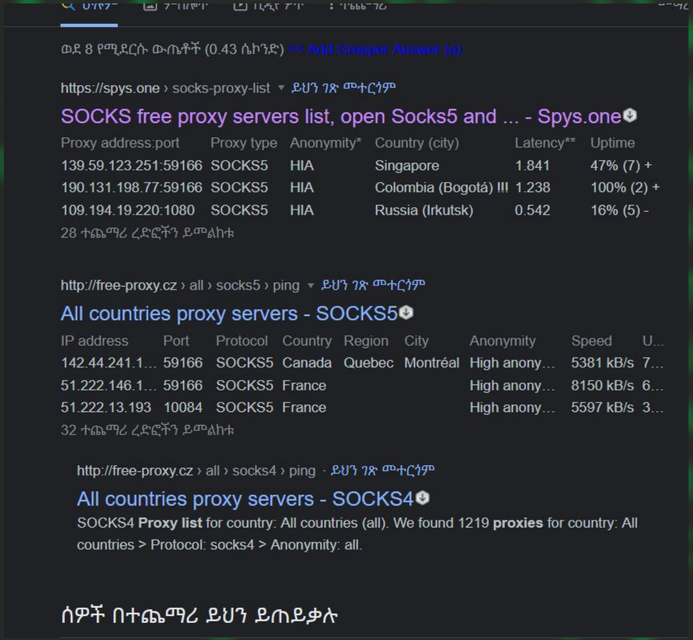
Start using our high quality proxies for $4. View plans →

Load proxies through a URL

```
https://proxylist.geonode.com/api/proxy-list?limit=500&page=1&sort_by=lastChecked&sort_type=desc
```

Export list as: JSON | TXT | CSV | Download

IP ADDRESS	PORT	COUNTRY	PROTOCOLS	ANONYMITY	ORG & ASN	SPEED	UPTIME	RESPONSE	GOOGLE	LATENCY	UPDATED ↓
41.215.33.186	4145	KE	SOCKS4	Elite (HIA)	AS15808	● 1ms	98%	41ms	✕	261ms	an hour
160.226.132.33	8080	ZA	HTTP	Anonymous (ANM)	AS328178	•408ms	76%	48ms	✕	204ms	an hour
119.82.241.21	8080	ID	HTTP	Anonymous (ANM)	AS24521	•457ms	100%	45ms	✕	191ms	an hour
27.123.1.37	4153	ID	SOCKS4	Elite (HIA)	AS45706	● 1ms	99%	52ms	✕	165ms	an hour
189.203.180.233	999	MX	HTTP	Anonymous (ANM)	AS22884 Total Play Te	•282ms	99%	40ms	✕	142ms	an hour
187.157.30.202	4153	MX	SOCKS4	Elite (HIA)	AS8151 Uninet S.A. de	● 1ms	99%	49ms	✕	155ms	an hour
38.49.129.154	999	MX	HTTP	Anonymous (ANM)	AS28458 IENTC S de RL	•265ms	99%	45ms	✕	133ms	an hour
203.24.108.231	80	CY	SOCKS4	Elite (HIA)	AS209242 Lachtaristo	● 1ms	100%	43ms	✕	1ms	an hour
177.38.240.74	4153	BR	SOCKS4	Elite (HIA)	AS52974 Araujo Moura	● 1ms	100%	38ms	✕	216ms	an hour
190.113.90.230	5678	GT	SOCKS4	Elite (HIA)	AS264637 BlueNet-BFgt	● 1ms	99%	71ms	✕	135ms	an hour



ወደ 8 የሚደርሱ ውጤቶች (0.43 ሴኮንድ) << Add Grepper Answer (a)

https://spys.one › socks-proxy-list ▾ ይህን ገጽ መተርጎም

SOCKS free proxy servers list, open Socks5 and ... - Spys.one

Proxy address:port	Proxy type	Anonymity*	Country (city)	Latency**	Uptime
139.59.123.251:59166	SOCKS5	HIA	Singapore	1.841	47% (7) +
190.131.198.77:59166	SOCKS5	HIA	Colombia (Bogotá) !!!	1.238	100% (2) +
109.194.19.220:1080	SOCKS5	HIA	Russia (Irkutsk)	0.542	16% (5) -

28 ተጨማሪ ረድፎችን ይመልከቱ

http://free-proxy.cz › all › socks5 › ping ▾ ይህን ገጽ መተርጎም

All countries proxy servers - SOCKS5

IP address	Port	Protocol	Country	Region	City	Anonymity	Speed	U...
142.44.241.1...	59166	SOCKS5	Canada	Quebec	Montréal	High anony...	5381 kB/s	7...
51.222.146.1...	59166	SOCKS5	France			High anony...	8150 kB/s	6...
51.222.13.193	10084	SOCKS5	France			High anony...	5597 kB/s	3...

32 ተጨማሪ ረድፎችን ይመልከቱ

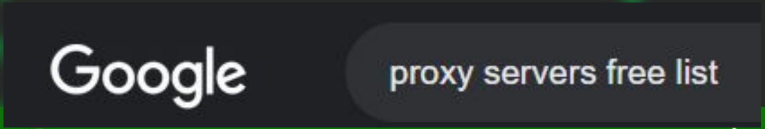
http://free-proxy.cz › all › socks4 › ping · ይህን ገጽ መተርጎም

All countries proxy servers - SOCKS4

SOCKS4 **Proxy list** for country: All countries (all). We found 1219 **proxies** for country: All countries > Protocol: socks4 > Anonymity: all.

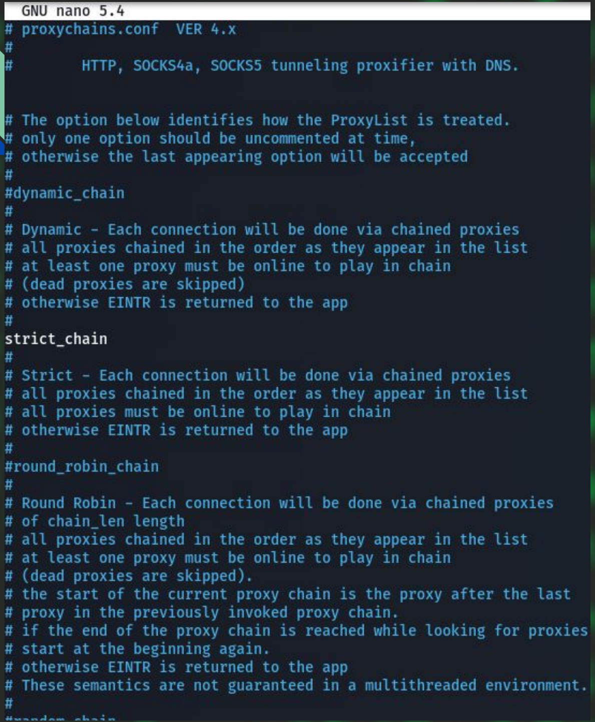
ሰዎች በተጨማሪ ይህን ይጠይቃሉ

1. Find some Proxy servers to use.
   a. google.com
   b. https://geonode.com/

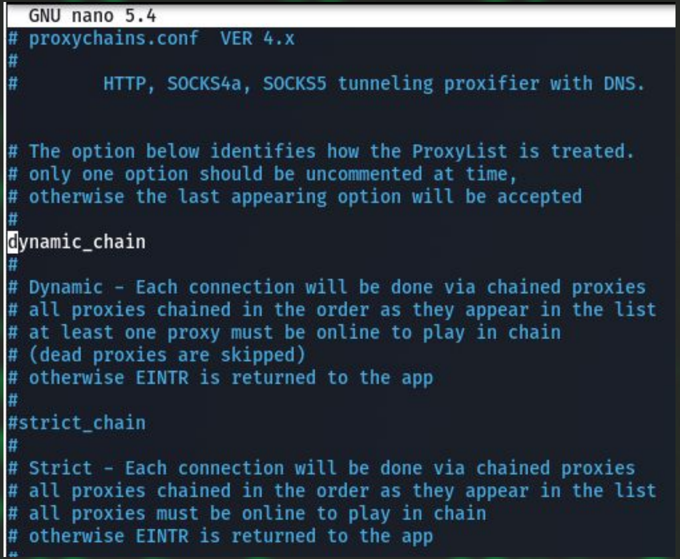


proxy servers free list

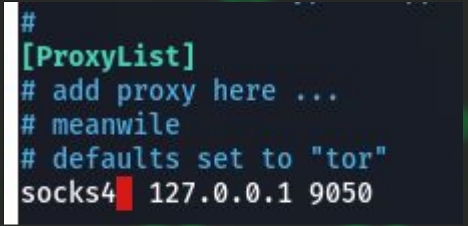
...



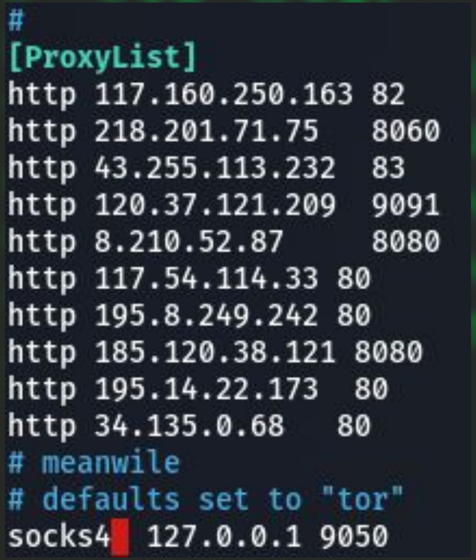
```
 GNU nano 5.4
# proxychains.conf  VER 4.x
#
#        HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.


# 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
# (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
#
#round_robin_chain
#
# Round Robin - Each connection will be done via chained proxies
# of chain_len length
# 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).
# the start of the current proxy chain is the proxy after the last
# proxy in the previously invoked proxy chain.
# if the end of the proxy chain is reached while looking for proxies
# start at the beginning again.
# otherwise EINTR is returned to the app
# These semantics are not guaranteed in a multithreaded environment.
#
#random_chain
```



```
 GNU nano 5.4
# proxychains.conf  VER 4.x
#
#        HTTP, SOCKS4a, 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
# (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
#
```



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



```
#
[ProxyList]
http 117.160.250.163 82
http 218.201.71.75   8060
http 43.255.113.232  83
http 120.37.121.209  9091
http 8.210.52.87     8080
http 117.54.114.33 80
http 195.8.249.242 80
http 185.120.38.121 8080
http 195.14.22.173  80
http 34.135.0.68   80
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

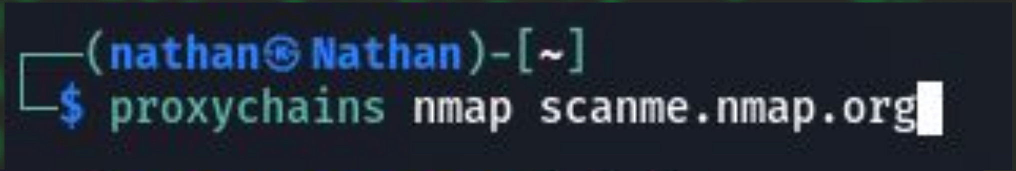
2. Open /etc/proxychains4.conf

   A. Turn on any kind proxychain you need
   B. Put your proxy servers

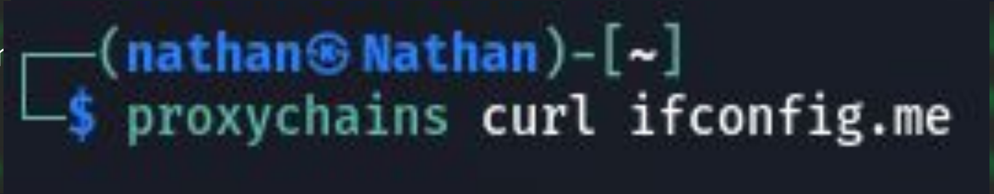
…

3. Accessing with proxychains
    1. Add “proxychains” in front of ar command.

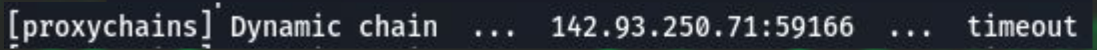
- Find a working proxy server and you are good to go!



