Spoonfed Hacking

This guide, written by me, glj12, is a fairly comprehensive tutorial that covers various methods that involve hacking particular types of "victims." I do not take any responsibility whatsoever if you choose to follow through the provided methods on non-accepting candidates.

But before we go any further, allow me to quote what a hacker actually is; "Among some computer programmers in good standing with the technical community, the words *hacker* and *hacking* are used more often in the admiring or awed sense of a skilled software developer. People favoring this usage typically look with dismay on the usage of the term as a synonym for security cracking.

In the non-technical community, the word *hacker* most often describes someone who "hacks into" a system by evading or disabling security measures." I tend to view the word as a person who is capable of cleverly resolving any given problem, aka, the ultimate critical thinker. Please ignore all statements made by the media that claim a 'hacker' to be that 'bad man' behind his computer. The following methods display acts of security cracking. Enjoy, and please remember the prior agreement in terms of usage of the provided knowledge below.

Anyway, let us continue, shall we?

There are two methods of hacking; locally, or globally. There are an infinite amount of subsets to the following ideas, but let us cover as much as we can. Let us start off with the first scenario.

Local Hacking

This method normally consists gaining access some way or another via the intranet. Let us test the following method.

-Wireless Hacking

Let us set up a scenario here. You are eager to gain access to a non-specific, (or specific, if you have an apparent grudge with a mean neighbor) to a local computer. Here are the tools needed to gain access before we go on our mission.

-Laptop with dual boot, (preferably Knoppix for Linux, and the second boot being Windows XP Pro)
-Aircrack-ng on the linux box
-Supported wireless card for injection to work properly
-Enough battery life to serve you well
-Kismet or netstumbler, (to each his own, preferably Kismet for Linux so you do not have to reboot back and forth so often)

Part 1

1. Start up your laptop into Knoppix. Download aircrack-ng, (any version will do). Install anywhere, follow the easy instructions. Basically, you open up a shell, su to root, cd to the directory of aircrack-ng, type make, then make install, etc. Very comprehensive instructions are found within the downloaded folder.
2. Thereafter, type apt-get install kismet
3. Should install kismet nicely, fairly easy, just follow the y/N questions provided when downloading/installing through the shell.

4. Now, type: cd /usr/bin/kismet kismet (or wherever it may have been installed).
5. Kismet will eventually load, and pull up a fairly primitive color GUI within the shell that shows all access points within your designated area, constantly being updated.
6. After selecting your target, find out by kismet if it is WEP, WPA, etc. Preferably, WEP 64 or 128bit.
7. Now, the fun begins. Open up a few tabs within the shell. Now type each line in each new tab. Everything within the parenthesis entails exclamations in terms of what it means, syntax, etc).
8. `iwconfig wlan0 mode monitor` (This places the wi-fi card in monitor mode; Syntax: iwconfig device_name_here mode command_monitor)
9. `airodump-ng --ivs --write file_name --channel 11 wlan0` (Starts the monitoring, collects weak IV packets. Syntax: airodump-ng –ivs_creates_extension_type –-write any_given_filename_here –channel this specifies any specific channel you wish to listen to, so you can filter out any unnecessary data).
10. `aireplay-ng -3 -b 00:16:B6:2E:C3:4E -h 00:14:A5:8A:02:CD wlan0` (Stimulates packets; injection. Syntax: aireplay-ng -3 attack level -b BSSID of router goes here, shown by kismet -h the attached computer to the bssid; the router wlan0=device that you are using, remains consistent).
11. `aireplay-ng -0 wlan0 -a 00:16:B6:2E:C3:4E wlan0` (This is the deauthentication attack. Aireplay-ng -0 attack number wlan0 device type of yours -a BSSID goes here again wlan0 repeat your device here, yet again).
12. Now, watch the magic happen. To put it in layman's terms, MANY numbers will appear to be rapidly increasing. Within the airodump-ng tab you had opened, the SSID of the attacked victim will increase quite a bit. Look under the IVS column to view how many you have saved to the file. Let's for now on call this default victim SSID. Once the number hits 250,000 (if it is 64-bit encryption) or 1,000,000 for 128-bit, you will be able to execute your cracking method on the IVS file you have been continuously writing.
13. Cracking time! Cd to the directory that the file you have been saving. Then, execute the following: `aircrack-ng -0 -n 128 -f 4 file_name.ivs` (Syntax: aircrack-ng -0 attack type -n number of the encryption type, 64 or 128 -fudgefactor 2-18 *.cap or *.ivs depending on what filetype you decided to save your file as while gathering packets).
14. After a minute or two, (possibly less) you will have your hexadecimal password so now you can connect to your noob, erm, I mean 'victim's' router.
15. Reboot your computer after jotting down the hex code, and log into your winbox on the same laptop.
16. I would recommend to now set up your 'anonymous tools.' I would suggest doing the following; download a program that IronGeek and I wrote that spoofs your MAC address and your netbios each time upon startup. It is entitled MadMacs, and may be found at irongeek.com. Execute it, and reboot back into Windows.
17. Connect to SSID, and input the hex code twice as required.
18. Hopefully, if you did not screw up, you will be connected.

