

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Privacy and Security Through Applied Network Routing](#)

Armada - May 18, 2015, 12:39 am

Introduction:

In this article I am going to discuss privacy and security through correct use of Applied Network Understanding and Theory.

Whats all this actually mean?

- The principal concept in this article is to demonstrate through correct use of networking you can reduce your real time foot print within the network, making it more difficult to trace to your originating IP#.

So, lets start with an A-Typical Network Scenario.

Figure 1.

[img]<http://imgazer.imageshack.us/a/img911/7281/d58E4D.png>[/img]

As we can see, we have the basics of Internet connectivity.

Although networks can vary greatly in configuration relating to connected devices, and/or network topology, I have created what we would Generally see in a Home network environment.

For connectivity, we have Our High speed (assume cable) modem, a Router w/ Wireless 802.1 connection.

And a couple of machines connected.

- As you will see I have designated a Laptop as the Specific "Hacking terminal"

I generally assign one specific device to all of these purposes. I highly recommend if you have the resources to do the same. Separating your activity (Especially when it could be considered, questionable) is always a great protocol to keep to.

For discussion purposes we are going to use a Botnet as the example of the "Hacking" being done. (I chose this as it seems to be the most popular desire for new Hackers.)

Figure 2 - A-Typical Botnet

[img]<http://imgazer.imageshack.us/a/img673/6995/jw2exp.png>[/img]

Now, Here is where we have to get technical.

The A-typical configuration or process to utilize this botnet would be as follows.

User 1 Uses Hacktop on Home Network to connect to the Command and Control Server of the botnet.

User 1 utilizes the botnet for whatever desires.

User 1 disconnects from C&C server, goes on about business.

This in general is a standard. Its how connectivity works.

However there is a fundamental flaw to Direct connectivity.

It leaves a direct path back to your originating IP#.

There is no way to sugar coat what is to be said next, so I will outright say it.

Do NOT fucking do this shit[/b]

[img]http://imageshack.com/a/img540/8425/0Osocs.png[/img]

Wait, What?

"But Armada, I need to connect to the C&C server to use the botnet"

- Of course, but do you REALLY need to connect directly?

No, and you never should.

So, how do we connect to our C&C safely and without leaving too many foot prints to our true whereabouts?

Well, this is where the understanding of solid technical foundations of networking comes in to play.

Let start by addressing the fact, that to reach ANY destination point, the technical back end routing can have numerous, if not thousands of possible routes to the destination.

Example:

User 1 uses computer at home network to access google.com

Depending on the exact network conditions at the point of making the request will determine how the network routes the request to the requested server/service, and further what the path will be taken to reach the destination.

User 1 Lives in Houston, TX.

Google Web Search Servers are Located in California.

Depending on what is happening within the Network (When I speak on the term "Network" I in fact am referring to the Internet as a whole) It will determine if User 1's web request to google get routed through New York's central hub, or Florida's, for example.

The end User will never really notice this as regardless of routing, they will ultimately get to their destination.

Sample exercise on routing:

Spoiler ([Click to View](#)) Open Command prompt, and type the following:

Code tracert google.com
tracert will now follow every destination/connection from your home machine to googles web servers. (In specific the load balancer on their end)

Try this every couple days, and note if the path ever changes. when it does this will indicate the original or first path taken is no longer the most efficient path for you at that current time.

So now that we have a basic understanding of Internet routing. How DO we actually make connectivity to a questionable resource like a C&C for a botnet?

Well, there are numerous methods to make the connection secure, but the most viable methods all boil down to the simplistic principal, You need a relay within your path to redirect the connection,

and the relay must have 1 critical configuration.

- It can not keep connection logs.

So what are you really talking about here? Stop it with this technical gibberish.

Put in plain text, I am talking about either a VPN tunnel or Socks5 Proxy connection which will not hold connection or session logs.

VPN tunnels are the absolute best recommendation if possible. As it will pipe ALL connectivity between the originating machine and the destination targets through an encrypted data stream.

YES

[img]http://imageshack.com/a/img537/3438/XtZM2m.png[/img]

Armada Recommended Configuration

[img]http://imageshack.com/a/img661/6523/62oQBY.png[/img]

To Explain in detail my Recommended Configuration.

I would firstly connect to a Virtualized Server, This server is where I would keep any licensed hackware which would require a call home or traceable functionality to it.

I never run Hackware on my own personal terminals. Its bad practice, Mokay.

Using a VPN tunnel to reach my Virtualized Hacking Terminal gives me shielding layer #1 - A securely routed connection to another originating IP#.

From my Hack terminal (The VPS) I then utilize a second VPN to make any direct connections to C&C servers, infected terminals or other such servers or services.

Using the VPS terminal and a second VPN (Separate company/provider and location than the first) also creates a secondary level of protection. If one VPN proves to be insecure, you have the VPS server (configured to not keep logs) as a level of protection from any nosy people from sourcing your originating IP#. and the First level of VPN protection.

By Using a VPS server for your hackware also gives you what many in the legal community call "Plausible deniability"

If the software is never located or seen your personal hard drives, it gets much harder for legal authorities to PROVE you were responsible for use of any said or questionable applications.

Conclusion:

I sat down and wrote this article for the primary reason, of new users need all the advantages they can get.

As a new comer to the Hacking scene, I can only say, when I grew up learning this stuff, the Network and technology was much different, much safer, and nowhere near the "Big Brother" type of monitoring we have going on now a days.

It is exceptionally risky for a new user to learn the techniques of the Hacker trade for the main reason, as a new user this is the most likely time when you will make a critical mistake, which could result in legal ramifications. It is important to understand how to protect yourself by correct applied knowledge of routing and general networking.

Time it took to write this: 2 hours roughly
Ability to give a new learning Hacker the opportunity to stay out of Hand cuffs: Priceless.

Regards to all. ?

Psst. Check out my other thread discussing Hackware licensing systems [Here](#)

<http://imgizor.imageshack.us/a/img913/2453/ELMK8l.png>

The_Defiant_One - May 18, 2015, 1:07 pm

Some interesting stuff here. Thanks for taking the time to share!

xxleonderpxx - August 29, 2015, 4:13 pm

Nice, I hope everyone doesnt get mad at me for necroing but this is a seriously good post.

Thanks for writing it armada.

?Cyber - August 29, 2015, 4:13 pm

Great thread as always, doing a great job un-skidding these kids

CrypteMyJar - September 2, 2015, 4:52 am

Thank you very much my friend.

inkbird - September 15, 2015, 7:10 pm

Great article. I tried clicking on the link at the bottom to download the .pdf but it seems to be broken.
Can you please update the link? I would love to have this saved as a reference
Thanks