IT ARMY OF UKRAINE

https://t.me/itarmyofukraine2022
itarmyua@gmail.com

DISCLAIMER : This manual is strictly for educational purposes only. Please be aware that attacking (port scanning, DDOS, probing, PEN, etc) is highly illegal in many countries and if caught, you may be looking a prison time. Although I believe that the secret services of many countries will not pursue any contesters actively due to the extraordinary circumstances, they have every right to do so. It's YOU that is doing something illegal. Give yourself a few minutes to think it through before you decide to participate!

Okay, so you thought it through … excellent. Oh, one more thing .. No one in our groups is responsible if you get caught and you'll spend a few years picking up your soap for a bloke called bubba. Also, most of us don't have the time to teach someone how to operate an operating system or install a program, so we assume that you know a thing or two about Linux/*nix OS. If you insist on using Windows, there will be a separate entry for that soon. This tutorial is not about reinventing the wheel. If you click on links, there will be explained of how to install stuff. For the sake of speed, this is not included in this manual.

If you have a good addition to this document, please don't hesitate to DM the group admin. He/she will make sure the the information is added to the next document version.

Step 1 : Operating system

1.1 TAILS OS

Pick your OS, preferably a System V (POSIX complaint OS). I suggest you install Tails, which is Debian based, for a number of reasons. First, it will hide your identity better than other OS and it will run off a USB stick. That means you can use your windows box to run it.

https://tails.boum.org/

Techrepublic also wrote a good article about TAILS, I suggest you read that, too :

https://www.techrepublic.com/article/getting-started-with-tails-the-encrypted-leave-no-trace-operating-system/

1.2 : ParrotOS

Parrot is a worldwide community of developers and security specialists that work together to build a shared framework of tools to make their job easier, standardized and more reliable and secure. Parrot OS, the flagship product of Parrot Security is a GNU/Linux distribution based on Debian and designed with Security and Privacy in mind. It includes a full portable laboratory for all kinds of cyber security operations, from pentesting to digital forensics and reverse engineering, but it also includes everything needed to develop your own software or keep your data secure.

https://parrotsec.org/

Step 2: Conseal your Identity

Get yourself a good VPN service. A VPN hides your public IP address by substituting it for the public IP address of the VPN termination host or its internet breakout. So in case of an investigation your public IP will not show. Here's a list of VPN providers. Some of them are paid and others come with a free trial:

https://www.top10vpn.com/top10/free-trials/?v=header&bsid=c15ense1kw287&gclid=EAIaIQobChMIs8i9ouii9gIVnIODBx07PgGMEAAYAiAAEgJkkfD_BwE IT Army of Ukraine

2.1 : Parrot OS and VPN:

If you're using ParrotOS, you may not need a VPN. (see STEP 2).

https://www.youtube.com/watch?v=6ICeYQvNmJ0&t=890s

If you use this, you do not need a VPN. Go to *Privacy* in the menu then *AnonSurf* and then start now. You're done, now you're using *the onion router*. And the advantage is that you can also use this as a Dos option.

2.2 : Install anon-surf on Kali :

https://cybernationalsecurity.net/how-to-install-anon-surf-on-kali-linux-step-by-step/

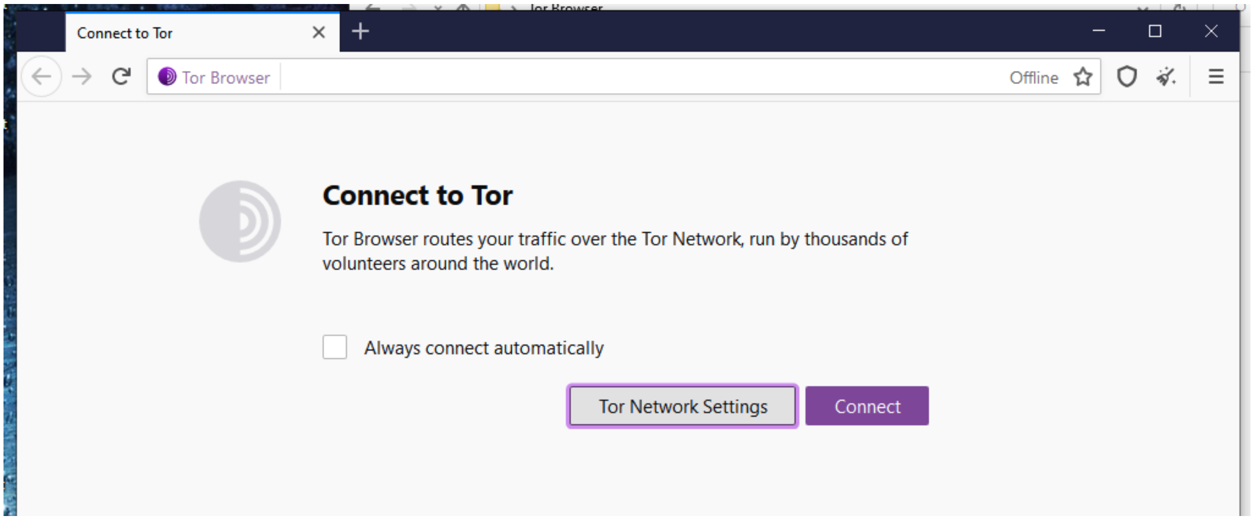
If you know any other good free VPN services, please DM the group admin and he/she will make sure the information is dispatched in the next version of this document.

