Learning Hacking? First learn how to hide...

Enhance your Anonymity Online with Tor, Proxychains & MacChanger!

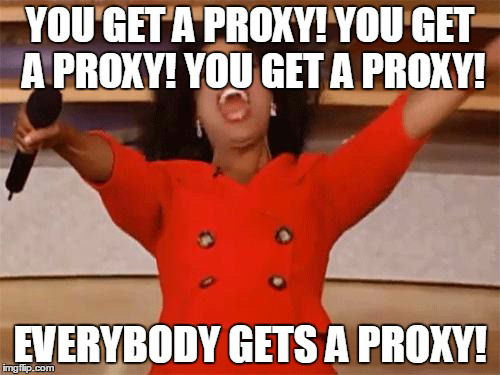
**Disclaimer**: All the information and scenarios presented below are for educational purpose only.

One of the best way to learn ethical hacking is by using **Kali Linux**, an advanced OS aimed at Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Kali Linux is a multi platform solution, accessible and freely available to information security professionals and hobbyists. The best thing? It’s open-source and completely free of charge, so you can get it right now. For the purpose of this tutorial, we will be using a VM (virtual machine) initialised with Kali. If you want to follow along, here is a great [link](https://www.youtube.com/watch?v=wX75Z-4MEoM) to get you started with setting up and configuring VMs.

So you want to hack... ethically, of course. You fire up your machine and start getting reckon on your mum’s laptop, because you really want that secret family recipe. You manage to get into her computer and find what you were looking for. Yey! But do you know what you just did? You may have learned a few things from your mom’s laptop, but she also learned a few things about you. All the scanning you just used, her system flaged it; her firewall saw what you were doing and blocked you. And worse, she knows it was you... not because of her 6th sense, but because of your IP address and she will send you to jail to get revenge („no one messes with grandma’s lasagna!”). So, hiding yourself is very important if you want to learn how to hack. This is a quick setup if you want to become anonymous in the virtual world.

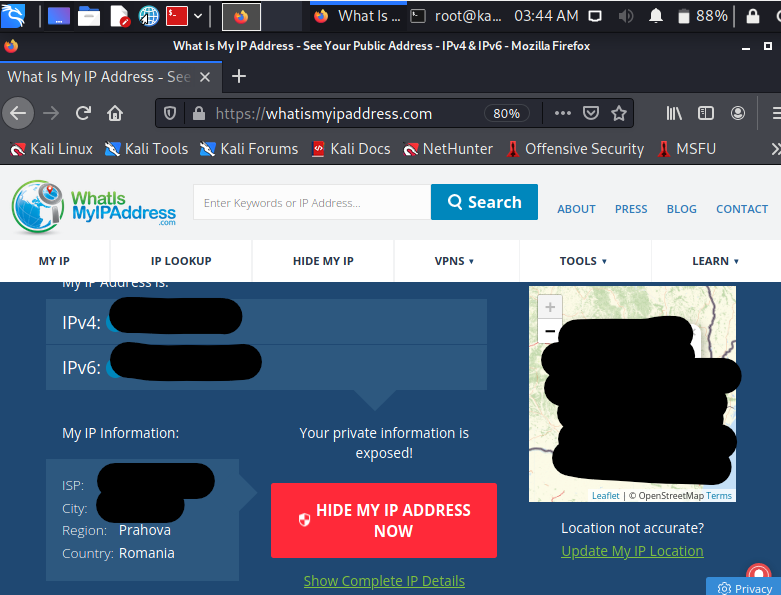
1. ***ProxyChains***:

To understand what a proxy is, we need to know what happens when we request a server for some web page. The request is sent from our system to the server. The server will then processes that request and respond with the data that we asked for and then, this response is sent back to our computer. But when we make that request, the server learns a lot of information about us, such as our IP address. And we don’t want that, so we use a proxy.

A proxy allows us to access information from a source and prevents that source from gaining intel about us. And when I say intel, I mean: IP addresses, contacts or even sites that we frequently visit. To do this the proxy acts as a third-party client that receives our browser requests and redirects them to the target server. The target server sends back the response to the proxy and the proxy will send it back to us.

