

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Asking the correct question about Anonymity](#)

cephregada - October 21, 2017, 2:15 am

It all comes down to who is trying to trace you

Multiple questions will surface when you are trying to stay anonymous on the internet, i will be going through techniques used to uncover the identity of an internet user.

1 - Tor is not a fool proof solution :

A - Even if you are using "Tor" service and the username you are using to browse forums on Tor is the same as other Social Media account like "Skype" for an example will uncover your identity even if your "IP" is anonymous.

B - Remember, "Tor" uses a browser and is based on Firefox and is prone to exploits like any other browser and an example is the JavaScript 0-Day that surfaced a year ago.

C - Be careful to what websites are asking for access because some plugins will try to pin point your location.

2 - VPNs are shit :

A - Don't ever believe whatever the "VPN" provider tells you because the law is much more powerful than any "Official VPN Service".

B - VPN Providers will not risk their "Profit Generator Company" for the sake of keeping your information private.

A small Scenario: Let's say there is a "Child Predator" investigation ongoing with the Police, and the law enforcement agency pin pointed an IP address of a VPN service. They would write a letter for that provider asking for Logs of a specific user. What will happen if the provider answers with "I don't keep any logs". I will tell you this, first they will be held responsible in assisting with a crime and they will be faced by charges, they don't wanna do that.

So never believe what you read about what the VPN will provide you.

3 - Pentesting through Proxies :

A - Sometimes not all attack vectors on "Kali" are routed through the Proxy you are using even if you are using Tor and "ProxyChains".

B - Never assume you are IP is hidden while initiating an attack on a service, my advise would be attack yourself first with the same attack vector you are trying to accomplish and check out the IPs that are attacking your service.

4 - Stay away from Mobile Phone Anonymity :

Don't rely on any firmware or software to keep you anonymous, mobile phones by default leak a lot

of information intentionally for "Advertisement" usage

As an example, by default your Android device will store all your "Browsing History" and location on your "Gmail"

5 - Who is tracing you :

A - If a user is tracing you, no matter how much advanced he/she is will use the known "tracing/doxing" techniques to get to your identity and won't be able to achieve this if you are using your "Logic" + any other VPN service (I would suggest TOR and no other).

B - If the Government is tracing you, the chances is that you did something illegal and in my humble opinion, nothing will assist you if that is the case. Remember 0-Days are there and they are called so because it is not known by the public, so never assume the "Software" or "OS" you are using are "Vulnerability-Free", just read a little bit on "WikiLeaks".

Remember, never do something illegal and expect to stay anonymous and get away with it, the most skilled hackers and the most notorious and underground forums got caught eventually, stay safe and act responsibly

h1tman - October 21, 2017, 4:54 am

It was very useful tnx ;)

Untraceable_Pro - October 23, 2017, 3:06 am

Now what if we use multi layer protection like

VPN -> TOR or TOR -> VPN

or something like that and hosting that VPN on a server situated in a country which have not so strong cyber laws ?

Will the user still be traced ? If so, how ?

Also, do you have any case studies of how hackers who used tor and VPNs got caught ?

DARK_PEPPINO - October 26, 2017, 12:30 pm

(Oct 23, 2017 03:06 AM)Untraceable_Pro Wrote: [\[CITE\]](#) Now what if we use multi layer protection like

VPN -> TOR or TOR -> VPN

or something like that and hosting that VPN on a server situated in a country which have not so strong cyber laws ?

Will the user still be traced ? If so, how ?

Also, do you have any case studies of how hackers who used tor and VPNs got caught ?

the connection would be really slow

Provexa - October 26, 2017, 3:38 pm

Quote:A - Sometimes not all attack vectors on "Kali" are routed through the Proxy you are using even if you are using Tor and "ProxyChains".

?

SleeplessXIII - October 27, 2017, 8:19 pm

Using public wifi to access whatever proxy you're using and making sure your mac is spoofed should be pretty safe though right? Especially if it's a crowded network and you stay of security camera footage, I'd imagine.

