Hands-on Bug Hunting

Active and Passive Reconnaissance and Dark Web Research

DAY 2 LAB GUIDE v.2

https://darknetrecon.com

Instructors:
Joseph Mlodzianowski (@cedoxx)
Omar Santos (@santosomar)

Introduction

This guide is a collection of exercises for the O'Reilly Live Training Hands-on Bug Hunting: Active and Passive Reconnaissance and Dark Web Research" authored and delivered by Omar Santos and Joseph Mlodzianowski.
For more information about the training visit https://darknetrecon.com

Learning Path: Additional Cybersecurity Training (Free with your O'Reilly Subscription)

This training is part of a learning path of numerous live training sessions and video courses that are available with your O'Reilly subscription. To access the learning path go to: https://h4cker.org/learningpath

Training Summary

This live and interactive training is designed to help you perform passive and active reconnaissance in ethical hacking and bug bounty hunting engagements. You will learn intermediate-to-advanced recon methodologies using open source intelligence (OSINT). In this training you will also learn how to perform dark web research and reconnaissance. You will learn how to use Tor, proxies and proxychains, and even how to create your own VPN servers in cloud environments.

Helpful Resources Prior to Taking the Live Training:

- Security Penetration Testing The Art of Hacking Series LiveLessons (video)
- Wireless Networks, IoT, and Mobile Devices Hacking (video)
- Enterprise Penetration Testing and Continuous Monitoring (video)
- Hacking Web Applications The Art of Hacking Series LiveLessons: Security Penetration Testing for Today's DevOps and Cloud EnvironmentsWeb (video)
- Security Fundamentals (video)

Lab Setup

Setup WebSploit Labs (https://websploit.org).
WebSploit Labs is a learning environment created by Omar Santos for different Cybersecurity Ethical Hacking (Web Penetration Testing) training sessions. WebSploit includes several intentionally vulnerable applications running in Docker containers on top of Kali Linux or Parrot Security OS, several additional tools, and over 8,000 cybersecurity resources. WebSploit comes with over 400 distinct exercises!

- Step 1: Download Kali or Parrot and install it on a VM
- Step 2: After you have installed Kali Linux, run the following command from a terminal window to setup your environment:

```
curl -sSL https://websploit.org/install.sh | sudo bash
```

This command will install all the tools, Docker, the intentionally vulnerable containers, and numerous cybersecurity resources.

A quick demo can be accessed at: https://websploit.org/install.gif or at websploit.org main website (landing page).

Exercise 1: The DeepWeb

Launch the Firefox browser on your VM Kali System and select one site from the list of deep web sites on the Deepweb page. Here we will select the WayBack machine:

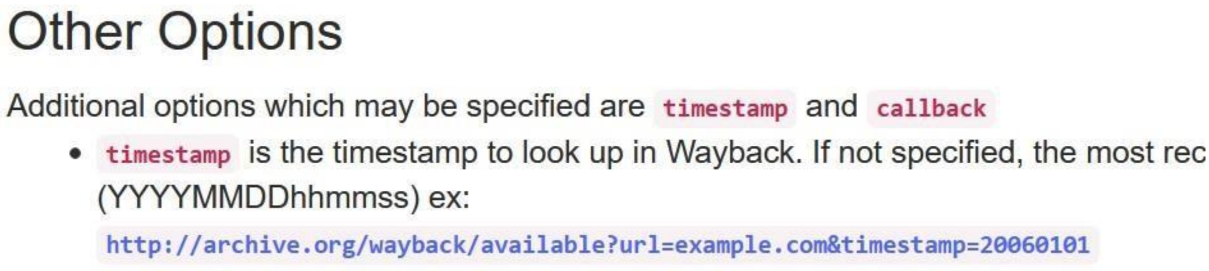
https://web.archive.org/web

Once on the page, select Wayback Machine Availability API , From the tools on the left

Tools

Wayback Machine Availability API

then scroll down to “Other Options” and click on the URL similar to this:

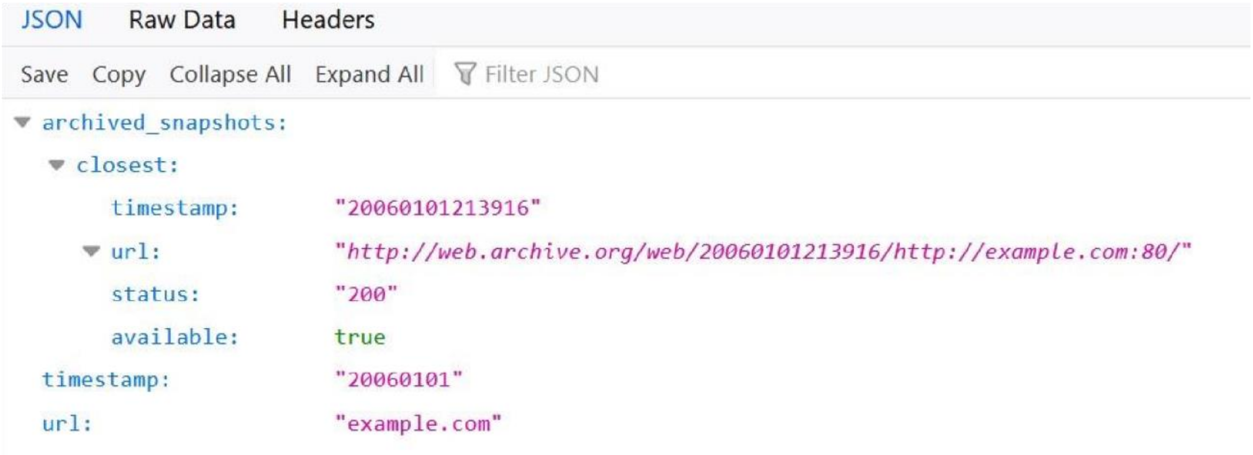

Other Options

Additional options which may be specified are `timestamp` and `callback`

- `timestamp` is the timestamp to look up in Wayback. If not specified, the most rec (YYYYMMDDhhmmss) ex: `http://archive.org/wayback/available?url=example.com&timestamp=20060101`

Now click on the blue http://archive.org ….. link as show on the page:

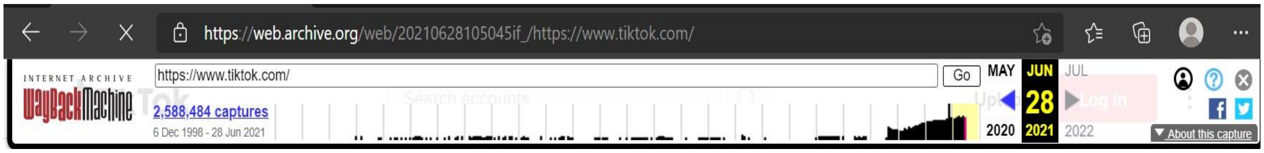
You should end up with json interface, this API interface is a completely non-indexed system



```
▼ archived_snapshots:
  ▼ closest:
      timestamp:      "20060101213916"
    ▼ url:            "http://web.archive.org/web/20060101213916/http://example.com:80/"
      status:         "200"
      available:      true
  timestamp:          "20060101"
  url:                "example.com"
```

https://web.archive.org/web/20060101213916/http://example.com:80/

TikTok - Make Your Day (archive.org)


https://web.archive.org/web/20210628105045if_/https://www.tiktok.com/

https://www.tiktok.com/

The url is set with an example so that when you connect with a json api compatible program you can query the database.

Notice that this doesn't give you much information, one of the reasons it wouldn't be spidered and added to a search engine, because its expecting an API to interface with it and push/pull data.

Selecting any of the other sites will lead you to some valuable deep web search engines and others will be either out of service or be rebranded to some other service, check them out when you get a chance.

Next let's try the online education database - https://oedb.org/ilibrarian/researchbeyond-google/

Beyond Google: 56 Autho...

oedb.org

Writing a research paper? Google has a lot of information indexed, but it's nothing compared to...

Notice it also shows a number of deepweb search engine capabilities, finding good deepweb search engines is a game of whack-a-mole the consistently either become commercial products or close entirely.

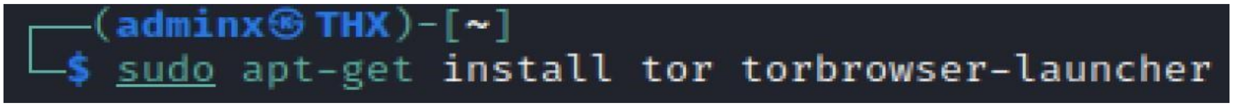
END:

Exercise 2: Installing & Using Tor on Linux

LAB1: In this exercise we will install the Tor Browser on your Kali Linux workstation

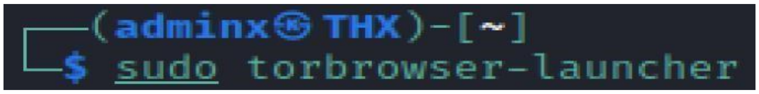
Command Line:

First from a terminal window - we run **"sudo apt-get install tor torbrowser-launcher"**



```
┌──(adminx㉿THX)-[~]
└─$ sudo apt-get install tor torbrowser-launcher
```

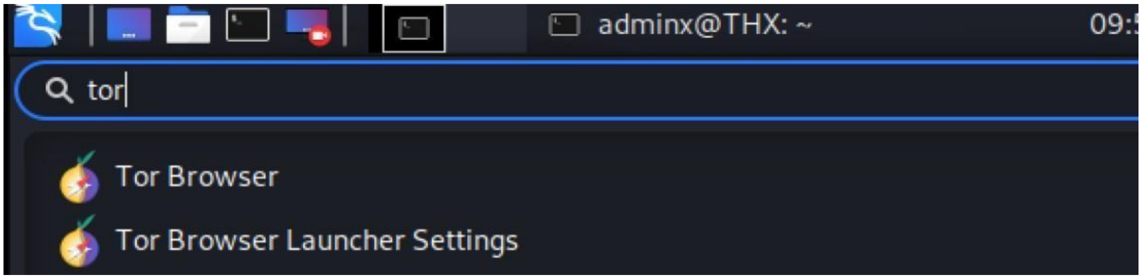
Next we run **"sudo torbrowser-launcher"**



