A Quick and Easy Intro to a Pen test

by Trevelyn

ABSTRACT

Penetration testing includes client espionage, port mapping, wireless scanning, password cracking, exploiting OS flaws, and often Social Engineering or “Pretexting.” I will cover a simple sweep of a target network using easy to follow dialog and pictures. Tools and references will be listed at the end of the paper.

This page is left blank intentionally.

Firstly, before we go mashing at our keyboards in Weak-Net we have to find out what we actually want from a penetration test. The methods I will cover will be sort of crude. By crude I mean, if you have a good setup or a good network admin, (like myself ;-) there will be a lot of flags set off from a NIDS or even bogging down bandwidth. And by "what we want," we mean info on the networks topology as well. Is there a wireless access point? If so, is it encrypted? If so, is it WPA or WEP? If WEP, is it 256, 128, or 64 bit? Well, as you can see this is similar to creating a tree like outline for someone who is scripting a movie, and the tree can stem off for ever if we don't get enough clues.

Theres been a lot of talk about Network Penetration testing, and a lot more work being done to let it thrive amongst the IT profession. First I would like to mention the now very popular Linux distributions which boot into RAM, called "Live Distros." There is a very large population of these to choose from on the internet. To name a few: I chose Back|Track>>2[1], NavyNos[2], Operator Linux[3], PHLAK[4], and our very own distro's – GunPointe Linux and Interrogation Linux. The latter two can be booted easily from USB drives if the BIOS is properly configured to do so. But again, the list could go on forever, and if you plan on doing a pen test, we recommend doing a little research on those.

Also, the exploits have given the pen test a good name too. Testing these exploits gives network administrators and large corporations, knowledge and experience in coping or solving their networks flaws. Exploits are a great way to get fast axx[10] (access) to a given machine, if it [the machine] were not patched. And network probes, with tools such as Ping, Tcpdump[5], Wire shark (ethereal)[6], Etherape[7], Ettercap[8], Nmap[9], and such will give you a better idea of what the network looks like physically – like making a map of the networks topology.

Well, i believe i have mentioned quite enough for my purpose of being here, so how about we get down to business?

Getting Access (wireless)

Are you close to the proximity of the network you want to get into? If so, start up Airodump with a network card in “promiscuous mode.” If you have a Laptop, and you downloaded a Linux Live CD with a security flavor, boot into the OS and open a terminal. In the Terminal, if you are not root, type SU. Once you are root, type iwconfig. Iwconfig is included in most Security Linux Live CD's as part of wireless-tools. Here is a quick description taken right from the “man pages” (Linux/Unix manual pages) [11]

DESCRIPTION

> **Iwconfig** is similar to **ifconfig(8)**, but is dedicated to the wireless interfaces. It is used to set the parameters of the network interface which are specific to the wireless operation (for example : the frequency). **Iwconfig** may also be used to display those parameters, and the wireless statistics (extracted from */proc/net/wireless*).
>
> All these parameters and statistics are device dependent. Each driver will provide only some of them depending on hardware support, and the range of values may change. Please refer to the man page of each device for details.

Iwconfig will show you the wireless interface if it exists or if the drivers have been loaded for it. If you don't see it, try Google by searching the model number and the word Backtrack. The Remote-exploit[12] team and forum members have extensive knowledge pertaining to wireless LAN cards and drivers. The card will have a name off to the left of the description given by iwconfig, such as wlan0, rausb0, ath0, wifi0, or sometimes even eth0 for wlan cards with orinoco based chip sets Get the name, and type ifconfig <name> up. Then, type “iwconfig <name> mode monitor. Or if you have a good security based distro, try airmon-ng start <name>. Then run airodump from the aircrack suite[13] by typing “airodump <name>”

Airodump is a great tool for wireless network analysis. Tons of valuable information gets sent through the air within packets if there is a wifi AP. It lists the clients using the AP (axx point) it lists the clients MAC (media axx control addresses) addresses, and the AP's MAC address. Even if there are non associated wifi cards within the proximity, they will be constantly probing for networks they were once attached to! So don't be confused if you see a laptop trying to authenticate and associate with an ESSID (extended service set ID) called “Grandma's House” nearby. Here is what a typical airodump screen looks like:

This was taken in Weak-Net Labs. The BSSID's are the MAC addresses of the axx points. The PWR shows the power or "proximity." The Beacons are the packets received from the time you started airodump. The "#Data" are the IV's (Initialization Vectors - first 24 bits of non-encrypted data in packets). "#/s" is PPS (packets per second) The CH is the channel or frequency in the 802 band used by the AP. ENC shows the encryption type. CIPHER shows the cipher used to make/break the encryption. AUTH shows the authentication type, and ESSID is the (case sensitive) name being broad casted by the router or AP.

The lower portion of the screen gives the same info basically but for each client. Probes are being made by station 00:19:84:1b:ee:a5 to "telco-mobile" a router we used to use for practice. That's a boat-load of information gathered from only a 56 second duration of airodump. If you see your target here, you can try to attach to the network by setting up your card in iwconfig. If the AP is encrypted with WEP you can crack it using the aircrack suite minus the aircrack part. We say this because of the emergence of aircrack-ptw.[13.5] The latter tool uses a more efficient algorithm to breaking WEP needing less data and less time from your part.