```
┌──(nathan㉿Nathan)-[~]
└─$ proxychains nmap scanme.nmap.org
```



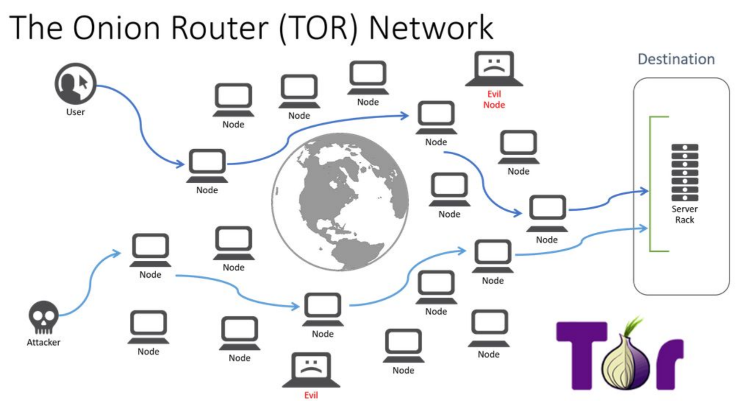
```
┌──(nathan㉿Nathan)-[~]
└─$ proxychains curl ifconfig.me
```

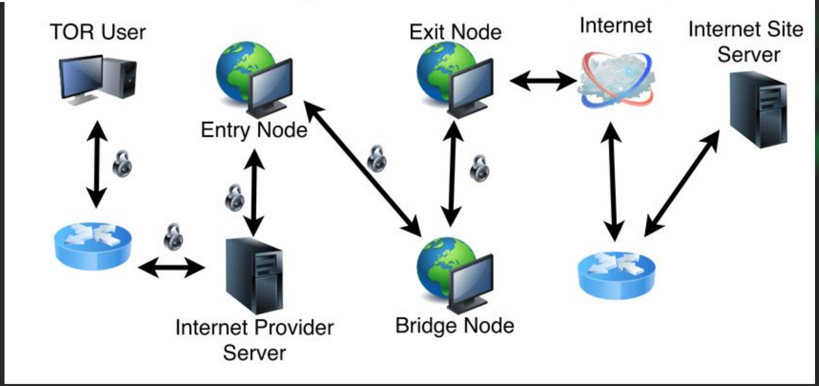


```
[proxychains] Dynamic chain  ...  142.93.250.71:59166  ...  timeout
```

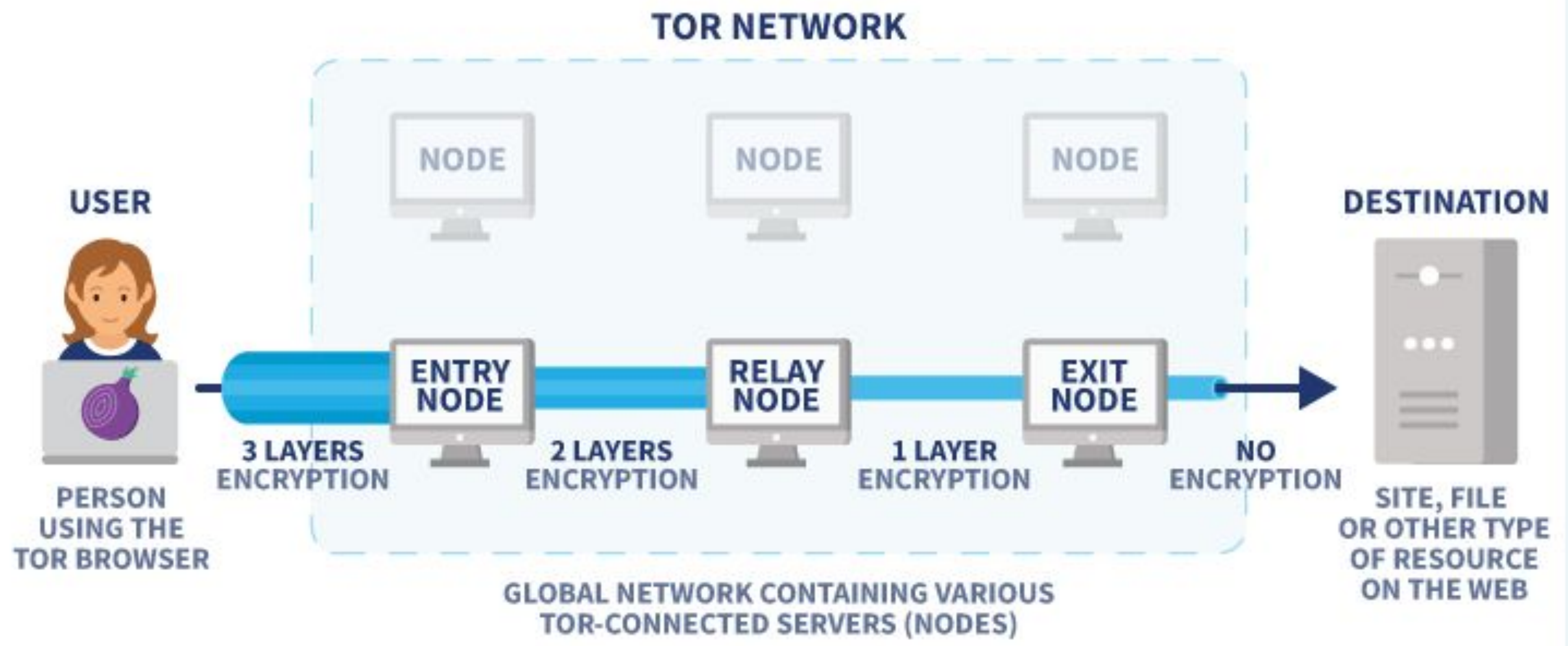
T.O.R/**T**he **O**nion **R**outing/ Network

- Tor is an open-source privacy network that enables anonymous web browsing.
- The worldwide Tor computer network uses secure, encrypted protocols to ensure that users' online privacy is protected.
- Tor users' digital data and communications are shielded using a layered approach that resembles the nested layers of an onion.
- Tor uses an onion-style routing technique for transmitting data.
- When you use the Tor browser to digitally communicate or access a website, the Tor network does not directly connect your computer to that website.
- Instead, the traffic from your browser is intercepted by Tor and bounced to a random number of other Tor users’ computers before passing the request to its final website destination.



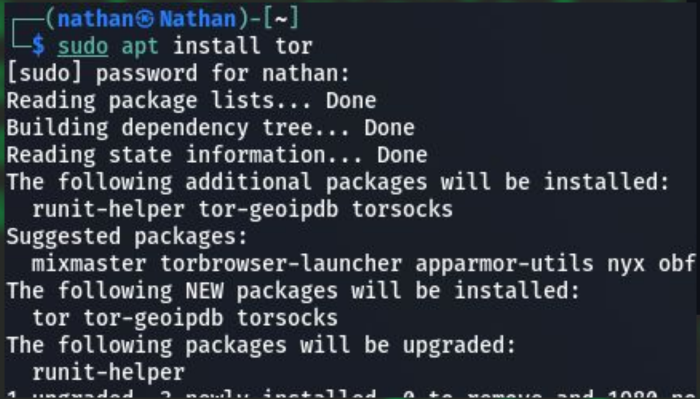


HOW DOES THE TOR NETWORK WORK?

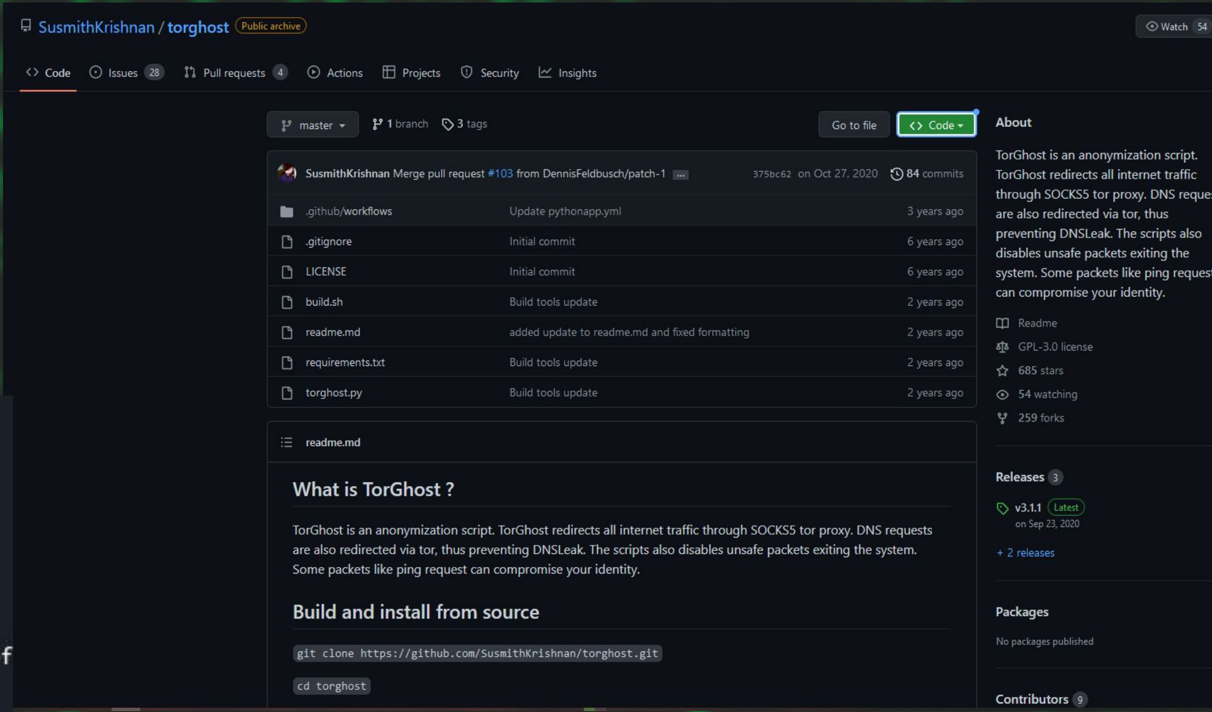

TOR NETWORK
USER
NODE
NODE
NODE
DESTINATION
ENTRY NODE
RELAY NODE
EXIT NODE
3 LAYERS ENCRYPTION
2 LAYERS ENCRYPTION
1 LAYER ENCRYPTION
NO ENCRYPTION
PERSON USING THE TOR BROWSER
SITE, FILE OR OTHER TYPE OF RESOURCE ON THE WEB
GLOBAL NETWORK CONTAINING VARIOUS TOR-CONNECTED SERVERS (NODES)

torghost

- Clone it from github
  - https://github.com/SusmithKrishnan/torghost
- Install tor
- Open it!



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo apt install tor
[sudo] password for nathan:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  runit-helper tor-geoipdb torsocks
Suggested packages:
  mixmaster torbrowser-launcher apparmor-utils nyx obf
The following NEW packages will be installed:
  tor tor-geoipdb torsocks
The following packages will be upgraded:
  runit-helper
1 upgraded, 2 newly installed, 0 to remove and 1080 no
```



SusmithKrishnan / torghost Public archive

SusmithKrishnan Merge pull request #103 from DennisFeldbusch/patch-1 … 375bc62 on Oct 27, 2020 84 commits

.github/workflows	Update pythonapp.yml	3 years ago
.gitignore	Initial commit	6 years ago
LICENSE	Initial commit	6 years ago
build.sh	Build tools update	2 years ago
readme.md	added update to readme.md and fixed formatting	2 years ago
requirements.txt	Build tools update	2 years ago
torghost.py	Build tools update	2 years ago

readme.md

What is TorGhost ?

TorGhost is an anonymization script. TorGhost redirects all internet traffic through SOCKS5 tor proxy. DNS requests are also redirected via tor, thus preventing DNSLeak. The scripts also disables unsafe packets exiting the system. Some packets like ping request can compromise your identity.

Build and install from source

```
git clone https://github.com/SusmithKrishnan/torghost.git
```

```
cd torghost
```

About

TorGhost is an anonymization script. TorGhost redirects all internet traffic through SOCKS5 tor proxy. DNS reque are also redirected via tor, thus preventing DNSLeak. The scripts also disables unsafe packets exiting the system. Some packets like ping reques can compromise your identity.

Readme
GPL-3.0 license
685 stars
54 watching
259 forks

Releases 3

v3.1.1 Latest
on Sep 23, 2020

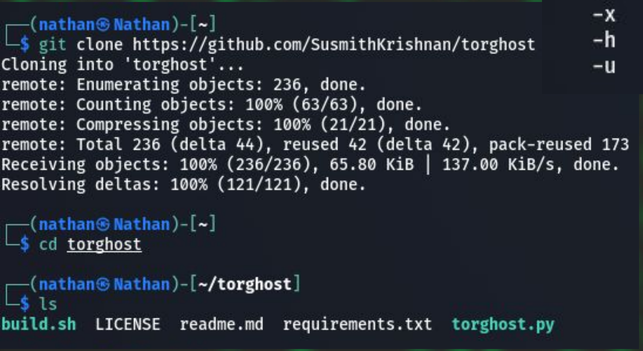
+ 2 releases

Packages

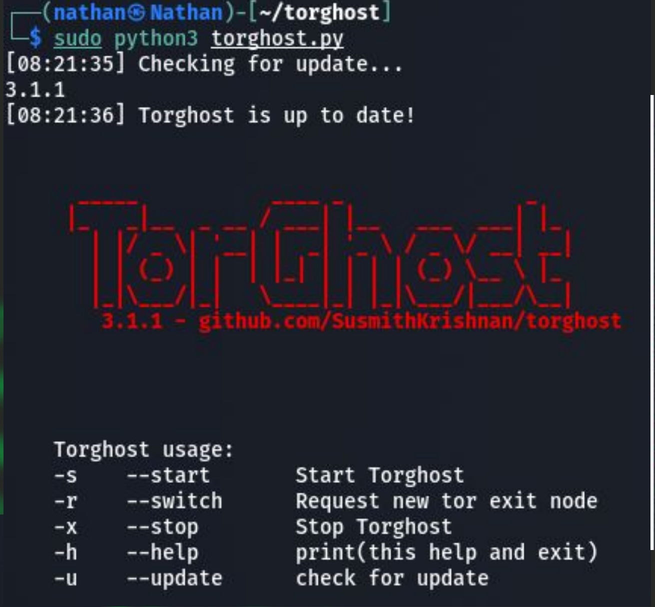
No packages published

Contributors 9

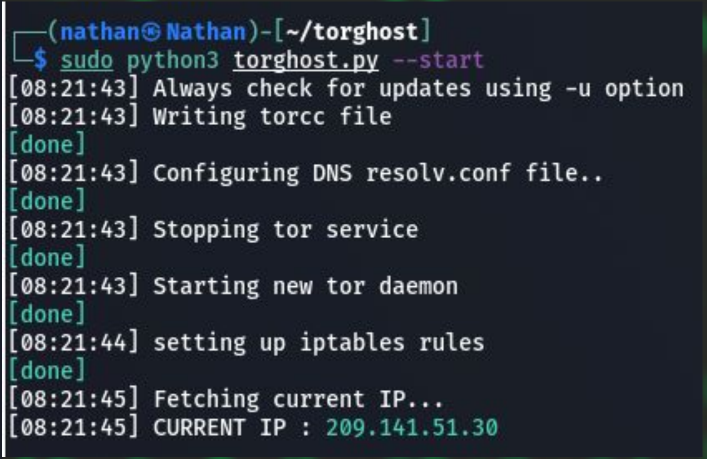
...