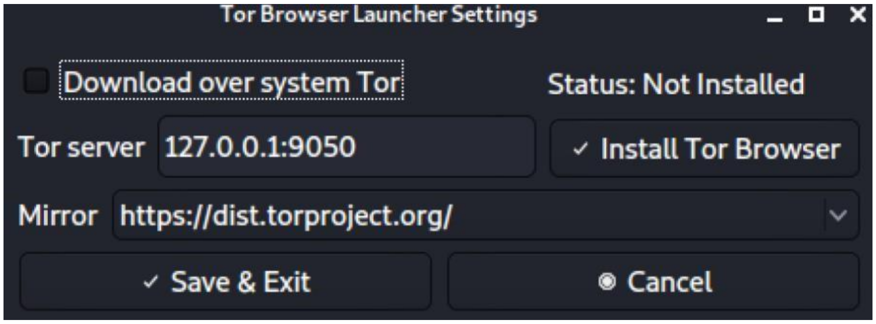
```
┌──(adminx㉿THX)-[~]
└─$ sudo torbrowser-launcher
```

Then it downloads the Tor Browser for the first time, verifies the signature, and installs Finally it warns you - Do not run Tor Browser as root and exits. "Ok"

Next click the kali icon on the left menu, type in tor and it should bring up two items



Select the Tor Browser Launcher Settings first



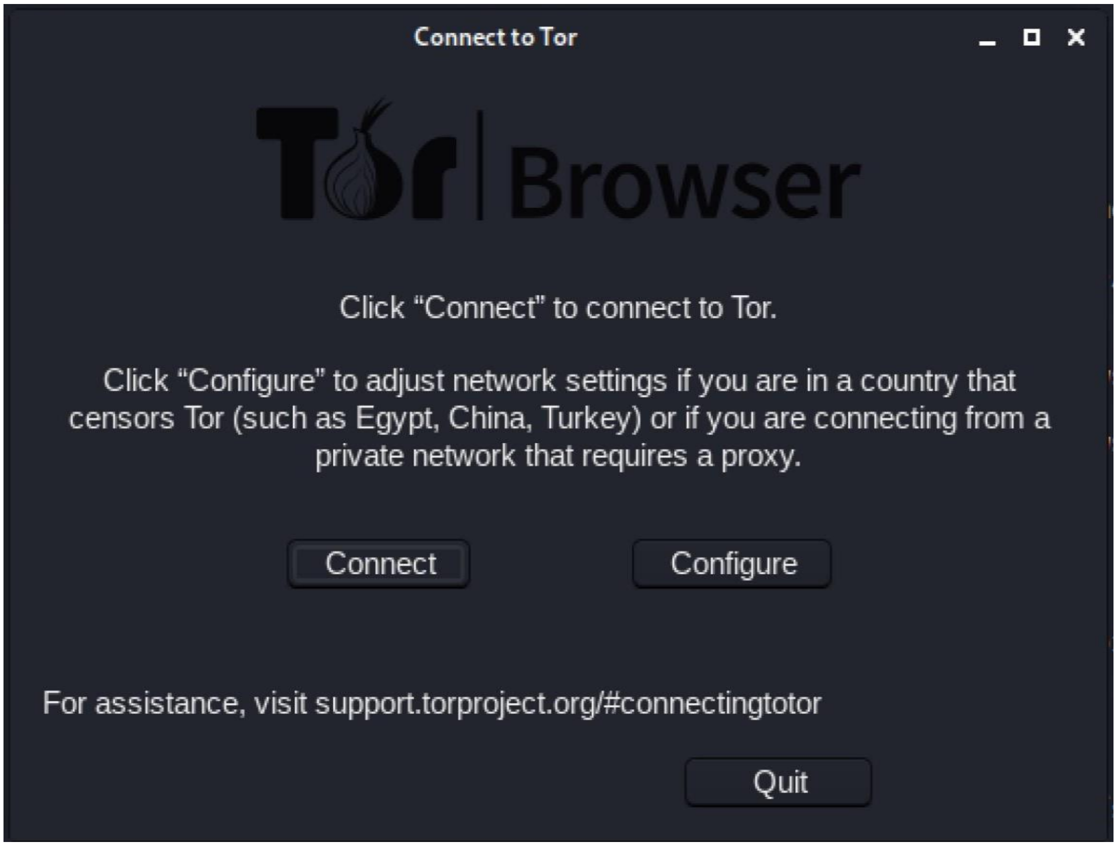
□ Download over system Tor

Status: Not Installed

Tor server 127.0.0.1:9050

Mirror https://dist.torproject.org/

Select - Install Tor Browser, which should install it locally. When it's all done we should be running at least version 10.0.12 or newer.

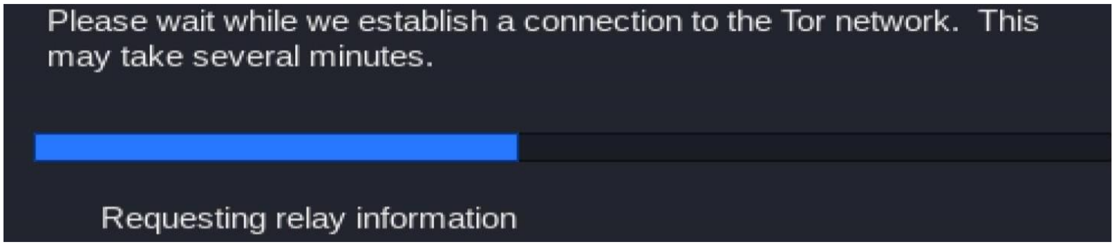


Click “Connect” to connect to Tor.

Click “Configure” to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.

For assistance, visit support.torproject.org/#connectingtotor

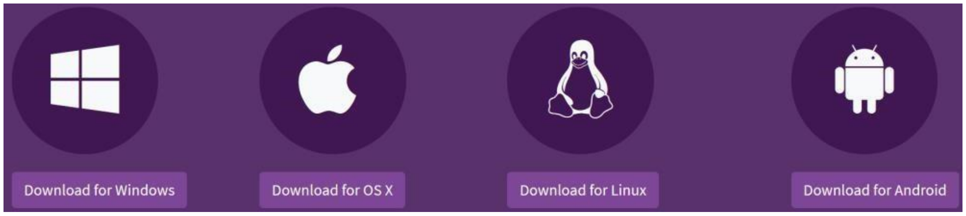
Select “Configure” **if you are in a country** that censors internet select the “Tor is censored in my Country” so it can locate open ports, otherwise select “Connect”



Please wait while we establish a connection to the Tor network. This may take several minutes.

Requesting relay information

You can download the Tor Browser for Android, Windows & Mac OS here: **https://www.torproject.org/download/**



LAB 2: After completion of the connection you now should have the Tor Browser up and running so now let's turn our attention to using the Tor browser to browse normal everyday traffic sites.

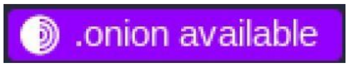
A. First lets check to see if our traffic is being forwarded through the Tor Network Browse to this site -> **https://check.torproject.org/** **if you are going through the Tor Network you should see: Congratulations - This browser is configured to use Tor**

B. Next Browse to **"whatismyipaddress.com**" and notice this ip address is not yours but the Tor exit node ip address.

C. Now browse to https://abcnews.go.com and/or https://duckduckgo.com

Notice you can reach any **surface website**, however your privacy is now being masked by the TOR / Onion network, so browse unattributed. Remember exit nodes can view your data so do not use this browser to access your BitCoin, purchase from Amazon or use your credit card or real name. *

LAB 3: Now use the ToR browser and browse to **nytimes.com** or **cia.gov**
Did you see the popup to prioritize onion sites ? for now select **not now**, and checkout the top url banner where you should see the ".Onion Available" in purple, as shown below.

Next Select: 

Notice you were redirected to a full .onion site. With a long and unrememberable address.
http://g7ejphhubv5idbbu3hb3wawrs5adw7tkx7yjabnf65xtzztgg4hcsqqd.onion/

A. Now browse around that site and see how long it takes for a response, this requires some patience when visiting and browsing sites on Tor because of the number of hops

B. Now close the Tor Browser window all together.

D. To open tor again, search for it on the menu or select the Kali image on the left and type in Tor again. Now you can just select "Tor Browser" to continue browsing.

E. *Advanced Settings* - In the Tor Browser, on the right is three dash (hamburger) select Preferences, and then Tor, here under bridges is where you can select a bridge. And under advanced we can change the type of connection we have to the internet.

F. On the Right three dash (hamburger) notice the second two items, "New Identity" and New Tor Circuit for this site" selecting a new identity will close your browser and terminate your connection to the network, likely selecting you a new gateway.

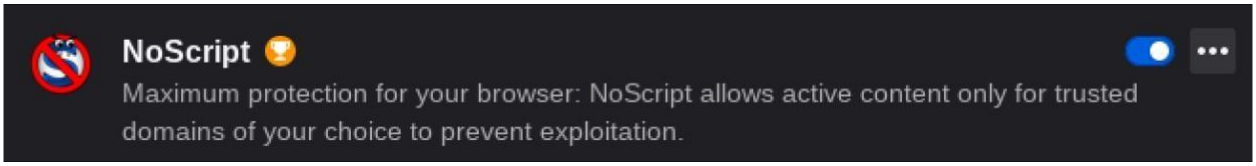
G. Next let's browse to a site that has been seized
   a. Hansa http://hansamkt2rr6nfg3.onion/

H. Now let's browse to the Darkweblink.com website and use the same .onion links make sure you are only using search engine sites to avoid illegal imagery.

LAB 4:

1. Javascript, flash, java, etc, website scripting all allow sites to glean information from you as you browse their sites, lets add a bit of protection and download and enable noscript.
2. Download the NoScript Firefox extension from Noscript.net
   Or obtain it from https://addons.mozilla.org/en-US/firefox/addon/noscript/

3. Next install the plugin



NoScript

Maximum protection for your browser: NoScript allows active content only for trusted domains of your choice to prevent exploitation.

4. Certain websites might like to fingerprint your browser as a way to determine your operating system, browser type, language, and how to display certain data.
5. Browse to https://www.amiunique.org and determine your level of protection.
6. You are running noscript globally, however you can add site exceptions as they come up, just be careful what you allow.
7. BTW, NoScript usually comes installed on the Tor browser by default, this is really meant to bring awareness to the tool, what it does and when you use your own distro, use a different browsers, or your personal machine, you should use noscript.

A few others are:

Cookie Manager: https://addons.mozilla.org/en-US/firefox/addon/cookie-quick-manager/ Foxyproxy: https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/

Follow the same process as the no script for installation.