I will cover a quick how to with aircrack now, to get into a network that has been encrypted by a genius admin. Start airodump. Airodump will log all the packets you discover to a file with a prefix of your choice and an extension of "cap." Here is an example of how to get airodump to log to a file called "h0h0"

airodump -c 11 -w h0h0 –bssid DE:AD:DE:AD:DE:AD

This not only creates the file "h0h0.cap" but also *only* reads from channel 11, and packets associated with my victims AP MAC address DE:AD:DE:AD:DE:AD. Airodump has turned out to be an extremely useful tool so far. Then, Aireplay will provide you with packet forging capabilities, allowing you to de-authenticate clients, associate and authenticate with the AP, and even catch an ARP (address resolution

protocol) request and then replay it over and over until you get the information needed to break into the network. Here is a quick and dirty hack using aireplay to get an ARP request:

```
aireplay -1 0 -a DE:AD:DE:AD:DE:AD -h 00:11:22:33:44:55 -e “Weak Net Labs” ath0

aireplay -3 -b DE:AD:DE:AD:DE:AD -h 00:11:22:33:44:55 -e “Weak Net Labs” -x 1024 ath0

aircrack-ptw h0h0.cap
```

That is basically telling the machine to make the WLAN card send a forged packet to the AP pretending to be a client. Then make the card await an ARP sent by the AP, and replay it until you get at least +50k IV's. You *have* to set the card to be on the same channel as the AP to associate and authenticate with it. This can be done by adding more info to airmon-ng.

```
airmon-ng start ath0 11
```

And that's it. Once you get 50+ IV's you can get the key. Now, to attach you have to put the card back down. and then back up with the following syntax, again using iwconfig.

```
Ifconfig ath0 down

ifconfig ath0 up

iwconfig ath0 mode managed essid <ESSID> key <WEPKEY> channel <CHANNEL NUMBER>

dhclient ath0
```

or:

```
dhcpcd ath0.
```

then once the gateway is listed:

```
route add default gw <AP IP>

echo 'nameserver <AP IP>' > /etc/resolv.conf
```

win!

If your victims AP is encrypted using WPA, you must get a handshake within your .cap file. A “handshake” is performed when a wireless client attaches to the network using the WPA pass phrase. This can be easily sniffed, and in *some* cases, artificially provoked. To get a handshake check the lower portion of the airodump

screen for wireless clients. The use aireplay to de-authenticate one of them.

```
aireplay -0 10 -a DE:AD:DE:AD:DE:AD -c 00:11:22:33:44:55 -e “Weak Net Labs” ath0
```

This sends a forged deauth packet to the MAC address of 00:11:22:33:44:55 that is associated currently with the AP with the MAC address of DE:AD:DE:AD:DE:AD with an extended service set identifier of “Weak Net Labs” (don't forget that it is case sensitive)

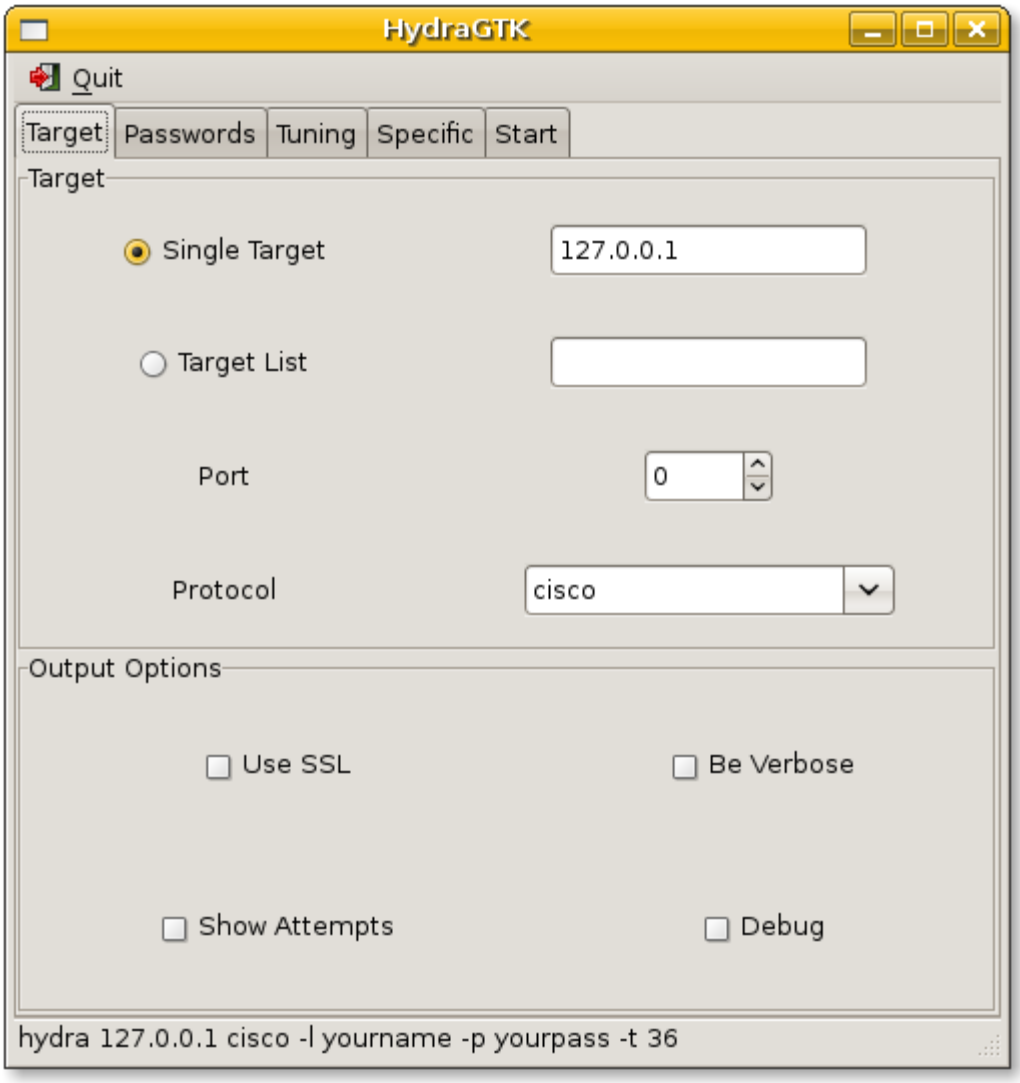
Then you have to do a dictionary brute force attack on the cap file. This is done using aircrack-ng not *-ptw. You need to get a word list from the internet, or if you have a good security distro it should already be there. If the WPA key is a good key then it maybe almost impossible to get the key. I would recommend writing up a quick Perl file that randomly generates a number of characters ranging from three to ten. Exempli gratia: aSd aSdf aSdF aSdfg aSdFg ... inf) This is very easily accomplished with even a small knowledge of Perl.