Part 2

Now that we are connected, we may now try a few methods of attack. Of course there are many, but allow me to test a few, and you may choose the one that best suits your situation.

Now that you are apart of the network by accessing the router, we may go back to the lovely command prompt, but this time within the Win32 environment. Open up the command prompt and type: ipconfig, so you can gain information about what the router gateway is, and what your IP is automatically assigned as, (such as, 192.168.1.XXX, or 172.16.1.XXX. Simple rule of thumb is, if it is a 192 prefix, then the router address will most likely be 192.168.0.1, and for 172, it will be 172.16.0.1). So, write down the default gateway, and paste it into your browser with http:// infront of it. Odds are, there will be a password. Considering yourself lucky if it does not require one. Second best bet is going to http://www.phenoelit.de/dpl/dpl.html, which lists all of the default username and passwords for each model number of a router out there that may be purchased by the public. If all works accordingly, now you will be able to poke around with all of the glorious settings, such as opening the ports, which is the MOST important thing to hold onto. We will discuss this later.

Let us poke around and try this method of attack. Go back to command prompt and type: net view. This will display all computers connected on the network that you have so rudely joined. Now, we whip out our handy dandy program called Nessus, (or any OS fingerprinting tool that you may prefer such as, GDI, etc). The point of this is to find out what OS is on each local intranet IP address. Now, as we all know, Windows XP Pro is the sweet OS. Why, you may ask? By default, XP Pro comes with remote registry enabled by default. I ask myself why everyday, but why not profit from Microsofts flaws. Also, no, you are correct, noobs do not disable this service. This may be time for you to turn off yours by going into services.msc. ;) So, let us proceed while ignoring that last sidenote. Open up your registry editor, regedit. Click File>Connect Network Registry. Follow the directions, click connect, etc. Now I know that you are thinking to yourself, we are riding on a lot of hope/faith here that everything the victim does fit's our needs. Well, yeah, duh. ;) This is why this is the 'non-preffered' method of choice. But its the, snowballs chance in hell, so 'never going to happen you have to try it anyway' method. Let us proceed. Now, browse to the `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server.` Under the Terminal Server key, you'll find a `REG_DWORD` value named `fDenyTSConnection`. Double-click on that value to open the `Edit DWORD` Value box and change the value data from 1 (Remote Desktop disabled) to 0 (Remote Desktop enabled). To reboot the machine if you are impatient, go back to the command prompt shell, and type:

```
shutdown -m \\servername_or_ip_of_server_here -r
```

Ah, now wait for the glorious boot up. If all goes accordingly, you will now be able to connect remotely to the noobs desktop, and do whatever the hell you want. Seriously, do I need to go into FURTHER detail!?

More plausible method

Let's say you are currently connected locally to the same access point, and are eager to try another form of attack. Now, since we wish to have remote access, let us apply what we call, a 'trojan.' A trojan gives you remote access from another place. So there are a couple of ways of doing this. One, you can download a program called Sub7. This is a VERY well known trojan. To get it, go to: http://www.hackpr.net/~sub7/. Follow the directions provided. Once you have created your server.exe, (tweaked it etc. and renamed it) we can proceed to our next step. Odds are, the noob has several victims on his network with open shares. Probably consists of .txt, .doc, .jpg, etc. files within its open shares. Usually, they are accessed quite often, especially if the document is currently being edited. Your job, (for once) is to google for something what we may call, a '.exe binder.' This is a beautiful tool indeed. It binds the server.exe that you have made, and enables you to spoof it as the picture file or text document that the person has in their shares. Once you spoof this, the victim will eventually execute the file, plus the hidden file that you have stealthily implemented. I would suggest to attach this on as many files as possible found on each computer. This is probably the most direct approach. Remember when you assigned a port to the Sub7 server.exe? Well, this brings us back to the default gateway IP address that we cracked, (accessed) earlier. Browse to the open port page, and add the port you had assigned to server.exe. While you're at it, you can go to a remote place such as a library and spoof send server.exe, (preferably rename it for the following instances to game.exe, or patch.exe, setup.exe. You get the picture. Or apply it to a .jpg as a picture of something random) to the e-mail address that you could have stealthfully acquired while sniffing on the network that you had connected to. (Such as, getting a packet sniffer for windows and waiting for anything that is sent out with an @. This could also be very useful to get passwords, usernames, and so on). Anyway, be creative in terms of getting the server file to some computer on that network. For the time being, go back home, and leave your Sub7 client on, and it will notify you when it is executed. Thankfully, the programmers of the Sub7 are quite brilliant, and have the server.exe copied to some ambiguous directory, without self-destructing itself. Thus eliminating the idea that the file that 'does nothing' is a trojan. Eventually, the victim will connect, and you will have some fun from there.