When we use Proxychain, instead of only one proxy server, our request gets redirected through multiple proxy servers, as the name suggests. This makes tracing back the IP very difficult.

Other benefits of proxies, without mentioning the enhancement in security, in which they act like a firewall between your systems and the internet, include: using them to gain access to location-specific content or preventing access from browsing inappropriate or distracting sites, just to name a few.

In Kali Linux, ProxyChains should be preinstalled. As I said previously, ProxyChains is a tool that forces any TCP connection made by any given application to go through proxies like TOR or any other SOCKS4, SOCKS5 or HTTP proxies. Essentially, you can use ProxyChains to run any program through a proxy server. This will allow you to access the Internet from behind a restrictive firewall, hide your IP address, run applications like SSH/ telnet/wget/FTP and Nmap through proxy servers, and even access your local Intranet from outside through an external proxy.

Let’s first check our location:

If you want my address, DM me 😏. As you can see, I am located in Romania. And now, let’s hide!

To configure proxies: *sudo nano /etc/proxychains.conf*.

We can choose between 3 types of proxychains:

• *Strict Chain*: where all proxies in the list will be used and they will be chained in order.

• *Dynamic Chain*: are the same as a strict chain, but dead proxies will be excluded.

• *Random Chain*: meaning, each connection made through ProxyChains will be done via a random combo of proxies in the proxy list and users have the option to specify the number of proxies to use.

Uncomment *dynamic\_chain* and comment *strict\_chain* and then scroll at the bottom of the page. As you can see, the default is set to tor, but, for now, we will comment this line and we will add our own proxies. To find some free proxies, check this [link](https://hidemy.name/en/proxy-list/?country=US&type=5#list). Of course, paid proxies work better, are faster and more secure, but we are poor so... beggers can’t be choosers.

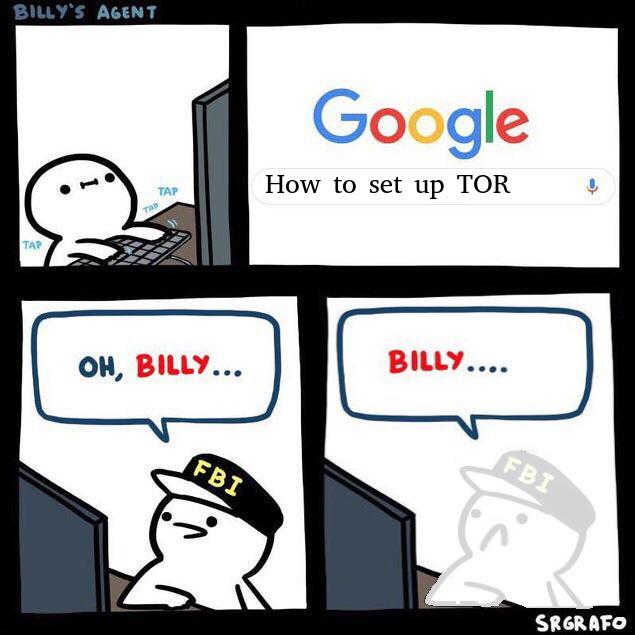
 

If we look at our IP address now, we will see that we are in the country of the proxy that we chose.

If we come back to the configuration file, we can notice that we are allowed to use only http, socks4 and socks5. The last 2 are very similar protocols to the http one, in the sense that, although we hide the origin of the request, we do not hide its content. If you want to know more about SOCKS4 vs SOCKS5, follow this [link](https://securityintelligence.com/posts/socks-proxy-primer-what-is-socks5-and-why-should-you-use-it/).

So, to conclude, proxyes will not encrypt your traffic, allowing leaks of information between your computer and the server. So they are useful only if you wish to browse the internet and nothing more. To make up for this shortcoming, we will be using TOR.

