

Forum:[Hack Forums](#)

Thread: [\[TuT\]Operation Security & Anonymity](#)

bleepsheep - October 10, 2021, 5:19 am

Taken from my website here: <https://hackguru.tech/>

Operation Security & Anonymity

There are many ways an individual can obfuscate his or her IP address/internet connection to avoid or impede detection. However, one must consider that there are prying eyes of various degree. You have your typical ethical hackers protecting a network, you also have nation-state spying, there is ISP spying, black hat spying, program tracking, and other hazards. In this paper I will give you a good blueprint that you can add to as your level of Operation Security skill/need develops.

Public Wifi:

Simply spoof your MAC address and connect to a public access point and you are anonymous. That does not mean you are off camera though.

VPN (Virtual Private Network):

It is good practice to stack these by using one solid one such as [censored] or ProtonVPN on your main OS. This encrypts our data and prevents ISP spying. This can also encrypt our connection when on public wifi networks. Yet, if a malicious attacker were to employ one of these methods for say a banking trojan he may get tracked down by authorities and do some serious prison time.

Virtual Machines:

Virtual Box allows us to stack a second vpn inside of our Virtual Machine this is a useful trick that can enable low level malicious attackers a better alternative. Typically in small operations the budget of an anti-criminal organization may not be large enough to de-obfuscate a two nested VPNs, but from a VPN provider standpoint your logs could jeopardize business. This is why it is important to choose a good VPN provider. Do your own research. It is not my responsibility what you do with this information.

Proxies:

If you really want to obfuscate your connection further (with less focus on speed that is)it is recommended to run proxy chains inside each machine that is already equipped with VPNs. There are places online you can purchase bulk proxies to connect through. Just give it a solid google

search and compare rates. Proxychains is a linux command line tool that helps make absolute anonymity possible.

Tor:

Finally you can connect to the Tor network via command line or browser. It is good we have a serious anonymity setup by now because anything could be lurking on Tor. The whonix operating system can help with the setup of this if you are confused. One could run a whonix VM instead.

Whonix:

This operating system focuses on anonymity and security and channels all information through Tor.

Qubes:

Out of the box qubes is almost a perfect OS for this kind of operating system setup, but it is absolutely not necessary. It comes with whonix preinstalled and allows for easy stacking of VMs(including a firewall) that can each have an effect on your connection. It is highly recommended to read the Qubes documentation for achieving highly advanced anonymity setups.