The #OpNewblood Super Secret Security Handbook

If you have not gone through the IRC chat client setup for your operating system, we recommend you go back and get started there.

Master Table of Contents

Section 1: Preface

NOTE: If at any time you need help with any topic found in this guide, feel free to join us at http://goo.gl/8zxwO and you'll be able to find someone to help you figure it out. It should be noted that this guide contains information that may be difficult to understand without an extensive technical and functional knowledge of information systems. While this guide does attempt to put it simply and in laymans terms, you the user are ultimatly responsible for the security of your own systems.

Section 2: Setting up Tor

Preface: Due to abuse in the past, users trying to connect to the AnonOps IRC servers using Tor will not be able to connect. This is nothing personal, there have just been problems with abuse of the program in the past on the IRC server. Therefore, we do not recommend using this for IRC connection, but merely as an easy to use tool for browsing the internet anonymously. Keep it in, for most users it's a relatively slow connection.

Windows:

Go download Tor here: https://www.torproject.org/dist/torbrowser/

After downloading Tor:

1) Run the .exe

2) Extract to your PC.

3) You will now have extracted TOR into the selected folder. You should have a button called „Start Tor" with an onion on it, click this to start (if you want you can make a shortcut by right-clicking create shortcut and drag it to your desktop, make sure the original stays in the same folder though).

4) You are good to go, if your ISP blocks connections to TOR and you need help setting up a bridge feel free to ask about it in the #OpNewblood channel, which again you can access through your web browser at this link: http://goo.gl/8zxwO

Linux:

1) Download Tor here: https://www.torproject.org/dist/torbrowser/linux/

2) Extract to destination of your choice

3) You should now be able to just click your start tor button to start.

4) For additional ease of use, try Tor Button for Firefox.

5) Once again for help with making a bridge if your ISP blocks Tor please ask for help in #OpNewblood via your web browser here:http://goo.gl/8zxwO

Mac OS X:

1) Download Tor here: https://www.torproject.org/dist/vidalia-bundles/

2) Mount the .dmg file and find it on your desktop

3) Move Vidalia to your applications folder

4) Download the Tor button for Firefox here: https://www.torproject.org/torbutton/index html.en

5) Once you have both installed, run Vidalia and make sure it says „Connected to the Tor Network!" and then go to your Firefox browser and right click on the indicator in the bottom right and click „Toggle Tor Status"

6) Read more on operating Tor here: https://www.torproject.org/docs/tor-doc-osx.html.en

7) Once again for help with making a bridge if your ISP blocks Tor please ask in the #Opewblood channel via your web browser here:http://goo.gl/8zxwO

A NOTE FOR ALL OS's:

1) To check anytime if TOR is working, you can go here: https://check.torproject.org/ and it will tell you if your TOR is working.

2) Highly reccomended is the TOR button for firefox: https://addons mozilla.org/en-us/firefox/addon/torbutton/ which will allow you to turn tor on/off as well see if it's disabled in your browser.

Anonymous Browsing Using Tor Button for Firefox

Start by install Tor on your computer and configuring it to your liking. Then, download the Tor Button add-on for Firefox, and use the options to configure the add-on the way you want it. Then, press the „Tor Button" and go to a test website to ensure you've done it correctly. If the website returns properly anonymous results, then you've correctly set up Firefox for anonymous browsing through Tor. Also worth doing: hit Tools>Start Private Browsing whenever you are browsing with Tor. It stops logging your web history, caching files, passwords, cookies, and download history, so you don't have to clear the history everytime you're finished.

Troubleshooting: refer to www.torproject.org

Section 3: Firefox recommended Add-ons

Adblock Plus: This plugin blocks around 90% of internet services that attempt to track your web activity and then send you targetted ads. It's crucial to use while browsing any aon websites or sites that have anon news articles, etc. http://goo.gl/fPmjm

NoScript: A very useful plugin that will disable javascript on sites to protect your privacy and stop malicious activity. Can set rules for individual sites or deny globally. http://noscript.net/

BetterPrivacy: This plugin is a tool to identify and remove cookies. It will also act as an „optout" from advertisement and other forms of web tracking. http://goo.gl/TL79Z

FoxyProxy: An Addon to the default way to handle connecting to proxies, the FoxyProxy addon will allow you to have easier access to enabling your proxy tunnels, also has advanced features, such as setting up a list of domains that you will always want to use a proxy to connect to, and to do so automatically, while still using another connection for non-listed sites. http://goo.gl/VRiHT