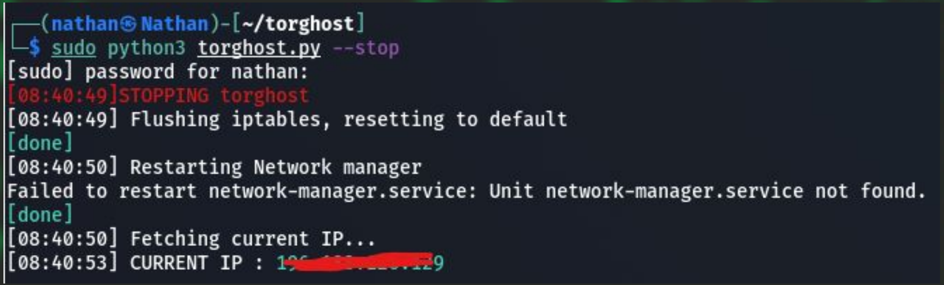
```
┌──(nathan㉿Nathan)-[~]
└─$ git clone https://github.com/SusmithKrishnan/torghost
Cloning into 'torghost'...
remote: Enumerating objects: 236, done.
remote: Counting objects: 100% (63/63), done.
remote: Compressing objects: 100% (21/21), done.
remote: Total 236 (delta 44), reused 42 (delta 42), pack-reused 173
Receiving objects: 100% (236/236), 65.80 KiB | 137.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.

┌──(nathan㉿Nathan)-[~]
└─$ cd torghost

┌──(nathan㉿Nathan)-[~/torghost]
└─$ ls
build.sh  LICENSE  readme.md  requirements.txt  torghost.py
```



```
┌──(nathan㉿Nathan)-[~/torghost]
└─$ sudo python3 torghost.py
[08:21:35] Checking for update...
3.1.1
[08:21:36] Torghost is up to date!

      TorGhost
   3.1.1 - github.com/SusmithKrishnan/torghost


    Torghost usage:
    -s    --start        Start Torghost
    -r    --switch       Request new tor exit node
    -x    --stop         Stop Torghost
    -h    --help         print(this help and exit)
    -u    --update       check for update
```



```
┌──(nathan㉿Nathan)-[~/torghost]
└─$ sudo python3 torghost.py --start
[08:21:43] Always check for updates using -u option
[08:21:43] Writing torcc file
[done]
[08:21:43] Configuring DNS resolv.conf file..
[done]
[08:21:43] Stopping tor service
[done]
[08:21:43] Starting new tor daemon
[done]
[08:21:44] setting up iptables rules
[done]
[08:21:45] Fetching current IP...
[08:21:45] CURRENT IP : 209.141.51.30
```

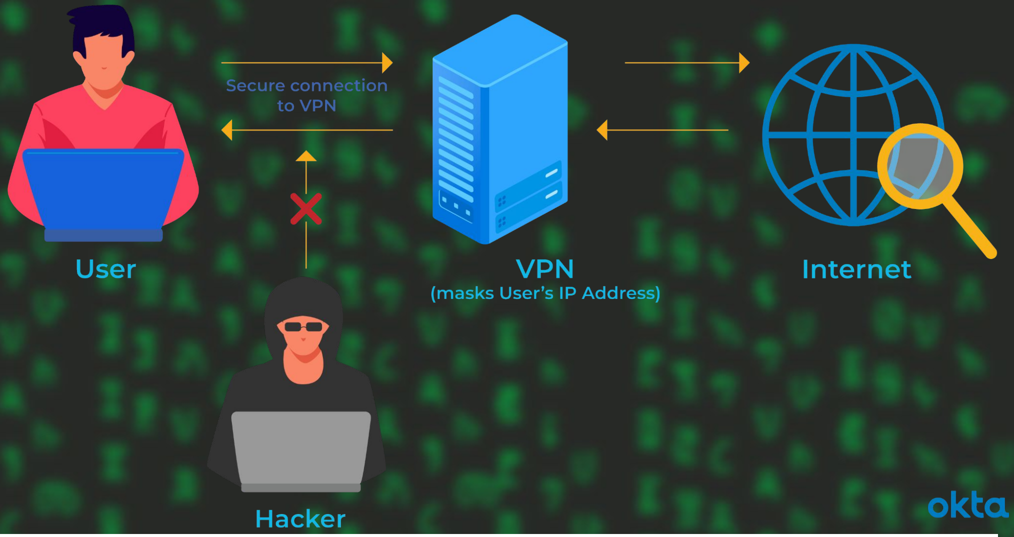


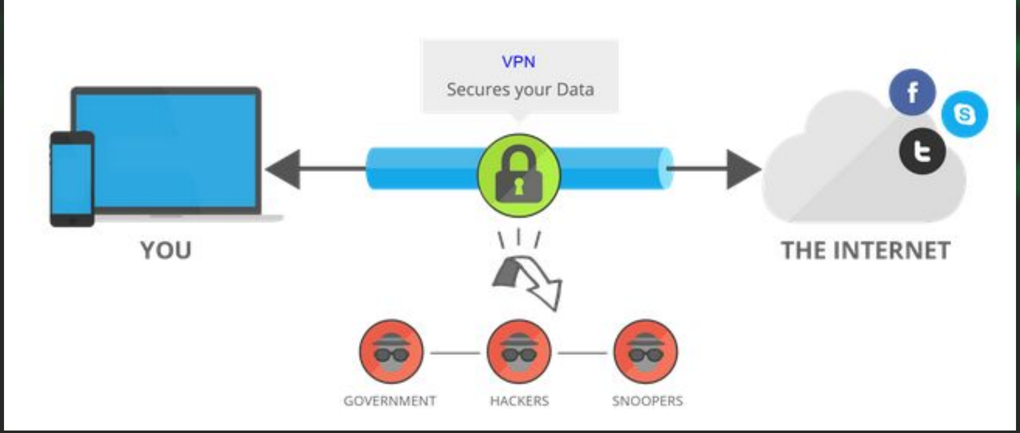
```
┌──(nathan㉿Nathan)-[~/torghost]
└─$ sudo python3 torghost.py --stop
[sudo] password for nathan:
[08:40:49]STOPPING torghost
[08:40:49] Flushing iptables, resetting to default
[done]
[08:40:50] Restarting Network manager
Failed to restart network-manager.service: Unit network-manager.service not found.
[done]
[08:40:50] Fetching current IP...
[08:40:53] CURRENT IP : [redacted]
```

- Your last Proxy IP will be shown(Public IP)

VPNs

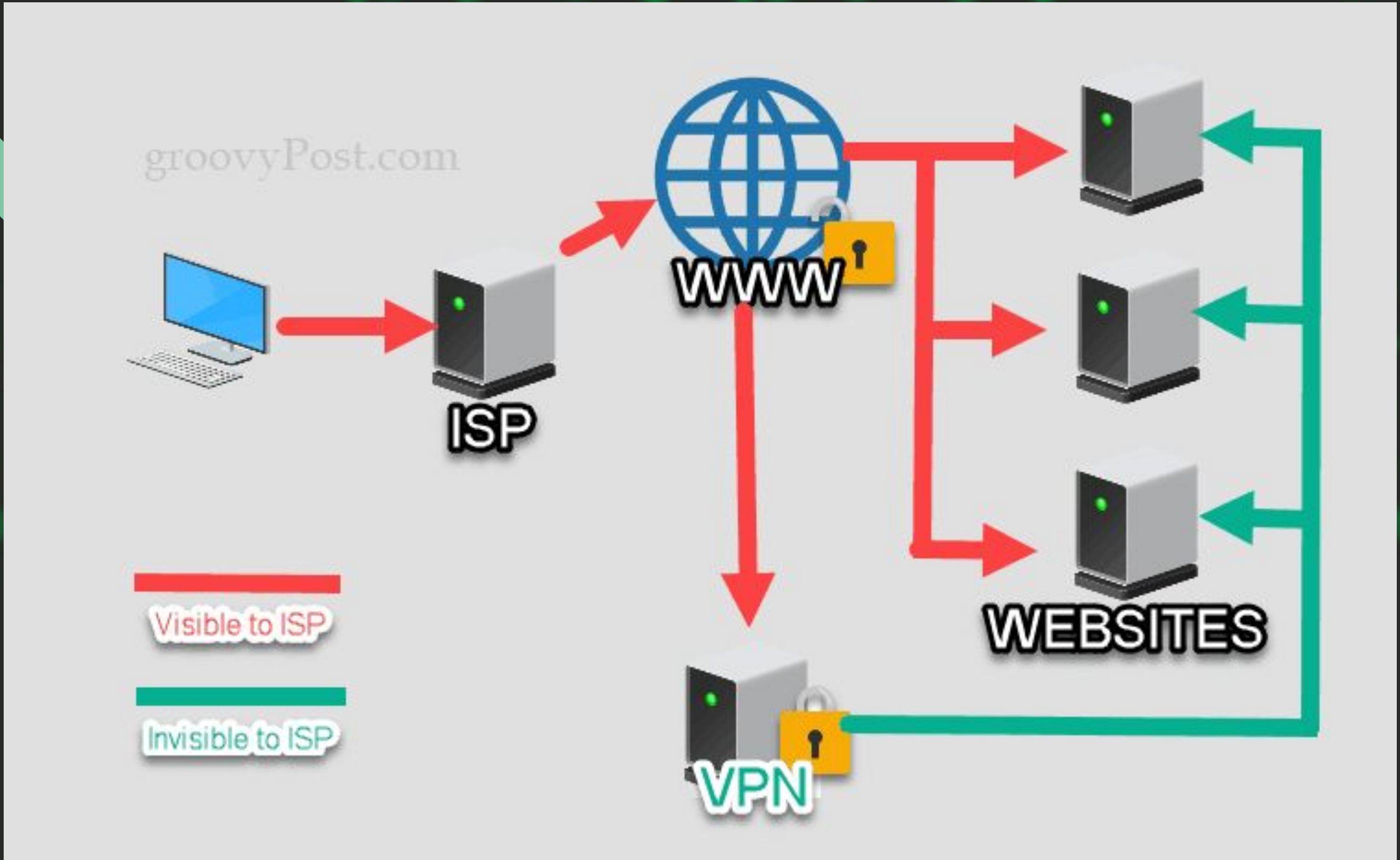
- VPN means Virtual Private Network.
- a service that helps you stay private online.
- A VPN establishes a secure, encrypted connection between your computer and the internet, providing a private tunnel for your data and communications while you use public networks