Getting Access (Wired)

You need to find your victims network gateway IP. A gateway is just as the name applies, a gateway to the internet. The fenced in area the gateway serves is the network. All of the machines are within that fence and then need to go through the gate to get to the internet. Most small networks are behind a gateway that is maintained by say a Linksys router, or a Belkin router. These routers have an option of “remote administration” that should always be enabled in case an attack occurs while the net admin is away, he or she can easily login and check the routers log file, change access restrictions, or even disallow internet axx completely for a small amount of time from him to come back to the network and diagnose what happened.

These admin programs are password protected, and you can use, again, your word list and a program called xhydra[14] to try to crack it. xhydra will try every word in your list and even every login name (usually “admin” for routers) that you specify. This tool is useful in a wide variation of protocols such as: TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, LDAP, SMB, SMBNT, MS-SQL, MYSQL, REXEC, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, Cisco auth, Cisco enable, Cisco AAA (incorporated in telnet module). And works great in our lab too! ;)

Here is a screen shot of xhydra, you absolutely need GTK libs for the xhydra. The console based hydra is very confusing because there is no output from the program, not even with the famous switches“-h” or “--help.”



Also, the router has open ports that are strictly forwarded to the machines intended. So if you can get admin axx to the router you can check the routers interface for maybe a list of DHCP clients. Then forward a few ports to them to run various remote exploits. Say for instance we are using the Metasploit[15] program and run:

```
./msfcli | grep smb
```

We can find a nice little samba exploit, so we would forward say, port 13370 to the IP of the victim machine, at the port 139. Then we could forward the 13370 port in *our* router to our machine, and then Simply give these parameters to Metasploit and cross our fingers.

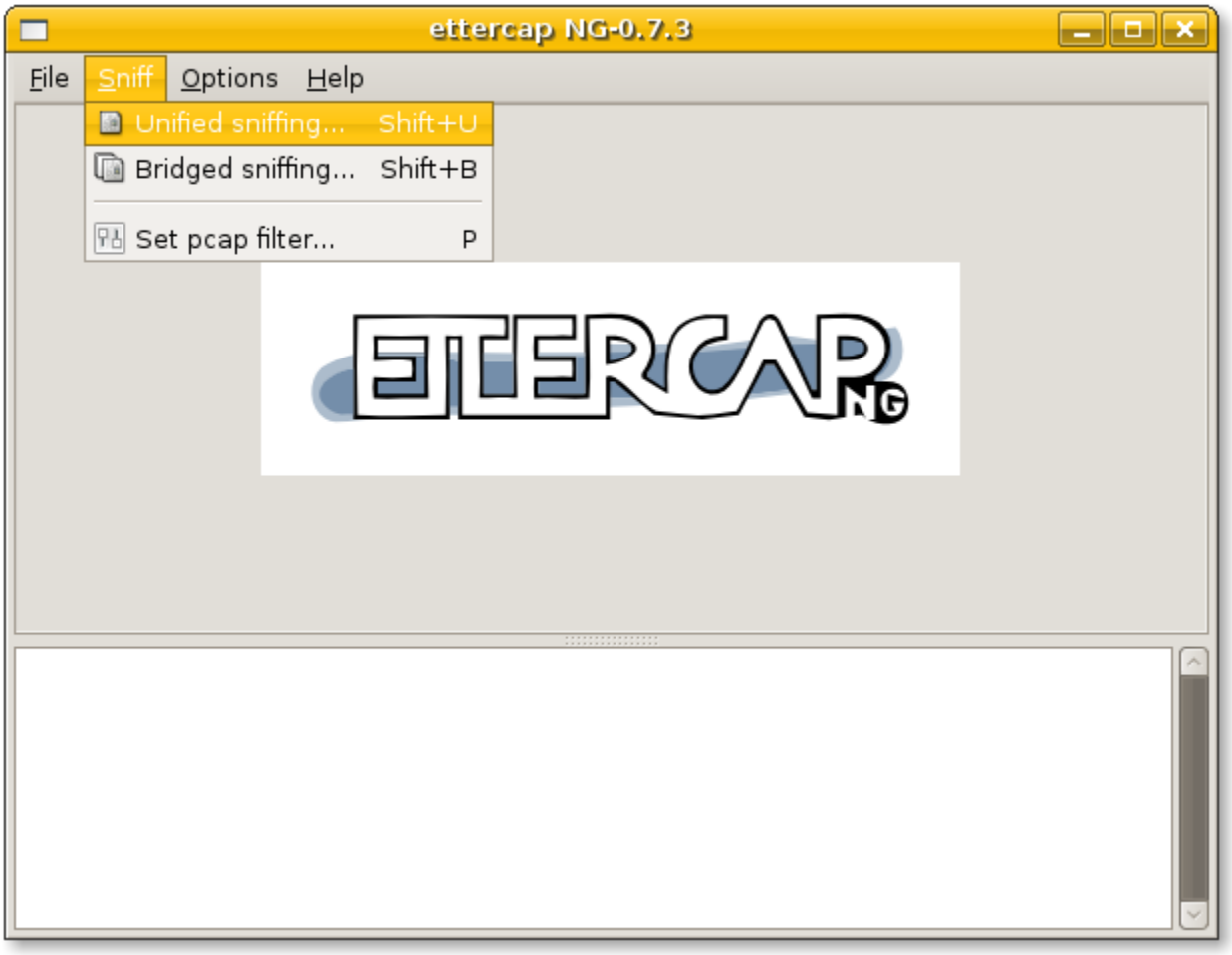
After the break in (from behind the fence)