Ghostery: Another tool to help manage and mitigate tracking cookies, Ghostery features tools that will alert you when there are tracking cookies on the websites you visit. You can also view information about each tracker that is trying to harvest your browsing data, and even view the source code of said tracker and see exactly how the cookie is tracking you. Make sure you get Fanboy list and Easy list to stay updated (these can be selected during setup or in the options of the addon itself) http://goo.gl/GoKQ1

Greasemonkey (GM): A great addon that allows you to edit the way websites show information to you, using bits of javascript code. This is more of an addon „engine" or development platform, allowing you to write and download scripts to do many different things using their addon. http://goo.gl/atGk7

HTTPS Everywhere: A Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites. http://goo.gl/fsKV

Section 4: Setting up i2p for IRC+Browsing

by cred

Section 4 table of contents:

4.1a) I2p Installation: Windows

1) Download:

You can download the latest version of the i2p software here:

http://www.i2p2.de/download.

2) Installing:

In windows, the installation, as with any other windows software, is relatively

straightforward. Double click on i2pinstall_(version).exe that you downloaded from the above website and follow the instructions.

3) Launching the router:

After the install has completed, you can access your router console (control panel for i2p software, in the form of a website) even when you're not actively using the i2p proxy by doubleclicking the „Start I2p" icon or by following http://127.0.0.1:7657 For those not versed in how the internet works, 127.0.0.1 is an IP address that always leads to Localhost, or webservices that are running on your machine. As long as you are connecting to that address, no other anonymizing software is needed, since you are only talking to your own machine.

4) Browsing I2p:

In order to access .i2p websites, or eepsites, you'll have to set up i2p as a PROXY on your web browser of choice, instructions for this on Firefox are in section 4.2

4.1b) I2p Installation: Linux

1) Easy way: Ubuntu.

- Open a Terminal and enter:

```
sudo apt-get install sun-java6-jdk
```

- Get the latest install package (yes, the .exe file, don't ask, it's java.) from http://www.i2p2.de/download. In the terminal window, navigate to the folder where you downloaded the .exe file and enter:`java -jar i2pinstall-*.exe`

- Follow the prompts

2) Other distributions:

Google instructions for installing the java JRE software on your distribution, typically it's not much more difficult than with Ubuntu, but different distros have their own package management systems, and the commands might be slightly different.

Once Java is installed, it's the same command as Ubuntu:

```
java -jar i2pinstall-*.exe
```

4.2) Firefox Configuration

1) Verify it's running:

Once the i2p client is installed, you can verify it's running an http:// tunnel by

going to http://127.0.0.1:7657/i2ptunnel/ Under the „I2p Client Tunnels" section, the first entry should be „I2p HTTP Proxy". On the right, under the „Status" column, there are three little stars, one red, one yellow, and one green. If red is lit up, hit the „start" button to the right of it, If it's yellow, you don't have enough peer connectionsyet, and you should let it establish a presence on the network. Leave it alone and grab a sandwich, it should be ok in an hour or two.

2) Set up localhost as a proxy

Goto Edit>Preferences

Goto the Advanced section

Under Connections click the Settings button

Select „Manual Proxy Configuration"

Enter the following:
- HTTP Proxy: 127.0.0.1 Port: 8118
- SSL Proxy: 127.0.0.1 Port: 8118
- SOCKS Host: 127.0.0 1 Port: 9050
- SOCKS V5 checked
- No Proxy for: 127.0.0.1

4.3) Various IRC Client configuration

IRC Clients need no special setup or proxies. Just visit your

http://127.0.0.1:7657/i2ptunnel/ and make sure IRC Proxy is running. If it is, justconnect to 127.0.0 1 on port 6668 like it's a normal IRC server. Your client will sendall data to the proxy that's running on your machine on port 6668, which will then send it, via I2p, anonymously and securely to the i2p IRC servers. You may enter additional i2p irc servers by clicking on *IRC Proxy* on the Tunnel manager page and pasting the addresses in the „Tunnel Destination" field (comma seperated).Take a look at this list of clients and choose the one that sounds right for you:

Windows: http://www.ircreviews.org/clients/platforms-windows.html

Linux: http://www.ircreviews.org/clients/platforms-unix-x.html

(This author is a proud owner of a Ubuntu box, chatting on Xchat)