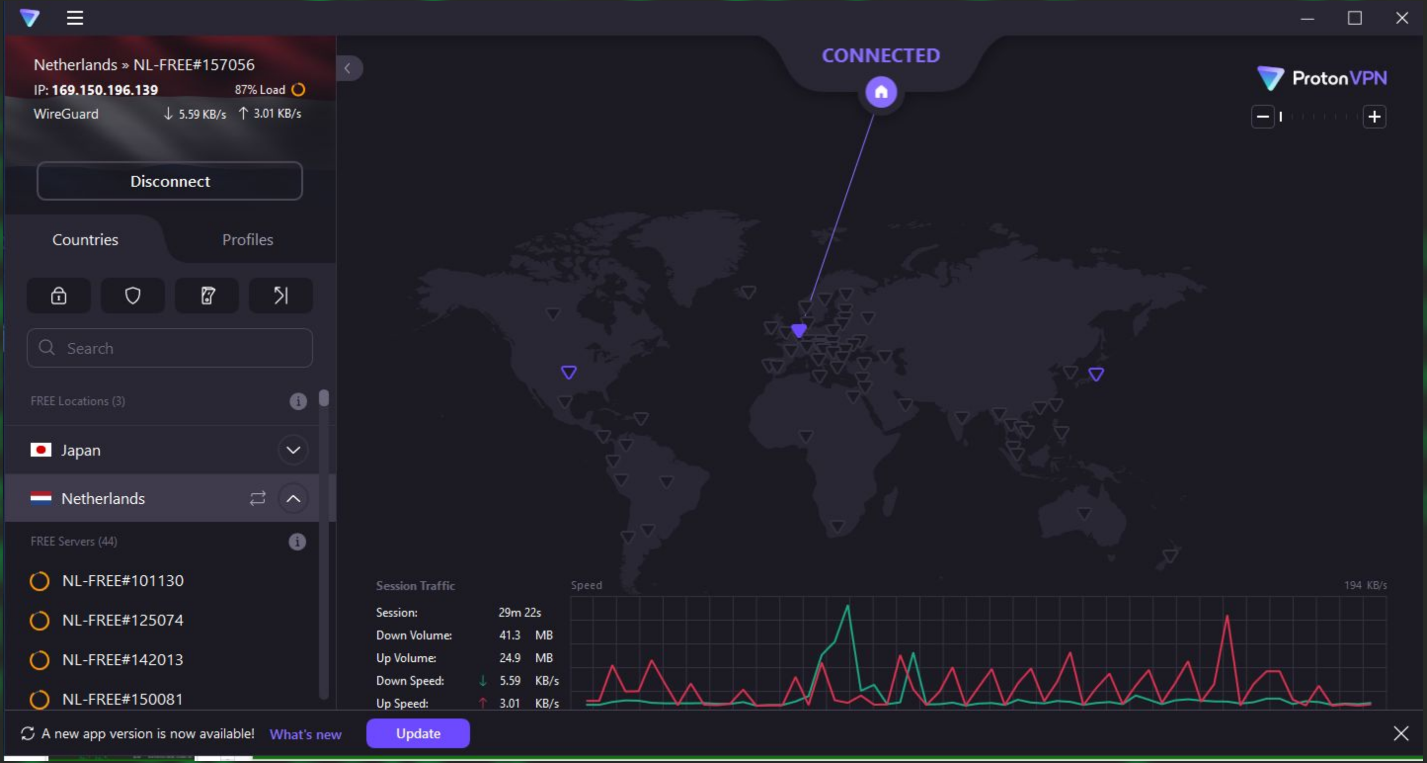


VPN...

- There are a lot of VPNS, those are paid and free
- The paid are more secured and private, still the free are Good
- Example: Nord VPN, Proton VPN, windscribe VPN,...



groovyPost.com
WWW
ISP
WEBSITES
VPN
Visible to ISP
Invisible to ISP



Netherlands » NL-FREE#157056

IP: 169.150.196.139 87% Load

WireGuard ↓ 5.59 KB/s ↑ 3.01 KB/s

Session Traffic

Session: 29m 22s

Down Volume: 41.3 MB

Up Volume: 24.9 MB

Down Speed: ↓ 5.59 KB/s

Up Speed: ↑ 3.01 KB/s

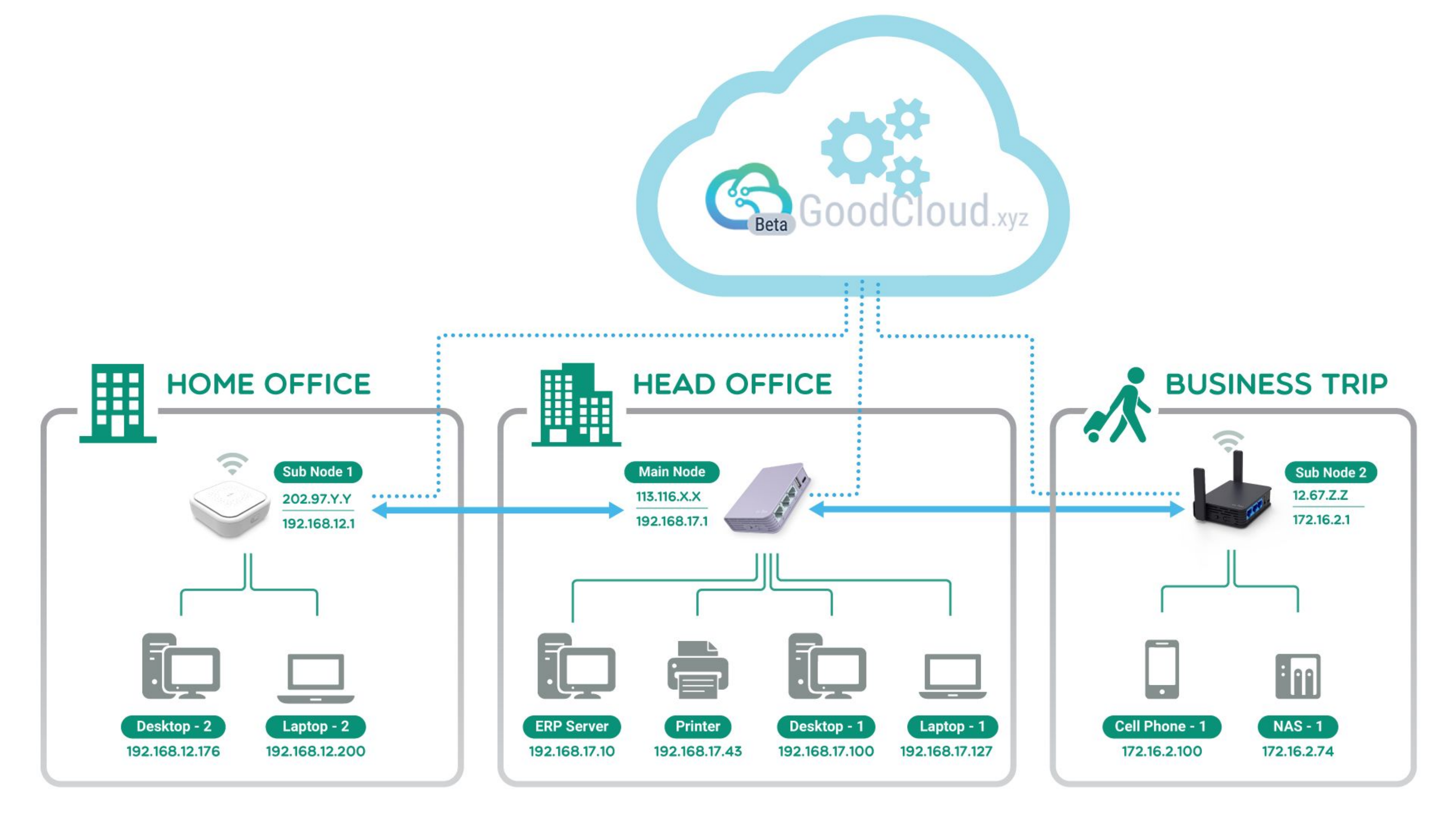
A new app version is now available! What's new Update

Buying premium VPNS are good.

Types of VPN

A) **SITE to SITE**

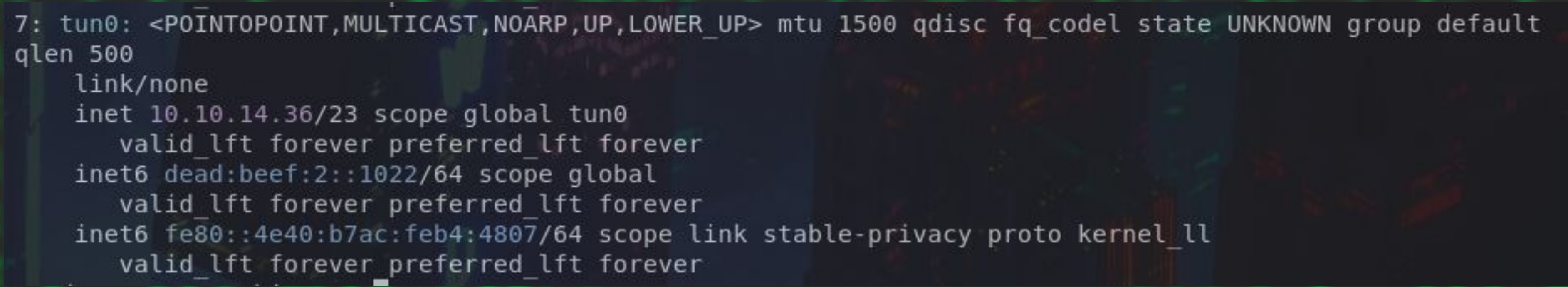
- This is most commonly used to join company networks together over the Internet
- allowing multiple locations to communicate over the Internet as if they were local.
- Router + Routers


Beta
GoodCloud.xyz
HOME OFFICE
HEAD OFFICE
BUSINESS TRIP
Sub Node 1
202.97.Y.Y
192.168.12.1
Main Node
113.116.X.X
192.168.17.1
Sub Node 2
12.67.Z.Z
172.16.2.1
Desktop - 2
192.168.12.176
Laptop - 2
192.168.12.200
ERP Server
192.168.17.10
Printer
192.168.17.43
Desktop - 1
192.168.17.100
Laptop - 1
192.168.17.127
Cell Phone - 1
172.16.2.100
NAS - 1
172.16.2.74

Cont...

B) Remote Access VPN

- involves the client's computer creating a virtual interface that behaves as if it is on a client's network
  - Hacking game utilizes `OpenVPN`, which makes a TUN Adapter letting us access the labs
- When analyzing these VPNs, an important piece to consider is the routing table that is created when joining the VPN.
- If the VPN only creates routes for specific networks (ex: 10.10.10.0/24), this is called a `Split-Tunnel VPN`, meaning the Internet connection is not going out of the VPN.
- This is great for Hacking Games because it provides access to the Lab without the privacy concern of monitoring your internet connection
-

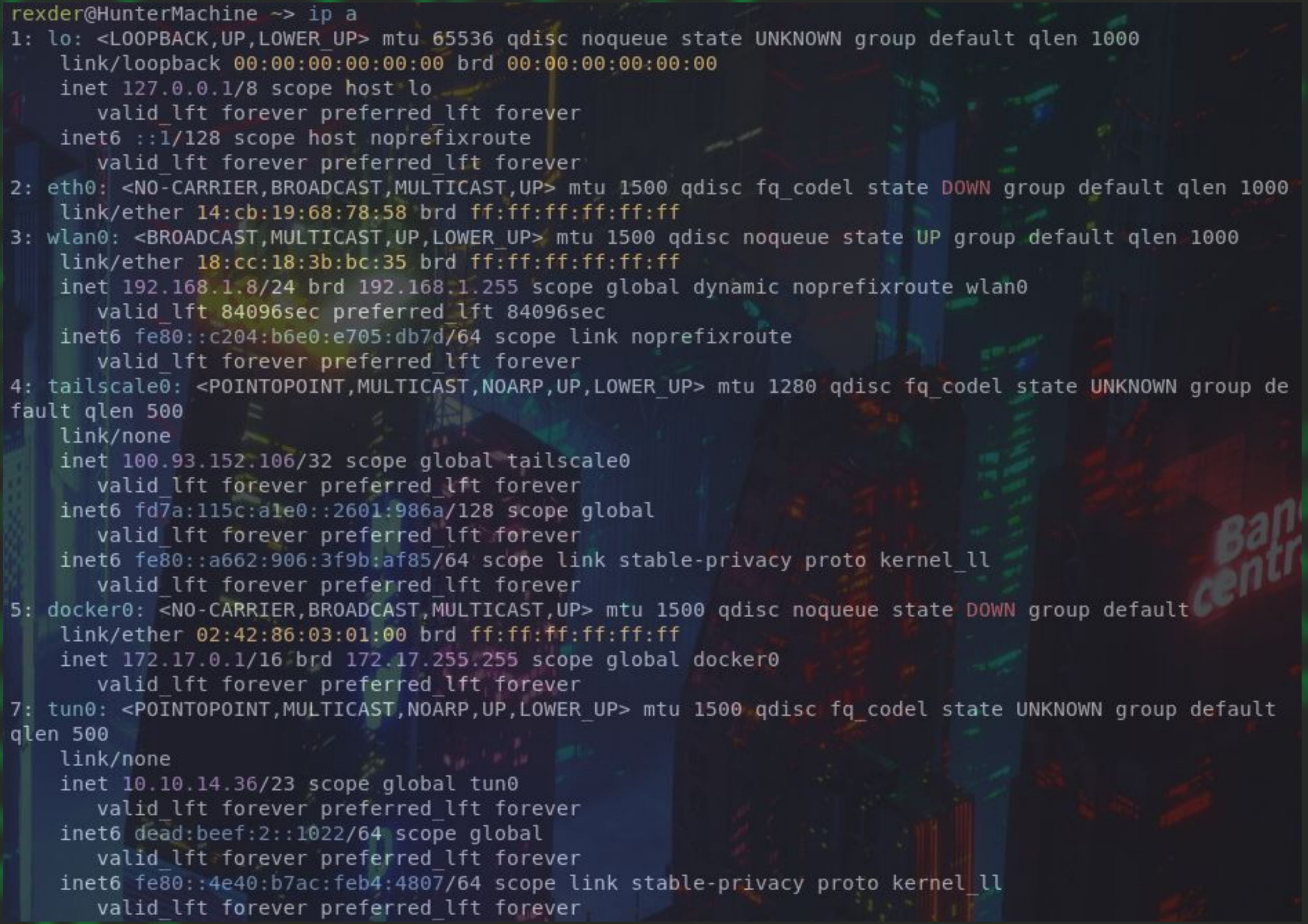


```
7: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default
qlen 500
    link/none
    inet 10.10.14.36/23 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:2::1022/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::4e40:b7ac:feb4:4807/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
```