END:

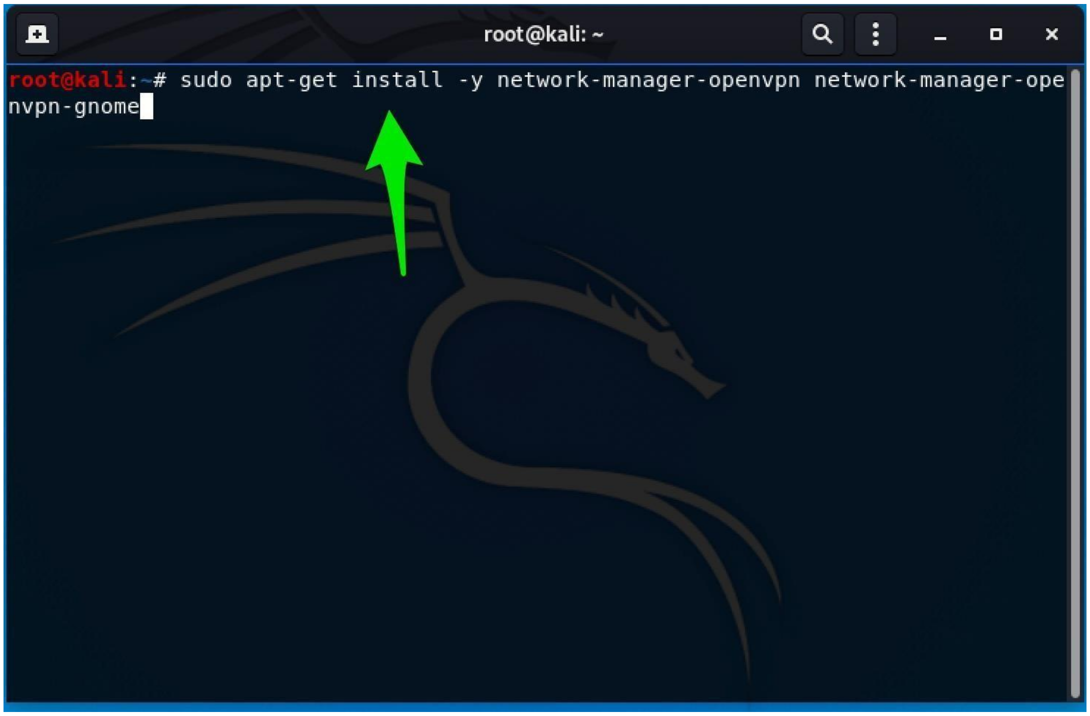
Exercise 3: VPN on Linux

Lets install a commercial VPN Service, almost any service will do, the steps are similar no matter the vendor. We make no preference or recommendation.

DEMONSTRATION PURPOSES ONLY

A. *Open a terminal window (ctrl + alt + T)*
B. *Type in: sudo (since we are regular user) and then install packages….*

```
sudo apt-get install -y openvpn network-manager-openvpn  sudo

apt-get install -y network-manager-openvpn-gnome
```



```
root@kali:~# sudo apt-get install -y network-manager-openvpn network-manager-ope
nvpn-gnome
```

C. Lets create a working directory:

```
mkdir ~/ipvanish
```

then change to the ipvanish directory

```
cd ~/ipvanish
```

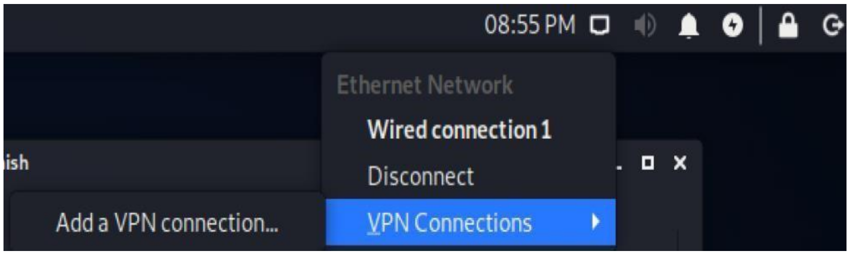
D. Lets grab the OpenVPN Configuration files

```
wget https://www.ipvanish.com/software/configs/configs.zip
```

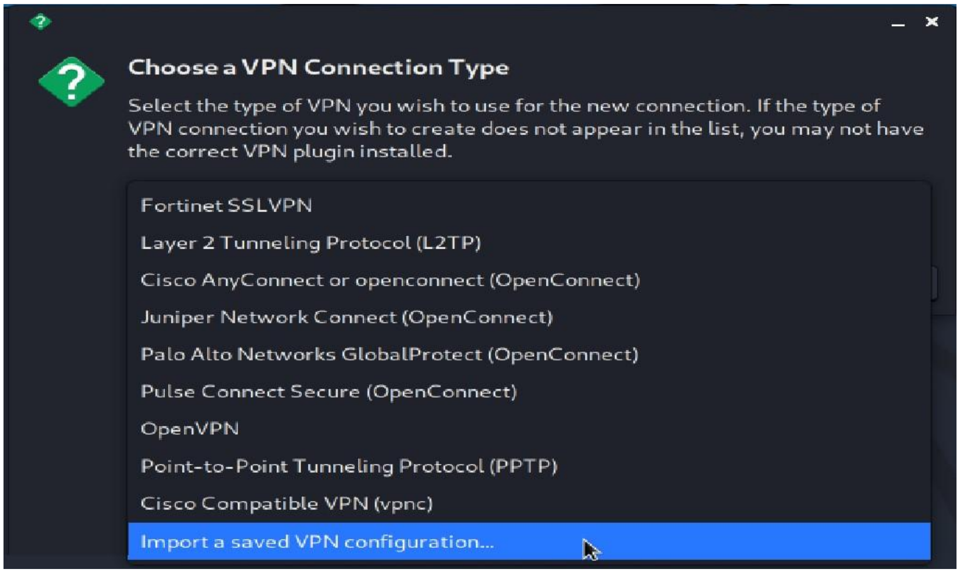
E. Next lets unzip the config.zip using “unzip” Run - Unzip configs.zip

You should see well over 100 files

F. Next let’s select the networking icon from the top toolbar of kali linux VPN Connection and select Add a VPN Connection



G. Choose a VPN Connection Type:



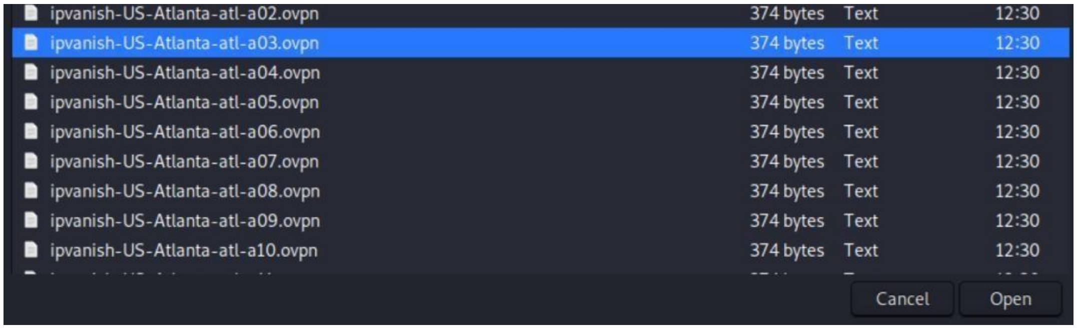
Choose a VPN Connection Type

Select the type of VPN you wish to use for the new connection. If the type of VPN connection you wish to create does not appear in the list, you may not have the correct VPN plugin installed.

Fortinet SSLVPN
Layer 2 Tunneling Protocol (L2TP)
Cisco AnyConnect or openconnect (OpenConnect)
Juniper Network Connect (OpenConnect)
Palo Alto Networks GlobalProtect (OpenConnect)
Pulse Connect Secure (OpenConnect)
OpenVPN
Point-to-Point Tunneling Protocol (PPTP)
Cisco Compatible VPN (vpnc)
Import a saved VPN configuration...

H. Select Import a saved VPN Configuration, then next, and Create.

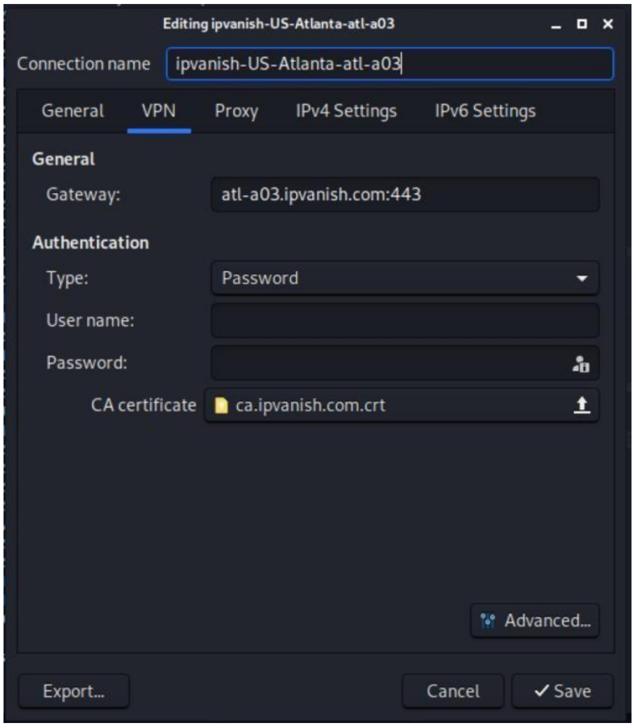
I. Now browse to the folder you created, double click, and then select a US location, I am selecting a Atlanta location seen below



ipvanish-US-Atlanta-atl-a02.ovpn	374 bytes	Text	12:30
ipvanish-US-Atlanta-atl-a03.ovpn	374 bytes	Text	12:30
ipvanish-US-Atlanta-atl-a04.ovpn	374 bytes	Text	12:30
ipvanish-US-Atlanta-atl-a05.ovpn	374 bytes	Text	12:30
ipvanish-US-Atlanta-atl-a06.ovpn	374 bytes	Text	12:30
ipvanish-US-Atlanta-atl-a07.ovpn	374 bytes	Text	12:30
ipvanish-US-Atlanta-atl-a08.ovpn	374 bytes	Text	12:30
ipvanish-US-Atlanta-atl-a09.ovpn	374 bytes	Text	12:30
ipvanish-US-Atlanta-atl-a10.ovpn	374 bytes	Text	12:30

Notice that all these locations are in order of Country first.