1. ***TOR***:

TOR stands for The Onion Router. The core principle of Tor is onion routing which is a technique for anonymous & secure communication over a public network. In onion routing, messages are encapsulated in several layers of encryption, just like an onion has several layers. Let’s dive in a little deeper to better understand what’s going on.

Tor works by bouncing connections from your computer to destinations through a series of intermediate nodes, also called relays. By default, Tor bounces connections through 3 relays. Each of these have a specific role to play:

• *Entry/Guard Relay* - This is the entry point to the Tor network. Relays are selected to serve as guard relays after being around for a while, as well as having shown to be stable and having high bandwidth.

• *Middle Relay* – Middle relays are exactly that - middle nodes used to transport traffic from the guard relay to the exit relay. This prevents the guard and exit relay from knowing each other.

• *Exit Relay* – These relays are the exit point at the edge of the Tor network. They send traffic to the final destination intended by the client.

How can we be sure relays won’t track who we’re connecting to and sniff the data we send across the wire? The short answer is: we don’t have to! Tor is designed to put as little trust in relays as possible.

First, each node in the path knows only its predecessor and successor, but no other relays in the circuit. The original author remains anonymous, unless you’re the first node in the path. No one knows what data is being sent until it reaches the last node in the path; who knows the data but doesn’t know who sent it. This has led to attacks whereby large organisations with expansive resources create Tor servers which aim to be the first and last onion routers in a path. If the organisation can do this, they get to know who sent the data and what data was sent, effectively breaking Tor. Also, each packet flows down the network in fixed-size cells. These cells have to be the same size so none of the data going through the Tor network looks suspiciously big.

Secondly, TOR uses encryption, specifically AES and the key is agreed using Diffie-Hellman. So what’s the deal with all the references to onions? To answer this question, let’s take a look at how the encryption works when a client makes a connection through the Tor network. Considering that we tipically have 3 nodes in our circuit, then:

1. The client encrypts the original data in such a way that only the exit relay can decrypt it.

2. This encrypted data is then encrypted again in such a way that only the middle relay can decrypt it.

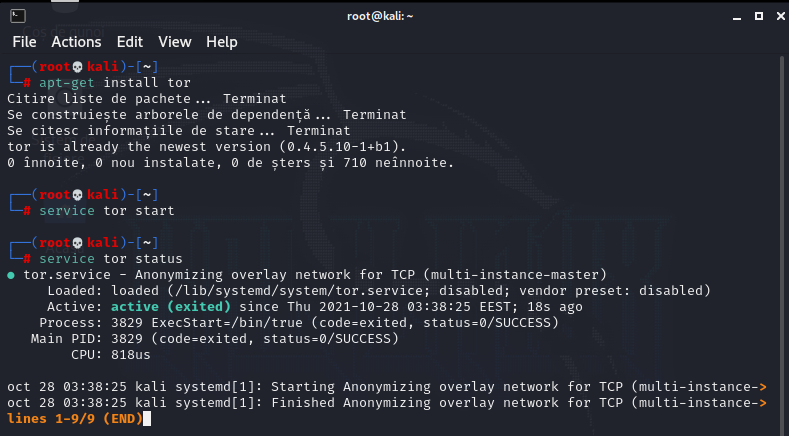
3. Finally, this encrypted data is encrypted once more in such a way that only the guard relay can decrypt it.

It’s important to note that exit relays can see the original data sent by the client, since they have to pass it to the destination. This means that, if credentials are passed over HTTP or other cleartext protocols, the exit relays can sniff the traffic!