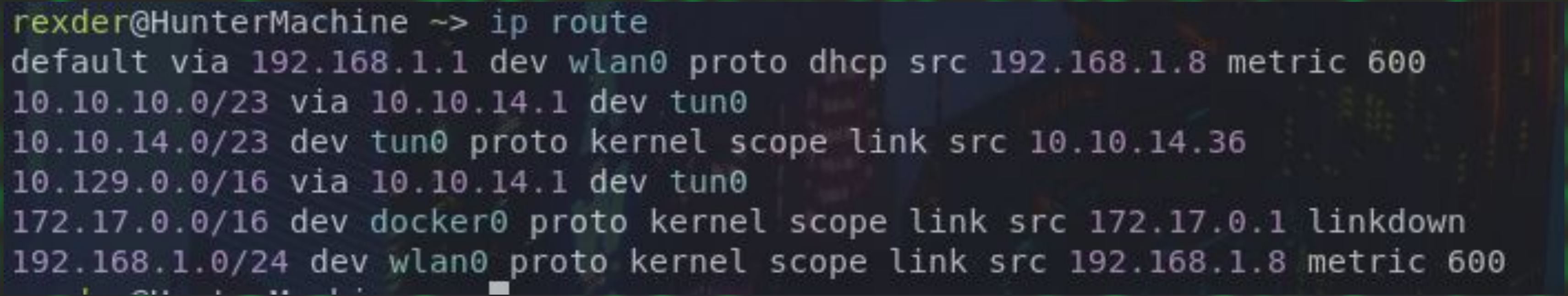
Additional Network Interface

These are all my Interfaces on my computer.

Foreach interfaces to work and communicate with the router they need to have Routing paths.



```
rexder@HunterMachine ~> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 14:cb:19:68:78:58 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 18:cc:18:3b:bc:35 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.8/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
       valid_lft 84096sec preferred_lft 84096sec
    inet6 fe80::c204:b6e0:e705:db7d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: tailscale0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1280 qdisc fq_codel state UNKNOWN group de
fault qlen 500
    link/none
    inet 100.93.152.106/32 scope global tailscale0
       valid_lft forever preferred_lft forever
    inet6 fd7a:115c:a1e0::2601:986a/128 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::a662:906:3f9b:af85/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:86:03:01:00 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
7: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default
qlen 500
    link/none
    inet 10.10.14.36/23 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:2::1022/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::4e40:b7ac:feb4:4807/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
```



```
rexder@HunterMachine ~> ip route
default via 192.168.1.1 dev wlan0 proto dhcp src 192.168.1.8 metric 600
10.10.10.0/23 via 10.10.14.1 dev tun0
10.10.14.0/23 dev tun0 proto kernel scope link src 10.10.14.36
10.129.0.0/16 via 10.10.14.1 dev tun0
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
192.168.1.0/24 dev wlan0 proto kernel scope link src 192.168.1.8 metric 600
```

As You see out TUN0 network have a route.

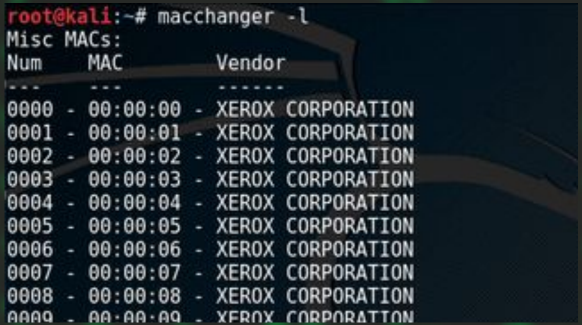
Cont...

C) SSL VPN

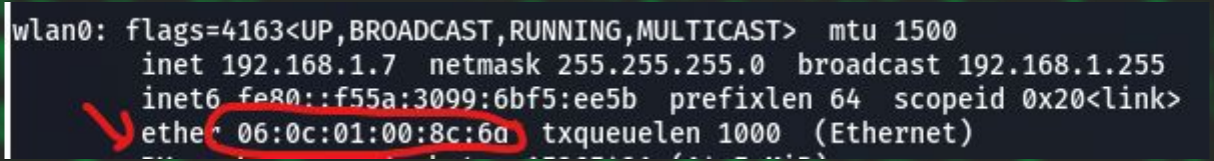
- essentially a VPN that is done within our web browser and is becoming increasingly common as web browsers are becoming capable of doing anything.
- These will stream applications or entire desktop sessions to your web browser.

Mac Changer

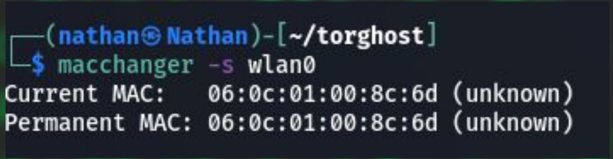
- As We saw MAC address can tell about our Device.
- SO , if we changed that we can change our device id.



```
root@kali:~# macchanger -l
Misc MACs:
Num    MAC          Vendor
---    ---          ------
0000 - 00:00:00 - XEROX CORPORATION
0001 - 00:00:01 - XEROX CORPORATION
0002 - 00:00:02 - XEROX CORPORATION
0003 - 00:00:03 - XEROX CORPORATION
0004 - 00:00:04 - XEROX CORPORATION
0005 - 00:00:05 - XEROX CORPORATION
0006 - 00:00:06 - XEROX CORPORATION
0007 - 00:00:07 - XEROX CORPORATION
0008 - 00:00:08 - XEROX CORPORATION
0009 - 00:00:09 - XEROX CORPORATION
```

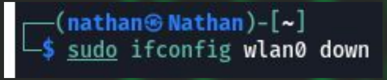


```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f55a:3099:6bf5:ee5b  prefixlen 64  scopeid 0x20<link>
        ether 06:0c:01:00:8c:6d  txqueuelen 1000  (Ethernet)
```

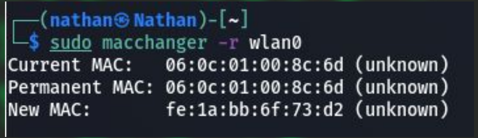


```
┌──(nathan㉿Nathan)-[~/torghost]
└─$ macchanger -s wlan0
Current MAC:   06:0c:01:00:8c:6d (unknown)
Permanent MAC: 06:0c:01:00:8c:6d (unknown)
```

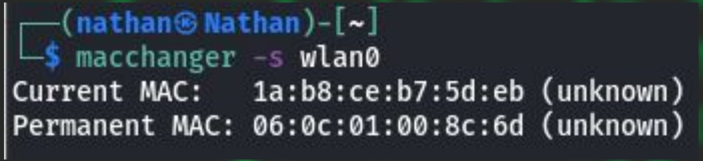
- We can use tool called “macchanger” on kali
- 1st turn off the interface you want to change.



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo ifconfig wlan0 down
```

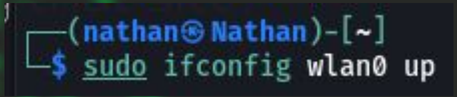


```
┌──(nathan㉿Nathan)-[~]
└─$ sudo macchanger -r wlan0
Current MAC:   06:0c:01:00:8c:6d (unknown)
Permanent MAC: 06:0c:01:00:8c:6d (unknown)
New MAC:       fe:1a:bb:6f:73:d2 (unknown)
```



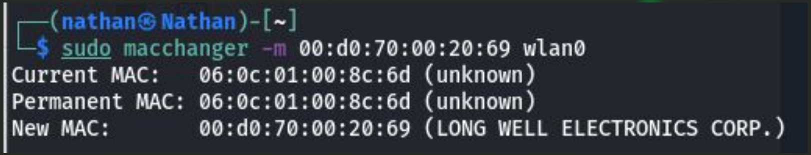
```
┌──(nathan㉿Nathan)-[~]
└─$ macchanger -s wlan0
Current MAC:   1a:b8:ce:b7:5d:eb (unknown)
Permanent MAC: 06:0c:01:00:8c:6d (unknown)
```

- Turn it on now!



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo ifconfig wlan0 up
```

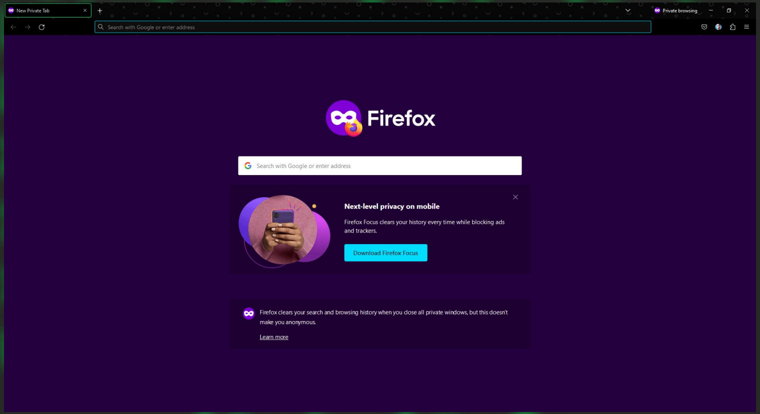
- You can add your specific MAC with -m option



