Using TOR For More Then Web

Recently I did a couple of pieces on some ssh bruteforcing I had seen (see here and here), and while I am sure these attempts are the results of botnets, I found myself thinking "Could just one person do it?". Now you may say that a botnet is just one person - the herder, but I was thinking differently. I mean could one person trigger such attempts without a botnet? Now a person could take over all those sources and use them, but thats still kinda a botnet and creates a lot more chances to get caught. Is there an easier, safer way some could do it?

And as you may have guessed from the title of this, thats when I thought of TOR. An acronym standing for "The Onion Router", it is an implementation of a system used to help anonymise traffic. Taken from the projects homepage..

> *"Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of your existing applications, including web browsers, instant messaging clients, remote login, and other applications based on the TCP protocol."*
> *Address : <http://www.torproject.org/>*

Now I am not going to go into the how it works, since they have already done so much better then I could, but suffice to say that it does work. Also bear in mind that they tell you, it does not provide encryption or suchlike, most of the attacks against the TOR network have involved malicious nodes. But for the purposes I was looking for, it matched. It is open-source, it is free, and it is cross-platform. Installation is also very easy. Downloading the source and compiling provides no problems, downloading packages is even easier. Almost all the downloads of tor now involve the downloading of a bundle. Included in these bundles are generally included a proxy of some sort usually used for the web browsing and other bits and bobs - firefox extension, gui control panels, etc. But you get tor, and it is easy. That is the main thing.

Now I am going to focus on linux, and I am going to assume you have tor, meaning that you should see this in your tor log files..

```
 [notice] Tor 0.2.1.23 opening log file.
 [notice] Parsing GEOIP file.
 [notice] We now have enough directory information to build circuits.
 [notice] Bootstrapped 80%: Connecting to the Tor network.
 [notice] Bootstrapped 85%: Finishing handshake with first hop.
 [notice] Bootstrapped 90%: Establishing a Tor circuit.
 [notice] Tor has successfully opened a circuit. Looks like client functionality is
working.
 [notice] Bootstrapped 100%: Done.
```

..if you have that, and you have not specifically changed anything, you should now have a tor socks tunnel setup on your localhost..

```
tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN      21037/
tor
```

Now, thats all great. But what if you want to actually use this now to launch hundreds of ssh attacks? Well thats why I love linux. Enter proxychains (homepage: http://proxychains.sf.net), once you have downloaded this, and done the "unextract/configure/make/make install" shuffle, you can pretty much start using it straight away since by default proxychains is setup to use TOR. Proxychains pretty much "socks-ifies" most applications. Take this for example, lets use links to see my un-TOR information..

```
# links http://www.whatismyip.org -dump
   174.112.xxx.xxx
```

When I feed that into a geoip app..

```
# links http://www.geoiptool.com/en/?IP=174.112.xxx.xxx -dump
    [IMG]                language: English Spanish Portuguese French German
                                                          Chinese Italian
        View my IP       More info     Firefox     Now online    In your
        information      about IPs      Plugin                   Website

  +-------------------------------------------------------------------------+
  |                                                                      New |
  |               Host / IP: ____________________ [ View                 tool|
  |                               info ]                                 for |
  |                                                                      your|
  | Host Name: CPE001b63942648-CM00195efb9002.   Web!|
  |         IP 174.112.xxx.xxx                                              |
  |   Address:                                                              |
  |   Country:                                                              |
  |    Country ()                                                           |
  |      code:                                                              |
  |    Region:                                                              |
  |      City:                                                              |
  |     Postal                                                              |
  |      code:                                                              |
  |    Calling +                                                            |
  |      code:                                                              |
  | Longitude:                                                              |
  |  Latitude:                                                              |
  +-------------------------------------------------------------------------+

   Add to Google [IMG] [IMG] [IMG] [IMG][IMG] [IMG][IMG][IMG][IMG][IMG]
   [IMG]
```

Now I am going to use proychains by just adding it to the start of the commandline..

```
# proxychains links http://www.whatismyip.org -dump
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| www.whatismyip.org
|S-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| www.whatismyip.org is 98.207.226.113
|S-chain|-<>-127.0.0.1:9050-<><>-98.207.226.113:80-<><>-OK
   62.141.58.13
```

