

Forum:[Hack Forums](#)

Thread: [\[TUT\] Simple Anonymity \(Linux Version\) A must read](#)

serial# - September 25, 2010, 1:28 am

Before you start launching all your scans and tests, It would make alot more sense to be "nameless". If your like me then you wouldn't want some IDS picking up your internet protocol right? I haven't seen a tutorial about running our favorite scanners and information grabbing program through something like a proxy that really made alot of sense so I decided to write something down.

There are a few packages you will have to download and install unless your already running backtrack.

Tor & Privoxy
Firefox's Torbutton addon
proxychains
socat

A quick google search will provide you with plenty of download links and even instructions on how to install them.

Now lets skip a few beats and say we have already downloaded and installed tor.
Now lets shut it down and restart it to make sure everything is running smoothly.

Code serial@home:~# /etc/init.d/tor stop

Stopping tor daemon: tor.

Now with out any error messages or warnings lets start tor back up.

We should get the following:

Code serial@home:~# /etc/init.d/tor start

Raising maximum number of filedescriptors (ulimit -n) to 32768.

Starting tor daemon: tor...

Sep 25 03:48:42.110 [notice] Tor v0.2.1.26. This is experimental software. Do not rely on it for strong anonymity. (Running on Linux i686)

Sep 25 03:48:42.111 [notice] Initialized libevent version 1.3e using method epoll. Good.

Sep 25 03:48:42.112 [notice] Opening Socks listener on 127.0.0.1:9050
done.

No error ro warnings messages...GOOD, There are other ways to check this but It's always better to second check things then to second chance them.

Now with tor up and running lets take a look at our privoxy.conf file.

Code serial@home:~# nano /etc/privoxy/config

Now at the very top add this line:

Code forward-socks4a / 127.0.0.1:9050 .Remember to add the period at the end.

Now with nano still up lets search for the words "logfile logfile"

You can do this my holding down the ctrl button and pressing the w key

It will find "logfile logfile" and will look like this:

Code #

Your logfile will grow indefinitely, and you will probably

```
# want to periodically remove it. On Unix systems, you can do
# this with a cron job (see "man cron"). For Red Hat based Linux
# distributions, a logrotate script has been included.
#
# Any log files must be writable by whatever user Privoxy is
# being run as (on Unix, default user id is "privoxy").
#
```

```
logfile logfile
```

```
#
```

```
#
```

Now we don't want to logging anything to a logfile so let's add a # to the beginning of that like this:

```
Code #
```

```
# Your logfile will grow indefinitely, and you will probably
# want to periodically remove it. On Unix systems, you can do
# this with a cron job (see "man cron"). For Red Hat based Linux
# distributions, a logrotate script has been included.
#
# Any log files must be writable by whatever user Privoxy is
# being run as (on Unix, default user id is "privoxy").
#
```

```
# logfile logfile
```

```
#
```

```
#
```

Next search for the words "jarfile jarfile" and do the exact same as you did with "logfile logfile"

Now save and exit the file by holding the ctrl and pressing o and then ctrl+x.

We are going to restart privoxy now since we made some changes:

```
Code serial@home:~# /etc/init.d/privoxy restart
```

Restarting filtering proxy server: privoxy.

Tor and privoxy are now complete, next step is adding the tor button to firefox:

Go to Tools>Add-ons>Get Add-ons and search for Torbutton and install it.

Now when you restart firefox you just click the Tor Disabled button and if it changes to Tor Enabled then go to www.whatismyip.com and see if it's changed, if it has then your browser is now finished.

Now I'm going to show you how proxychains work, it's really simple and for an example I'm going to use the network program nmap.

Open up your terminal and type:

```
Code serial@home:~# proxychains nmap -sT -PN -n -p 80 google.com
ProxyChains-3.1 (http://proxychains.sf.net)
```

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-09-25 04:09 EDT
```

```
[DNS-request] google.com
```

```
[S-chain]-<>-127.0.0.1:9050-<>-4.2.2.2:53-<>-OK
```

```
[DNS-response] google.com is 209.85.225.105
```

```
[S-chain]-<>-127.0.0.1:9050-<>-209.85.225.105:80-<>-OK
```

```
Nmap scan report for google.com (209.85.225.105)
```

```
Host is up (1.8s latency).
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.14 seconds
```

I just did a pretty basic nmap on google.com:80 as just an example but what we did here was we using proxychains to tunnel our nmap scan through tor.

You can use this same feature through all your terminal scanners.
Lets look at another good scan using proxychains

```
Code serial@home:~# proxychains fping -a -g 192.168.1.0/24
ProxyChains-3.1 (http://proxychains.sf.net)
192.168.1.97
ICMP Host Unreachable from 192.168.1.97 for ICMP Echo sent to 192.168.1.2
ICMP Host Unreachable from 192.168.1.97 for ICMP Echo sent to 192.168.1.3
ICMP Host Unreachable from 192.168.1.97 for ICMP Echo sent to 192.168.1.4
ICMP Host Unreachable from 192.168.1.97 for ICMP Echo sent to 192.168.1.5
ICMP Host Unreachable from 192.168.1.97 for ICMP Echo sent to 192.168.1.6
ICMP Host Unreachable from 192.168.1.97 for ICMP Echo sent to 192.168.1.7
Just a simple ping sweep.
```

Now on to socat, this package is a big one so I would highly recommend reading or learning all you can about this one before using it fully. But as an example situation let's say I did a nmap scan on someone and found out they was running a webserver. One super good way to find out what type of server they are running is simply connecting to it and requesting "HEAD / HTTP/1.0"

I open my terminal and type:

+TECH NOTE: A quick way to find out a website's Ip address is to use the tor-resolve function

Code tor-resolve google.com

+++++