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo macchanger -m 00:d0:70:00:20:69 wlan0
Current MAC:   06:0c:01:00:8c:6d (unknown)
Permanent MAC: 06:0c:01:00:8c:6d (unknown)
New MAC:       00:d0:70:00:20:69 (LONG WELL ELECTRONICS CORP.)
```

Incognito mode

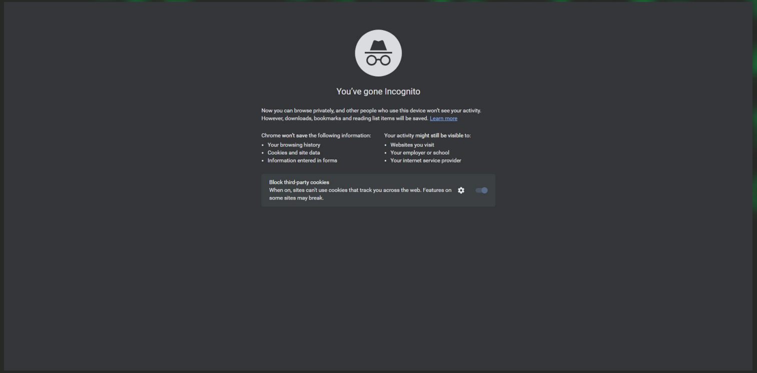
- This is a mode that browsers have.
- This will help you to have a browser with out logging your history,cookies,cache,..
- This will help you when you are try to surf some site but if you dont need the site to know your identity, you can use this because it doesnt have any recording process.


New Private Tab
Private browsing
Search with Google or enter address
Firefox
Search with Google or enter address
Download Firefox Focus
Learn more

Next-level privacy on mobile

Firefox Focus clears your history every time while blocking ads and trackers.

Firefox clears your search and browsing history when you close all private windows, but this doesn't make you anonymous.


You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save the following information:
- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:
- Websites you visit
- Your employer or school
- Your internet service provider

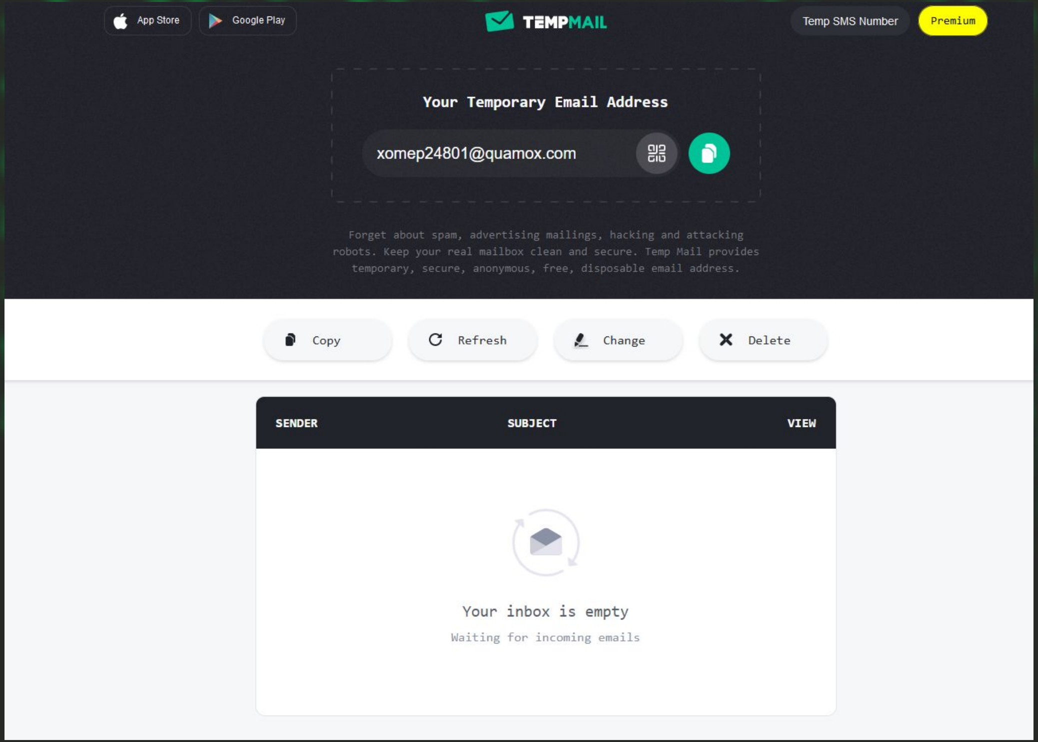
Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

Secure OS

- This are Operating systems, that have a security and privacy feature.
- Windows and Mac OS will record some of your activity also they are not good on privacy and security.
- There for the always Best OS Linux is always recommended when you think about privacy and Security.

Temporary mail

- While You do some pentest you dont have to expose your email and profile for this purpose u need fake emails,
- but if you dont have to time create one you can use fake email providers.
- https://temp-mail.org/
- It have a browser extention too



Your Temporary Email Address

xomep24801@quamox.com

Forget about spam, advertising mailings, hacking and attacking robots. Keep your real mailbox clean and secure. Temp Mail provides temporary, secure, anonymous, free, disposable email address.

SENDER	SUBJECT	VIEW

Your inbox is empty

Waiting for incoming emails

Exercise 1 10 min

1. Interact with torghost
2. Change your mac to 00:d0:70:00:20:69
3. Create a fake email

True anonymity is hard

- Every server you connect to on the internet — be it a web server, a mail server, or a VPN server — can see your IP address. This is a number that uniquely identifies your internet connection and can be easily traced back to you. Achieving true anonymity on the internet therefore requires good operational security (OPSEC) on your part to ensure your real IP address is not revealed.
- Tools that can hide your IP address and protect anonymity include VPNs and the Tor anonymity network, but there's no solution that can guarantee 100% anonymity. Tor is sometimes considered to be more anonymous than VPNs due to its decentralized nature, but it comes at the cost of lower performance, ease of use, and stability.
- Full anonymity is difficult because you must always use anonymity tools for all aspects of your online life, as even a temporary lack of anonymity is sufficient to expose your identity.

Deep web

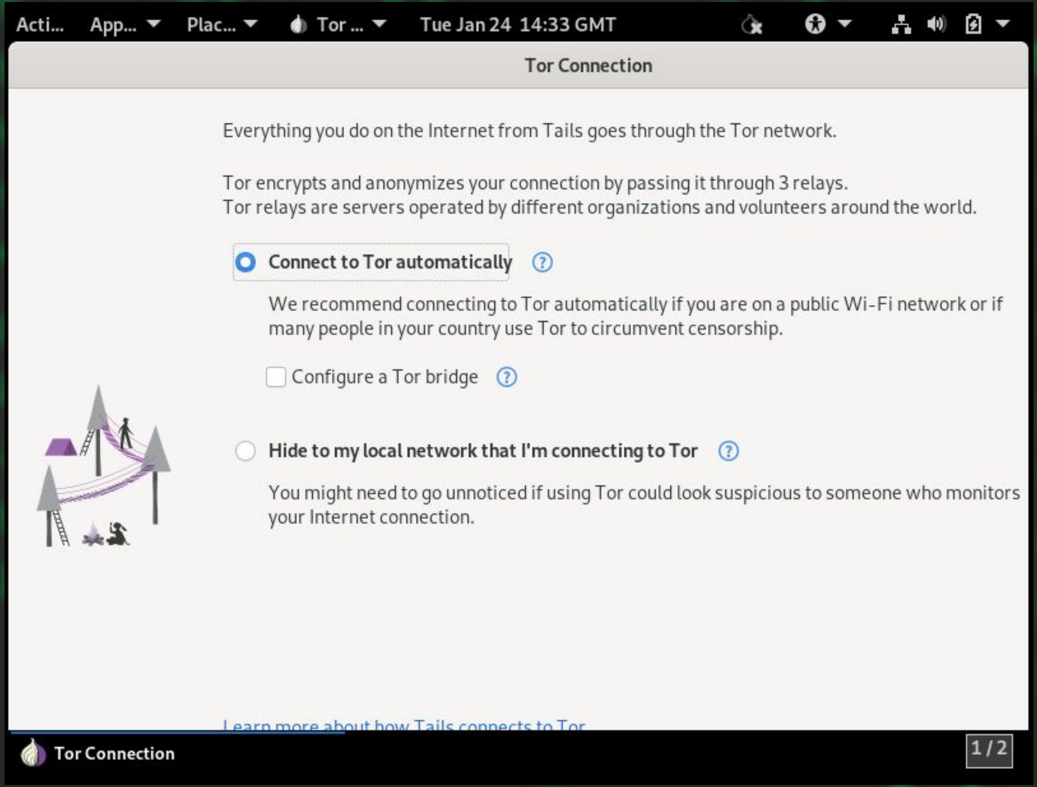
- The deep web refers to all the web pages and data that are not indexed by search engines and cannot be accessed through traditional search methods. It includes content that is protected by passwords, databases, and other security measures.
- Examples of deep web content include private email accounts, online banking portals, subscription-based websites, and more.
- Essentially, the deep web is the part of the internet that is not easily accessible to the general public.

DARK WEB

- The dark web is a part of the internet that isn't indexed by search engines.
- You've no doubt heard talk of the “dark web” as a hotbed of criminal activity
- The dark web is a small portion of the deep web that is intentionally hidden and requires specific software or configurations to access.
- It is unique type of internet world.
- Their link ends with .onion , this is because it uses TOR networks.
- Also this kinds of links won’t be opened by normal browser.
- For this purpose we need a special .onion reading browser,
    - Example: Tor browser.
- Many kinds of websites are there.
    - You can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you break into other people’s computers.
    - Buy login credentials to a $50,000 Bank of America account, counterfeit $20 bills, prepaid debit cards, or a “lifetime” Netflix premium account.
    - You can hire hackers to attack computers for you. You can buy usernames and passwords.
- Also there are emailing service sites and normal facebook too(but more secured).
- As you see This side of internet is little bit dangerous because a lot of evil hackers are there.
- For this purpose we have to change our identity, so we use Anonymity.
- ALSO REMEMBER YOUR ISP WONT ALLOW YOU TO ACCESS IT.

sTARTING.

- There are Specific OS that are planned and Made for darkweb access.
- Like,
  - Tails OS
  - Whonix OS
  - Qube OS
- We can use these OS for more Anonymity, but still the dark web sites are not easy to find.
- Also TOR browser is so slow, based on your internet speed, it might not show you the correct result.



Tor Connection

Everything you do on the Internet from Tails goes through the Tor network.

Tor encrypts and anonymizes your connection by passing it through 3 relays.
Tor relays are servers operated by different organizations and volunteers around the world.

● Connect to Tor automatically

We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.

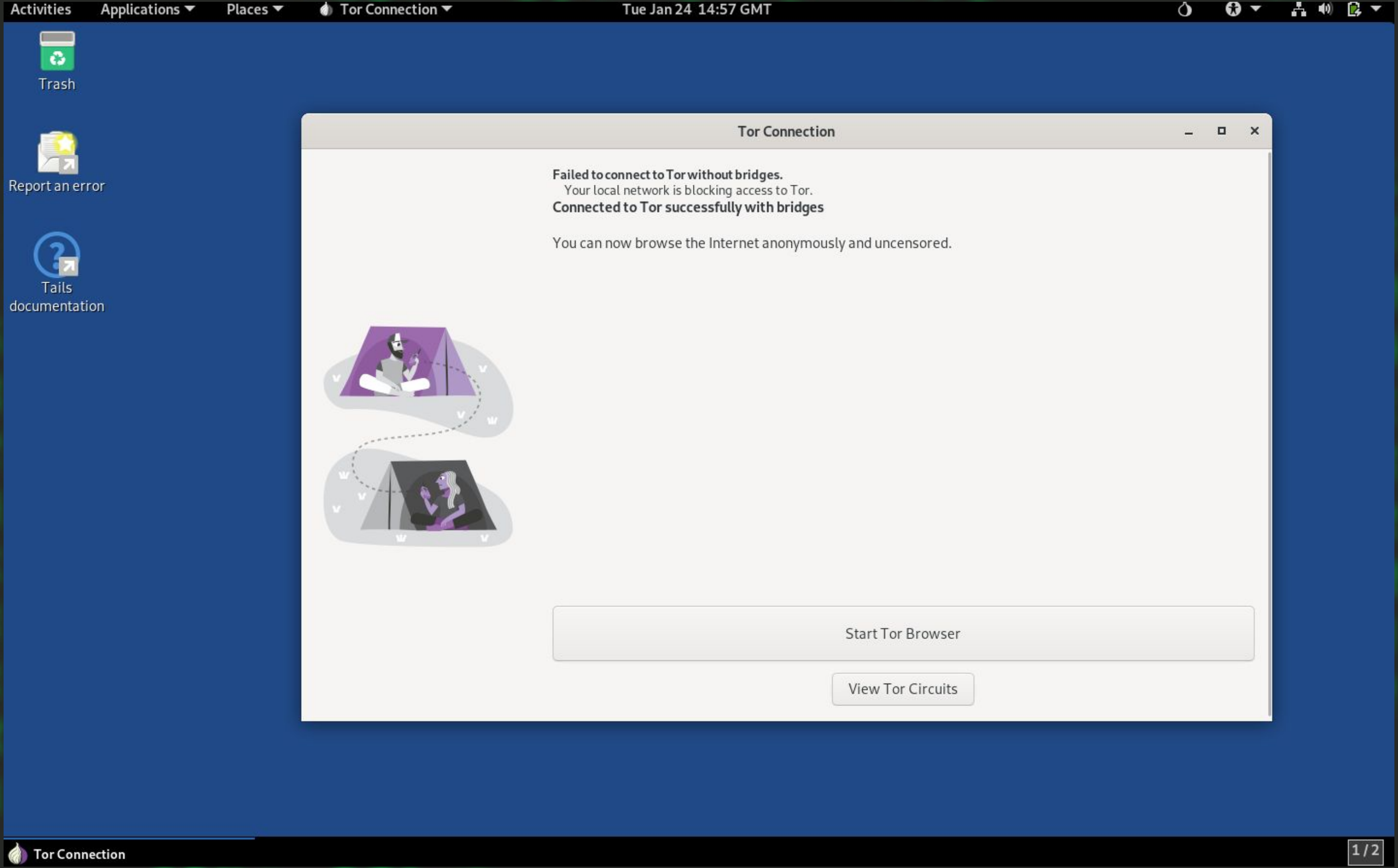
□ Configure a Tor bridge

○ Hide to my local network that I'm connecting to Tor

You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.

Learn more about how Tails connects to Tor

