

Forum:[Hack Forums](#)

Thread: [Detailed Anonymity tutorial. \(How to really be secure!\)](#)

uSploit - September 23, 2013, 9:23 am

I wont be explaining how the tunneling/ programs i use work.

Thats unnecesairy information for starters.

If you really want to know how things work use google!

Google is smarter then i am. This isnt a fancy tutorial. I kept it short and to the point!

No one would understand this stuff as a starter anyway.

Lets start, anonymity is a verry important step into the hacking world.

If you fail at doing this part you could aswell go to the police and tell them you hack.

There is more then one way to prevent your identity from beeing leaked.

These are the ones we will be using and will be combining, maxing the effects of the anonymity they provide.

- VMWARE or virtual machine.
- VPN or virtual private network.
- How to stop dns leaking
- Proxy's and proxy chaining.
- Tor network.
- polipo http proxy cache
- Chatcrypt, for private chats.

This is what i will be talking about.

How to install them. How to run them alongside.

How to test if you are secure.

VMWARE or virtual machine:

To be more secure it is an advantage if you used a virtual machine and run a distro using that machine.

That prevents from leaking information about your real computer!

Code

http://www.oracle.com/us/technologies/virtualization/oraclevm/overview/index.html?sckw=srch:virtual_machine&SC=srch:virtual_machine

<https://my.vmware.com/web/vmware/downloads>

VPN Setup, using it and preventing DNS leaks.

VPN Setup + free VPN list.

First of all i do not support free VPN's.

Free VPNs can be a good thing but i dont trust the use of them.

Because theyd leak information if they really have to.

But its always better then no VPN ;).

Free VPN's:

<http://www.openvpn.com> Windows/Mac/Linux

<http://www.securitykiss.com> Windows/Mac/Linux

<http://www.cyberghostvpn.com> Windows only and limited use.

To get more free VPN's please use google i am not a search engine.

Paid VPN's:

<http://strongvpn.com> Windows/Mac/Linux

<http://www.#.net> Windows/Mac/Linux

Its up to you what you want what you think is best. I am only helping you on the path of anonymity!

I am using <http://www.securitykiss.com> Windows/Mac/Linux in this tutorial.

Not all vpn's work on all distro's. Some or for both some are for windows some for mac some for linux.

Go to the site of the vpn choose the operating system. Download the client or do as they tell you have to do.

If you have trouble doing this you can allways pm me or answer in the thread. As i cant explain you how to do it whitout knowing what distro you have.

As soon as you got your vpn set up we have to check for DNS leaking.

Prevent DNS leaking!

To test if you have DNS leaks: <https://www.dnsleaktest.com>

Extra info about DNS leaking on this page: http://wiki.hidemyass.com/Stop_DNS_leaks

If you have DNS leaks it will list them below the warning message.

Code Your DNS test results

This page shows the DNS servers that your computer is using to resolve DNS names. The owners of the servers listed below have the ability to log the names of all websites you connect to.

WARNING: If you are connected to a VPN service and ANY of the servers listed below are not provided by the VPN service then your DNS may be leaking. (You should be able to recognise them based on the hostname, ISP and location). This is not an issue if you trust the owners of these servers with your private data.

We detected the 2 DNS server listed below.

At the last line of the warning message it said i got 2 dns servers i was connected to.

Both where google. But i do not want to leak anything right now! Even if its google.

So lets get rid of the dns leaks.

There are many ways to do so.

I used openDNS.

<https://store.opendns.com/setup/>

I am using a linux distro based on ubuntu (backbox).

I used that setup. But as told before this differs from Operating system to operating system.

Open that link and click on the computer.

Choose your operating system.

If you have a different os then the ones listed like i have a backbox it isnt listed.

Google it on how to do it for your distro or do as i do i clicked ubuntu since backbox is build on it. And watched the steps there verry similar for all the linux distros.

Do all the steps they ask you to do.

Ofcourse instead of using it on wireless use it on the vpn connection you made erlier.

Now go back to: <https://www.dnsleaktest.com>

Code Your DNS test results

This page shows the DNS servers that your computer is using to resolve DNS names. The owners of the servers listed below have the ability to log the names of all websites you connect to.

WARNING: If you are connected to a VPN service and ANY of the servers listed below are not provided by the VPN service then your DNS may be leaking. (You should be able to recognise them based on the hostname, ISP and location). This is not an issue if you trust the owners of these servers with your private data.

We detected the 0 DNS server listed below.

As you can see i have 0 dns leaks left! Like a baws.

Proxychain, Tor and polipo setup + use and expelation.

Lets install more great stuff!

Proxychains is a chain that switches between proxies a little like tor itself.

But we can chain this to tor so its even more secure! Sory i will only explain the instalation for ubuntu distro.

Install proxychains command: `sudo apt-get install proxychains`

If you have backbox kali linux or backtrack you probably wont have to do this instalation step.

Now to chain the proxychains to the tor network. Makes you extremely secure.

But there will always be text exit nodes, the chance there usefull is small.

What i am saying you cant be a 100% secure.