4.4) Fun shit

1) If you have a Linux machine, you can connect to the i2p irc servers through your home computer from your Android phone from anywhere in the world.
- What you need:
- Ubuntu Linux: http://www.ubuntu.com
- irssi connectbot for Android

https://market.android.com/details?id=org.woltage.irssiconnectbot

- openssh for Ubuntu: sudo apt-get install openssh-server
- irssi for Ubuntu: sudo apt-get install irssi

2) open irssi connectbot on your android and enter [your linux username]@yourip:port

Now, since most people are behind a firewall, or a router, or something, there's

probably some port forwarding you're going to have to do, but for now, just connect to your own wireless router with your android's wifi. It's safer anyway.

3) First thing you want to do is login with your password (that's why it's better to do it locally before doing it over the web… Make sure you've got encryption on your wifi, by the way)

4) Once you have a command prompt on your android, hit the back button to get back to the host list, then the menu button, and tap „Manage Pubkeys" Hit the menu again, and select „generate". Name your key, make it RSA and give it at least a 1024 bit hash, (I go to 2048, you can't be too careful) No password, and hit „Generate"

5) Now it will have you fuck around with your touchpad to generate randomness, and create your pubkey. Once you're back on the pubkey list with your new pubkey, longpress on it and select „Copy Public Key"

6) Now hit the back button and click your host connection in the host list, which will bring you back to your command prompt. Enter cat „(hit menu and select paste to paste your pubkey into these quotes)" >> .ssh/authorised.keys

7) Now enter exit which will take you back to your server list, and disconnect you. Tap your server to connect again, and this time, it should not ask you for a

password. This means you are connected using a shared 1024 bit (at least)

pubkey, which ain't bad.

 To connect from outside your home network, you need a few more things:

- Your external IP address: http://www.whatismyip.com
- Port forwarding to port 22 on your machine (if you have a router and multiple machines on your home network as most do) See step 9

9) Most routers are set up with a web interface for changing settings. If you have

wireless security enabled, then you or whoever set up your home network for you, have already accessed the web interface, and should have set up a password. You'll need to log into that web interface, go to the section on port forwarding, and forward an available external port (22 will do) to port 22 on your machine's local IP address (usually 192.168 1.101 or something) for BOTH tcp and udp. This is as clear as I can make it without router specific instructions. (Talk to your router provider or local geek for help in this regard)

10) Now all you need to do is connect through irssi connectbot to (your

username)@(your external IP address):(port you set up to forward to ssh on your

machine)

11) Once you're connected to a ssh server on your home computer (which by now

should be running i2p) you may launch irssi, a command line irc client, and connect to the i2p servers with irssi using:

```
/connect 127.0.0.1 6668
```

Questions? Comments? Concerns? Join into #OpNewblood via your web browser here: http://goo.gl/8zxwO or you can contact cred via i2pmail cred@mail.i2p or from the insecure web (securely) at http://privacybox.de/cred.msg (include return contact info, since it doesn't store or transmit any identifying information)

Section 5: Advanced IRC Commands

5.1) Commands

1) /join

Self explanatory, this is used to join a channel, to join #opnewblood , you would type */join #opnewblod*

2) /me

Not really as necessary, but used sometimes. for instance if you wanted to wave at someone, you would type */me waves* it would appear as „anon waves“

3) /msg

if you want to have a conversation with a specific person outside of the channel the best thing to do is message them, just type */msg username message here.* just make sure to use a space between their name and the message.

4) /query

Same thing as msg, except this will open up a new window for you to have a conversation with this person.

5) /nick

This command will change your nickname for instance if you wanted to be called gigapuddi you'd type */nick gigapuddi.* Remember though if you do this you won't be registered unless you re-register with nickserv (see the walkthrough to anon if you dont know what nickserv is, or want help with it)

6) /quit

This will let you quit.

7) /ignore

Trolls are plenty, and it's best not to feed them, and just ignore them. To ignore someone type */ignore username*

 **/whois**

This will display information about the person you selected, such as their vhost, what channels they're in ect. to find a whois just type*/whois username*

9) /away

To mark yourself away, you can use this, if you were persay making a sandwich, you could do */away making sammiches* and people will know you're making sandwiches.

10) /ping

This is to see the latency to the server, if you're lagging this might give you more information, to ping a server just type /ping ipadresshere

11) /notify on/off

This will change if you get a notification (a beep sound) whenever someone types your name. to turn off /notify off to turn on do */notify on*

12) /topic

If you want to see a topic in a certain channel just type /topic and it will read it out to you.