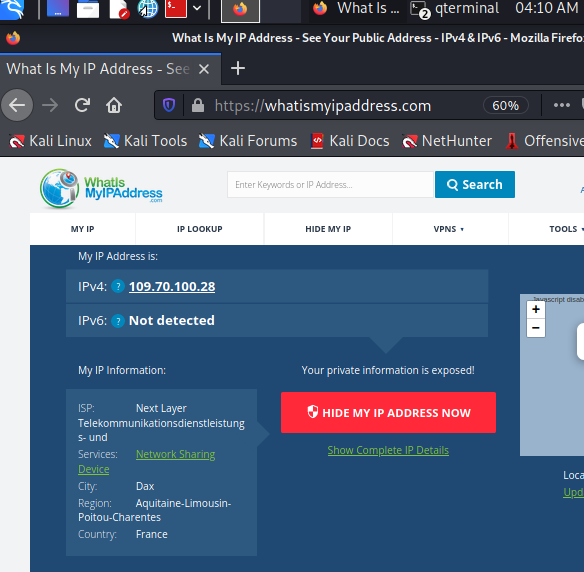
In Kali Linux, you have 2 options: either you install tor browser, or configure the proxychains service to use tor, as tor should be already preinstalled in your machine. And if you don’t want the server that you are trying to reach to know that you are using an exit relay, you can add some more proxies at the end of the file.

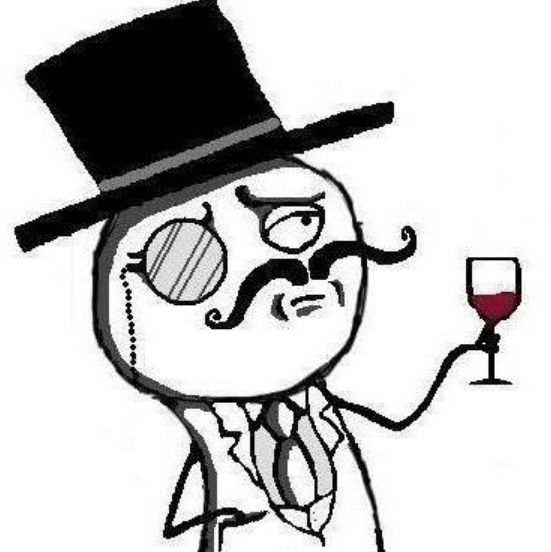
To start the tor network: *service tor start*. (*stop* – for closing)

To make sure it’s running: *service tor status*.



Using the command *proxychains firefox whatismyipaddress.com*, we can notice that our IP has been changed:



And just like that, we are now in France .

We’ve talked about how to hide your IP address. But is hiding the IP address enough? Not at all! The next level of Anonymity can be achieved by changing the MAC address.

1. ***MacChanger***:

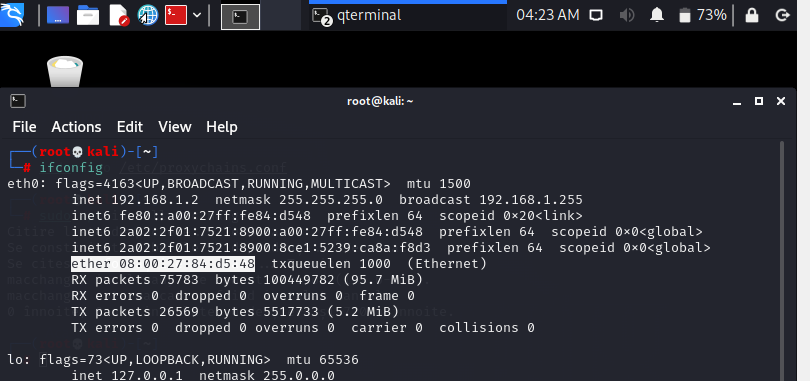
Each network interface card (NIC) has it’s own unique hardware address (MAC). The first half of a MAC is the Organisational Unique Identifier (OUI) (“manufacturer”) and the second half is the Network Interface Specific Identifier. Every device has a unique MAC address assigned to it by the manufacturer. This MAC address is stored in the router’s table when you are connected to it. Because the MAC address is unique to every device, it can be used to identify the system/device that was used by the hacker, which might result in revealing your identity.

Hopefully you will at least know the basics of networking but a MAC is only used at layer-2. It does not leave your Local Area Network (LAN) and can’t be seen when you are routing externally.