Method 3 The Destructive Form of Hacking, (my fave!)

Ah, if all else fails, this is what I resort to. Let's be a little bastard, shall we? Say all of the prior methods failed, and you just want to have some fun with these people that you apparently have a grudge against. Go have fun, and open all ports on the router. Let's flood the hell out of it. Go get any sort of program that consists of a UDP flooder, (or TCP) and flood the port that you have now opened on the router. This is amazingly straight forward, and takes pretty much no thought. Just flood the default gateway, plus the given port that you have opened, (or IP of the intranet computer). Eventually, your connection will time out if you do it while connected to the 'SSID' example. So it is best to do it from another host, and be sure to get a port flooder that spoofs your IP. Use your elite Google skills. :) So where was I? Ah, yes, flooding. The router will eventually die from massive packets per second, and their connection will be terminated until they decide to reset their router. Now wasn't that fun? I always prefer that method, it is the easiest, and consists of the fastest instant gratification.

Global Hacking – on a 'Personal' Scale

In terms of 'global hacking,' you may, for obvious reasons, skip the wireless hacking part. On a global scale, it may be someone that you know on an instant messenger on ICQ or AIM, etc. Or, it may be some random person on an IRC that ticks you off. All you have to do is cleverly bind the server.exe as mentioned so many times before and send it as a picture via an instant messenger, or whatever you please. Same goes for DCC on an IRC. You do the math. Use your enginuity.You could also apply the port flooding mentioned mentioned earlier if one obtains the user's IP address, then follow from there. In terms of AIM or any other instant messaging service, coax him/her to direct connect to you to 'send some pics, etc.' Use your social engineering skills, which are useful in any 'hacking' situation. Once you are DC'd, open up the command prompt and type: netstat -a to view the victim's IP address. For IRC, just right click on the user's name, and hopefully the server will not mask with a random name as opposed to the IP. Usually, the person has to auth with nickserv, (generic command is /msg nickserv IDENTIFY) but as we all know, people are lazy. This is where you take advantage of this. Next step covers your original editing the router configuration, (since you obviously do not have access to this, duh). Whip out your blueport scanner, or superscanner, whatever you can find on Google. Try to find one that limits it from spamming, thus triggering the user/ISP to be alarmed, and feel the need to contact you. BluePortScanner does the best job of this, and does a brilliant job. Now that we have the port, we may resort to the destructive aspect of the tutorial, (as explained earlier). Get a flooder/nuker and spam the specified port while masking your IP, (usually built into the program if you find a good one). It would be funny to make your IP 127.0.0.1, but that's just a thought. :)

Global Hacking – on a Web Site Level

Simply put, do your research about the given site, and cover your rear in the most blatant ways, (spoofing IP's etc). Apply the method above that occurs after the gaining the IP address aspect. Simply get the IP address of the server by pinging it, port scan while spoofing, proceed with the given procedure above, and don't blame me when the CIA comes to kill you. Just throwing that out there.

Scare Tactics:

Say you just want to scare someone who owns a website, and not necessarily hurt anyone, (good call if you choose this, you won't get in trouble!) Get a Linux box up, and open up a shell. Paste the following code in after gaining internet access. This is kind of a lame attack, and if the person has half a brain, may be determined what has actually happened here. You take some website, and plug-and-chug, as they say into the code provided below. Let us look at it, shall we?

```
wget http://microsoft.com/ --user-agent="Mozilla/5.0 (Windows; U; Windows NT 5.1;
rv:1.7.3) Gecko/20041001 Firefox/0.10.1" --
referer=http://I_SEE_YOU!_By_the_way_I_Cant_wait_for_windows_Vista!.com -O
/dev/null sh scarenoobs.sh
```

Copy the supplied string an paste it into a file called scarenoobs.sh. Execute it in a new window, and have fun! But first, you might want to edit I_SEE_YOU! Etc and the website. So what is happening here you say? We are spoofing the refferer is all. The refferer just tells the website admin, (in a log) what webpages have redirected the user to your website. This may be a stealthily way of transporting messages, or taunting web admins who do not have much experience in such a realm. The I_SEE_YOU normally is the refferer site but here, you can obviously change it to whatever you want. If it is a 'warez' site, you could make the refferer http://cia.gov, implying that the website owner is constantly begin pinged/browsed by the CIA. Somewhat absurd, but use your imagination in terms of what it could be used for.

One other way of toying around with a noob's heart would be with the wireless connectivity method. Go get an amazingly simple program, (but brings much joy to us all) called FakeSend.exe. You may find the source code and executable here: http://www.codeproject.com/internet/fakesend.asp. Follow the directions, and send a message from some made up address, and send it to the given address found within net view. Now the user on the other end may find a lovely message that you have written for them. Aw, how nice.

There are so many other methods in terms of 'hacking,' but I will let this tutorial come to an end, and let you, the user, soak in what you have read. If you have any comments or suggestions, please contact me at: glj12 -at- flanga.net. Cheers!