13) /list

Lists the channels that are available to you.

5.2) Browsing IRC

NickServ

When you arrive on the IRC for the first time, you will be using an unregistered nickname. If you plan on becoming a regular user, it is vital to register your nick. This is important for several reasons:

- It ensures that nobody can impersonate you.
- It grants you various abilities which non registered users do not have
- (Most importantly) It allows you to use a vhost – this hides your location and ISP information from other users.

To register your nickname, refer to the IRC guide for your operating system on the original #OpNewblood page.

When you connect to the server, type /msg nickserv IDENTIFY password

This will tell nickserv that you are the real owner of your nickname. If you do not do this, you will not have access to registered-only chans or your vhost. For safety reasons, it is recommended that you type the command in your status window so, in the event of an error on your part, you do not post your password to an entire channel.

Groups

If you plan to use more than one nickname, you can group them together. This has several uses, the main ones being to tell people where you are connecting from, or that you are away.

For example: a user called „JohnDoe“ might be going out for a while but leaving his laptop on, in which case he could change his nick to JohnDoe|Away or JohnDoe|AFK to let other users know he was away. This is important so as, for example, people will know why you are not replying to messages. He might also use the nick JohnDoe|Mobile to let people know he is on a mobile client, and therefore cannot use certain functions such as possibly recieving PMs or visiting links people might send him.

To change your nick, type /nick newnick. However, when you do this, you will lose any access levels, vhost, and other settings associated with your nick.

To avoid this, when you choose your new nickname, switch to it using /nick, then type /msg nickserv GROUP nick password – where nick and password are your MAIN nick and its password. This ensures that these nicks will share passwords and settings.

Ghosts

Let’s face it, sometimes shit happens. Sometimes your internet connection will randomly decide to die on you. Sometimes your laptop’s battery might run out, sometimes your IRC client will crash, sometimes you might accidentally close a window. There are many reasons one might suddenly find themselves accidentally disconnected from the IRC.

The problem is that unless someone signs off in „an orderly fashion“, the server will not actually realize they are gone. Think of it like somebody who puts down a phone and walks away, but without hanging up the call. Or like when your computer crashes without shutting down the correct way. In these circumstances, the IRC server does not realize you’re gone, and assumes your nick is still connected. This situation remains until the next time the IRC pings your nick and gets no response (‘ping timeout’). This can take a while though, and very often the person who has disconnected, will manage to get themselves back online *before* the server has time to realize they ever left in the first place. When this happens, the user’s nick is

already in use, so the server will assign them a new one (usually just by adding a ` or _ to the end, so if JohnDoe tries to connect when there is already a JohnDoe connected, they will be signed on as JohnDoe_ or JohnDoe`.
The problem with this, of course, is that just like an un-identified nick, these nicks have no modes, no vhosts, no access levels – because the „ghost“ of the nick is still occupying them.

To force the dead session to disconnect and replace its nick with yours, type /msg nickserv GHOST password, where password is the pass to the original nick. This would, in this example, disconnect JohnDoe and change JohnDoe_ to JohnDoe automatically, identifying and setting up the nick as normal. When this happens, you will probably see something like this in the channel:

JohnDoe left the chat room (GHOST command used by JohnDoe_)

JohnDoe_ is now known as JohnDoe

It is very important to do this as quickly as possible when re-connecting, as you will be locked out of your vhost until you have done this.

Vhosts

Obviously one of the main priorities of any Anonymous is to be, well… *Anonymous*.
When you connect to our IRC server, the server will automatically mask your IP address (your computer's „phone number“). This is the most important layer of anonymity, but unfortunately there is a catch. Most of the time, it will NOT automatically hide your ISP (Internet Service Provider)'s name. So for example the fact that your IP is from a certain town might be hidden, the fact that you are a comcast customer may not be.

To rectify this, we have a vHostServ. It gives you a fake host name, which masks the true ISP you are connecting through. It can be anything you want – for instance, if anyone ever tries to check where I am connecting from, they will see „fuck.off.you.bollocks“ instead. 

To get a vHost, you must be registered and identified. This is why it is CRUCIAL that you identify ASAP when you connect, as your vHost will not be activated until you have done so.

