

Forum:[Hack Forums](#)

Thread: [Kali tools through tor](#)

Gruja - July 28, 2015, 8:46 am

I searched whole Internet to find how to make my traffic go through tor.

For example, if I do an Nmap scan on an Internet website to discover all open ports and running services, can I make it go through tor so my IP is hidden?

I found some blogs and videos about that. They use tool called socat but I don't understand it well how it works.

Can I use Iptables to redirect all traffic to go through that particular port where tor is running? Can I even add proxychain and ssh tunneling?

If I do this then I can't use reverse payloads, right?

I would really like if someone has time and desire talk about these things and explain them to me?

Thanks in advance.?

Chillingworth - July 28, 2015, 9:14 am

torsocks is probably what you're looking for. If you intend to transparently proxy Kali virtual machine, run torsocks virtualbox via the command line on your base operating system. This will force all of VirtualBox's traffic through the Tor network and effectively prevent DNS leaks. If you use VM software other than VirtualBox (I.e. KVM) then replace virtualbox with the name of the software.

Gruja - July 28, 2015, 9:26 am

If I do this and launch a metasploit attack, everything will go through tor, right?

I am using VMware software. Is it supported?

And thank you for answering:D

PhantomElite - July 28, 2015, 9:33 am

(Jul 28, 2015 09:14 AM)Chillingworth Wrote: [\[CITE\]](#) torsocks is probably what you're looking for. If you intend to transparently proxy Kali virtual machine, run torsocks virtualbox via the command line on your base operating system. This will force all of VirtualBox's traffic through the Tor network and effectively prevent DNS leaks. If you use VM software other than VirtualBox (I.e. KVM) then replace virtualbox with the name of the software.

That sounds like Whonix to me with Kali as the workstation.

Gruja - July 28, 2015, 10:11 am

Oh. But, I don't want every single tool that I use to go through tor just as in Whonix. I want just tools that I use to touch some server and computers like Nmap, metasploit... Can I do that?

Inferno - July 28, 2015, 12:53 pm

tor is slow :/ i use vpn with no logging

Gruja - July 28, 2015, 1:16 pm

What the others think? What is better option?

Supreme.tm - July 28, 2015, 1:21 pm

I would just use a VPN. They are faster, and also more secure than the tor network, it also protects everything on your computer that uses the internet, not just your browser.

Chillingworth - July 28, 2015, 3:37 pm

(Jul 28, 2015 10:11 AM)Gruja Wrote: [\[CITE\]](#) Oh. But, I don't want every single tool that I use to go through tor just as in Whonix. I want just tools that I use to touch some server and computers like Nmap, metasploit... Can I do that?

Why not? What difference does it make?

(Jul 28, 2015 09:33 AM)PhantomElite Wrote: [\[CITE\]](#) That sounds like Whonix to me with Kali as the workstation.

Pretty good analogy ?

(Jul 28, 2015 01:21 PM)Hatley123 Wrote: [\[CITE\]](#) I would just use a VPN. They are faster, and also more secure than the tor network, it also protects everything on your computer that uses the internet, not just your browser.

If you knew how Tor and VPNs work then you would realize that Tor by design is much more robust than any VPN out there.

Goodies - July 28, 2015, 4:21 pm

(Jul 28, 2015 03:37 PM)Chillingworth Wrote: [\[CITE\]](#) If you knew how Tor and VPNs work then you would realize that Tor by design is much more robust than any VPN out there.

And if you knew how Tor and VPNs actually work, then you'd realize that VPN's, by design, are far more robust than Tor. Tor provides better encryption and anonymity, but VPN's provide better stability, reliability, usage, and overall security. But of course you have a rigorous and incorrect understanding of what a VPN is. Relying on anonymous relay servers to handle your data is not what I'd call "robust." Tor is a major target of every branch of every three-letter federal acronym. Don't delude yourself into thinking that Tor provides anonymity in some ethereal, impenetrable sense. VPN's don't either, but they are inherently more robust than Tor ever will be.

hahdbwoannniabs - July 28, 2015, 4:56 pm

Find proxychains + tor Debian installation instructions, then before every command you run in terminal put "proxychains " in front of it.

Chillingworth - July 28, 2015, 5:39 pm

(Jul 28, 2015 04:21 PM)Goodies Wrote: [\[CITE\]](#) And if you knew how Tor and VPNs actually work, then you'd realize that VPN's, by design, are far more robust than Tor. Tor provides better encryption and anonymity, but VPN's provide better stability, reliability, usage, and overall security. But of course you have a rigorous and incorrect understanding of what a VPN is. Relying on anonymous relay servers to handle your data is not what I'd call "robust." Tor is a major target of every branch of every three-letter federal acronym. Don't delude yourself into thinking that Tor provides anonymity in some ethereal, impenetrable sense. VPN's don't either, but they are inherently more robust than Tor ever will be.

Not saying that Tor is some sort of utopia because it definitely is not. We can both agree that Tor provides better encryption and anonymity and I can agree with you in that VPNs provide better stability and usage but reliability and security depends entirely on the context. If you're an avid Internet inhabitant that's looking for increased privacy then VPNs are the way to go. However, if you are subject to law enforcement intervention then Tor is by far the better solution. In regards to security, with Tor you have a greater chance of having your traffic maliciously handled by arbitrary exit nodes although with VPNs, you're more susceptible to targeted attacks against YOU specifically (i.e. there's a better chance of an adversary compromising your VPN provider than hoping you'll build a Tor circuit containing their exit node). Which is overall more robust depends on your threat

model. For the cyber criminal, Tor is undoubtedly the superior choice. For the average Internet denizen? A trustworthy VPN that won't sniff your traffic is the better option.

Goodies - July 28, 2015, 7:21 pm

(Jul 28, 2015 05:39 PM)Chillingworth Wrote: [\[CITE\]](#) Not saying that Tor is some sort of utopia because it definitely is not. We can both agree that Tor provides better encryption and anonymity and I can agree with you in that VPNs provide better stability and usage but reliability and security depends entirely on the context. If you're an avid Internet inhabitant that's looking for increased privacy then VPNs are the way to go. However, if you are subject to law enforcement intervention then Tor is by far the better solution. In regards to security, with Tor you have a greater chance of having your traffic maliciously handled by arbitrary exit nodes although with VPNs, you're more susceptible to targeted attacks against YOU specifically (i.e. there's a better chance of an adversary compromising your VPN provider than hoping you'll build a Tor circuit containing their exit node). Which is overall more robust depends on your threat model. For the cyber criminal, Tor is undoubtedly the superior choice. For the average Internet denizen? A trustworthy VPN that won't sniff your traffic is the better option.

I just wish you explained yourself like this in the first place because there's very little, if anything, that I disagree with here.

Culperring722 - July 28, 2015, 7:34 pm

Na bro its all about that proxyham you can connect to wifi hotspot from 2 miles away. Then you use VPN, or Tor , or Proxychain or nothing cuz you 2 miles away so who cares.

Gruja - July 29, 2015, 3:52 am

(Jul 28, 2015 05:39 PM)Chillingworth Wrote: [\[CITE\]](#) Not saying that Tor is some sort of utopia because it definitely is not. We can both agree that Tor provides better encryption and anonymity and I can agree with you in that VPNs provide better stability and usage but reliability and security depends entirely on the context. If you're an avid Internet inhabitant that's looking for increased privacy then VPNs are the way to go. However, if you are subject to law enforcement intervention then Tor is by far the better solution. In regards to security, with Tor you have a greater chance of having your traffic maliciously handled by arbitrary exit nodes although with VPNs, you're more susceptible to targeted attacks against YOU specifically (i.e. there's a better chance of an adversary compromising your VPN provider than hoping you'll build a Tor circuit containing their exit node). Which is overall more robust depends on your threat model. For the cyber criminal, Tor is undoubtedly the superior choice. For the average Internet denizen? A trustworthy VPN that won't sniff your traffic is the better option.

Yes, you are definitely correct. The best way would be to use them both.

But let's come back on my question. How to make my traffic go through tor? If I use both, how to make my traffic go through both, VPN and Tor.

Can I use proxychains or what?

Let's say like this. In my configuration file of proxychains is a line that would redirect traffic through Tor port, 9050. So, if I use command proxychains msfconsole or proxychains nmap, would all traffic go through Tor?

Is it correct?

DrDinosaur - July 29, 2015, 4:51 am

(Jul 29, 2015 03:52 AM)Gruja Wrote: [\[CITE\]](#) Yes, you are definitely correct. The best way would be to use them both.

But let's come back on my question. How to make my traffic go through tor? If I use both, how to make my traffic go through both, VPN and Tor.

Can I use proxychains or what?

Let's say like this. In my configuration file of proxychains is a line that would redirect traffic through Tor port, 9050. So, if I use command proxychains msfconsole or proxychains nmap, would all traffic go through Tor?

Is it correct?

Jesus, this is an easily searchable question.

Just set up proxychains.

Gruja - July 29, 2015, 5:13 am

I just wasn't sure if this is the right way.

Thank you!:D

hahdbwoannniabs - July 29, 2015, 7:27 am

(Jul 29, 2015 03:52 AM)Gruja Wrote: [CITE](#) Yes, you are definitely correct. The best way would be to use them both.

