Cable Modem IP Hijacking in Win95/98

The purpose of this is to show you how bad cable modems security is and that even with a win box you can take someone else's IP. You can hijack IP's using a cable modem and it's very simple in any operating system. Just follow the steps:

1) Choose someone's IP that you wish to have. Make sure the IP is on the same network. Most cable modem providers use DHCP. The fist thing you have to do is find the victims IP. Remember the victims IP has to be in the same network and with the same service provider for this to work.

2) Now this is probably the hardest thing in this file (but it's still easy), you have to wait until the victims computer is off or you can Smurf kill his connection. When you think his computer is off-line just try to ping it to see if you get a response. Do this by going to a DOS prompt and typing "ping <victims IP>". If you get a response then you have to try harder.

   After you get his PC off-line then you go into your network properties and edit the IP settings, but instead of having yours there you put the victims IP, host, and domain.

3) Restart. If you restart and you get an IP conflict this means that the victims computer is on, if you don't get an IP conflict then try to go to your web browser and see if it works. With some cable modem providers you might have to also add the Gateway, Subnet mask (255.255.55.0), Host, DNS search, and Domain.

Now you can go. Everything will work until the victims PC is back on. Once it is back online it will take the IP away because it will tell you that you have the wrong Mac addresses.

Linux
This is also possible in Linux, but is not the best way. You can change your Mac address to the victims PC and this is more secure and much easier. There are a couple of scripts to change your address, just look around.

Warning: Some cable modem service providers will know when you're using the wrong IP, but hey, it might be useful.

Copyright (c) 1999 Wildman

www.hackcanada.com