

Forum:[Hack Forums](#)

Thread: [Complete Anonymity Using Layered Virtual Machines and Tor](#)

PunchingMule - November 7, 2017, 4:45 pm

Good afternoon all,

This tutorial is more conceptual in nature so that you can achieve actual anonymity when carrying out your nefarious (just kidding... ethical) hacking activities.

Here's the overview (and, it's overkill... but the concept is good):

Start with the native machine (turn it on, dummy).

Connect to the internet via your Torguard VPN (purchased with Bitcoin).

Install VMWare.

Inside VMWare... install Kali Linux (this will be your Kali Linux ONE machine).

Connect to the internet (again) via your Torguard VPN (again).

Install Virtualbox on the Kali Linux ONE machine.

Download and apply Whonix Gateway to your Virtualbox (this sends your connections through the Tor network).

Install the Whonix Gateway machine and turn it on.

Inside Virtualbox, install Kali Linux TWO. When installing this second Kali Linux machine, make sure all traffic is directed through the Whonix Gateway by changing the adaptor setting to "Internal Network." This will ensure that Kali Linux is sending traffic through the Tor network.

This structure is complicated, takes a while to set up, but CAN circumvent the complicated and sensitive protections of GMail... so, I mean, it's pretty awesome.

Net Hunter - November 8, 2017, 11:45 am

Great stuff, always can add in a few extra steps into this like being on public wifi from long using a hop from a bot. Or maybe modded modem for spoofing to ISP.

PunchingMule - November 10, 2017, 5:29 pm

(Nov 8, 2017 12:45 PM)Net Hunter Wrote: [\[CITE\]](#) Great stuff, always can add in a few extra steps into this like being on public wifi from long using a hop from a bot. Or maybe modded modem for spoofing to ISP.

A modded modem is brilliant... do you have a tutorial for that? A website that provides good instruction?

hackforums4life - December 4, 2017, 7:20 am

Is it as good as using Tails? Tails have proven to be very good anonymity, which doesnt even store logs on computer.

Asdethprime - December 6, 2017, 5:05 pm

(Dec 4, 2017 08:20 AM)hackforums4life Wrote: [\[CITE\]](#) Is it as good as using Tails? Tails have proven to be very good anonymity, which doesnt even store logs on computer.

It's the same stuff just made unnecessarily complex with multiple virtual machine, which will make the connection slower but not necessarily make it harder to track.

Eventually though the suggestion is to use Whonix in the tutorial which is very much like Tails.

The difference to this vs using plain tails / whonix is the tutorial has used a Tor Guard Vpn (actually twice) .

The downside though, 1 it's going to be much much slower and 2 there is a central point of failure. You are totally dependent on TorGuard Vpn to protect u. If they fail all else u apply does not matter at all.

Using tails alone would be faster than this (though yeah it's o
Tor it's pretty slow) and u don't have to worry about a central point of failure. Security wise if u wanted just as strong you can easily just increase the number of hops on tor setup giving u just as robust security.

???? - December 6, 2017, 5:41 pm

...why don't you just use whonix on qubes? Qubes runs layered VM's just like Whonix, except qubes is security oriented and whonix is anonymity oriented. It's a little difficult to set up but it's much better than everything you can come up with on your own.

Kali linux isn't magically more safe than an OS than qubes, which is built to negate attacks...

Asdethprime - December 6, 2017, 11:10 pm

(Dec 6, 2017 06:41 PM)???? Wrote: [\[CITE\]](#) ...why don't you just use whonix on qubes? Qubes runs layered VM's just like Whonix, except qubes is security oriented and whonix is anonymity oriented. It's a little difficult to set up but it's much better than everything you can come up with on your own.

Kali linux isn't magically more safe than an OS than qubes, which is built to negate attacks...
Exactly.

Not to mention Qubes by default, under VM manager, has a built in option for a Whonix VM. You literally just have to turn it on, follow the prompt and the operating system will automatically do all the installation for you (you will have to restart it once though).

That's not even considering the fact that going in and out of TOR network 3 times as suggested by the OP will mean you are looking at an internet speed of few bytest(not KB or MB just bytes) per second. A run of the mill nmap scan will , for a small network will likely take u multiple days (i am not evrn exaggerating a little.)

Big_mp5 - February 25, 2018, 4:43 am

This is very useful, I'm gonna try it. Is it really slow?