- Tails OS is a Linux Based OS, that on USB drivers only. It flashes anything after you shutdown the PC, also Connets to Tor network authomatically when it is turned on

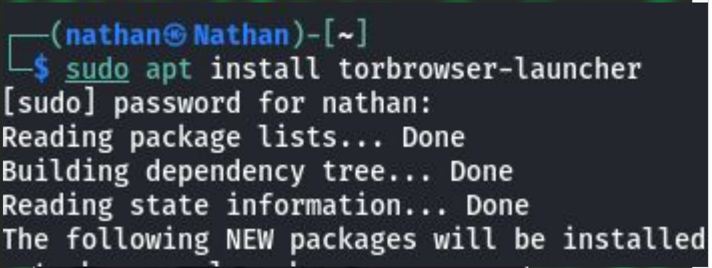


Failed to connect to Tor without bridges.
Your local network is blocking access to Tor.
Connected to Tor successfully with bridges

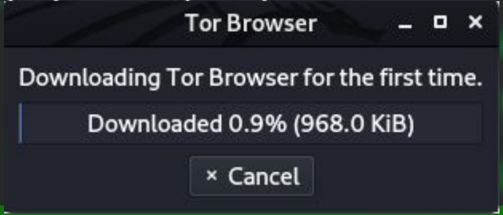
You can now browse the Internet anonymously and uncensored.

Tor Browser

This is How Tor browser looks it is almost same with firefox but this have more privacy settings.



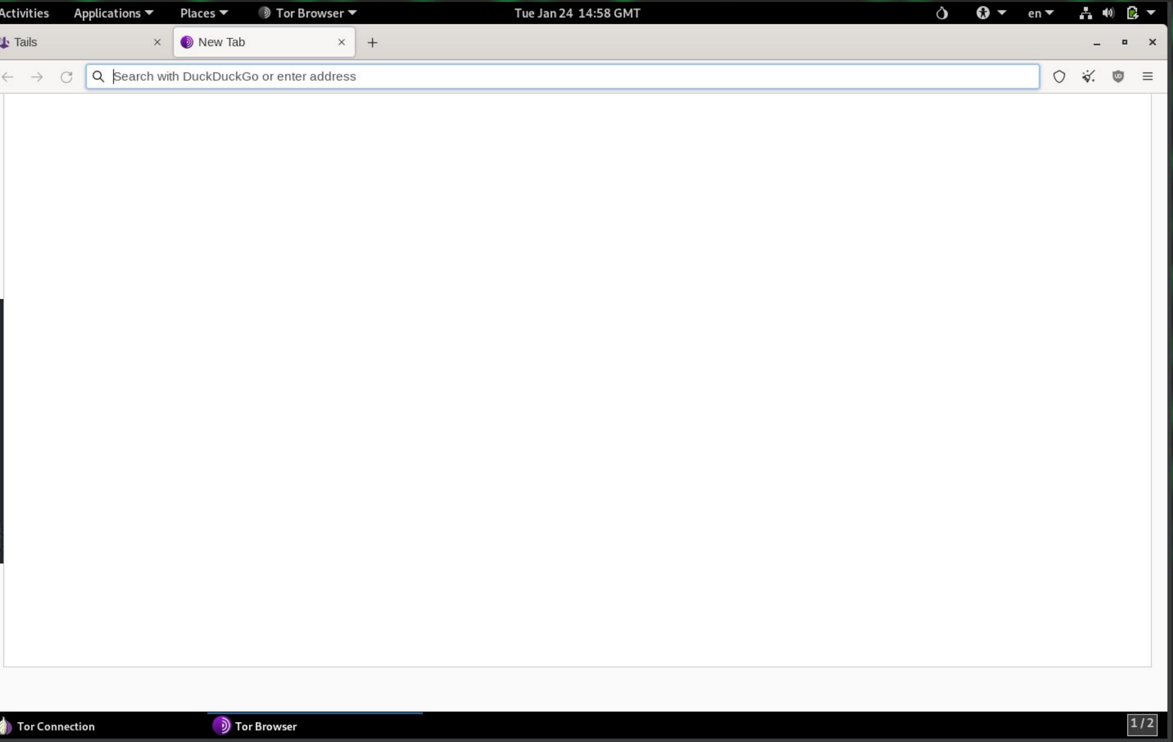
```
┌──(nathan㉿Nathan)-[~]
└─$ sudo apt install torbrowser-launcher
[sudo] password for nathan:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed
```



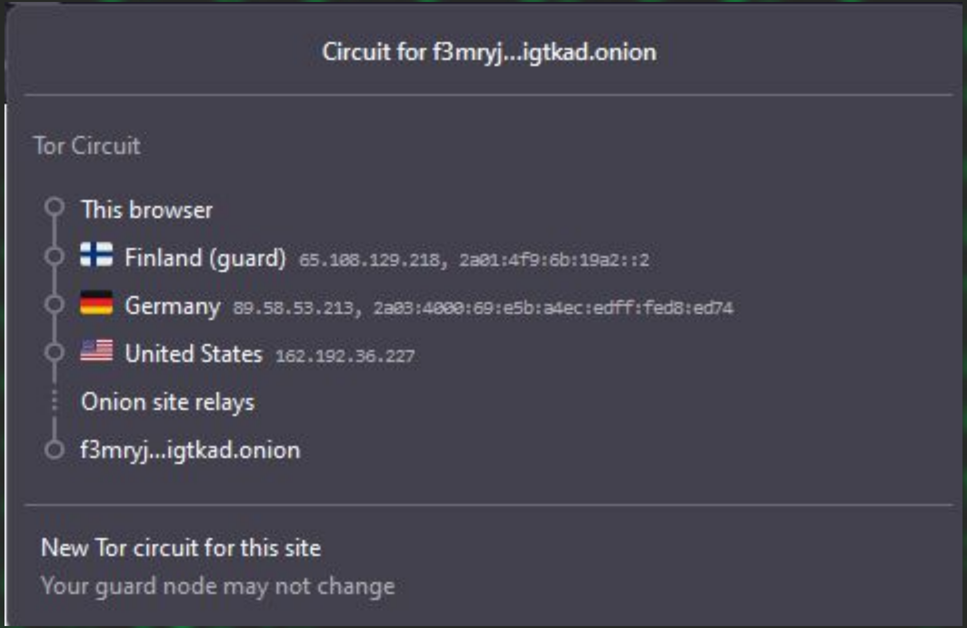
Tor Browser

Downloading Tor Browser for the first time.

Downloaded 0.9% (968.0 KiB)



When you try to access websites.



Circuit for f3mryj...igtkad.onion

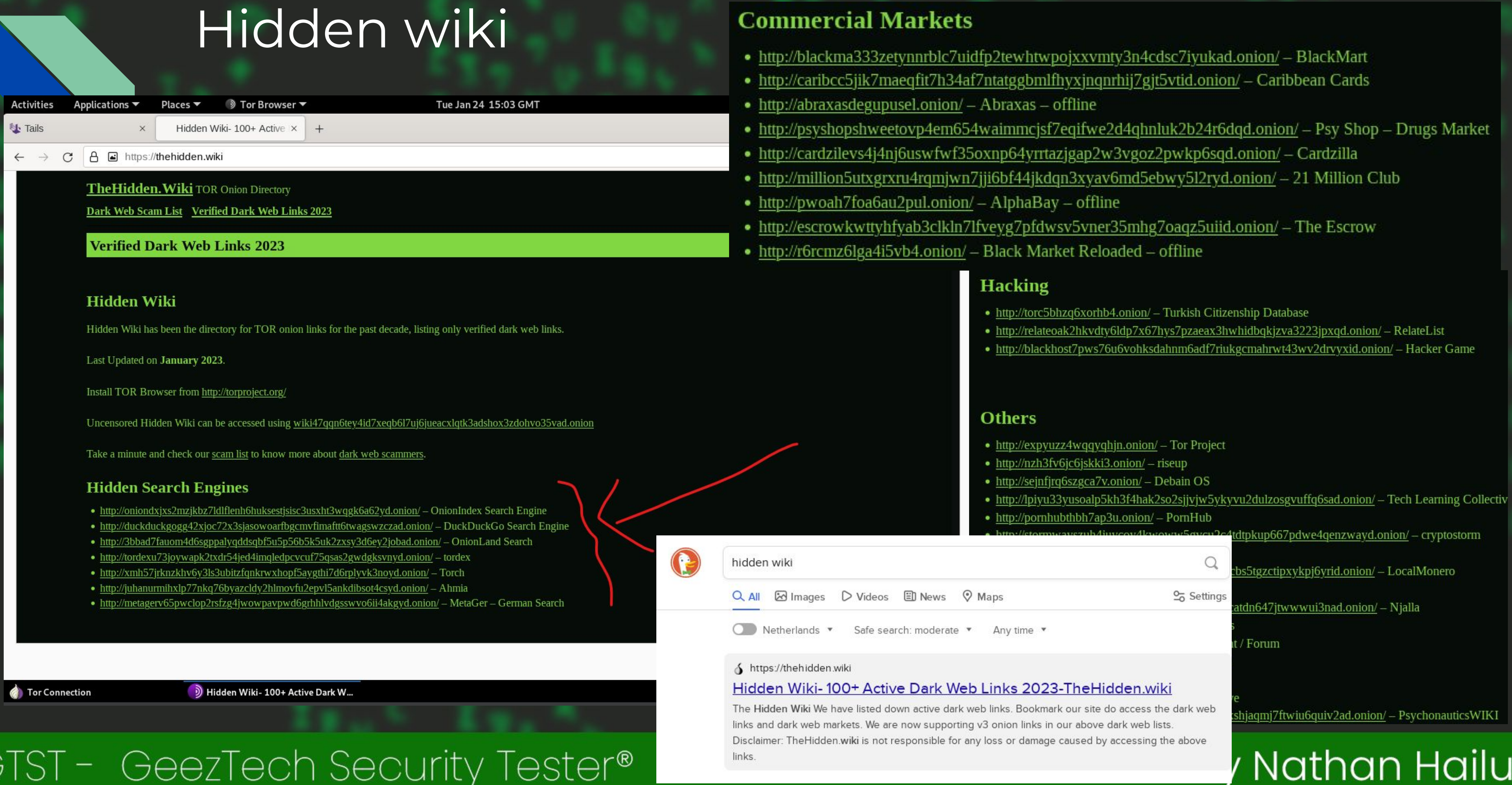
Tor Circuit

- This browser
- Finland (guard) 65.108.129.218, 2a01:4f9:6b:19a2::2
- Germany 89.58.53.213, 2a03:4000:69:e5b:a4ec:edff:fed8:ed74
- United States 162.192.36.227
- Onion site relays
- f3mryj...igtkad.onion

New Tor circuit for this site

Your guard node may not change

Hidden wiki



TheHidden.Wiki TOR Onion Directory

Dark Web Scam List **Verified Dark Web Links 2023**

Verified Dark Web Links 2023

Hidden Wiki

Hidden Wiki has been the directory for TOR onion links for the past decade, listing only verified dark web links.

Last Updated on **January 2023**.

Install TOR Browser from http://torproject.org/

Uncensored Hidden Wiki can be accessed using wiki47qqn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion

Take a minute and check our scam list to know more about dark web scammers.

Hidden Search Engines

- http://oniondxjxs2mzjkbz7ldlflenh6huksestjsisc3usxht3wqgk6a62yd.onion/ – OnionIndex Search Engine
- http://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/ – DuckDuckGo Search Engine
- http://3bbad7fauom4d6sgppalyqddsqbf5u5p56b5k5uk2zxsy3d6ey2jobad.onion/ – OnionLand Search
- http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onion/ – tordex
- http://xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion/ – Torch
- http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/ – Ahmia
- http://metagerv65pwclop2rsfzg4jwowpavpwd6grhhlvdgsswvo6ii4akgyd.onion/ – MetaGer – German Search

Commercial Markets

- http://blackma333zetynnrblc7uidfp2tewhtwpojxxvmty3n4cdsc7iyukad.onion/ – BlackMart
- http://caribcc5jik7maeqfit7h34af7ntatggbmlfhyxjnqnrhij7gjt5vtid.onion/ – Caribbean Cards
- http://abraxasdegupusel.onion/ – Abraxas – offline
- http://psyshopshweetovp4em654waimmcjsf7eqifwe2d4qhnluk2b24r6dqd.onion/ – Psy Shop – Drugs Market
- http://cardzilevs4j4nj6uswfwf35oxnp64yrrtazjgap2w3vgoz2pwkp6sqd.onion/ – Cardzilla
- http://million5utxgrxru4rqmjwn7jji6bf44jkdqn3xyav6md5ebwy5l2ryd.onion/ – 21 Million Club
- http://pwoah7foa6au2pul.onion/ – AlphaBay – offline
- http://escrowkwttyhfyab3clkln7lfveyg7pfdwsv5vner35mhg7oaqz5uiid.onion/ – The Escrow
- http://r6rcmz6lga4i5vb4.onion/ – Black Market Reloaded – offline

Hacking

- http://torc5bhzq6xorhb4.onion/ – Turkish Citizenship Database
- http://relateoak2hkvdty6ldp7x67hys7pzaeax3hwhidbqkjzva3223jpxqd.onion/ – RelateList
- http://blackhost7pws76u6vohksdahnm6adf7riukgcmahrwt43wv2drvyxid.onion/ – Hacker Game

Others

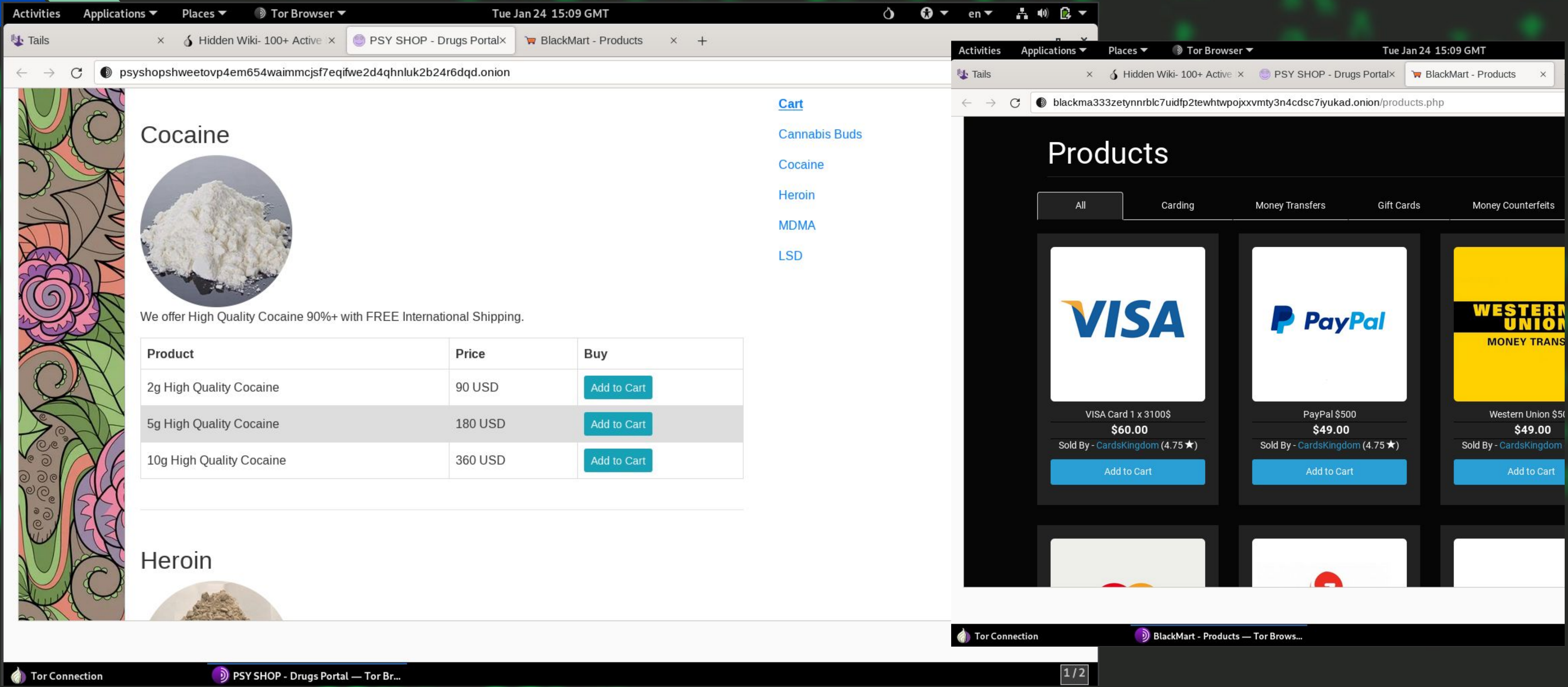
- http://expyuzz4wqqyqhjn.onion/ – Tor Project
- http://nzh3fv6jc6jskki3.onion/ – riseup
- http://sejnfjrq6szgca7v.onion/ – Debain OS
- http://lpiyu33yusoalp5kh3f4hak2so2sjjvjw5ykyvu2dulzosgvuffq6sad.onion/ – Tech Learning Collectiv
- http://pornhubthbh7ap3u.onion/ – PornHub
- http://stormwayszuh4juycoy4kwoww5gvcu2c4tdtpkup667pdwe4qenzwayd.onion/ – cryptostorm
- cbs5tgzctipxykpj6yrid.onion/ – LocalMonero
- atdn647jtwwwui3nad.onion/ – Njalla
- s
- t / Forum
- e
- shjaqmj7ftwiu6quiv2ad.onion/ – PsychonauticsWIKI

https://thehidden.wiki

Hidden Wiki- 100+ Active Dark Web Links 2023-TheHidden.wiki

The **Hidden Wiki** We have listed down active dark web links. Bookmark our site do access the dark web links and dark web markets. We are now supporting v3 onion links in our above dark web lists. Disclaimer: TheHidden.**wiki** is not responsible for any loss or damage caused by accessing the above links.

sites...



psyshopshweetovp4em654waimmcjsf7eqifwe2d4qhnluk2b24r6dqd.onion

Cocaine

We offer High Quality Cocaine 90%+ with FREE International Shipping.

Product	Price	Buy
2g High Quality Cocaine	90 USD	Add to Cart
5g High Quality Cocaine	180 USD	Add to Cart
10g High Quality Cocaine	360 USD	Add to Cart

Heroin

blackma333zetynnrblc7uidfp2tewhtwpojxxvmty3n4cdsc7iyukad.onion/products.php

Products

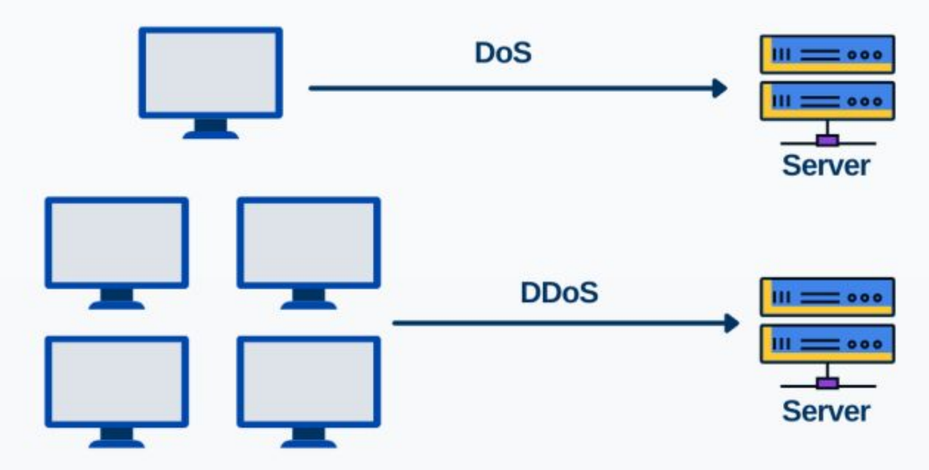
VISA Card 1 x 3100$
$60.00
Sold By - CardsKingdom (4.75 ★)
Add to Cart

PayPal $500
$49.00
Sold By - CardsKingdom (4.75 ★)
Add to Cart

Western Union $5
$49.00
Sold By - CardsKingdom
Add to Cart

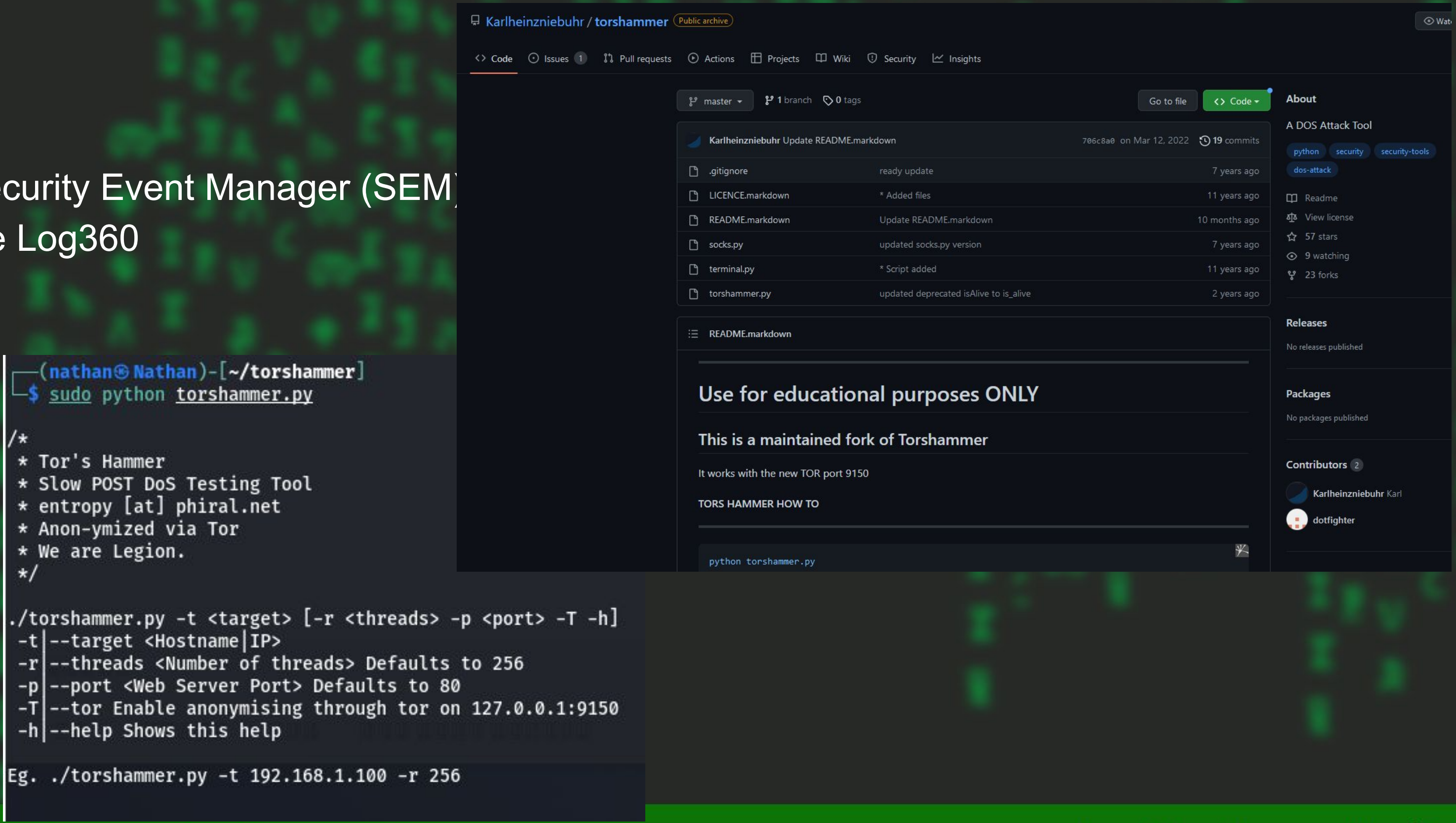
DOS and DDOS Attacks

- **DoS is short for Denial-of-Service attacks.**
- **DDoS stands for Distributed Denial-of-Service attack**.
- It's used to crash a website by overwhelming the network with access requests from a computer. This method also crashes a targeted website and makes it unavailable to legitimate users.(like Mac spoofing)
- It is purposeful attack
- On DDOS, the request will be sent from DIfferent Computers/hosts this will make the attack harder.
- IT is Highly illegal!
- Techniques:
  - SYN floods
    - Sending lots of SYN
  - Service Request floods
    - Create many connections
  - Application level DOS
    - Exploiting vulns like
      - Buffer Overflow
      - SQL injection



Tools For DOS

1. SolarWinds Security Event Manager (SEM)
2. ManageEngine Log360
3. HULK
4. Tor’s Hammer
5. Slowloris
6. LOIC
7. Xoic
8. DDOSIM
9. RUDY
10. PyLoris