J. In the Add VPN window appears that requires you to enter your username and password for your account



Editing ipvanish-US-Atlanta-atl-a03

Connection name: ipvanish-US-Atlanta-atl-a03

General

Gateway: atl-a03.ipvanish.com:443

Authentication

Type: Password

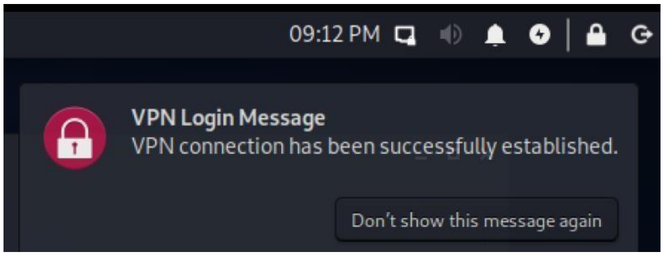
User name:

Password:

CA certificate: ca.ipvanish.com.crt

K. After that under IPV6, you can disable IPv6, and Save.

L. Next select the network icon again, and you will see the profile for the site you selected, **simply click on it** and you will connect and shortly see the following message confirming you are connected



VPN Login Message

VPN connection has been successfully established.

WARNING: You do not have an account with this company so this will not work.

M. Now you can open your web browser (not Tor) and browse to what is my ip address .com - you should see your traffic is now coming from the VPN sites location.

N. To set up more locations start with step E. and add them.

O. Now you can launch your Tor Browser over the VPN and have that added protection of the Entry node not seeing your real ip address , try browsing to the darknetlive.com site and select the purple .onion to see/test your speeds. Should be similar to previous tests speeds.
END:

Exercise 4: Using a Proxy, Proxies and ProxyChains

LAB1:

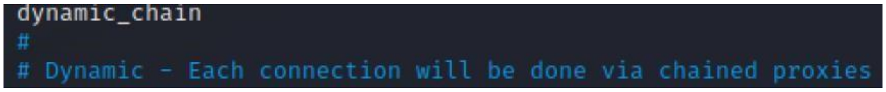
A. The proxychains configuration file is located under /etc/ directory. We will open the **proxychains4.conf** file - first open a terminal - the enter the following sudo (using VI,View or Nano) edit -> **/etc/proxychains4.conf**

i. **Strict_Chain**, this chains the ip's you list in order so that the final ip address is the last one on your list, if a chain is unresponsive the chain fails and you get nothing. ii. **Dynamic Chain** works similar to strict chain, only it does not require all proxies in the Chain configuration file to work, if a proxy is down then the connection jumps to the next proxy in the list, you will see these on the command line, this lets you remove unresponsive proxies.

iii. **Random Chain** ads randomness proxy select ability to the list and the chain will look different each time its used.

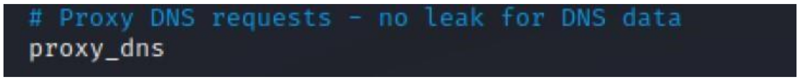
B. To use one of the three selected methods, comment (#) out two and leave the one you want to use uncommented.

C. We are going to select **dynamic_chain** and comment out the others. Its the best for speed and skips offline or non responsive proxies



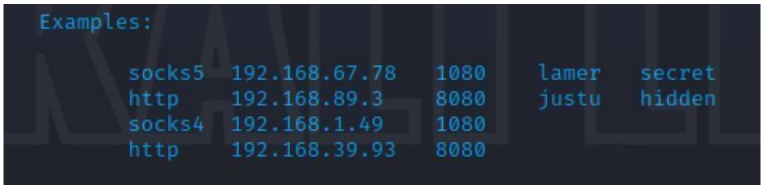
```
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
```

D. Make sure you uncomment #proxy_dns this protects your dns requests so that they appear to be coming from the same source ip (and not yours)

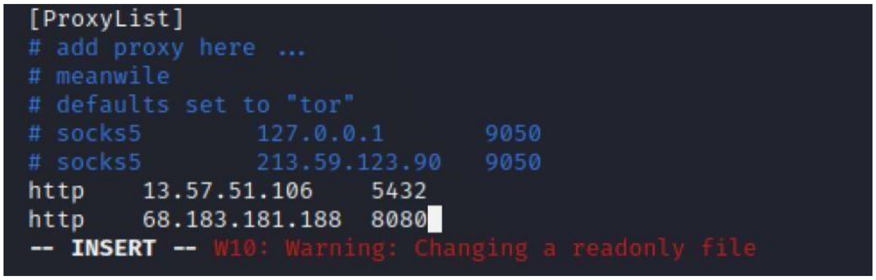


```
# Proxy DNS requests - no leak for DNS data
proxy_dns
```

E. Next we will locate and place all of our proxies in the file, to find a list of open proxies, there are a couple sites, for this exercise we will use "freeproxylists.net" https://www.freeproxylists.net or https://spys.one has a nice layout, there are lots of proxies and a google search can help you find even more.



```
Examples:

        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
```



```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
# socks5        127.0.0.1       9050
# socks5        213.59.123.90   9050
http    13.57.51.106    5432
http    68.183.181.188  8080
-- INSERT -- W10: Warning: Changing a readonly file
```

F. Now lets launch proxy chains and see if it works:

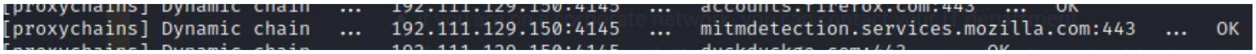
From a terminal window enter:

proxychains firefox duckduckgo.com,

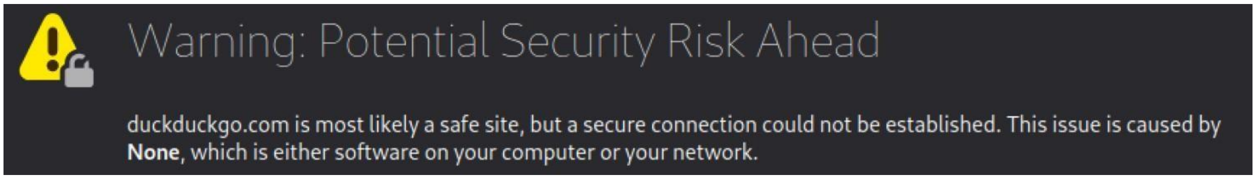
You will need a socks5 proxy(s) to perform the nmap scan mentioned below:

proxychains nmap -sT -p 80,443 1.1.1.1

If you see something like this or a yellow box around your page, know that they are trying to snoop on you with a man in the middle. Close, and locate another proxy server.



```
[proxychains] Dynamic chain  ...  192.111.129.150:4145  ...  accounts.firefox.com:443  ...  OK
[proxychains] Dynamic chain  ...  192.111.129.150:4145  ...  mitmdetection.services.mozilla.com:443  ...  OK
[proxychains] Dynamic chain  ...  192.111.129.150:4145  ...  duckduckgo.com:443  ...  OK
```



Warning: Potential Security Risk Ahead

duckduckgo.com is most likely a safe site, but a secure connection could not be established. This issue is caused by **None**, which is either software on your computer or your network.

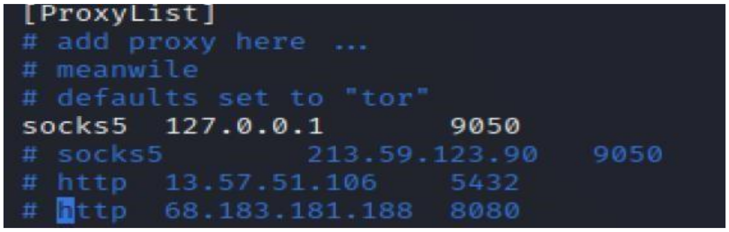
LAB2:

G. Now let’s try it with Tor in the picture:

H. From a terminal, First type in “Service tor status” you should see “inactive” (dead)

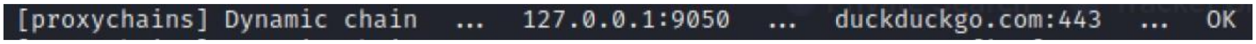
I. Next let’s start Tor “Service tor start” you may get prompted for the root password, enter that and continue. Now check the status again, up arrow twice to find the previous command. You should see (Active)

J. Open your terminal window and edit the proxychains4.conf file sudo (View or Nano) /etc/proxychains4.conf



```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks5  127.0.0.1        9050
# socks5          213.59.123.90   9050
# http  13.57.51.106     5432
# http  68.183.181.188   8080
```

Notice I commented out the proxy servers, I am doing this to test to make sure TOR is working properly, you should always remove as many configuration changes when starting something new. Once that is done, save the file and launch the proxychains firefox duckduckgo.com cmd. And the results - ok

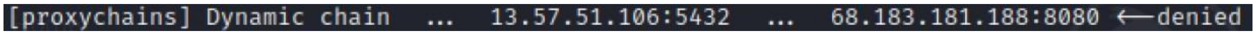


```
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  duckduckgo.com:443  ...  OK
```

K. Now lets add back in our proxies,
L. From your terminal window and edit the proxychains4.conf file sudo (View or Nano) /etc/proxychains4.conf

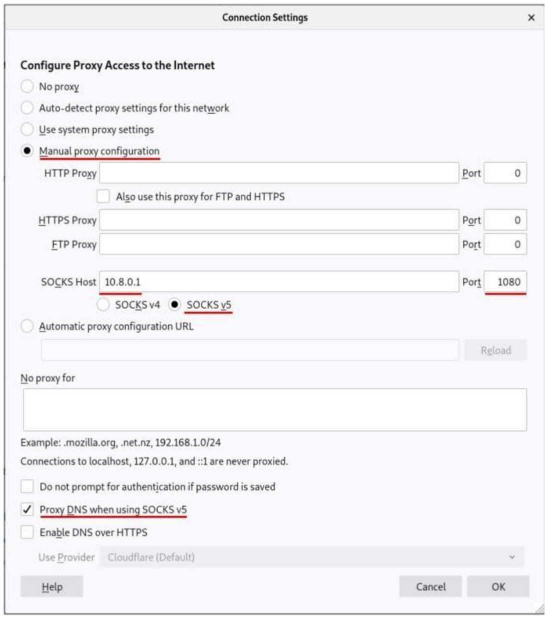
And uncomment the proxies for http and Socks if you managed to find working ones.