Please be aware that 99% of VPN services sell information to third parties. A few good free VPN providers are :

- TunnelBear
- PureVPN
- Proton VPN
- Express VPN (12$)
-

Step 3 : Get TOR Browser

If you're thinking about using HTTP based (DDOS) attacks, get yourself the TOR browser. TOR stands for "The Onion Routing" which, as the name suggests, uses different layers and hops of routing in order to obscure the traceability of your terminal and let you remain anonymous.



Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

□ Always connect automatically

TOR can be found here : https://www.torproject.org/

Opera Browser has a built-in VPN option :

https://blogs.opera.com/news/2016/09/how-to-set-up-a-vpn-mac-windows-linux/

NEVER EVER attack a target without proper concealment of your identity. You WILL go to jail otherwise.

3.1 Whonix

We got some questions from MAC users if they could participate as well. Of course you can !!! Install Whonix in a Virtual Box on your MAC and then harden it. Whonix utilizes TOR, which provides an open and distributed relay network to defend against network surveillance. However, you will need to configure it though. It does provide some security out of the box but you will need additional configuration to harden it. So after you've installed Whonix and fired it up , please visit :

https://www.whonix.org/wiki/System_Hardening_Checklist

Step 4 : Attack (Test) Programs

Get yourself a good attack (DDOS) program. On the sites themselves are examples on how to use them. If you have to bypass Cloudfare UAN anti-DDOS, you could use :

https://github.com/yottaiq/CloudAttack

Here are a few others (non Cloudfare) :

https://github.com/gkbrk/slowloris
https://github.com/codesenberg/bombardier/releases/tag/v1.2.5

(example use : Example usage - ./bombardier-linux-amd64 --duration=240h --connections=1000 --latencies https://lenta.ru)

It maybe wise to run your query in a docker :

https://github.com/nitupkcuf/runner

[More information required]

GEEK INFO :

Here's a cool neat ARP Spoofing article, also known as ARP Poisoning actually used for Man in the Middle (MitM) attacks. This can be very effective if you happen to know the IP addresses of routers along the way.

https://medium.com/geekculture/simple-but-powerful-denial-of-service-dos-attack-8c7dfd60045f

Step 5 (optional): SOCKS Proxy

If you're really paranoid you can also run your network connection through several proxy (socks) services but this is not strictly necessary. Here's a list of free proxy services (servers) :

https://spys.one/en/socks-proxy-list/

GEEK INFO :

SOCKS is an Internet protocol that exchanges network packets between a client and server through a proxy server. SOCKS5 optionally provides authentication so only authorized users may access a server. Practically, a SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded.

SOCKS performs at Layer 5 of the OSI model (the session layer, an intermediate layer between the presentation layer and the transport layer). A SOCKS server accepts incoming client connection on TCP port 1080, as defined in RFC 1928.

Step 6 (optional): NMAP Port Scanner

If you want to scan ports of a remote host, you can install the tool *nmap* :

https://nmap.org/

Please read the manual carefully. NMAP is a very powerful tool with many options to discover open ports. A good site to learn quickly is :

https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

For the WINDOWS users among us, there is a GUI for *nmap*, called *zenmap* :

https://nmap.org/zenmap/

It does the same thing except it comes with a nice user-friendly GUI (Graphical User interface).

TIPS and tricks :

TIP 1: NMAP

For anyone who has access to nmap already, nmap is pre-installed in Kali and ParrotOS.
Check if you have this script by running this in the terminal "locate http-slowloris.nse"
if you see this:

```
/usr/share/nmap/scripts/http-slowloris.nse
```

You can then use it on any desired IP.

```
nmap -vv --script http-slowloris --max-parallelism 400 <target IP>
```

TIP 2: DNS

We also recommend changing your DNS to 9.9.9.9. This is an open DNS recursive service for free security and high privacy since your local DNS service may not always give you what you need in terms of reliability.

https://www.windowscentral.com/how-change-your-pcs-dns-settings-windows-10

Another thing that will greatly improve your security is DNS over HTTPS.

TIP 3: Randomized MAC addresses

There's two controls for using random hardware addresses—one is for all Wi-Fi networks and the other is for the specific Wi-Fi network you choose. When you turn it on for all networks, random hardware addresses are used while your PC scans for networks and connects to any network. When it's turned on for a specific network you choose, random hardware addresses are used the next time you connect to that network.

https://support.microsoft.com/en-us/windows/how-to-use-random-hardware-addresses-in-windows-ac58de34-35fc-31ff-c650-823fc48eb1bc#:~:text=a%20specific%20network%3A-,Select%20the%20Start%20button%2C%20then%20select%20Settings%20%3E%20Network%20%26%20Internet,hardware%20addresses%20for%20this%20network

GEEK INFO :

Some of the information (webbrowsers) in this article was taken from the following article :

https://hackmd.io/pl_ucHTWQUmO9ubmzRT1tQ

Please check it out. It has a lot of additional information. Credit where credit due.

So please always remember this order :

- **Install OS**
- **Hide identity !!**
- **Attack (test)**