SSH - DYNAMIC FORWARDING

We have already gone through how to do port forwarding with ssh (here), and that in itself is cool. But ssh has another trick, dynamic port forwarding. You see ssh is capable of functioning as a socks proxy. And thus, can forward any number of ports needed by a socks aware application through that setup. Very nice, and yes I can see how that could also be very nasty, but lets focus on the positives.

What is needed?
First you need an ssh client which you want to use as a proxy, and the ssh server which you want to use as a gateway. Lets use an example, you are attending Defcon, one of the most hostile networks you will ever come across. You will not want to send anything out unencrypted, at all. So your machine (lets call it *Small-Bob*) connects to your ssh server on your network (lets call the server *Big-Bob*) and sets up a local port as a socks server port, so all your socks-aware apps are thus encrypted. You would do this by going..

```
Small-Bob# ssh -D 4040 root@Big-Bob
```

That will make port 4040 on *Small-Bob* your socks proxy port. So if you point your application to it, all your proxied traffic to your proxy, and all traffic from proxy back to you, will be encrypted (if, for whatever reason, you wanted to allow others to use this socks proxy, add the *-g* option to the above command).

Now in order to use a socks proxy, you need an application that can "*talk*" socks. Most proper internet capable applications have "*socks'ified*" variants. Take firefox for example, just setup a proxy under "*network connections*" in "*options*" (this location may differ from version to verison, but the setting is still there so look for it) and change the socks setting to "127.0.0.1" and port "4040". And that is pretty much it. One gotcha though, ssh v2, when used as a socks proxy, uses socks v4, so just keep that in mind when setting your connection options.

Now windows can use this as well. You can use putty as the ssh client which will setup a local port as a socks proxy, so even if you have to use a windows machine, you can still make your traffic secure.

Final Words
Thats it. Short is'nt it? While the method of setting this functionality up is simple, never forget that the usabilty and application of this functionailty can make a lot more of your public traffic more secure (even if it can also be used to "escape" from restrictive firewalls). So definitely play around with this, have fun and learn.