What I initially saw was that the proxies denied connections from the TOR ip address, so what I did was moved it down to the bottom, and then restarted. You may see proxies not accepting proxied traffic from another proxy, you will just need to spend some time finding GOOD proxies, specifically look for good solid socks5 proxies because they proxy all traffic.



```
[proxychains] Dynamic chain  ...  13.57.51.106:5432  ...  68.183.181.188:8080 <--denied
```

SINGLE PROXY: If you want to add a single proxy and use it from your browser you can add them under Firefox "General Settings" then select "Network" and fill in the configuration for the single proxy ip address as outline below:



Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy Port 0
□ Also use this proxy for FTP and HTTPS
HTTPS Proxy Port 0
FTP Proxy Port 0
SOCKS Host 10.8.0.1 Port 1080
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved
☑ Proxy DNS when using SOCKS v5
□ Enable DNS over HTTPS
Use Provider Cloudflare (Default)

END:

Exercise 5: (optional) Private Cloud VPN Demo

This exercise is for demonstration purposes only. You can use the cloud provider of your choosing. Make sure that you pay attention to their cost and pricing structure. ***(see slide deck for more info)***

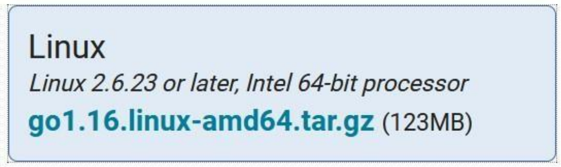
Exercise 6: Onionscan Demo

1. Remove already installed Go **From a terminal:**

```
sudo apt-get remove golang-go
```

```
sudo apt-get remove --auto-remove golang-go
```

2. Browse to the Go website and download https://golang.org/ version 1.16



Linux

Linux 2.6.23 or later, Intel 64-bit processor

go1.16.linux-amd64.tar.gz (123MB)

3. Suggest you reboot after you remove the old version of Go.
4. Go to your downloads directory under your user and open a terminal window

```
tar -C /usr/local/ -xzf go1.16.linux-amd64.tar.gz
export GOROOT=/usr/local/go export
GOPATH=/root/go-workspace
PATH=$PATH:$GOROOT/bin/:$GOPATH/bin go version
```

5. Next we download Onionscan

```
go get github.com/s-rah/onionscan
```

a. Next do a “go get” for each of the below packages

```
go get golang.org/x/crypto/openpgp/packet
```

go get golang.org/x/net/proxy - For the Tor SOCKS Proxy connection go get golang.org/x/net/html - For HTML parsing go get github.com/rwcarlsen/goexif - For EXIF data extraction go get github.com/HouzuoGuo/tiedot/db - For crawl database

6. To test you can find an .onion address and scan similar to below:

```
onionscan --verbose cardsa2u7pvmdamw.onion onionscan --
jsonReport cardsa2u7pvmdamw
```

7. There is a OnionScan Correlation Lab you can try out as well depending on where your onionscandb is located you may need to change the path.

```
onionscan --mode analysis --dbdir ~/go/bin/onionscandb
```

END:

Exercise 7: DarkWeb OSINT

LAB 1: Performing OSINT and Recon on the Darkweb is similar to conducting it on the surface web, as a matter of fact there is a point where your intel converges and can give you even better attribution.

We are going to start with installing a 30 day trial of Hunch.ly , go to the website select free 30 day trial that will take you to the registration page, you must register to get a key.

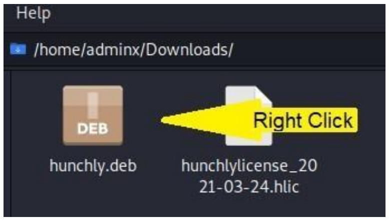
1. https://www.hunch.ly//try-it-now
2. Select Download for Linux, Download the .deb file
3. After download select “Show in Folder”, it show up as hunchly.deb
4. Next download your key file from email to the same download folder
5. Next open a terminal and type: **sudo apt install gnome-software**
6. Lets install google chrome next, a requirement for Hunchly
    a. Using a **terminal** window type in the below wget to obtain the latest .deb file

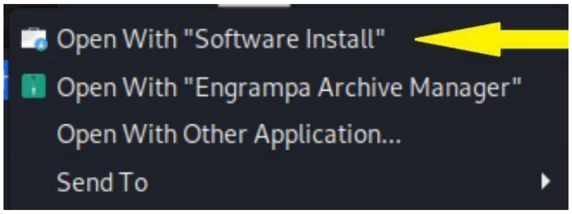
wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb

7. From the same terminal window, Now lets install Google Chrome **apt install ./googlechrome-stable_current_amd64.deb**

8. From the same terminal window you can launch chrome by type in **google-chrome --nosandbox**

9. With Chrome browse to the chrome webstore and add the Hunchly 2.0 extension https://chrome.google.com/webstore/detail/hunchly-20/amfnegileeghgikpggcebehdepknalbf?hl=en
10. Next locate the Hunchly .deb file you downloaded using your file manager, and right click

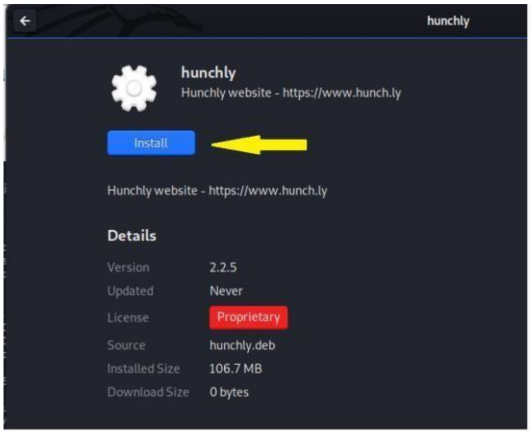



Open With "Software Install"
Open With "Engrampa Archive Manager"
Open With Other Application...
Send To

Select “Open with “Software Install” if this doesn't appear you skipped step 5.

Next screen is the install screen, click the blue “Install” button

Once it says installed you can close the window by the right x



Hunchly website - https://www.hunch.ly

Hunchly website - https://www.hunch.ly

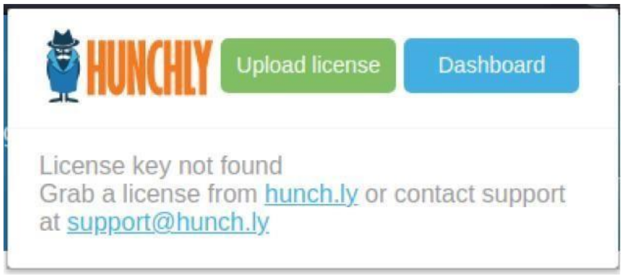
Details

Version 2.2.5
Updated Never
License Proprietary
Source hunchly.deb
Installed Size 106.7 MB
Download Size 0 bytes

11. Once you close out the installer, you will need to install (if you already haven't) the Chrome extension for Hunchly from step 9.

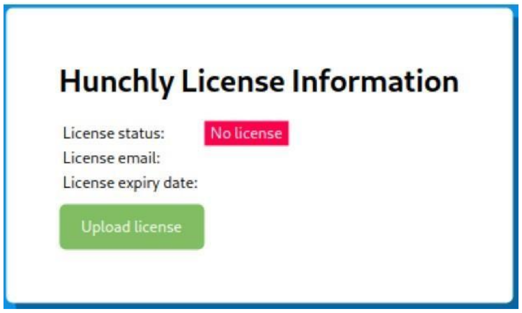
12. Next “Open Google Chrome” and select the “Extensions” 🧩 icon,

13. You can click the Red Hunchly ! Hunchly 2.0 2.0 icon and a window with licensing will appear - License Key not found



License key not found
Grab a license from hunch.ly or contact support at support@hunch.ly

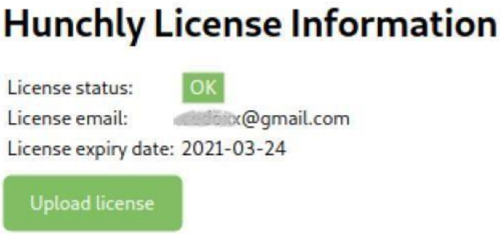
14. Select “Upload License” and another popup with “licence status” and an option to upload a licence. Select the green upload license and browse to locate the license file under downloads - Select that file and “okay”



Hunchly License Information

License status: No license
License email:
License expiry date:

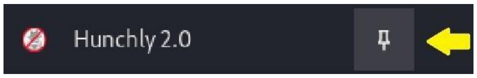
15. Once your product has been licensed, you will see the license status change to green



Hunchly License Information

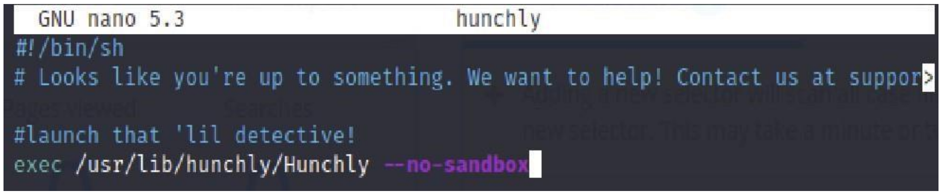
License status: OK
License email: [redacted]x@gmail.com
License expiry date: 2021-03-24

16. Now lets pin the hunchly icon to your toolbar so you don't need to search for it under extensions again, go to extensions, and notice the thumb-tac icon next to Hunchly 2.0



Select that icon and it should now appear on your main browser window

17. Next let's fix the Kali linux issue with launching Hunchly since Kali main OS is a bit different then Ubuntu we have to edit the “**/usr/lib/hunchly**” parameter file
    a. In a terminal window, sudo nano (or view) /usr/lib/hunchly



```
  GNU nano 5.3                        hunchly
#!/bin/sh
# Looks like you're up to something. We want to help! Contact us at suppor>

#launch that 'lil detective!
exec /usr/lib/hunchly/Hunchly --no-sandbox
```

*We will add a space and then **--no-sandbox** (as shown) and then save the file.*

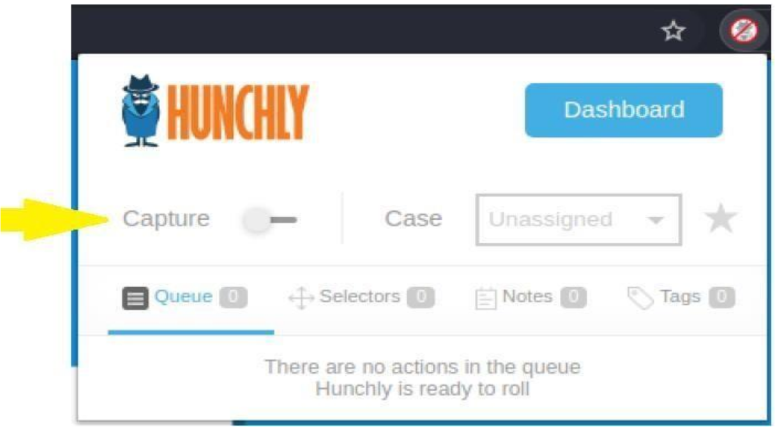
LAB2: Start an Investigation

18. First launch Tor Browser (Required to proxy the Chrome Browser to Tor)

19. Next enter the line below in a terminal window to launch Chrome

```
google-chrome --proxy-server="socks5://localhost:9150" --host-
resolverrules="MAP * ~NOTFOUND , EXCLUDE localhost"/Applications/Google\
Chrome.app/ Contents/MacOS/Google\ Chrome --proxyserver="socks5://localhost:9150" -
-hostresolverrules="MAP * ~NOTFOUND , EXCLUDE localhost"
```