If you can make your way into the network (congrats if so) theres a few things you must do in order to get individual axx to the machines or for privilege escalation. Personally, i like to open up a console and type:

```
smbtree -N
```

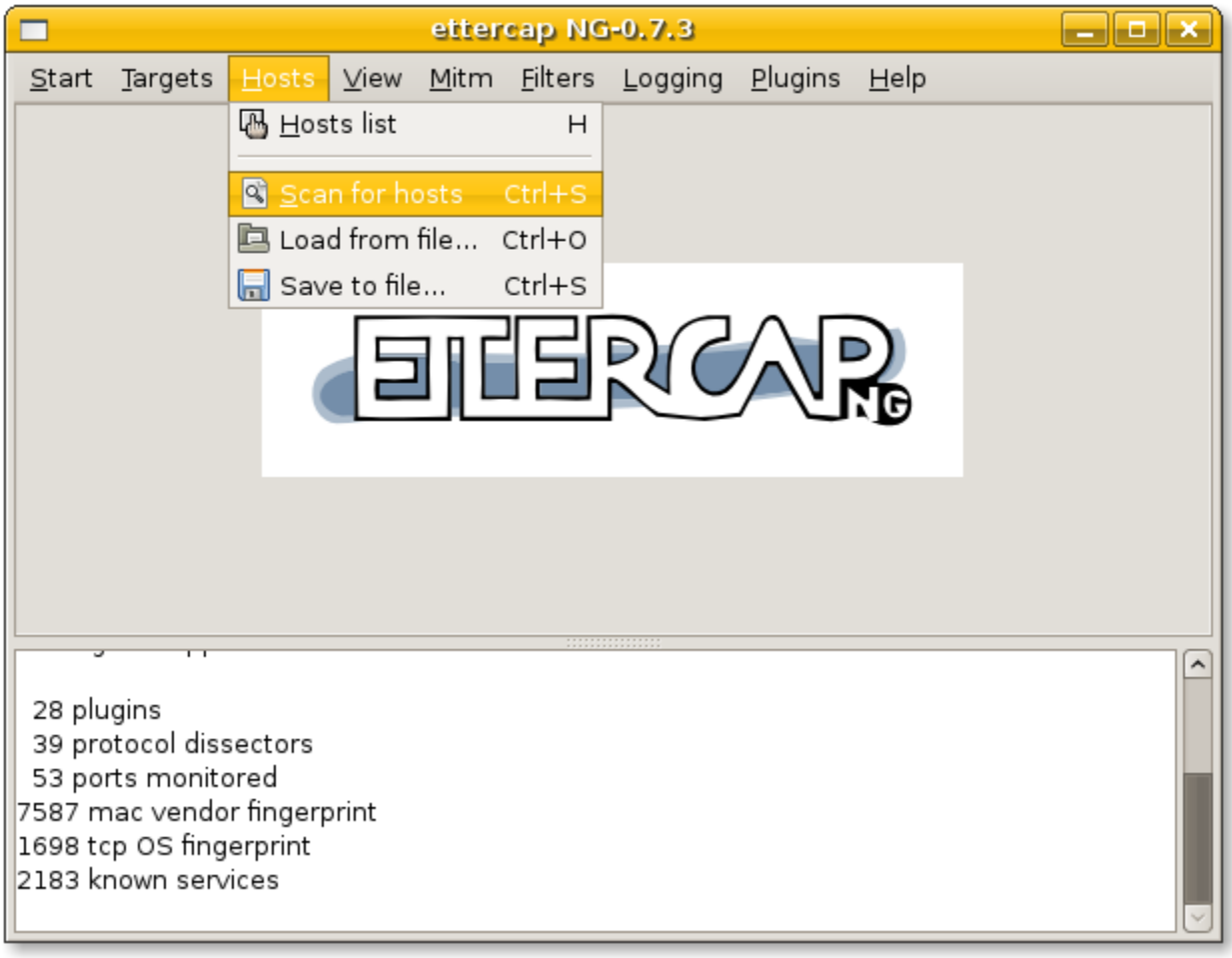
This will list all of the shared folders on the network. Shared folders from windows machines are immediately ready to be friendly and allow you axx. If your pen test is for a big company, get as much files as you can that would give you any information in regards to the company. Also shared folders and files are good places to plant Trojans. Simply name your Trojan something like “payroll.exe” or “employee-raises.doc.” That is excellent bait for simpleton employees looking to get gossip. Remember these machines are behind that gateway, so you must forward a port such as 31337 in the router interface to that IP where your bait resides.

