

Forum:[Hack Forums](#)

Thread: [Tutorial: On Secure Anonymity With Tor – SSH, and SOCKS \(n00b approved\)](#)

-Gohan- - November 28, 2010, 7:07 pm

This guide was NOT written by me it ALL! All credits go to : [This guy](#)

This is the best tutorial on how to secure a TOR connection to the net with the best chances of remaining totally anonymous. This tutorial was originally posted over at milw0rm forums, at my request, by .deus_eX_machina. That's his purdy little tag on your left. I also asked him to make it easy to understand for the most n00biest of n00bs, which he kindly did. He knows his shit. So read on and learn. I know I will.

Introduction

On-line privacy is very important, for the vast majority of people Tor provided this privacy, but even now this is in danger. The author of Metasploit HD Moore has apparently developed a tool to link content handled by the exit servers, thus being able to discover the data source, however this technique does require the targeted user to take risky actions; such as allowing Javascript in his/her browser, his tool has been dubbed Torment. Not only this but any one who actually owned two nodes, and they became two exit nodes in the route, he can use statistical analysis to discover that they are part of the same circuit. Once the data leaves the onion route there is no longer any encryption on it this is what I will be looking at soon. First a brief explanation on the way Tor works:

“The user's software or client incrementally builds a circuit of encrypted connections through servers on the network. The circuit is extended one hop at a time, and each server along the way knows only which server gave it data and which server it is giving data to. No individual server ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.”

[img]http://tor.eff.org/images/htw2.png[/img]

What you will need:

- Tor (Install the Package)
- Putty
- TorDNS Localhost 1.7 (Not essential)
- Freecap
- Shell account (This isn't essential either, but will be used to demonstrate this concept)

And that's just the intro, so be prepared to ACTUALLY read every word of this tutorial or I can guarantee that you will miss some important detail. I had to read it like three times before I caught everything. [/align]

Step 1 – Getting Prepared

Get you self a copy of the above programs and install them all, TorDNS is just a standalone application just leave it be for a minute. What we are going to do now is set up FreeCap to use Tor as its proxy enter FreeCap, go to settings like so, and enter this data;

[img]http://i151.photobucket.com/albums/s135/thomarsefatman/TORCAP.jpg[/img]

OK now make sure Tor is active, see that little black thing with a red cross over it in the system tray (LOL), click on it and click start, it should turn into a little green onion. Now what we can do is add some programs to FreeCap, you can either drag a short cut into the window, or add the program directly by browsing for it.

As a proof of concept add you browser to FreeCap, this is not a good idea for web browsing though – “using Privoxy is necessary because browsers leak your DNS requests when they use a SOCKS proxy directly, which is bad for your anonymity. Privoxy also removes certain dangerous headers from your web requests, and blocks obnoxious ad sites like Doubleclick.”

..do it anyway, if your using Firefox you may need to clear your cache and cookie's first, and close all other instances. Now if you browse to google or a site like <http://ip-adress.com/> it should be fairly clear whether your using SOCKS or not. Now I believe the most important addition to FreeCap is “cmd.exe”, browse to system32 and add it. When you then load it up via FreeCap, ping 127.0.0.1, and you should see at the top of the window “cmd.exe -ping 127.0.0.1 via FreeCap”. So we know its working right, at this stage anything you do via the command line is pretty much completely anonymous, and as we all know nearly is not not good enough.

Step 2 – DNS requests and Leaks

Now TorDNS can be a real bitch, so just load it up and should be found down in the system tray. Then go into you network connections (or maybe even your router) and change the Primary DNS server to 127.0.0.1, and delete the secondary one. Now go into FreeCap, Settings, Program & where it says “DNS name resolving” choose local. Again open up TorDNS and your command prompt via FreeCap. Here I have shown you two methods to resolve DNS through TOR, handy if your ISP is watching you, or if your target is even remotely clever. I would also recommend going into “services.msc” via run, switching “DNS Client” to manual, and then turning it off.

So this is handy for a lot of those applications that do not directly support the use of SOCKS, as you can imagine there is a lot crazy stuff you can do up to this point. But I'm afraid it ignores the point I made earlier about this new program Torment. In the next step I will show you a new level of anonymity, we will be disregarding a few of the things I have taught you so far, anyway, read on to find out!

Step 3 – SSH

At this point it would be nice to understand exactly what SOCKS is, and what it does.

“SOCKS is an Internet protocol that allows client-server applications to transparently use the services of a network. SOCKS is an abbreviation for “SOCKetS”.

Clients behind a firewall, needing to access exterior servers, may connect to a SOCKS proxy server instead. Such proxy server controls the eligibility of the client to access the external server and passes the request on to the server. SOCKS can also be used in the opposite way, allowing the clients outside the firewall (“exterior clients”) to connect to servers inside the firewall (internal servers).