20. Next Lets start a new case - Select the Hunchly icon from your Chrome Browser 21. Select Capture to to on (blue) then

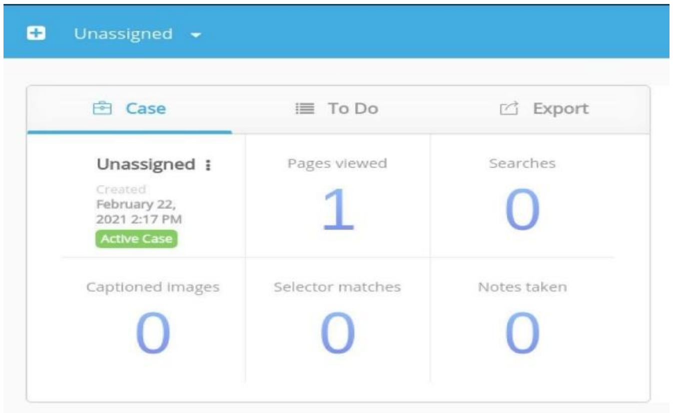


Case: Unassigned

There are no actions in the queue
Hunchly is ready to roll

22. Now you will browse to your questionable site, and review the items you are investigating while Hunchly captures all in the background.

23. To launch the Hunchly (another Quark of Kali) from a terminal window type in hunchly - enter. You should see Hunchly dashboard come up, as shown below.



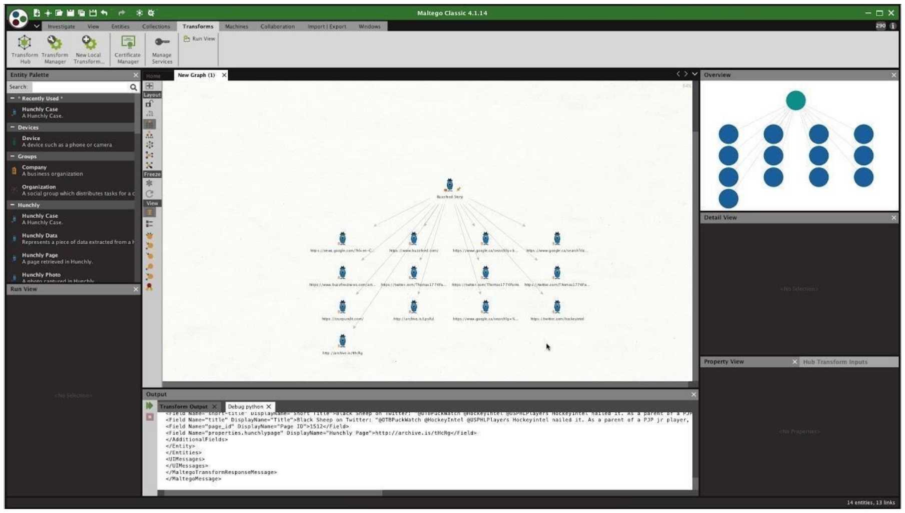
Unassigned
Created
February 22, 2021 2:17 PM
Active Case

Pages viewed 1
Searches 0
Captioned images 0
Selector matches 0
Notes taken 0

You should see one or more page views, and one unassigned active case, you can review all the details of the browse at the bottom section, or add details of what was found in notes.

24. There is an integration for **Maltego** transforms with Hunchly and data forwarding.
25. You can signup for the Hunchly mailing list where they send a daily “hidden services” spreadsheet each day, it includes a ton of information and can help you with your investigation.

26. If you want to continue with learning the in’s and outs of hunchly which is way beyond what this class teaches - checkout [Hunchly support]

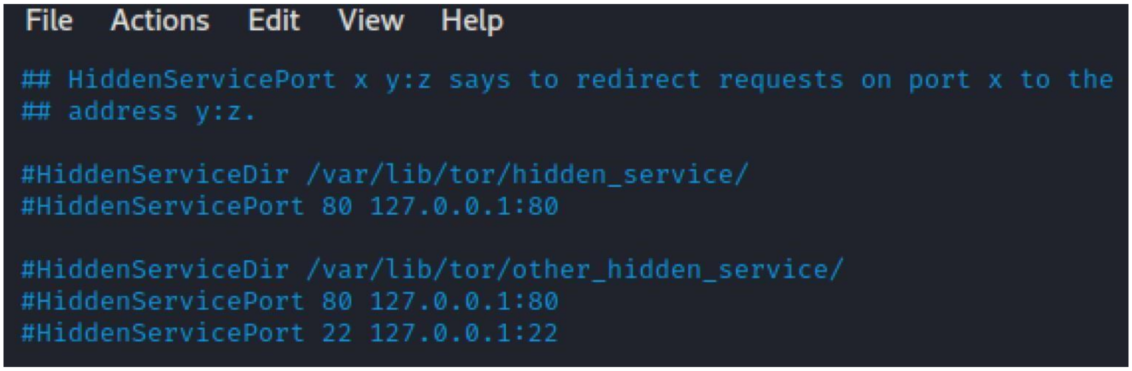


```
<Field Name="short-title" DisplayName="Short Title">Black Sheep on Twitter: "@OTBPuckWatch @HockeyIntel @USPHLPlayers Hockeyintel nailed it. As a parent of a PJP
<Field Name="title" DisplayName="Title">Black Sheep on Twitter: "@OTBPuckWatch @HockeyIntel @USPHLPlayers Hockeyintel nailed it. As a parent of a PJP jr player,
<Field Name="page_id" DisplayName="Page ID">1512</Field>
<Field Name="properties.hunchlypage" DisplayName="Hunchly Page">http://archive.is/tMcRg</Field>
</AdditionalFields>
</Entity>
</Entities>
<UIMessages>
</UIMessages>
</MaltegoTransformResponseMessage>
</MaltegoMessage>
```

Exercise 8: Let's Build a DarkWeb Server

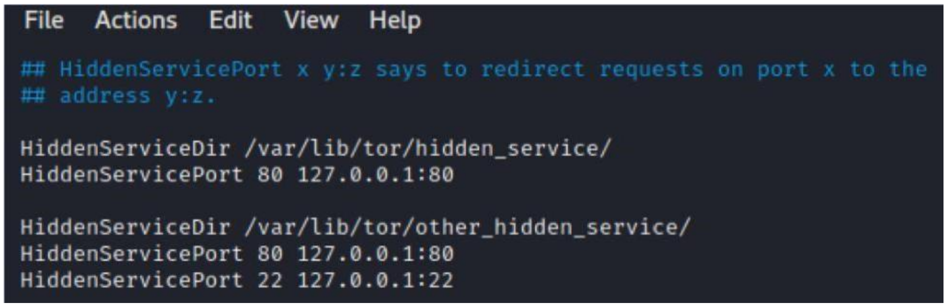
LAB1: This is an optional exercise

1. Lets configure our workstation to host a website on the darkweb, step 1 is already done, installing “TOR” and making sure you can run it as a service, lets check that out.
    a. From a terminal run “Service tor status” if its not running you can start it with running “service tor start” or “service tor restart” or to stop it service tor stop.
    b. Next lets edit the Tor RC file located under /etc/tor/torrc using view, leafpad or nano which ever your comfortable using: From a terminal window enter:
        i. sudo /etc/tor/torrc



```
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
```

c. You should scroll down until you see the #HiddenServiceDir notice the path to those services /var/lib/tor/other_hidden_service/ Next we will edit the file making the following changes:



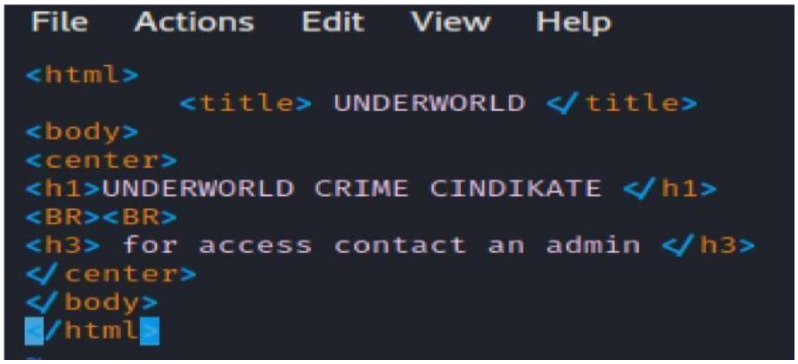
```
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80

HiddenServiceDir /var/lib/tor/other_hidden_service/
HiddenServicePort 80 127.0.0.1:80
HiddenServicePort 22 127.0.0.1:22
```

d. Now lets change to the directory we created to host our website,

cd /var/www/onion And create a simple webpage touch index.html

view index.html (or which ever editor you prefer)

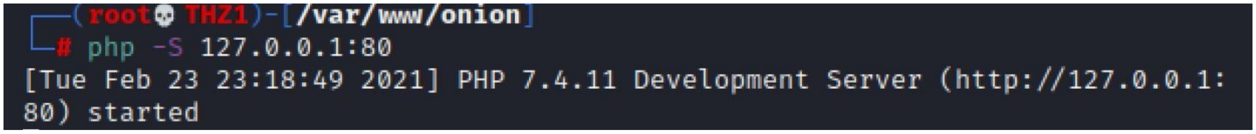
Add content similar to below and save the file



```
<html>
        <title> UNDERWORLD </title>
<body>
<center>
<h1>UNDERWORLD CRIME CINDIKATE </h1>
<BR><BR>
<h3> for access contact an admin </h3>
</center>
</body>
</html>
```

e. Next we will use php to create a simple web server

i. Where the page is execute: **php -S 127.0.0.1:80**

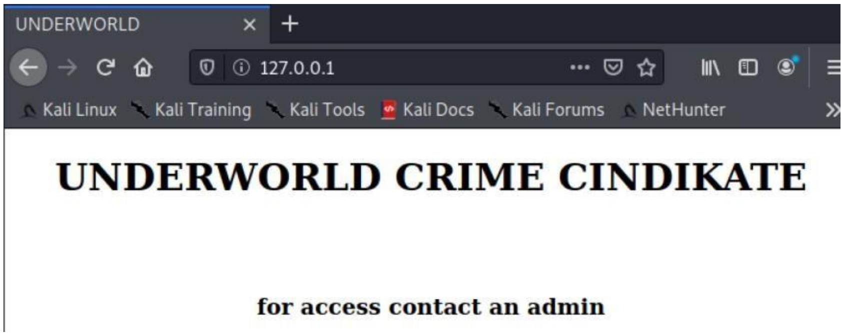


```
┌──(root💀THZ1)-[/var/www/onion]
└─# php -S 127.0.0.1:80
[Tue Feb 23 23:18:49 2021] PHP 7.4.11 Development Server (http://127.0.0.1:
80) started
```

You should receive feedback similar to the above output, showing the service started.

f. Next lets open firefox and browse to http://127.0.0.1:80 with or without the 80 should work, since its the default port, but this is a simple php server so there is no https. You should see a similar page as shown below to confirm your system is working.

g.