```
Code serial@home:~# socat TCP4-LISTEN:8080, fork
socks4a:127.0.0.1:<google's ip address>:80, socksport=9050 &
Now in a new terminal I type:
Code jnc 127.0.0.1 8080
And send the command
"HEAD / HTTP/1.0"
voila!
```

If you liked this or enjoyed please let me know I'll be glad to help you with your own projects on my own time.

Thanks for reading.

Middle - September 27, 2010, 12:39 pm

Could you go into more detail on how to use proxychains? I have been trying to set it up for ages now with no luck.

Thanks a lot

serial# - October 1, 2010, 2:18 pm

(Sep 27, 2010 12:39 PM)Middle Wrote: [\[CITE\]](#) Could you go into more detail on how to use proxychains? I have been trying to set it up for ages now with no luck.

Thanks a lot

What distro are you using?

Middle - October 1, 2010, 2:53 pm

Backtrack 4 So everything is pre-installed I have added a proxy list, but i probably need a new one now, where is best for a proxy list? and any ideas on how to get it working?

RogueR3x - October 1, 2010, 3:53 pm

now THIS is the kinda hacking we all love..if I could call it hacking of course...but this...nice stuff..love it..if I could rep ya for it I would..I don't even know how to rep..but seriously...really good..love this. It's not harmful to anyone if you just leave it at anonymity, nobody knows who you are, which is great defense, and you can use it for attacking without being caught so easily, great weapon.

Once again: love it, haven't seen anything this good on HF. And I'm not lying.

Scar3croW - October 1, 2010, 4:58 pm

Just what I needed for my Ubuntu 10.04 setup. :)

serial# - October 2, 2010, 1:48 am

(Oct 1, 2010 02:53 PM)Middle Wrote: [\[CITE\]](#) Backtrack 4 So everything is pre-installed I have added a proxy list, but i probably need a new one now, where is best for a proxy list? and any ideas on how to get it working?

Run your proxychains through your tor network then there is no need for a proxylist

EDIT: You shouldnt have any problems with this on bt4

(Oct 1, 2010 03:53 PM)RogueR3x Wrote: [\[CITE\]](#) now THIS is the kinda hacking we all love..if I could call it hacking of course...but this...nice stuff..love it..if I could rep ya for it I would..I don't even know how to rep..but seriously...really good..love this. It's not harmful to anyone if you just leave it at anonymity, nobody knows who you are, which is great defense, and you can use it for attacking without being caught so easily, great weapon.

Once again: love it, haven't seen anything this good on HF. And I'm not lying.

Cool man I have a few others in my threads, I took a long break from writing and other computer related fun but now I'm back

Middle - October 2, 2010, 4:46 am

OK im going to ask a very special question now so i apologise for lowering the tone of the thread.

How do i run it through my "tor network"?

serial# - October 2, 2010, 11:44 pm

(Oct 2, 2010 04:46 AM)Middle Wrote: [\[CITE\]](#) OK im going to ask a very special question now so i apologise for lowering the tone of the thread.

How do i run it through my "tor network"?

open terminal and type

Code nano /etc/proxychains.conf

Scroll all the way to the bottom and make sure you have this:

Code # defaults set to "tor"

socks4 127.0.0.1 9050

If not then add that and press ctrl+o then ctrl+x or just press ctrl+x to save and close the file

hottentot - October 2, 2010, 11:54 pm

great? niccee verry good!

Middle - October 3, 2010, 4:27 am

(Oct 2, 2010 11:44 PM)serial# Wrote: [\[CITE\]](#) open terminal and type

Code nano /etc/proxychains.conf

Scroll all the way to the bottom and make sure you have this:

Code # defaults set to "tor"

socks4 127.0.0.1 9050

If not then add that and press ctrl+o then ctrl+x or just press ctrl+x to save and close the file

Thanks for the help, but i don't see how that chains proxies? And when i went to check my IP address it was the same as before

serial# - October 4, 2010, 1:45 am

(Oct 2, 2010 11:54 PM)hottentot Wrote: [\[CITE\]](#) great? niccee verry good!

[/quote]

No problem

[QUOTE='Middle' pid='6811949' dateline='1286105263']

Thanks for the help, but i don't see how that chains proxies? And when i went to check my IP address it was the same as before

Im assuming your using backtrack....if you are setup snort and scan yourself with nmap and see if snort is logging your information view it through base <http://localhost/base> If your not on backtrack and some other distro then show me how your trying to view your ip address another way

Middle - October 4, 2010, 9:49 am

I am running Backtrack 4

So i have ran the following:

Code apt-get install snort

nmap 127.0.0.1

And i got this

Code Starting Nmap 5.00 (<http://nmap.org>) at 2010-10-04 17:51 BST

Interesting ports on localhost (127.0.0.1):

Not shown: 998 closed ports

PORT STATE SERVICE

9050/tcp open tor-socks

10000/tcp open snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

So i am running tor...

And to check my ip i am typing

Code proxychains firefox whatismyip.com