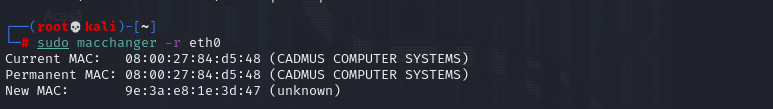
There may be limited cases where you need to change your MAC (especially in a virtual machine) but it is still useful to know how to do it. An example I can think of is if there is some sort of layer-2 filtering only allowing connectivity from a specific vendor or MAC. If you know what MAC address(es) are allowed you can set yours accordingly.

MacChanger is a tool that will change the MAC address of a device to a fake MAC address until the device is rebooted.

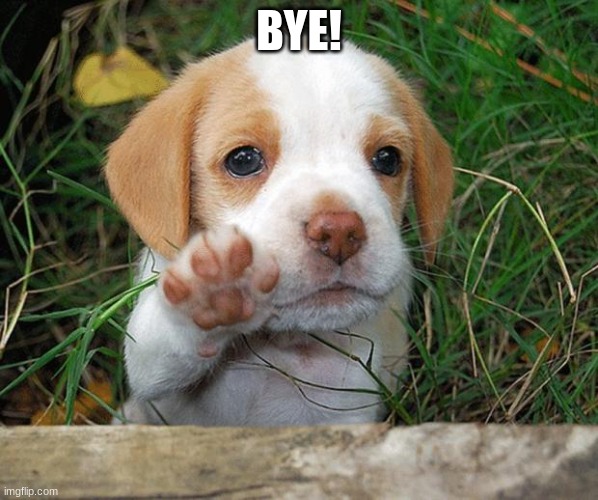
To find out your MAC address: *ifconfig*. (Or, you can use *sudo macchanger -s eth0*)



To change it: *sudo macchanger -r eth0*.



Yeyyy! You have learned 3 ways to maintain your anonymity. There are many such tools hackers use to keep themselves anonymous, such as [anonsurf](https://linuxhint.com/anonsurf/), for example (I attached a tutorial). I suggest you research more on how else you can increase your anonymity. Thank you for reading and stay safe!



***Resources (Why are you still here? 😊):***

1. [Proxychains, Anonsurf & MacChanger](https://medium.com/edureka/proxychains-anonsurf-macchanger-ethical-hacking-53fe663b734)
2. [Mastering Kali Linux for Advanced Penetration Testing, Vijay Kumar Velu and Robert Beggs](https://books.google.ro/books?id=kQGGDwAAQBAJ&pg=PA83&lpg=PA83&dq=what+is+the+difference+between+tor+service+and+bundle+in+kali+linux&source=bl&ots=N0tKC286yd&sig=ACfU3U1ZYaMyq4WacNqM8onZd_a4GTFm3Q&hl=ro&sa=X&ved=2ahUKEwjsyZrWg_jzAhUGvosKHUSiCbwQ6AF6BAgREAM#v=onepage&q=what%20is%20the%20difference%20between%20tor%20service%20and%20bundle%20in%20kali%20linux&f=false)
3. [What is Tor and how does it work?](https://cybernews.com/privacy/what-is-tor-and-how-does-it-work/)
4. [How does Tor \*really\* work?](https://hackernoon.com/how-does-tor-really-work-c3242844e11f)
5. [How Does Tor Really Work? The Definitive Visual Guide (2020)](https://skerritt.blog/how-does-tor-really-work/)
6. [Penetration testing: TOR, VPN or proxy](https://resources.infosecinstitute.com/topic/penetration-testing-tor-vpn-or-proxy/)
7. [Proxies Vs. VPNs Vs. Tor Browser](https://www.linuxandubuntu.com/home/proxies-vs-vpns-vs-tor-browser)
8. [Tor vs VPN vs Proxy: Which Should I Use To Secure My Internet?](https://www.vpn.com/guide/tor-vpn-proxy/)
9. [Hide TOR Exit Node](https://medium.com/@nima.nikjoo/hide-tor-exit-node-38d7dc4cd7ab)
10. [How to Protect Yourself from Malicious Tor Exit Nodes](https://www.maketecheasier.com/protect-yourself-from-malicious-tor-exit-nodes/)