Introduction:
This is a tutorial on chaining proxies for the use of becoming more anonymous while online. There aren’t enough tutorials online about this subject so I decided to make an attempt at writing one. Since it’s on the subject, I included a section on chaining wingates to become anonymous on telnet.

I’m going to assume that most of you have already used a proxy before to hide your real IP address or domain or maybe just used one to surf anonymously online. If you didn’t, well hopefully you can keep up and possibly learn how to use a proxy. Its also best if you know what an IP address or Domain is first, before reading this tutorial. Hmm, I guess I have to show you where to find a proxy too. Well I find that good, updated proxy websites are…

http://www.multiproxy.org/anon_list.htm
http://tools.rosinstrument.com/proxy/

It will be up to you to figure out which ones work or not. I’m not going to do all the work for you icon_smile.gif. You can check and see if the proxy works by going to http://www.privacy.net to see if your IP address changed.

Proxy Servers
A proxy is a server that acts as a gateway between your computer and your destination (website, IRC chat, etc.). These proxies receive requests from users to view, for example, a web page. The proxy will then forward the request to the internet, find your requested page, then send the web page back to you, the user. Most proxies come with a cache (sounds like “cash”) feature that saves former websites that were visited on that proxy. Think of cache as a proxy’s storage room. Each site that you make the proxy visit, it saves in its own storage area (cache). So if the user or someone else requests the same site again later on, the proxy will go back into its cache, find the web page and send it back to the user. This saves time because the proxy doesn’t have to go search the Internet for the web page. It just pulls the site out of its cache.

The use of proxies to stay anonymous is a favorite thing to do among people on the Internet who are either paranoid or just security conscious. The anonymity factor comes from the proxy’s ability to hide your true Internet address. For example, if I were to run a scan on your computer right now, I would get the Internet address that was given to you by your ISP (internet service provider), but if I were to scan you while you were using a proxy, then I would get the Internet address of the proxy server. Basically the whole proxy picture looks like this…

[User]>>>>>[Proxy]>>>>>[Web Pages]

Simple enough, right? Right. So now let’s get to the chaining part.

Proxy Chaining
Proxy chaining is merely connecting to more than one proxy and then to your intended destination. You can use as many proxy servers as you can or want. The more you have, the more anonymous you will be. Remember, it doesn’t matter how many proxies you chain together, you will never be 100% anonymous. Let’s look at an example…

[User]>>>>>[Proxy1]>>>>>[Proxy2]>>>>>[Proxy3]>>>>>[Proxy4]>>>>>[Destination]

The example shows that for a proxy chain to be created, the user must first connect to Proxy1. Once the user is connected to Proxy1, from Proxy1, the user will connect to Proxy2, from Proxy2, the user will connect to Proxy3, from Proxy3, the user will connect to Proxy4, from Proxy4, the user will then connect to the intended destination (web page, Unix server, ftp server, etc.). All together we have 4 proxies in this example. Each proxy is a link in the chain. If the user would be scanned while on the proxy chain in the example, the IP address or domain of Proxy4 would appear on the scan. Now the problem with proxies is they tend to "die out" in a few weeks or less. It all depends. So if Proxy2 were to cease functioning, the chain wouldn't work. You would need to get rid of Proxy2 and just use Proxy1, Proxy3, and Proxy4 or find another proxy to take Proxy2's place. This is why proxy chaining can be a real pain if you are using them just to surf the net. If one dies, you have to figure out which one is the one not working, so you have to go through each one to check them or until you find the one that isn't working.

Proxy chaining is a necessity if you plan on using proxies to execute a "hack". If you are attempting to gain unauthorized remote access to any server, whether it is through telnet, ftp, or http, chaining is a must. As I said, you will never be 100% anonymous no matter what you do online so it is possible that you still can be tracked even if u chain proxies. Chaining just makes it a lot hard to track someone. To make it even harder, its best to use foreign proxies because if someone wanted to trace you, they would need to get logs of your use of each proxy from each proxy administrator. This could take quite a while or even never at all if one of the proxy's, or all for that matter, belong to an admin in a country that isn't too fond of the country you are located in. The longer it takes for the authorities to subpoena the logs of your usage of a single proxy from that proxy's administrator, the more chance that the other proxies that you used in the chain will have their logs deleted by the time anyone gets to the server administrators of those proxies. So when attempting to do any kind of "hack", it's best to use at least five or six proxies in a chain.