How to get a vHost :

1. Type /join #vhost in your IRC.
2. Once inside the vHost channel, type !vhost (insert.clever.name.here).

NOTE : You can, indeed, use whatever you want as a vhost – provided it is a valid one, i.e. no spaces, and must contain at least one dot. The most common way to do this therefore is.to.use.dots.as.spaces.in.your.vHost.

When you have done this, vHostServ will automatically kick and ban you from the #vhost channel. This is normal and expected, and simply means the vHost as worked. You will be banned from the channel (#vhost) for a certain amount of time, after which you will be able to change your vHost if you like. Now that you have a vhost, you are fully set up to use the IRC, any other settings you may set on your nick are purely optional.

*Note: If you join a #chan before you vHost, your new anonymized information will not automatically update in the channel. Be sure to exit and rejoin any channels you are connected to after you vHost, or your real connection information will still be viewable.

**NOTE: If you use Xchat along with auto-join channels, you can tell xchat to wait longer before joining channels on server connect using the /set irc_join_delay X command, where X is the number of seconds xchat will wait before joining channels. Setting this to something like 10 seconds helps if you're using automatic channels

Invite-only channels (mode +i)

Some channels, for various reasons, are invite-only. Commonly this is because the channel has a very specific purpose and only users who have a specific job in the channel can access it – for example, there are private channels for operators and hackers. Sometimes, a channel will also be set to +i if it is being invaded or flooded by bots or trolls.

If a channel is +i, you will not be able to join it using /join. You will simply get an error message telling you that the channel is invite only. However, if you are an operator yourself, or are on the invite exception list, you can force the server to let you in.

To do this, you send a message to another bot called ChanServ, which is not covered in this guide as in general only more advanced users will ever need to use it. However, to request an invite, type /msg chanserv INVITE #channel, where #channel is the channel you are trying to connect to. It is important to include the # at the start of the channel name, or ChanServ won't recognize it.

If you are on the list, you will then gert a message asking you if you would like to join the channel. Otherwise, chanserv will tell you that you do not have permission.

If you are NOT on the invite or operator list for a channel, but you feel you should be allowed in to it anyway, you can type /knock message, where message is your message to the channel admins. So for instance, if there was a channel called #brits only for British people, and you didn't have access, you could type /knock #brits Hey, I'm British, let me in!

This will send a message to the channel admins, and cause your message to appear in the channel. The admins will then (if they decide to let you in), send you an invite just like chanserv does. You will receive the same message you would receive from chanserv asking you if you would like to join the channel.

NOTE: Knocking on a channel 10 times in a row is not going to amuse anyone. In all likelihood, it will actually make it almost certain that you will NOT be invited into the channel. If you receive no invite it either means the admins are not active at that time, or have decided for whatever reason not to invite you. If it does happen, you could maybe try again later, but don't knock 10 times in one minute, this is more likely to get you banned.

If no one replies to your knock, another option you have is to type /msg chanserv INFO #channel, where #channel is the name of the channel (again, include the # or chanserv will ignore your message). This will tell you what the channel is for, and who created it. You could then message the room founder and ask for access, but this is generally not recommended unless it is extremely urgent.

Section 6: Advanced Defense Techniques

USING Virtual Machines

It is strongly recommend you consider making a Virtual Machine (VM) to seperate your personal OS instance with you anon activity OS instance.

This ensures that personal data does not leak while viewing anon related social media on such sites as Twitter or Facebook.

It has several other advantages such as allowing you to quickly delete all anon activity off your computer by simply deleting the VM itself.

Virtual Machine Software

VirtualBox – x86 and x64

VMWare Workstation 7 – x86 and x64

Windows Virtual PC – x86

etc. (do a google search for „virtual machine)

DISK ENCRYPTION

Disk encryption is another way to protect yourself. Disk encryption software will make it pretty much impossible for any one but yourself to access the data on any physical disk.

Disk Encryption Software

TrueCrypt – http://www.truecrypt.org/

Bitlocker – (Win 7 Ultimate only)

File and Email encryption and validation `(added by cred)`

Using the openPGP standard, the following software creates a „Keyring“ for you, bound to your name and email address (neither of which needs to be real, I have two, one for my real life identity and another as cred) The private key is a password protected key you keep on any system on which you will be DECRYPTING information; your home computer, and if you're brave, your Android phone. The public key is used to ENCRYPT information or files, and is available to anyone. So if you wanted to encrypt information to send to me, you'd have to search from my public key, (cred@mail.i2p will find it for you) encrypt the data with it, and send it to me. The only thing that can now recover that data is my private key and password. PGP is the industry standard for high level encrypted email.

