

Forum:[Hack Forums](#)

Thread: [Working environment](#)

jasrrow - May 30, 2024, 2:25 pm

Hello there,

since last couple of months i started into cybersec research and learning.

The more information I have, the more I wonder: what is the safest environment to work in (and i do not mean pentest focused linux distros)

what i mean is how to stay possibly safe and untraceable:

is only VPN enough?

VPN + VM?

VPN + nested VM's + VPN?

VPN + RDP + VPN?

tor network based environment? (but its crazy internet works like DSL)

what would be your advises about this or what setup environment are you using?

Burger - May 30, 2024, 4:30 pm

You don't need a VM unless you are running malware and around sketchy shit all day.

I recommend if you really want to be safe have a good VPN or a Private VPN that you're hosting and also have some VPSs for Tunneling as well. I run a tunnel and a VPN all the time with DNS Leak Protection and Killswitch Enabled. I use one of my VPSes as a Socks Tunnel as well to route some data through on my web browser and other software that are P2P or will have a chance of leaking my identity to someone.

Now if you want to take it an extra mile, you could do all the above and also have an RDP that you work out of, I would make sure you connect to the RDP through your Socks5 Proxy and you would be connected to your tunnel via the VPN!

A Virtual Machine is only good for testing and sandbox environments, not really OpSec. However, They do come in handy. If you want to ensure your data is secure from Govt or Thieves then you would want to encrypt your drives. There are tons of software you can achieve this with but VeraCrypt took over after TrueCrypt became insecure.

Nomad.Null - May 30, 2024, 5:53 pm

The main protection you have is full disk encryption (not Windows Bitlocker) and minimum extranational VPN with no extradition Treaty. Routing through Russia all but guarantees your information will not be shared.

There are other ways to stay more anonymity like TOR and i2pd, but these are the essentials.

A VM is more of a convenience than a security feature.

jasrrow - May 31, 2024, 6:06 am

thanks for response firstly,

as i understood and then made a little research on your posts guys:

good VPN encryption is more or less ok, i mean 2 VPS for private VPN and for browser tunneling for socks5 proxy. with addition of Killswitch and DNS leak protection.

as i understand first one is changing and encrypting data for full OS/PC and second one is ensuring web browsing in addition. am i correct?

what about device tracking or identifying?

despite mac address can be changed, a lot of web servers are collecting metadata about device right?

is that not so important?

Bry4n_1337 - May 31, 2024, 9:39 am

Just use public WiFi or proxy through TOR. There's only a handful of VPNs that are trust worthy, like Mullvad, but personally I wouldn't recommend using VPN.

happygonutty - May 31, 2024, 5:44 pm

(May 31, 2024 09:39 AM)Bry4n_1337 Wrote: [\[CITE\]](#) Just use public WiFi or proxy through TOR. There's only a handful of VPNs that are trust worthy, like Mullvad, but personally I wouldn't recommend using VPN.

I agree with Bry4n_1337 that there are only a handful of VPNs that are trustworthy since most are just giving out information if "needed" by the feds or they have the rights to take out information. And also, being too paranoid about security is totally not a must if you aren't a special snowflake or you doing some illegal business that would end you up in jail. ?