UNDERWORLD CRIME CINDIKATE

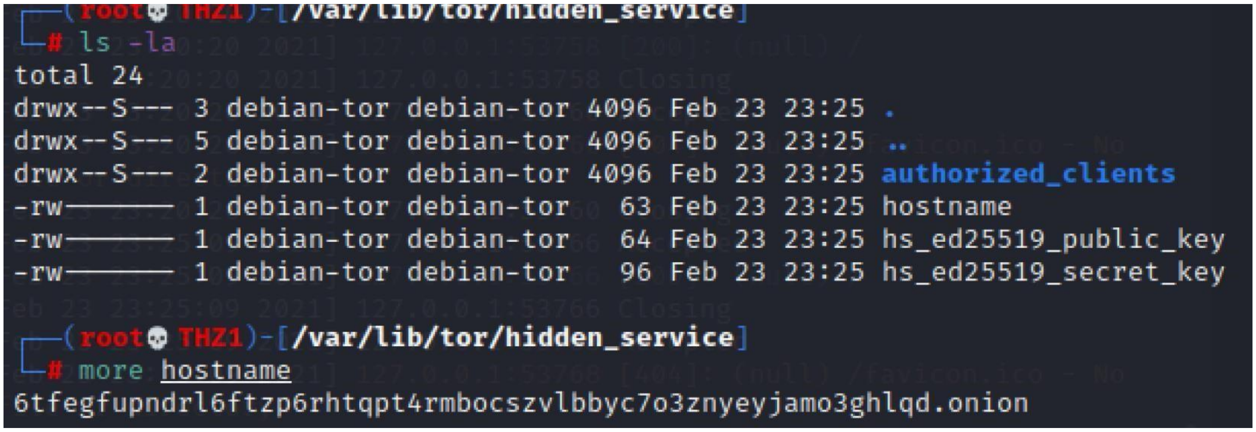
for access contact an admin

h. Now lets see if its accessible from the “DeepWeb” so whats our onion address and how can people find it ?

i. Just run this command from a new terminal window, we do not want to close the one hosting the php server so open a new terminal and type in

j. cat /var/lib/tor/hidden_service/hostname

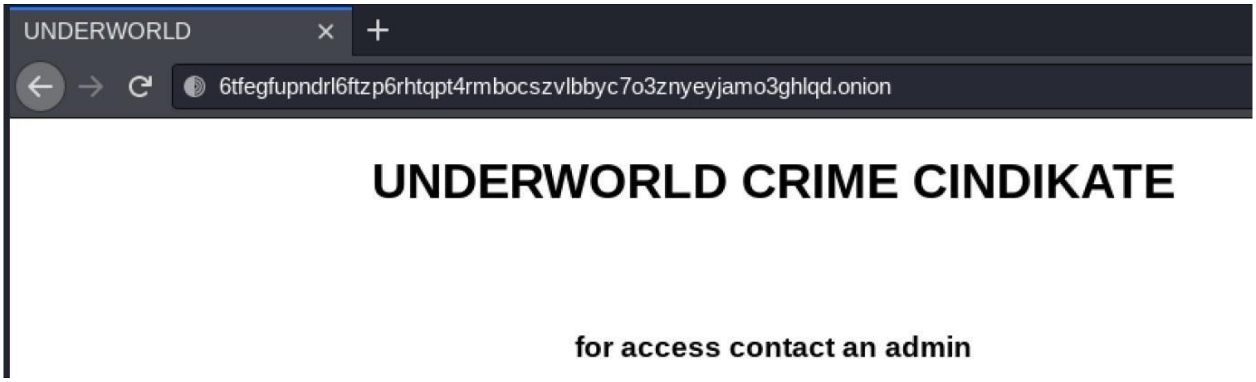
    ii. Or you can change to the directory and see the key’s and the hostname file as shown.



```
┌──(root💀 THZ1)-[/var/lib/tor/hidden_service]
└─# ls -la
total 24
drwx--S---  3 debian-tor debian-tor 4096 Feb 23 23:25 .
drwx--S---  5 debian-tor debian-tor 4096 Feb 23 23:25 ..
drwx--S---  2 debian-tor debian-tor 4096 Feb 23 23:25 authorized_clients
-rw───────  1 debian-tor debian-tor   63 Feb 23 23:25 hostname
-rw───────  1 debian-tor debian-tor   64 Feb 23 23:25 hs_ed25519_public_key
-rw───────  1 debian-tor debian-tor   96 Feb 23 23:25 hs_ed25519_secret_key

┌──(root💀 THZ1)-[/var/lib/tor/hidden_service]
└─# more hostname
6tfegfupndrl6ftzp6rhtqpt4rmbocszvlbbyc7o3znyeyjamo3ghlqd.onion
```

I. Now lets test this from a Tor browser

    A. 6tfegfupndrl6ftzp6rhtqpt4rmbocszvlbbyc7o3znyeyjamo3ghlqd.onion



6tfegfupndrl6ftzp6rhtqpt4rmbocszvlbbyc7o3znyeyjamo3ghlqd.onion

UNDERWORLD CRIME CINDIKATE

for access contact an admin

There you have it, your now a webhoster on the Darkweb. Now this is extremely unsafe the way we ran php, and didnt setup rights and such, you can install/run apache or nginx for more robust and secure hosting.

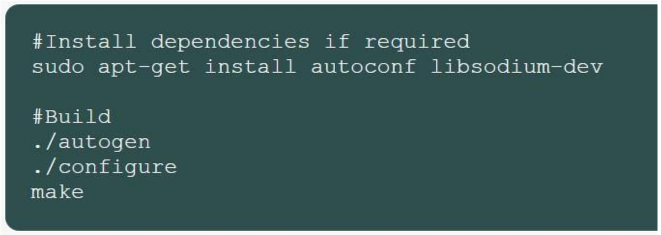
Another option would be to run this:

```
python3 -m http.server --bind 127.0.0.1 80
```

But I hate my long address and it doesn't make any sense….

LAB 2: Vanity TOR URL

A vanity url, instead of all these weird combo of letters and numbers, no problem there is a tool for that, it's called **mkp224o** and it is a vanity address generator for Tor Onion v3 Hidden Services, created by cathugger and available on Github.



```
#Install dependencies if required
sudo apt-get install autoconf libsodium-dev

#Build
./autogen
./configure
make
```

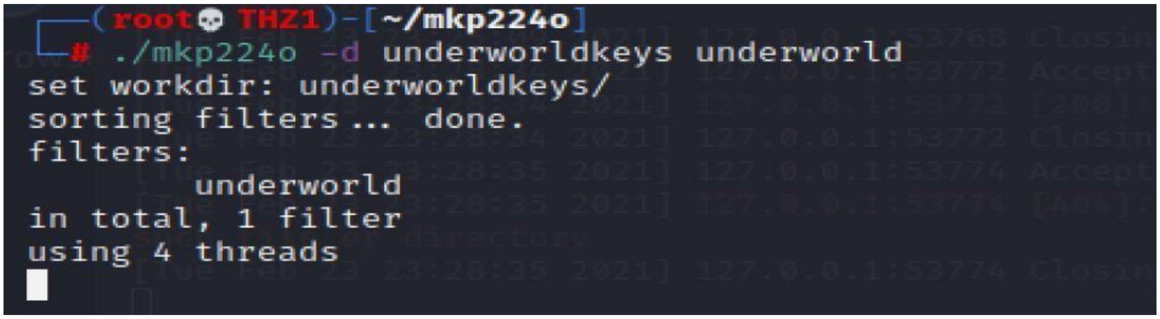
You should clone the repository to your workstation under your home directory. 1. You will need to add some dependencies 2. Open a terminal window:

```
apt install gcc libsodium-dev make autoconf
```

```
git clone
https://github.com/cathugger/mkp224o.git cd mkp224o ./autogen.sh
./configure Make
```

To Launch: **./mkp224o -S 5 -d onions underworld**

./mkp224o -d underworldkeys underworld



```
┌──(root💀 THZ1)-[~/mkp224o]
└─# ./mkp224o -d underworldkeys underworld
set workdir: underworldkeys/
sorting filters ... done.
filters:
        underworld
in total, 1 filter
using 4 threads
█
```

How do I make tor use of generated keys?

Copy key folder (though technically only hs_ed25519_secret_key is required) to where you want your service keys to reside:

```
> sudo cp -r onionsite54....onion /var/lib/tor/onionsite
```

You may need to adjust ownership and permissions:

```
> sudo chmod -R u+rwX,og-rwx /var/lib/tor/onionsite
```

Then edit torrc and add new service with that folder. After reload/restart tor should pick it up.

- Generate addresses with 1-2 and 7-9 digits?

  Onion addresses use base32 encoding which does not include 0,1,8,9 numbers. So no, that's not possible to generate these, and mkp224o tries to detect invalid filters containing them early on.

- How long is it going to take?

  Because of the probabilistic nature of brute force key generation, and variance of hardware it's going to run on, If your machine is powerful enough, 6 character prefix shouldn't take more than hours, where a 7 characters url can take days.