Unofficial SOCKS 4a extensions add support for DNS names to resolve names with SOCKS server. The current version 5 of the protocol, RFC 1928 or authenticated firewall traversal, extends the previous version by supporting UDP, authentication, letting the SOCKS server resolve hostnames for the SOCKS client, and IPv6.

The SOCKS reference architecture and client are owned by Permeo Technologies, a spin-off from NEC.

According to the OSI model it is an intermediate layer between the application layer and the transport layer.”

Ok, Tor supports the SOCKS4, SOCKS4A, and SOCKS5 standards. Also remember that when you data leaves the final Tor exit node that it no longer is encrypted.

I will now show you how to configure Putty to get your DNS information via TorDNS, and then set up a SSH tunnel to a remote shell account. I will be using a shell account at <http://sdf.lonestar.org/> which could be a shell anywhere right? maybe its a machine of your own, maybe that machine also runs Tor, or maybe its a compromised machine, just maybe.

Open up Putty, go to connection, SSH, Tunnels, enter the source port as 9050, and the destination as 127.0.0.1:9050, now click add. Obviously thats our SSH tunnel. Then go to Connection, Proxy, where it says “Do DNS lookup at DNS end” choose no (oh and remember to save this profile).

[img]<http://i151.photobucket.com/albums/s135/thomarsefatman/PuttyTunnel.jpg>[/img]

[img]<http://i151.photobucket.com/albums/s135/thomarsefatman/PuttyDNS.jpg>[/img]

[img]<http://i151.photobucket.com/albums/s135/thomarsefatman/SSHTunnel-1.jpg>[/img]

srbin1 - November 29, 2010, 8:49 am

What exactly are you supposed to do after you have logged in to sdf.lonestar.org in the Putty-application?

Reminiscent - November 29, 2010, 9:28 am

Nice share.

Images:5/5

Content:5/5

Noob-proof-ness:4/5 (noobs can fuck anything up)

-Gohan- - November 29, 2010, 8:15 pm

(Nov 29, 2010 10:28 AM)IronClad Wrote: [\[CITE\]](#) Nice share.

Images:5/5

Content:5/5

Noob-proof-ness:4/5 (noobs can fuck anything up)

Thank you, but once again its not my guide, I don't even think the guy is on this forum.

(Nov 29, 2010 10:28 AM)IronClad Wrote: [\[CITE\]](#) Nice share.

Images:5/5

Content:5/5

Noob-proof-ness:4/5 (noobs can fuck anything up)

Thank you, but once again its not my guide, I don't even think the guy is on this forum.

?MGK - November 29, 2010, 8:32 pm

This is not bad, thanks for the post!

-Gohan- - November 30, 2010, 12:38 pm

No problem, thank you for posting.

-Gohan- - December 16, 2010, 12:04 pm

Has anyone tried this yet?

calamus - December 16, 2010, 12:27 pm

thanks for sharing

it is important steps

-Gohan- - December 16, 2010, 1:53 pm

(Dec 16, 2010 01:27 PM)calamus Wrote: [\[CITE\]](#) thanks for sharing

it is important steps

No problem, glad you liked it.

-Gohan- - December 31, 2010, 8:11 pm

Hmm.. Will the people who did this please post.

bernardbear - January 1, 2011, 12:37 am

i use yourfreedom,its that nice ?

seskanda - February 2, 2011, 10:42 pm

This tut is bit hard to follow and unclear, but still decent overall

Taicho58 - February 7, 2011, 6:59 am

TorDNS Localhost 1.7 is impossible to find. I searched google, usenet etc. Maybe i should search more

Do0ks - February 11, 2011, 7:14 am

Nice share. Thanks ill add to bookmarks.

Lucky™ - February 15, 2011, 7:17 am

(Feb 7, 2011 07:59 AM)wopa82 Wrote: [\[CITE\]](#) TorDNS Localhost 1.7 is impossible to find. I searched google, usenet etc. Maybe i should search more

yes, where to download TorDNS?

Matthew 6:33 - February 15, 2011, 10:47 am

thanks man +rep you if i could :(

msn to short

Seed - February 15, 2011, 2:29 pm

Thank you for sharing this.

bcom_bad - February 16, 2011, 12:27 am

looking good. i used proxy soft like hide my ip bla bla lets try this one

-Gohan- - July 18, 2011, 10:40 pm

(Feb 15, 2011 11:47 AM)Futurama Wrote: [\[CITE\]](#) thanks man +rep you if i could :(

msn to short

You can man lol, no problem.

DarkHorseRising - August 4, 2011, 1:04 pm

If anyone is interested in anonymity and anti-forensics then check out my tute - check it out

Easy Anonymity Through Basic Anti-forensics: A comprehensive (noob friendly) guide to covering

your tracks

<https://hackforums.net/showthread.php?tid=1561351>

Eminent - August 4, 2011, 1:14 pm

If I had a penny for every time this thread was brought back to life...

fortitude123 - August 4, 2011, 2:51 pm

Nice tutorial.... Thanks for it really helped.