```
┌──(nathan㉿Nathan)-[~/torshammer]
└─$ sudo python torshammer.py

/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * entropy [at] phiral.net
 * Anon-ymized via Tor
 * We are Legion.
 */

./torshammer.py -t <target> [-r <threads> -p <port> -T -h]
 -t|--target <Hostname|IP>
 -r|--threads <Number of threads> Defaults to 256
 -p|--port <Web Server Port> Defaults to 80
 -T|--tor Enable anonymising through tor on 127.0.0.1:9150
 -h|--help Shows this help

Eg. ./torshammer.py -t 192.168.1.100 -r 256
```

Karlheinzniebuhr / torshammer Public archive

Karlheinzniebuhr Update README.markdown 706c8a0 on Mar 12, 2022 19 commits

.gitignore	ready update	7 years ago
LICENCE.markdown	* Added files	11 years ago
README.markdown	Update README.markdown	10 months ago
socks.py	updated socks.py version	7 years ago
terminal.py	* Script added	11 years ago
torshammer.py	updated deprecated isAlive to is_alive	2 years ago

README.markdown

Use for educational purposes ONLY

This is a maintained fork of Torshammer

It works with the new TOR port 9150

TORS HAMMER HOW TO

```
python torshammer.py
```

About

A DOS Attack Tool

python security security-tools dos-attack

Readme
View license
57 stars
9 watching
23 forks

Releases

No releases published

Packages

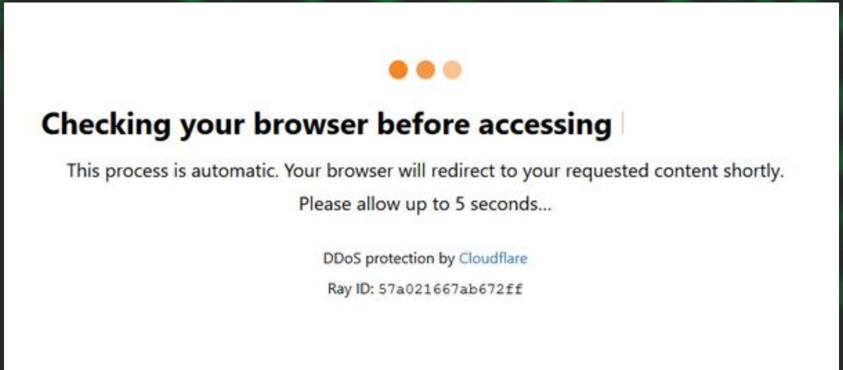
No packages published

Contributors 2

Karlheinzniebuhr Karl
dotfighter

Prevention ways

- Have you seen Cloudflare, These pages are One of the prevention ways.
- Limit or shut off broadcast forwarding where possible
- Set up firewalls
- Eliminate and patch known vulnerabilities
- Monitor network inbound traffic



Checking your browser before accessing

This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds...

DDoS protection by Cloudflare

Ray ID: 57a021667ab672ff

Class is Over

1. DO notes
2. explorer some Darkweb sites and tell us what you have got something special
3. Ask questions