PGP (Windows) http://gpg4win.org/download.html

PGP (Linux) http://www.gnupg.org/

APG (Android) https://market.android.com/details?id=org.thialfihar.android.apg

PROXY LISTS

- http://www.freeproxies.org

- http://www.socks24.org

- http://www.samair.ru/proxy

LINUX TOR VM's

It's possible to use Tor as a VPN using some prepackaged linux VM's. Once these VM's are started it's possible to create a VPN connection to the Tor VM. These VM include additional privacy goodies such as Squid and Privoxy.

Linux Tor Software

JanusVM – http://janusvm.com/

TAILS – https://amnesia.boum.org/

Section 7: Portable Solutions

Portable refers to self-contained OS and software packages that can be run from CD, DVD or USB device. This allows you to carry your anon OS instance in your pocket, plug it into or insert into another computer and be ready to access anon resources in a secure way.

The Amnesic Incognito Live System: https://amnesia.boum.org/download/index.en.html

A bootable, live, Linux distribution focusing on security and privacy, Basically this entire document in a single download.

Gnacktrack: http://www.gnacktrack.co.uk/

For the hacker anons among us, a live linux distribution with all the tools a good hacker needs to control the fate of the world from a laptop at a Starbucks.

BackTrack: http://www.backtrack-linux.org/

Gnacktrack, only for people who prefer the K desktop environment over GNOME.

Ubuntu Privacy Remix: https://www.privacy-cd.org/

Intended solely for Live Booting, no installation on the local system is required, and none of the data on it is touched.

Section 8: ADVANCED GUIDE TO HACKING AND SECURITY VULNERABILITY

by Denizen

Preface: Information in this section can be extremely confusing for new users, and those without the sufficient technical knowledge to understand. Always be cautious when tinkering with systems you don't fully understand, as this may lead to undesirable results, detection, and in extreme cases system failure or legal trouble.

For those interested, an excellent guide to Denial of Service Attacks or DDoS can be found here: http://insurgen.cc/index.php?title=DDOS

Guide By: Denizen

As the ultimate denizen, you must be able to enter systems at will in various ways. There are many ways to reach a website, and to add protection for yourself in terms of anonimity and minimized vulnerability.

Table of Contents

1. USING PUTTY TO SETUP AN SSH TUNNEL

http://oldsite.precedence.co.uk/nc/putty.html

Normal connections to the internet, unless using SSL, are typically unencrypted transmissions divided into data packets. Using a packetsniffer, it is possible to capture most packets, and look at their payload in plain text. This can include usernames, emails, IM's, and sometimes even passwords and

sensitive information. When you set up a tunnel securely, you are connecting to a secure, encrypted connection to the machine you are connecting to, helping to prevent the use of packetsniffers to steal your information.

Not only is this useful for keeping your local connection to the internet secure, it is also one of the basic ways you can hide which IP address you are connecting to the internet from at home. When using the tunnel for your transmissions, all of your packets will have that machine's IP address on the source address section instead of your own. Again, as covered above, you cannot trust a VPN (SSH) provided at no cost. It is in your best interests to use a paid hosting provider.

2.OPENVPN GNU/LINUX HOWTO (what if they don't have linux) list alternatives for vpn/ instructions for other os's?)

Information on how to set up a GNU/Linux system to use open VPN can be found here: http://openvpn.net/howto.html (openvpn only secures you between your server and you, not between your server and the internet. your server will be the middle man and is identifieable unless augmented with additional obfuscation techniques)

3. USING SOCKS4/5 PROXIES WITH FIREFOX

If you're interested in using SOCKS 4/5 proxies with the Firefox browser, you can find instructions here:http://uniqueinternetservices.com/configure-proxy-for-firefox html

4. CHANGING LOCAL DNS SERVICES

This section explains how to change the nameserver that resolves domain names into IP adresses that is sometimes used as an ideal way to trace you by your ISP, even if the data you used is encrypted via RSA or a strong triple des encryption the request to the domain name to an ip still is carried out by someone, make sure it's you, or someone friendly.

DNS requests in an ideal situation should be encrypted, if you're super paranoid, and some proxies offer this. I can't list which ones off the top of my head, sorry.

http://dnscurve.org/in-benefits.html ?