-Gohan- - August 4, 2011, 6:11 pm

(Aug 4, 2011 02:51 PM)fortitude123 Wrote: [\[CITE\]](#) Nice tutorial.... Thanks for it really helped.
No problem man glad it helped.

SIM-73089 - August 8, 2011, 1:17 pm

Very Informative and Detailed. Well done. ?

I don't really use any Proxies while hacking.. Is it really necessary? ?

-Gohan- - August 8, 2011, 1:26 pm

(Aug 8, 2011 01:17 PM)sylvertch Wrote: [\[CITE\]](#) Very Informative and Detailed. Well done. ?

I don't really use any Proxies while hacking.. Is it really necessary? ?Matters, if you're hacking something high profile it can be. It can be the difference between freedom and jail time.

SIM-73089 - August 8, 2011, 1:28 pm

(Aug 8, 2011 01:26 PM)al7bar Wrote: [\[CITE\]](#) Matters, if you're hacking something high profile it can be. It can be the difference between freedom and jail time.

I don't really live anywhere with extradition to the US. Do you think this is good?

Also.. Not Europe, Not China, Not North America, Not Australia.

~Aer - August 8, 2011, 2:30 pm

Thanks for this! Helped a lot!

??? Matto ??? - August 8, 2011, 2:42 pm

Nice guide thanks dude :D

-Gohan- - August 9, 2011, 1:48 pm

(Aug 8, 2011 01:28 PM)sylvertch Wrote: [\[CITE\]](#) I don't really live anywhere with extradition to the US. Do you think this is good?

Also.. Not Europe, Not China, Not North America, Not Australia.

Yea that helps a lot when it comes to getting caught. You should be fine, I just like to be safe.

~Aer - August 16, 2011, 3:29 pm

Thanks for sharing. I'm gunna have to come back to this and set it up when I get home

-Gohan- - August 16, 2011, 7:04 pm

(Aug 16, 2011 03:29 PM)ster76 Wrote: [\[CITE\]](#) Thanks for sharing. I'm gunna have to come back to this and set it up when I get home

Yea no problem, if you need any help just ask, I would be glad to help you.

hamilton - August 18, 2011, 4:12 pm

wooww dancer cat very nice.very For sharing.thanks

-Gohan- - August 18, 2011, 6:07 pm

No problem glad it helped. Hit me a pm if you need any help with it.

darkyoshi22 - November 13, 2011, 3:16 pm

Thanks for this, will really help a lot of people configure tor. Bookmarked:)

-Gohan- - November 13, 2011, 3:41 pm

(Nov 13, 2011 04:16 PM)darkyoshi22 Wrote: [\[CITE\]](#) Thanks for this, will really help a lot of people configure tor. Bookmarked:)

No problem, it's good to always be secure no matter what you're doing.

Wendys - November 13, 2011, 6:06 pm

Great Tutorial bro, ill save this as TXT on my desktop. BOOKMARKED

Oryinn - November 13, 2011, 8:11 pm

Thank you for sharing this. I'm saving and bookmarking.

pachapichi - November 13, 2011, 10:48 pm

As the other say's over me (Bookmarked)

And thanks for posting this guide

Transcendance - November 21, 2011, 4:45 pm

Tor is too slow for normal use in my opinion.

-Gohan- - November 21, 2011, 5:26 pm

(Nov 21, 2011 05:45 PM)Transcendance Wrote: [\[CITE\]](#) Tor is too slow for normal use in my opinion. This is a bit out of date. But it is still useful.

TheHackerRasim - November 21, 2011, 5:30 pm

i m waiting to try it out thnks i think it is helpfull

-Gohan- - November 21, 2011, 5:33 pm

(Nov 21, 2011 06:30 PM)TheHackerRasim Wrote: [\[CITE\]](#) i m waiting to try it out thnks i think it is helpfull

It is pretty basic, if you need any help shoot me a PM.

SliPC - December 1, 2011, 3:19 pm

Bookmarking this. Cant wait to try it and surf anonymously. Thanks in advance!

-Gohan- - August 26, 2012, 11:27 am

There's an updated version of this, I will be posting it soon.

YoYoZ - August 26, 2012, 12:23 pm

Thank you so much man, just got the help I needed.

-Gohan- - August 26, 2012, 1:06 pm

(Aug 26, 2012 12:23 PM)YoYoZ Wrote: [\[CITE\]](#) Thank you so much man, just got the help I needed. No problem dude, but this is an outdated version.

laillaha - May 19, 2013, 12:12 am

nice for the job hope just we will have update time by time

-Gohan- - *May 19, 2013, 2:07 pm*

This still works, give it a go if you need help ask.

gemen - *May 19, 2013, 4:15 pm*

Good tutorial, nice to see this, thanks