And now I see a totally different IP address. Lets see where that IP address is..

```
# links http://www.geoiptool.com/en/?IP=62.141.58.13 -dump
    [IMG]                language: English Spanish Portuguese French German
                                                          Chinese Italian
        View my IP       More info     Firefox     Now online    In your
        information      about IPs      Plugin                   Website

   +-------------------------------------------------------------------------+
```

```
|                                                  New tool for your Web!  |
|    Host / IP: _____________________ [ View                                |
|                  info ]                                                   |
|                                                                           |
|   Host Name:  gpftor3.privacyfoundation.de                                |
|  IP Address:  62.141.58.13                                                |
|     Country:  Germany germany                                             |
|      Country  DE (DEU)                                                    |
|        code:                                                              |
|      Region:  Thuringen                                                   |
|        City:  Erfurt                                                      |
|       Postal                                                              |
|        code:                                                              |
|      Calling  +49                                                         |
|        code:                                                              |
|   Longitude:  11.0333                                                     |
|    Latitude:  50.9833                                                     |
+---------------------------------------------------------------------------+

Add to Google [IMG] [IMG] [IMG] [IMG][IMG] [IMG][IMG][IMG][IMG][IMG]
[IMG]
```

I have to tell you that I did not suddenly move to Germany to write this, this is what the website see's my TOR traffic as. You will also note that I did not setup the links proxy options (which you could do) I just used proxychains. Now as much as all of this is fun, what does this mean for my questions about a single source? Well, like I said this can be used with a lot of normal attack tools, for example (using a host people are ALLOWED to scan)..

```
# proxychains nmap -sT -PN -n -p 80 scanme.nmap.org
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-24 15:41 EST
|DNS-request| scanme.nmap.org
|S-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| scanme.nmap.org is 64.13.134.52
|S-chain|-<>-127.0.0.1:9050-<><>-64.13.134.52:80-<><>-OK
Interesting ports on 64.13.134.52:
PORT   STATE SERVICE
80/tcp open  http

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

# proxychains ./whatweb scanme.nmap.org
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| scanme.nmap.org
|S-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| scanme.nmap.org is 64.13.134.52
|S-chain|-<>-127.0.0.1:9050-<><>-64.13.134.52:80-<><>-OK
http://scanme.nmap.org [200] md5[b2a24d35ffb001ed815a41578134bd46], server-
header[Apache/2.2.3 (CentOS)], title[Go ahead and ScanMe!]
```

Now the bad news. TOR is a socks proxy and proxychains works, but there are still some things that do not play nice. For example, the NSE scripts did not like this setup, and in some brief tests httprint and nikto did also not

play well with this setup and I am sure there are others. Another drawback is the speed. TOR is not blindingly fast, in fact it can be very, very slow when trying to access ports that may be closed.

But even so. We can see that a single person can use TOR to launch many normally used tools against your network, and TOR by it's nature makes many of the normal defenses at best, useless and at worst, dangerous. You see, TOR by default does retrys for ports it cannot connect to, you will see this in your TOR log files..

```
 [notice] We tried for 15 seconds to connect to '[scrubbed]' using exit 'AoF'. Retrying
on a new circuit.
 [notice] We tried for 15 seconds to connect to '[scrubbed]' using exit 'bach'.
Retrying on a new circuit.
 [notice] We tried for 15 seconds to connect to '[scrubbed]' using exit 'p0x'. Retrying
on a new circuit.
 [notice] We tried for 15 seconds to connect to '[scrubbed]' using exit 'xpdmSaphira'.
Retrying on a new circuit.
```

Now what this means is that if you automatically blacklist ip's, then TOR will just start trying from another circuit automatically. Nice for the attacker, bad for the defender. The defender will end up automatically blocking very large swathes of the internet. And if you have tried to be smart by only blocking for a little while, then you have actually not really down anything against an attacker using TOR. It becomes very difficult for a defender to trust the source ip's that attacks may be seen as coming from. Basically, using source ip's as your data point of choice to decide on defenses is not valid. It is now a requirement for a defender to start thinking - is there a trend? is there a single purpose? what is the timeline? are there corresponding events?

Is this more difficult? Yes. Will this always work? Not sure. There is no nice simple technical silver bullet, this requires thought, focus and dedication. But regardless, there is a new reality and we need to be aware of it otherwise we start to become candidates for this:

> *Insanity: doing the same thing over and over again and expecting different results. - Albert Einstein*

.