5. CHANGING WINDOWS HOSTNAMES PERMANENTLY

This hackers trick is a good way to associate a permanent IP mirror for your favourite social networking site like facebook, twitter, etc etc. If this is something you're interested in, more information can be found here: http://www.ehow.com/how_5225562_edit-windows-hosts-file.html

If you want cannabis.com to goto 4.2.2.1 then you can enter it just like the

localhost 127.0.0.1 entry you'll find in your windows setup. This bypasses nameserver requests to most browsers (check to be sure with a packet sniffer)

6. MISC PACKET CAPTURE SECTION

All of these need PCap drivers installed and are included in the downloads of each…

Understanding packets takes time and practice. To get started install a copy of wireshark (http://www.wireshark.org/); or MS Network Monitor 3.4, both are free. If you don't see any capture interfaces listed then you may need to run it as administrator. To identify which interface is seeing your traffic click the first (top-left) icon „list available interfaces" and look for the one with the numbers counting up; it's the active one. Start it and watch all the packets flow. You might see lots of traffic, start closing shit that's downloading or streaming stuff. You'll get down to a slower scroll of ARP and NetBios traffic, the occasional UPNP burst and other stuff. If you're on a secure VPN or something you'll see just about ALL SSL/TLS grey

colored packets or all UDP blue packets in some cases. Try another active interface (like a TAP interface) to see the goods. Get on your home network and play around; see what DHCP handshakes look like, DNS requests/responses, navigate a shared folder and see what it shows you, stuff like that. If you know how, do an nmap scan and see how obvious and loud it is and learn techniques to use it in a more covert manner.

http://www.wireshark.org/docs/ <- read and watch the videos. There's a lot to it but once you catch on it's quite simple to grasp.

TCPDump(linux)/WinDump(windows) – Command line packet capture for gathering to analyze later. http://www.tcpdump.org/ andhttp://www.winpcap.org/windump/

NetworkMiner (http://networkminer.sourceforge.net/) is an alternative that allows you to sort collected packets however you want (by host for example) for easy digging around.

7. TCP/IP AND THE WIDER INTERNET

(DNS/HTTP Port 80/Logging/Secure ways to connect to your 'crack' machine).. PROXY CHAINING, SSH CLI Chaining maybe?

- Change DNS Settings in Windows XP

http://www.mediacollege.com/computer/network/dns.html

Network Layers & OSI Model

In order for a security expert to truly understand a software or hardwares running on a network or security system, they must be able to relate to and fully conceive the implications of changes that are made to an existing setup.

No matter what you do at any level of the network layer, you will be interacting at other levels also. E.g. The data link layer (Layer 2 OSI) must make use of the physical layer (Layer 1 OSI), and so on.

Layer 1 : Physical layer

This is the electrical and physical specification of the devices. In particular it will refer to pins, voltages, repeaters, hubs, network adapters, host bus adapters and SANs (Storage Area NEtworks). Standards such as the RS-232C Com port standard popularised in the 90′s uses such physical wires to access medium.

One such popular medium would be the internet. To which the early modems connected.

Layer 2 : Data Link Layer

The Data Link Layer provides functional and procedural means to transfer data between network entities using physical layers (or cabling/adapters/routers/repeaters) so on and so forth. Originally Layer 2 was intended for point 2 point transfer only. LAN and multi-broadcast media (multicast et al) were developed independant of the ISO standard (IEEE 802).

WAN and LAN are services on the data link layer that arrange bits, from physical layer into logical fram sequences.

These frames contain important information that is relative to your Transmission Control Protocol, and includes information such as your IP (Internet Protocol) address.

This address is binded through service levels by the TCP (Transmission Control Protocol) transport layer.

8. Hack in a sack:

The Metasploit Framework

Metasploit is a software suite created for penetration testing, and is included in both Backtrack and Gnacktrack LiveCDs listed in the mobile solutions section. It has a command line interface, a GUI interface, and a Web interface, creating what is, in a real way, the world's first point-and-click hacking software. It has a massive, constantly updated Database of usable exploits, which you can use to gain access to vulnerable remote systems. http://www metasploit.com/

Sign off

Thanks for reading this whole doc, you did right? Please ask questions in #OpNewblood (Again, you can reach us via your web browser athttp://goo.gl/8zxwO) and refer back to this document and remember to stay safe. Protecting your anonmity is the most important part of being Anonymous.

In our world a good defense is the best offense.