But let's come back on my question. How to make my traffic go through tor? If I use both, how to make my traffic go through both, VPN and Tor.

Can I use proxychains or what?

Let's say like this. In my configuration file of proxychains is a line that would redirect traffic through Tor port, 9050. So, if I use command proxychains msfconsole or proxychains nmap, would all traffic go through Tor?

Is it correct?

If you knew how tor worked you'd know that using a VPN at the same time is pointless.

And yes, install proxychains, configure it correctly, and put "proxychains " before every command you run and it will force all of your traffic through tor.

Gruja - July 29, 2015, 7:44 am

But why is that pointless? It would add some extra security and be harder to track, right?

I will try with proxychains later, I am currently doing something else.

hahdbwoannniabs - July 29, 2015, 7:59 am

(Jul 29, 2015 07:44 AM)Gruja Wrote: [CITE](#) But why is that pointless? It would add some extra security and be harder to track, right?

I will try with proxychains later, I am currently doing something else.

No, once again, if you knew how tor worked you'd realize that adding a VPN to it is useless. In fact, it would make your anonymity worse if the VPN keeps logs because all of your requests and connections would go through the VPN first.

Gruja - July 29, 2015, 8:07 am

That is true only if I connect to VPN first. But, if I first connect to Tor and then to VPN and if VPN keeps logs, they will not see my real IP, only the IP from exit node which is really good. This way of using Tor and VPN does not have any cons except the very slow bandwidth.

hahdbwoannniabs - July 29, 2015, 8:29 am

(Jul 29, 2015 08:07 AM)Gruja Wrote: [CITE](#) That is true only if I connect to VPN first. But, if I first connect to Tor and then to VPN and if VPN keeps logs, they will not see my real IP, only the IP from

exit node which is really good. This way of using Tor and VPN does not have any cons except the very slow bandwidth.

Sigh, I was trying to keep my patience here but you are really, really fucking stupid. I'm finished trying to explain things to you.

Gruja - July 29, 2015, 10:39 am

Well, take a look here <http://www.hackforums.net/showthread.php?tid=4888771>, go down there where is a title "Tor through VPN vs. VPN through Tor" make sure you read it carefully. I can see that you have really good reputation over there ;)

Delete brackets in the link above please because I can't post links yet.

I have problem when launching an Nmap scan through Tor. It repeatedly shows this message: Rejecting SOCKS request for anonymous connection to private address [scrubbed]

Why does it not let me do the scan? What is wrong and how can I fix it?

I was trying to find a solution on Internet but didn't find useful things. They all just refers to something but there are no solutions.

Can someone help me, please? I can't find anything useful on Internet.

nyquist - July 30, 2015, 3:08 pm

(Jul 29, 2015 08:07 AM)Gruja Wrote: [\[CITE\]](#) That is true only if I connect to VPN first. But, if I first connect to Tor and then to VPN and if VPN keeps logs, they will not see my real IP, only the IP from exit node which is really good. This way of using Tor and VPN does not have any cons except the very slow bandwidth.

I think it really doesnt matter.... it could make it worse, but in any case it wont make it "safer". If a VPN Provider is either at the beginning of your transmission OR at the end and he could log everything you do. So ALL of your traffic would be at ONE single place each time you send packets in the net. So lets say you connect to TOR, leading all further traffic to your VPN. That would mean instead of normal traffic you would send (which could be identified as malicious, but in the first place it looks like normal traffic) you will create really, really, really suspicious packets. The VPN Provider would see tons of addresses connecting through your paid account. In case of a investigation against you the provider (if hes logging) would instantly know that you do malicious stuff since all your traffic is "anonymized". Yeah imho you could really fuck up doing this. But its only an opinion. Correct me if im wrong.

greetz

DarkTruTH007 - July 30, 2015, 9:03 pm

still confused here.....help me also

Gruja - August 1, 2015, 1:54 am

I still have problem with launching some tools through tor with proxychains. It constantly gives me an error. I have described my issue a couple of posts above. I really appreciate any help.

Phurkus - August 1, 2015, 3:16 pm

change mac adress too OP in case something fails

Gruja - August 1, 2015, 4:30 pm

What do you mean? I am not sure if that can cause the problem.

Goodies - August 1, 2015, 11:57 pm

(Aug 1, 2015 03:16 PM)Phurkus Wrote: [\[CITE\]](#) change mac adress too OP in case something fails

You know what would really help?

Knowing what a MAC address is and does before making ill-informed comments.

Gruja - *August 2, 2015, 1:29 am*

Do you probably know why this is not working?