HTTP Chaining
HTTP chaining is basically chaining a proxy server in your browser's address bar. Example:

http://proxy.magusnet.com/-_-http://www.google.com

Notice how the above proxy and destination (yahoo) are seperated by a (-_-) If you wanted to make a chain out of this you would simply add another proxy ex. (http://proxy.server1.com/-_-http://proxy.server2.com/-_-http://www.destination.com)

Another way to use proxys in your address bar is by adding the proxy IP or domain then the port number. Example…

http://anon.free.anonymizer.com:80/http://www.google.com

Notice how the above proxy and destination server are seperated this time by a (/) forward slash instead of a (-_-) dash, underscore, dash. To make a chain out of this you would again simply add another proxy ex. (http://proxy1:80/http://proxy2:80/proxy3:80/http://www.yahoo.com)

Browser Chaining
To browser chain is fairly easy. I'll use Internet Explorer as an example since I believe it is the browser that most people have and use. First you need to find the Internet Options. You can do this by either finding the Explorer icon on the desktop, right click on it, then press properties or if you have a browser window already opened if you are online then you can go to Tools (or sometimes its View) and press Internet Options. Now that you have the Internet Options window up you can now go to the Connections tab, then go to the first Settings button (not LAN Settings, the one above it) and click it. Now you should be in the Settings box. Put a check in the box where it says to Use a proxy server. Now if you wanted to surf using one proxy you would merely put the proxy in the Address: space and put the proxy's port number in the Port: space. To use a chain here you would put in a proxy along with a ":" colon then the port number followed by a space separting the next proxy then a ":" colon then the port number then a space and so on. The last proxy you add should have its port number placed inside the Port: space. If you did it, then it should look like this exactly…

Address: 213.234.124.23:80 121.172.148.23:80 143.134.54.67 Port: 80

Notice that each proxy:port is separated by a space and that the last proxy has its port number placed in the Port: space. Do not check the box marked "Bypass proxy server for local addresses". Press OK when you see that everything is in working order

Wingates

A wingate is a proxy server that someone installs onto his/her computer which allows for a single or multiple online connection to take place through port 23, the default telnet port. Depending on their security, some wingates will allow anyone online to connect to them and usually stay “alive” or “working” anywhere from a few days to even months. There are people out there that scan for these Wingates and post the computer’s IP number or domain on their website to give anyone online a free list of them to use. You can also scan them yourself by using programs like WinScan.

Chaining Wingates Using Telnet

I’m going to assume you already know what telnet is so I will just get right down to it. To chain using telnet, you would first bring up the DOS prompt and type in “telnet” then your wingate. (Since telnet’s default port is 23 and all wingates run on port 23, the port number is not necessary but I will add it just to show you how you should type any port number out on screen) Example…

```
C:\WINDOWS>telnet 61.133.119.130 23
```

So now you have “telnet”, a space, the wingate IP, a space, then the port number 23. Once you are connected to the wingate it should look like this…

```
Wingate>
```

Now you would type your next wingate and port number in, then press enter like so…

```
Wingate> 203.207.173.166 23
```

You can continue to do this until you connected to as many Wingates as you need. Once you are finished with your wingates you would connect to your destination. Example…

```
WinGate>arbornet.org
```

So now the entire picture would look something like this…

```
C:\Windows> telnet 61.133.119.130 23

Wingate>203.207.173.166 23

Wingate>135.245.18.167 23

Wingate>m-net.arbornet.org
Connecting to host arbornet.org...Connected

Welcome to the Once and Future M-Net
FreeBSD 4.3 (m-net.arbornet.org) (ttypv)

Enter newuser at the login prompt to create a new account
Enter upgrade at the login prompt to find out about increased access

login:
```