Exercise 9: i2P - The Garlic Router

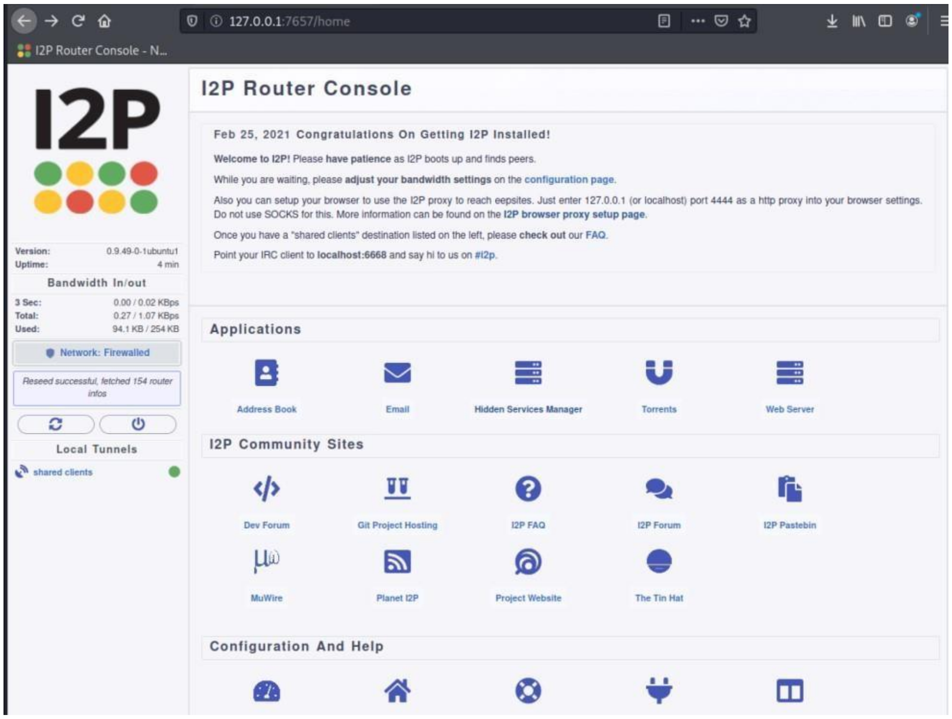
LAB1: This is an optional exercise to get i2P ver 9.49 running on your system, there quite a few debian apps and commands required to get it up and running, and of course do not run as root after you finished installing.

1. From your Debian VM Host open firefox and Download https://geti2p.net/en/download#deb
2. Make sure your Tor demon is stopped - > service tor stop
3. > sudo apt-get install apt-transport-https curl
4. Create /etc/apt/sources.list.d/i2p.list (use nano or view) and add the following repos
   deb https://deb.i2p2.de/ buster main
   deb-src https://deb.i2p2.de/ buster main

5. curl -o i2p-debian-repo.key.asc https://geti2p.net/_static/i2p-debian-repo.key.asc
6. gpg -n --import --import-options import-show i2p-debian-repo.key.asc
7. sudo apt-key add i2p-debian-repo.key.asc
8. sudo apt-get update
9. sudo apt-get install i2p i2p-keyring

Now from a web browser: http://127.0.0.1:7657/welcome

It will test your bandwidth, give it a minute, you wont be able to click next until its finished.



I2P Router Console

Feb 25, 2021 Congratulations On Getting I2P Installed!

Welcome to I2P! Please **have patience** as I2P boots up and finds peers.

While you are waiting, please **adjust your bandwidth settings** on the configuration page.

Also you can setup your browser to use the I2P proxy to reach eepsites. Just enter 127.0.0.1 (or localhost) port 4444 as a http proxy into your browser settings. Do not use SOCKS for this. More information can be found on the **I2P browser proxy setup page**.

Once you have a "shared clients" destination listed on the left, please **check out** our FAQ.

Point your IRC client to **localhost:6668** and say hi to us on #i2p.

Version: 0.9.49-0-1ubuntu1
Uptime: 4 min

Bandwidth In/out

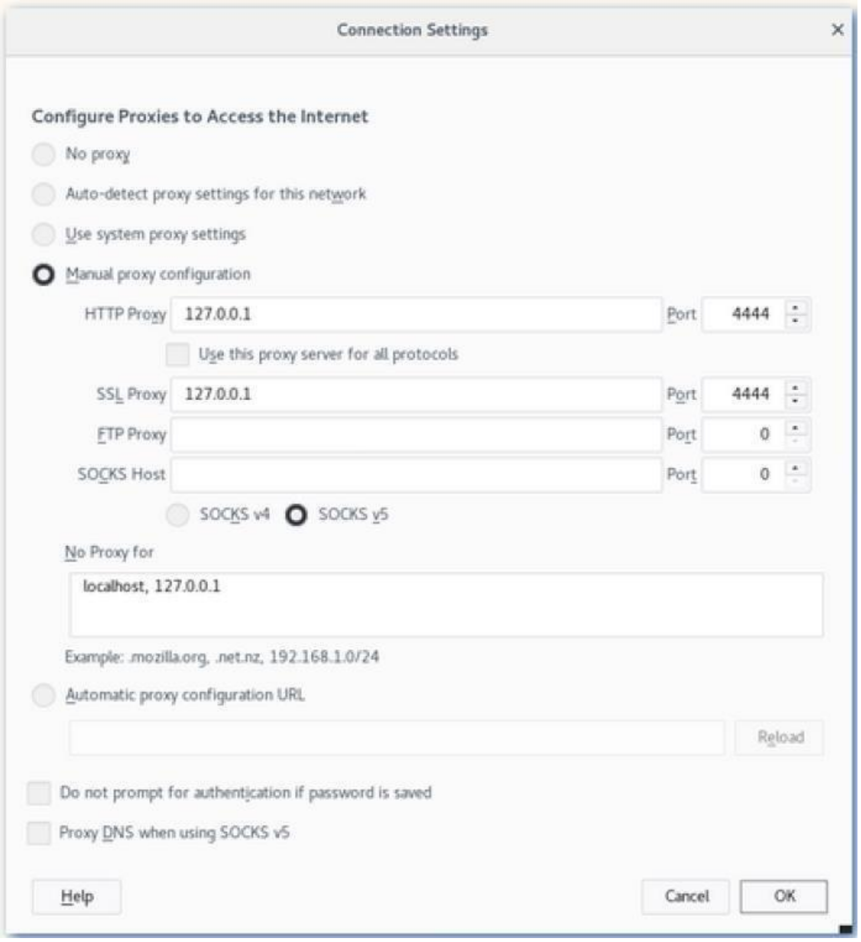
3 Sec: 0.00 / 0.02 KBps
Total: 0.27 / 1.07 KBps
Used: 94.1 KB / 254 KB

Network: Firewalled

Reseed successful, fetched 154 router infos

Make sure you setup your browser for the proxy, settings can be found here

Go to Preferences, Network proxy : In the Connection Settings pop-up, select Manual proxy configuration. Set both the HTTP and SSL Proxy to address 127.0.0.1 with port 4444 as shown in the following screenshot.



Connection Settings

Configure Proxies to Access the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 4444
□ Use this proxy server for all protocols
SSL Proxy 127.0.0.1 Port 4444
FTP Proxy Port 0
SOCKS Host Port 0
○ SOCKS v4 ● SOCKS v5

No Proxy for
localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

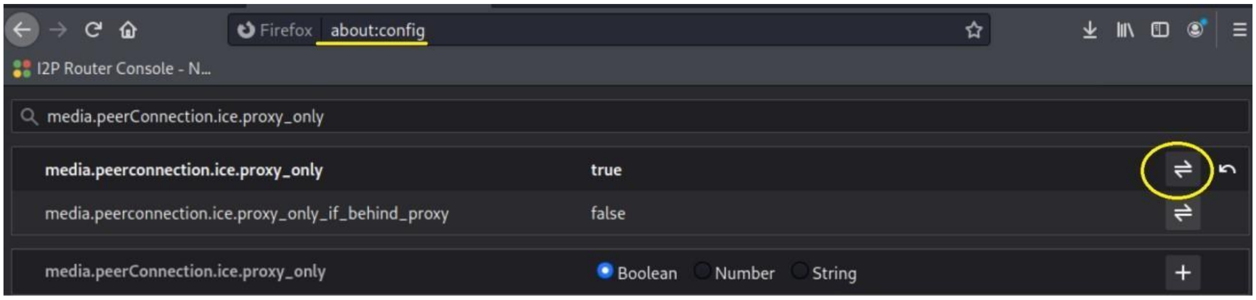
○ Automatic proxy configuration URL

Reload

□ Do not prompt for authentication if password is saved
□ Proxy DNS when using SOCKS v5

Help Cancel OK

Finally, go to the address about:config and find the property media.peerConnection.ice.proxy_only. Ensure that this setting is True



Firefox about:config

I2P Router Console - N...

media.peerConnection.ice.proxy_only

media.peerconnection.ice.proxy_only true
media.peerconnection.ice.proxy_only_if_behind_proxy false

media.peerConnection.ice.proxy_only ● Boolean ○ Number ○ String +

END:

LAB2:

I2P Anonymous Webserver, Anonymous Web Serving on I2P

This is your own anonymous I2P webserver (traditionally referred to as an eepsite). To serve your own content, simply edit the files in the webserver's root directory and the site will be public once you follow the instructions below.

The webserver's root directory can be found in one of the following locations, depending on your operating system:

Standard install: ~/.i2p/eepsite/docroot/
Package install, running as a service: /var/lib/i2p/i2p-config/eepsite/docroot/

In I2P, hidden services are addressed using a Base32 address ending in ".b32.i2p", or a Destination represented as a long Base64 string. The Base32 address may be used as a hostname, until you register a name following the instructions below. The Destination is somewhat like an IP address, and is shown on the Hidden Service Configuration page.

The instructions below detail how to assign a name like "mysite.i2p" to your website and enable access by others. You may reach your site locally via http://127.0.0.1:7658/.

http://127.0.0.1:7658/help/

How to set up and announce your hidden service

Your webserver is running by default, but is not accessible by others until you start the hidden service tunnel. After you start your I2P Webserver tunnel, it will be difficult for other people to find. It can only be accessed with the long Destination or with the shorter Base32 address (.b32.i2p), which is a hash of the Destination. You could just tell people the Destination or the Base32 address, but thankfully I2P has an address book and several easy ways to tell people about your website.

Here are detailed instructions.

Pick a name for your website (something.i2p), using lower-case. You may wish to check first in your own router's address book to see if your name is already taken. Enter the new name for your website on the Hidden Service Configuration page where it says "Website name". This will replace the default "mysite.i2p". Also, if you would like your I2P Webserver tunnel to be automatically started when you start I2P, check the "Auto Start" box. Your website will now start every time you start your router. Be sure to click "Save".

END: