

Forum:[Hack Forums](#)

Thread: [Anti-Forensics Guide - Networking](#)

Arbitrage - January 12, 2013, 2:37 pm

Anti-Forensics Guide (Networking)

Anti-Computer forensics is a set of techniques used as counter measures against computer forensics. Reading this guide will certify you with knowledge that will carry you milestones into staying anonymous and out of jail.

This Guide is centered around the Networking part of Anti-Computer forensics. This guide provides an in-depth overview, explanations and tips on how to implement anti-forensic techniques to secure yourself and cover your traces while online.

Networking

Networking is a fundamental part of computers, and covering your traces over networks, is a critical part into staying anonymous. Most of your daily lives revolve around the internet and the use of computers, and you'd be lying if you mention otherwise. As a hacker, regardless of hat, it's only without question, that you would want to make yourself anonymous while on the internet. And thanks to the work of programmers, there are many solutions to masking yourself while in the cloud.

Basic Terminology

Network - A way for computers to communicate with one another. The internet is a type of network, but it is not the only one.

TCP/IP - TCP stands for Transmission Control Protocol and IP stands for Internet Protocol. The TCP/IP protocols are the protocols used to send data across the internet.

IP address - This is the address that your router uses to connect with everyone else on the internet. There are currently two standards of the IP address (IPv4 and IPv6). Whenever you visit a website, they instantly have access to your IP address. Your IP address can give off information such as your location or ISP so treat it like your actual address, and be mindful of what websites you visit. To view your IP address, visit whatismyipaddress.com.

DHCP - DHCP also known as Dynamic Host Configuration Protocol, is the protocol that automatically assigns your computer an IP address that can be used to connect to the internet. If you disable DHCP, then you will have to manually configure your IP address.

Default Gateway - This is the address that allows your router to access other networks.

What are Proxies?

A proxy is simply a way to protect mask your IP address when browsing websites. As you already know, your IP address gives off vital information about you when you browse websites. With a proxy, those websites will no longer gain that vital information about you.

Web based proxies are proxies that you use inside of your web browser. Using a web based proxy will hide your IP address from web servers and will make you a bit more anonymous over the web. Although, using a web proxy does not make you completely anonymous. Therefore, you do not use a proxy for hacking. Instead a proxy can for things like gaining access to blocked websites on an enterprise network.

You can find web based proxies in the below links:

<http://www.proxynova.com/web-proxy-list/>
<http://www.azproxies.com/>
<http://anonymouse.org/anonwww.html>

You can also configure a proxy through your web browser if you have the IP address of a proxy server.

There is also Tor which is a download that comes with it's own browser and can be used to hide your identity from websites. You can put it on your flash drive and use Tor as a proxy anywhere you go. (<https://www.torproject.org/>)

Furthermore, if you want to use a web proxy that does not keep any logs, than make your own one! (<http://www.glype.com/>)

There are many other ways to get your own proxy, just find a free web host to upload the files.

Using your own web proxy behind a VPN (next chapter) is a good way to stay anonymous over the internet as just using a proxy only keeps you anonymous from web servers and not your ISP (Internet Service Provider).

What are VPNs?

VPN stands for Virtual Private Network. This is when your computer connects to another network virtually that could be thousands of miles away from your current location. Doing so protects your IP address while browsing the internet from both web servers and your ISP. A proxy does not protect your web traffic from your ISP, thus, there is an advantage to using a VPN. As mentioned earlier, using a VPN along with your own proxy is a good way to better secure yourself while browsing the web.

Although, in reality, being completely anonymous with a VPN comes with a price. Yes, there are free VPNs, but those VPNs keep logs of your web traffic. So if you want to completely stay anonymous while browsing the internet, you must pay for a VPN from a VPN provider. Below I will only be listing free VPNs, as I can not vouch for any paid VPNs.

- SecurityKISS
- Spotflux
- Hotspot Shield
- Keplar
- OpenVPN
- ProXPN

And don't be discouraged if you cannot pay for a VPN, using a free VPN is better than nothing and being out in the open to your ISP. Even if you're a beginner at hacking, maybe one day, you'll be great. When that day comes, you don't want your ISP to have logs of you spending 24 hours a day learning over a hack forum. That can be used against you if you ever get into any trouble.

I cannot stress over how important it is for a hacker to use a VPN, even if you don't do anything bad. Your ISP keeps internet traffic logs from the second you connected to your network! If you ever do something bad, your ISP can give all of those logs to court to be used against you! So if you aren't already using a VPN (not Tor), than do so now!

When downloading hacking tools/program, never download them on a home, work or school network, especially not without a VPN! And when downloading Torrents, be sure to use a VPN or a

method for anonymous Torrent downloads. Taking these measures helps hide your hacking persona from your ISP. ISPs see what websites you visit and what you download.

Your Identity

Now that you know how to hide your web traffic from your ISP while in the cloud, you must also know how to maintain your online identities.

Firstly, always THINK before you DO something over the internet. As a hacker, you want to separate your internet usage into three main sections.

1. Hacking persona (your hack forums identity)
2. Online persona (your identity on forums, and stuff not hacking related but not personal either)
3. Social life (if you have one)

I will tell you how to keep each of your three persona's separate and the risks of not doing so!

Hacking persona

It is important to keep your hacking persona separate from your online persona and your social life. Always use a VPN/proxy when doing your "dirty hacking business". And never use the same email address that you use in your online persona or social life. Not only should you never use the same email address, but you should also never use the same username, avatar, signature, and never link to any profiles in those persona's. You should never tell anyone anything about you in your hackers identity, and there should be no similarities in your hacker identity as in any of your other persona's. Pretend to be someone who you are not. The goal is to remain anonymous.

Online persona

This is your persona that is separate from your Hacking persona and your social life. Regardless of why you've chosen to separate yourself on these communities from your hacking and social lives, it is important to keep them separate. In online persona's, avoid using the same email address/usernames for everything, and avoid giving actual information about yourself such as your age, location, etc. Doing so helps you from being traced as your image on every community is different and not under the same name. Also be sure to never tell people that you are a hacker, you never know what might happen if you do! You may lose trust, you may get banned, or you may be talking to a FBI agent!

Social life

If you are apart of a social networking site on top of being a computer specialist, than you may want to reconsider having a social life over the internet. For starters, colleges and employers have access to your face book account per se, allowing them to see everything you've done since you made your account (all of your photos, friends, statuses). This is a true story, and they do not even need your password to obtain this information. But if you're someone who is not a member of a social networking site, you will not need to worry about this. Secondly, having a social networking site makes you less anonymous online. Your ISP can see your activity on that site, and keeps logs of it. Facebook (or whatever site you're using) has instant access to all of your activity, and your account. If you are ever a victim of a RAT or keylogger, your attacker will have access to all of your information. And not only that, but your friends have access to all of your photos and information about you! You never know when they might take your pictures and post them elsewhere online! Now then, there is nothing wrong with having a social life on the internet, but just be aware of all of the side effects in the long run to make healthier choices. And if you do have a social life online, keep it completely separate from your other lives. Use a specific browser, email address, etc, all for your social life and nothing else! And never talk about hacking!

Fake identity

Lastly, to stay anonymous online, create a fake identity! Get fake images, and everything! Whenever you meet someone personally over the internet, you will be two steps ahead, because everything that you telling them is fake! Your name, location, school, age, gender, fake it! There are millions of people in this world, people will never know the truth! Plus, making a fake identity for yourself can be fun!

Web Browsers

When browsing the internet, be sure to not save web history, or any web logs. You can save cookies, but be wary of tracking cookies as they are hard to get rid of. And be mindful of the sites you visit on each of your online persona's. When browsing the internet, act as if you are always being watched.

Here are two Firefox Addons to help with staying anonymous.

Multifox - Allows you to create an infinite number of Firefox profiles without having more than one Firefox installation!

ipFuck - Simulates the use of a series of proxies changing at each connection.

Summary

Staying anonymous over the internet involves being pro-active to prevent your ISP from logging activity, creating a fake identity, and taking counter measures when downloading or signing up for websites.

jamestien - January 14, 2013, 9:04 am

good information dear..

thanks for that..

Arbitrage - January 14, 2013, 11:56 am

(Jan 14, 2013 10:04 AM)jamestien Wrote: [\[CITE\]](#) good information dear..

thanks for that..

No problem, I'm glad that you enjoyed it.

Milky Way - January 14, 2013, 12:29 pm

Solid tutorial, I've already messed up quite a bit according to this

What about recovery? When you do slip up, what can you do? For instance, I've already joined hackforums with my primary email and I'm not behind any kind of proxy. I rarely am behind a proxy of any kind and I've downloaded a few tools while not connected through a vpn

Arbitrage - January 14, 2013, 12:53 pm

(Jan 14, 2013 01:29 PM)Milky Way Wrote: [\[CITE\]](#) Solid tutorial, I've already messed up quite a bit according to this

What about recovery? When you do slip up, what can you do? For instance, I've already joined hackforums with my primary email and I'm not behind any kind of proxy. I rarely am behind a proxy of any kind and I've downloaded a few tools while not connected through a vpn

Can't recover from what's been done because the ISP keeps internet traffic logs on all of it's customers. And you should assume that the logs will be there for many months.

As for a "proxy", at least use Tor to browse hack forums if you don't feel like getting a VPN. Neither Tor or a VPN keeps you completely safe, only paid VPNs do, but it's better than telling your ISP that

you're on a hack forum.

As for the hacking tools that you've downloaded, it's not a big deal as long as you don't get caught by the cops because you hacked some large website. It's rare for the police to show up at your door, but if you're doing something like using Dark Comet without protection and you have like 1000 slaves, you better be prepared. xD

ilea510 - January 14, 2013, 1:01 pm

quick read tnx (: got some new information out of it and tnx for putting the effort (:

Arbitrage - January 14, 2013, 1:06 pm

(Jan 14, 2013 02:01 PM)ilea510 Wrote: [\[CITE\]](#) quick read tnx (: got some new information out of it and tnx for putting the effort (:

No problem, glad you enjoyed it. ?

ebohackerdotcom - January 14, 2013, 1:15 pm

thanks bro for the tutorial
its really helpfull thanks

grizzlylol - January 14, 2013, 1:33 pm

Short sweet and to the point. I like it. Thanks

TheCl0wnhelper - January 15, 2013, 3:47 am

Thank you sir. Will be ing your thread.

Arbitrage - January 15, 2013, 6:38 am

No problem, be sure to recommend this thread to other people! <3

?Fear - January 15, 2013, 8:43 am

Nice tutorial, you should mention TOR next time though. TOR is safer than free VPN's. Free VPN's don't do shit. Most sites block the free VPN's IP because spammers use it.

Arbitrage - January 15, 2013, 9:15 am

(Jan 15, 2013 09:43 AM)Iridescence Wrote: [\[CITE\]](#) Nice tutorial, you should mention TOR next time though. TOR is safer than free VPN's. Free VPN's don't do shit. Most sites block the free VPN's IP because spammers use it.

There's a link to Tor in the Proxies section. :P

ninjaw95 - January 15, 2013, 11:29 pm

Thanks, this stuff is really nice to know.

ObeseViking - January 16, 2013, 2:32 am

although i already knew most of it i enjoyed reading it, it was really well written.

Thank you.

Keystrokes - January 16, 2013, 10:54 am

thanks for the tutorial it was very easy to understand!

Blazeingstorm - January 19, 2013, 5:18 am

Good brush up on some important topics.

Evanescence - January 19, 2013, 6:04 am

Good information you have explained the basics.

Arbitrage - January 19, 2013, 8:19 am

Glad that you guys like my tutorial! ;P

DEVIL X - January 21, 2013, 2:10 am

very nice guide, i read all of it two times... Fake identity option is cool...

Arbitrage - February 11, 2013, 12:44 pm

Updated the VPN portion of the OP. Glad you enjoyed it @above.

4RG0S - February 11, 2013, 1:37 pm

Nice Thread, thanks for sharing it :)

Arbitrage - February 11, 2013, 5:10 pm

(Feb 11, 2013 02:37 PM)4RG0S Wrote: [\[CITE\]](#) Nice Thread, thanks for sharing it :)

No problem, glad you enjoyed it! :3

teonanacalt - February 11, 2013, 5:27 pm

Very useful guide/information, thank a lot very nice tutorial.

Helpful contribution...appreciate.

daydreamer14002 - February 11, 2013, 9:27 pm

Nice tutorial and thanks, bt whenever i try to access hackforums with spotflux, hf doesnt let me access the site because i have some weird ip address. do i need to get a new ip with the VPN, or does hf just not allow access with VPNs?

What is this voodoo?

Arbitrage - February 12, 2013, 2:24 am

(Feb 11, 2013 10:27 PM)daydreamer14002 Wrote: [\[CITE\]](#) Nice tutorial and thanks, bt whenever i try to access hackforums with spotflux, hf doesnt let me access the site because i have some weird ip address. do i need to get a new ip with the VPN, or does hf just not allow access with VPNs?

What is this voodoo?

Hackforums blocks some IP addresses from VPN and proxies. You will have to find another VPN.

Voodoo means that something is bad.

sevenyears26 - February 18, 2013, 12:38 am

good read sir good read. thanks for the info

Arbitrage - February 18, 2013, 2:47 pm

(Feb 18, 2013 01:38 AM)sevenyears26 Wrote: [\[CITE\]](#) good read sir good read. thanks for the info

No problem, glad you liked the thread! :)