<https://forum.intern0t.org/security-tutorials-guides/3787-proxychains-tor.html>

`sudo nano /etc/proxychains.conf`
to edit the config file for proxy chains.

you should see this:

PHP Code

```
<?php
```

```
# proxychains.conf VER 3.1
```

```
#
```

```
# HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.
```

```
#
```

```
# The option below identifies how the ProxyList is treated.
```

```
# only one option should be uncommented at time,
```

```
# otherwise the last appearing option will be accepted
```

```
#
```

```
#dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see chain_len) from the list.
# this option is good to test your IDS :)
# Make sense only if random_chain
#chain_len = 2

# Quiet mode (no output from library)
#quiet_mode

# Proxy DNS requests - no leak for DNS data
proxy_dns

# Some timeouts in milliseconds
tcp_read_time_out 15000
tcp_connect_time_out 8000

# ProxyList format
# type host port [user pass]
# (values separated by 'tab' or 'blank')
#
#
# Examples:
#
# socks5 192.168.67.78 1080 lamer secret
# http 192.168.89.3 8080 justu hidden
# socks4 192.168.1.49 1080
# http 192.168.39.93 8080
#
#
# proxy types: http, socks4, socks5
# ( auth types supported: "basic"-http "user/pass"-socks )
[ProxyList]
# proxy chains here.
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 9050
```

at the end of the file it said #proxy chains here.
there is where you add the free proxys or paid ones up to you what you want.

thats how mine looks:

```
Code socks5 119.37.195.59 1080
```

```
socks5 119.184.214.18 1080
```

```
http 118.175.28.3 1080
```

```
socks5 146.115.61.107 1328
```

extra info on proxy chains:

<https://forum.intern0t.org/security-tutorials-guides/3787-proxychains-tor.html>

its quite easy to edit these ones you know the cmd command :).

Now to use proxychains use this command:

Code proxychains <name_of_application>

We can chain whit tor, nmap, metasploit and so on... :) No limits!

But before we can do that we need to install tor:

before i forget install tor.

<https://www.torproject.org/docs/tor-doc-unix.html.en#installing>

Installing tor is not the same for anyone.

Please google how to do this using your linux distro or windows/mac pc.

I recomand installing the tor browser bundle.

also install polipo:

Polipo is a http proxy cache for your computer.

- 1 It allows sharing of the Internet connection
- 2 The cache will display pages faster, even if you do not share your connection
- 3 It offers an optional filtering utility.

Polipo is an efficient and lightweight HTTP proxy cache.

To install polipo use the next command:

Code sudo apt-get install polipo

for example we want it to run through tor:

Code proxychains /home/unxposed/Documents/tor-browser_en-US/start-tor-browser

That is where i saved my tor browser bundle.

This differs for everyone.

open a terminal and open the location of your tor browser.

write proxychains in the terminal and simply drag the start-tor-browser inside your terminal.

then hit enter.

if you get something like this:

```
[s-chain|-<>-176.36.188.188:52592-<--timeout
```

```
[s-chain|-<>-176.36.188.188:52592-<--timeout
```

```
[s-chain|-<>-176.36.188.188:52592-<--timeout
```

then go to terminal and use this command:

```
sudo nano /etc/proxychains.conf
```

then comment in strickt chains

```
#strickt chains
```

and uncomment dynamic chains so it would choose a new proxy if one failed.

Now what if they all fail:

```
|D-chain|-<>-176.36.188.188:52592-<--timeout  
|D-chain|-<>-146.115.61.107:1328-<--timeout  
|D-chain|-<>-108.62.75.9:23537-<--timeout  
|D-chain|-<>-119.37.195.59:1080-<--timeout  
|D-chain|-<>-180.246.109.97:8080-<--timeout  
|D-chain|-<>-127.0.0.1:9050-<--timeout
```

!!!need more proxies!!!

```
|D-chain|-<>-176.36.188.188:52592-<--timeout  
|D-chain|-<>-146.115.61.107:1328-
```

Means your proxy's are bad get some new ones.

As soon as you get a good one tor will run chained with the proxies you provided.

We ofcourse want our exit nodes to be more safe. In case a hacker tries to get to us.

Here is a link that explains how to force all traffic over the tor network.

You can do the same for your vpn using your firewall. Even your basic firewall can do this.

To make sure all our traffic goes over vpn and only used the end points of the vpn not allowing any other connections.

In this case we will tell our os only to allow connections through the vpn. Using ip tables.

This again differs from which operating system you use.

<https://www.digitalocean.com/community/articles/how-to-set-up-a-firewall-using-ip-tables-on-ubuntu-12-04>

an example that only allows vpn connections:

Code iptables -P OUTPUT DROP

iptables -I OUTPUT -p udp --dport 53 -d 8.8.8.8 -j ACCEPT

iptables -I OUTPUT -d vpn.endpoint.ip.addr -j ACCEPT

iptables -I OUTPUT -o tun+ -j ACCEPT

Ofcourse please use google and write send all connections through a vpn using ip tables + your Operating system.

And as a final: chatcrypt.

<http://www.chatcrypt.com/>

This is where you can be in a aes encrypted chatroom.

I assume you are using the tor chained with proxies and a vpn on top of it.

Now its time to talk secure. Start your chatroom share the pass with only the people you want in and voila!

You can have a nice what.

Ofcourse nothing but nothing is 100% secure only if you leave your phone home and go to a hidden location you have only talked about in real life with the guy you want the conversation.

only then you are secure and even that's a no 100%!

Sorry for grammars and spelling i am not that good at english.

Good luck on being anonymous uSploit.

UnXpanded - *September 23, 2013, 9:51 am*

Detailed in a sence, at least explains how to really get of the radar.
Thanks.

uSploit - *September 23, 2013, 11:33 am*

Thought this would be usefull :) in time i might do improvements on this thread. Atm i did not have to many time for it.