I also like to run Ettercap. Ettercap is an invaluable tool for mapping out networks. It is primarily used for MITM (man in the middle attacks) but I actually have never used it for that. I only use Ettercap to get a list of machines using the router. If you cant get the password for the routers interface, to check the DHCP list, run Ettercap. Ettercap will list all of the machines using that particular router, but not machines using other routers that use your victims router as a gateway. You can think of routers analogous to extension cords for electricity, they can but put in series and “hide” IP addresses in whats called DMZ's. (demilitarized zones) A DMZ uses a different subnet mask, for example say your victims router gives you an IP like 192.168.2.1, then a different router plugged into that router in series would give all of *its* clients addresses like 192.168.3.1 or whatever you specify. If you gave the clients the same IP addresses under router B as you did under router A, then router B would simply lose internet service, almost as if it get shorted circuited. Here are a few Ettercap screens in action here at Weak-Net:



select “unified sniffing” then your LAN interface:

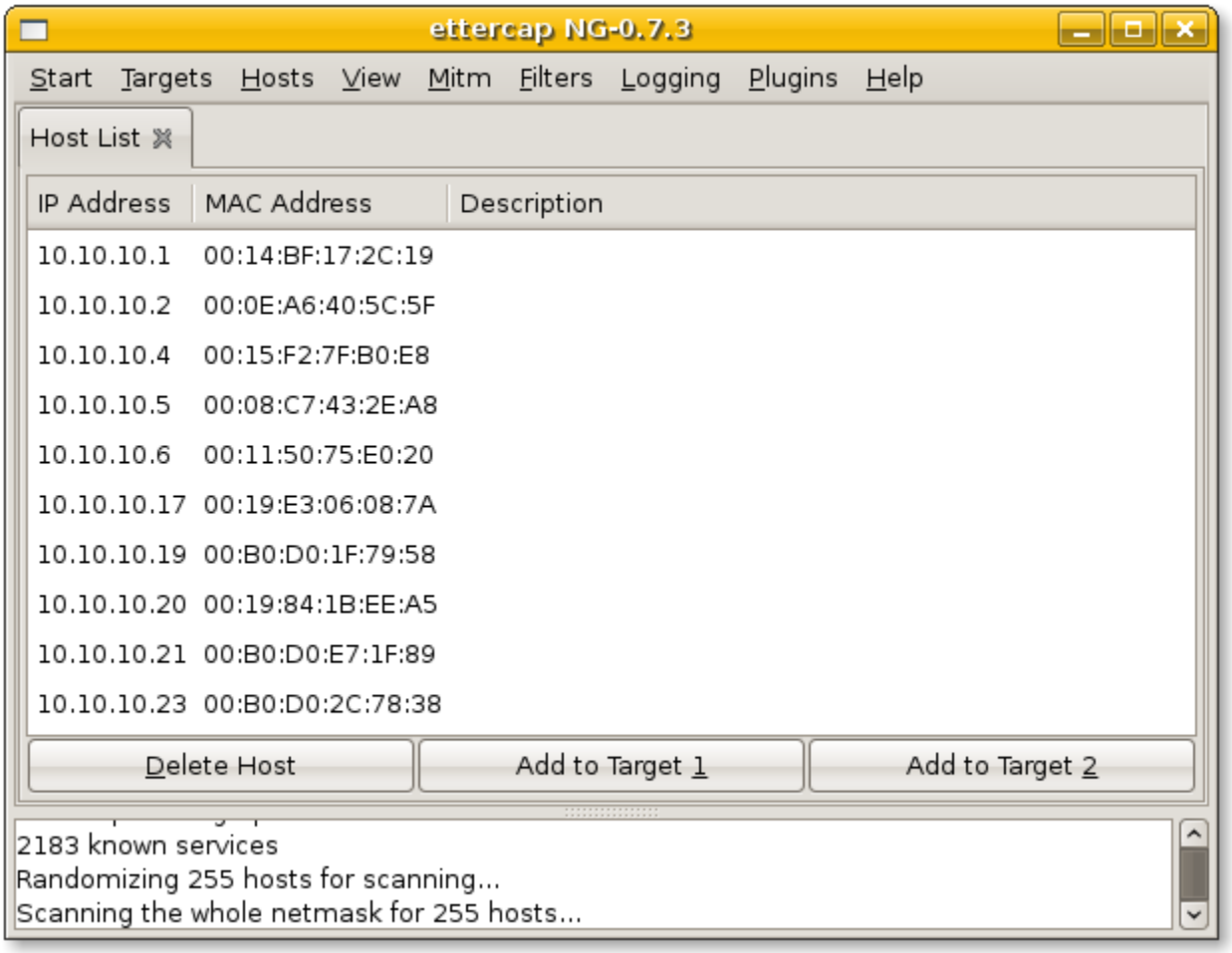
Here i have chosen “rausb0” which is my little ralink chip set WUSB54GC linksys adapter. After i click “OK” i then choose “scan for hosts” under the “hosts” drop down menu above like so:



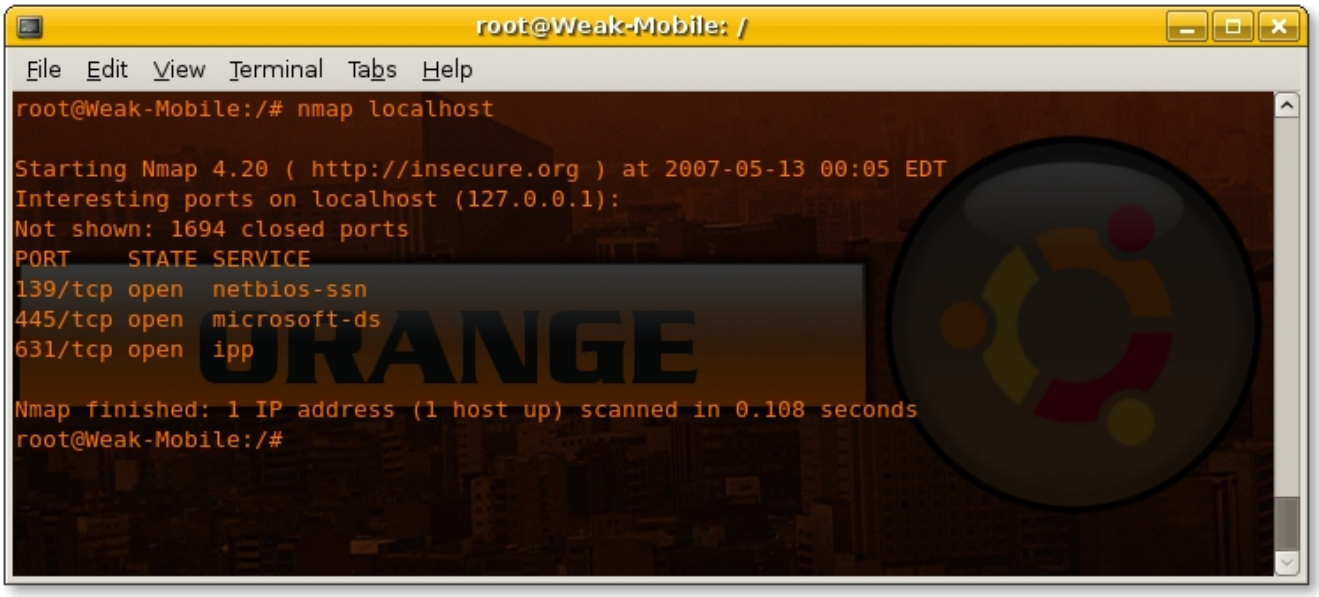
Then I watch it scan out the whole net mask 255:255:255:255 looking for hosts (or victims) :

This is again, an amazing tool for finding hosts in our network. Its very easy to work with and does its job quickly. Once the scan is over you will see a list of IP addresses all of which reside within our fenced off area, all of which communicate endlessly with each other And each machine communicates with the internet via the gateway.

Here is a sample picture of Weak-Net Labs:



Notice how you can get the MAC addresses too? Once you have this list you can begin scanning each machine for open ports using Nmap. Nmap has a great way of finding which ports are open and has a list of programs that commonly use those ports which it gladly gives you along with the open port list. If the machine blocks ping requests to its ports individually then you can turn on the “-P0” switch. So far we have drawn ourselves a good diagram of what this network looks like. We got our router, our machines IP's and now our machines open ports. Once you have the open ports list you can check the machines for telnet, ftp, ssh, smb, or any other flaw in which you can exploit. Metasploit has a wide array of exploits that can be tested to get shells reverse VNC connections, or even to add you as a user! Here is a list of open ports gathered by nmap as a screen shot:

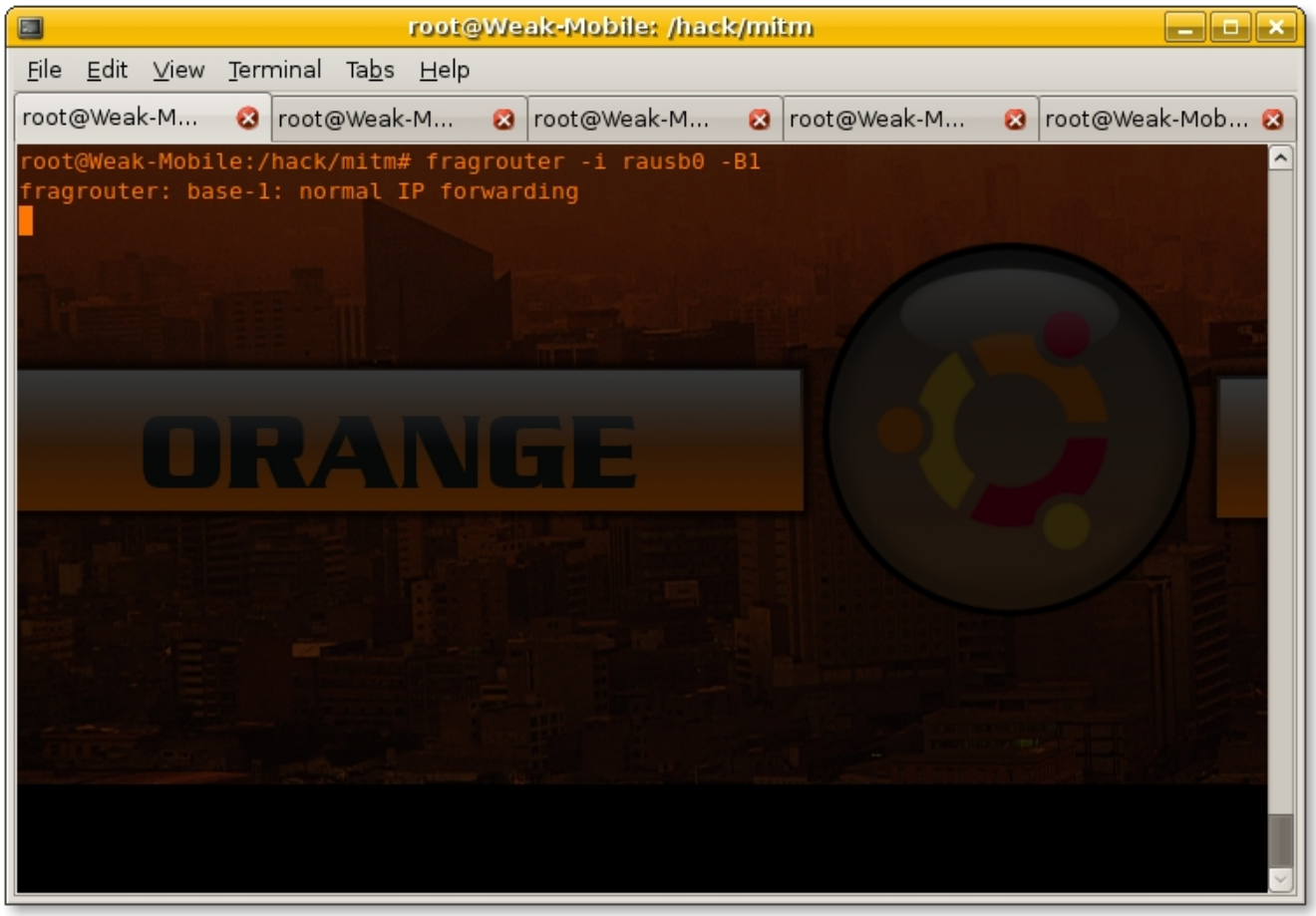


See the port 139? That's usually samba or shared folders. now simply grep for samba exploits in msfcli as we did before.

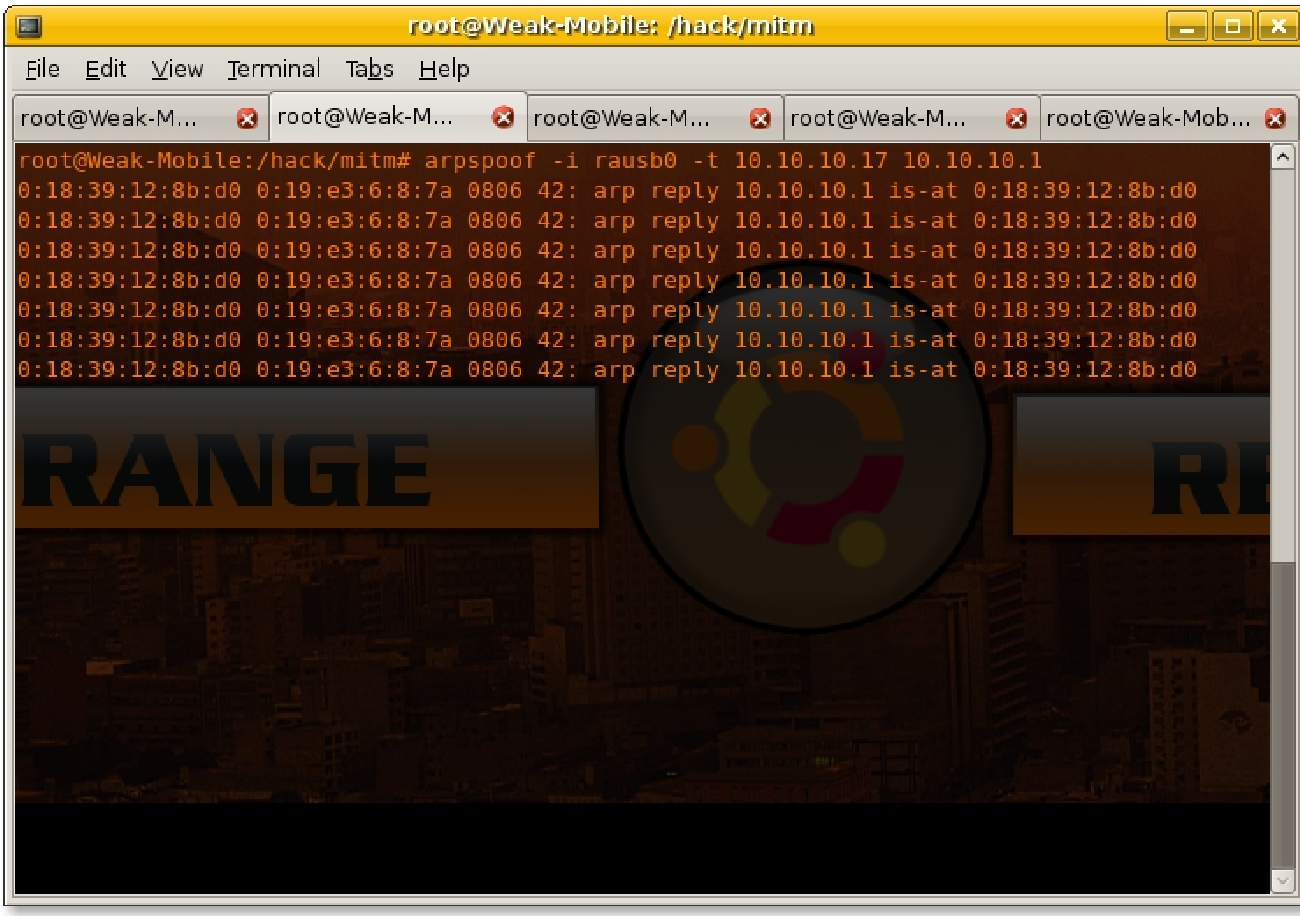
Another good thing to do, is to snort traffic along the network with Wire shark Wire shark puts your card into promiscuous mode allowing you to “see” everything that happens. On some switched networks you wont see too much because switched networks means that not all packets are shot at all machines like in hub or simple router based networks. But you can overcome this by watching everyones traffic individually. This is where Dsniff[16] comes into place.

A Quick Introduction to MITM attacks

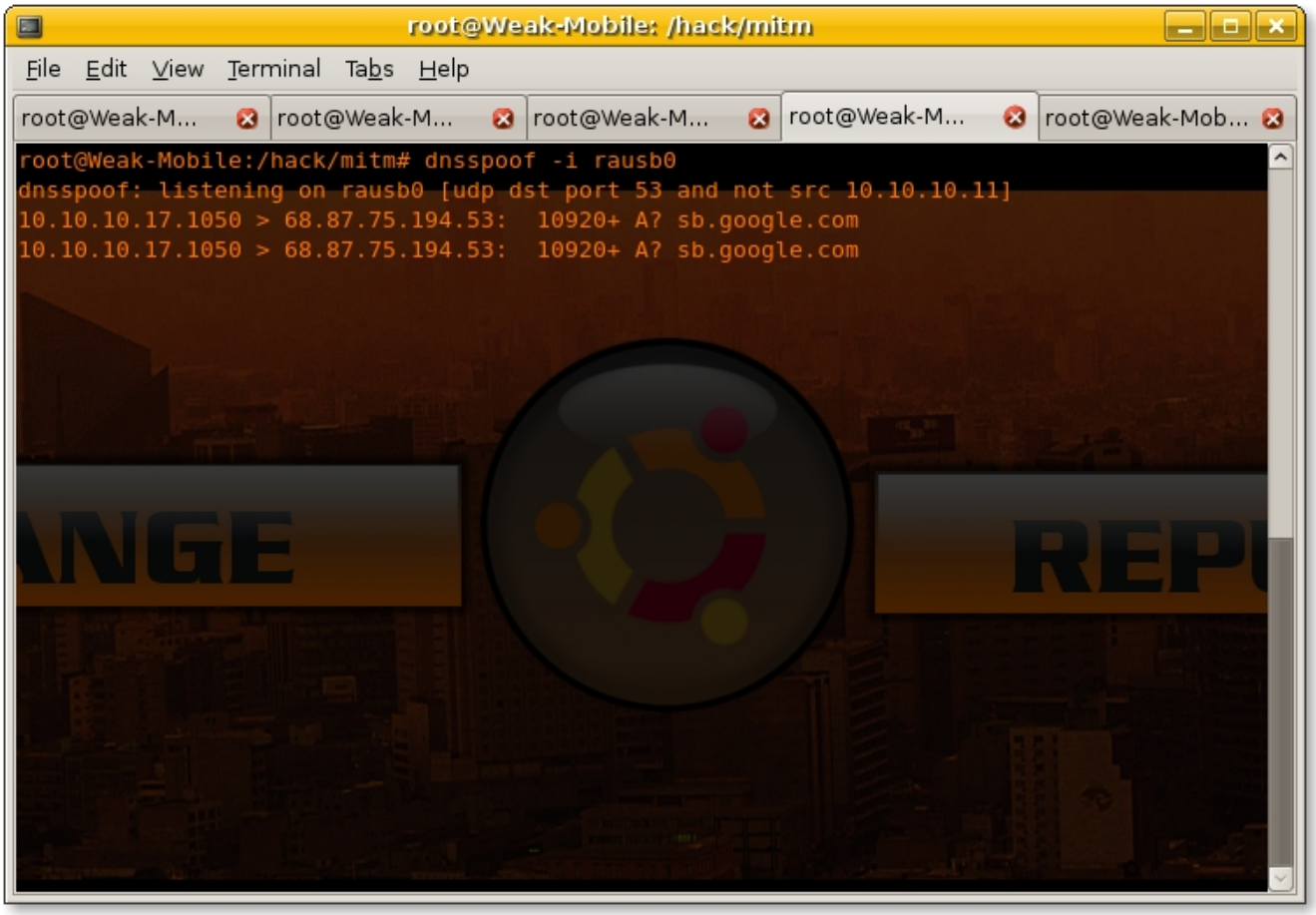
You as the attacker *could* simply pretend to be the router by sending forged ARP packets to the victim machine saying you *are* the router. And Dsniff is just the tool to do that! First, open up 5 terminals or 1 terminal and 4 tabs within that terminal, and SU in each one. Then in the first one run “Fragrouter” with the -B1 or “normal port forwarding mode” switch, like so:



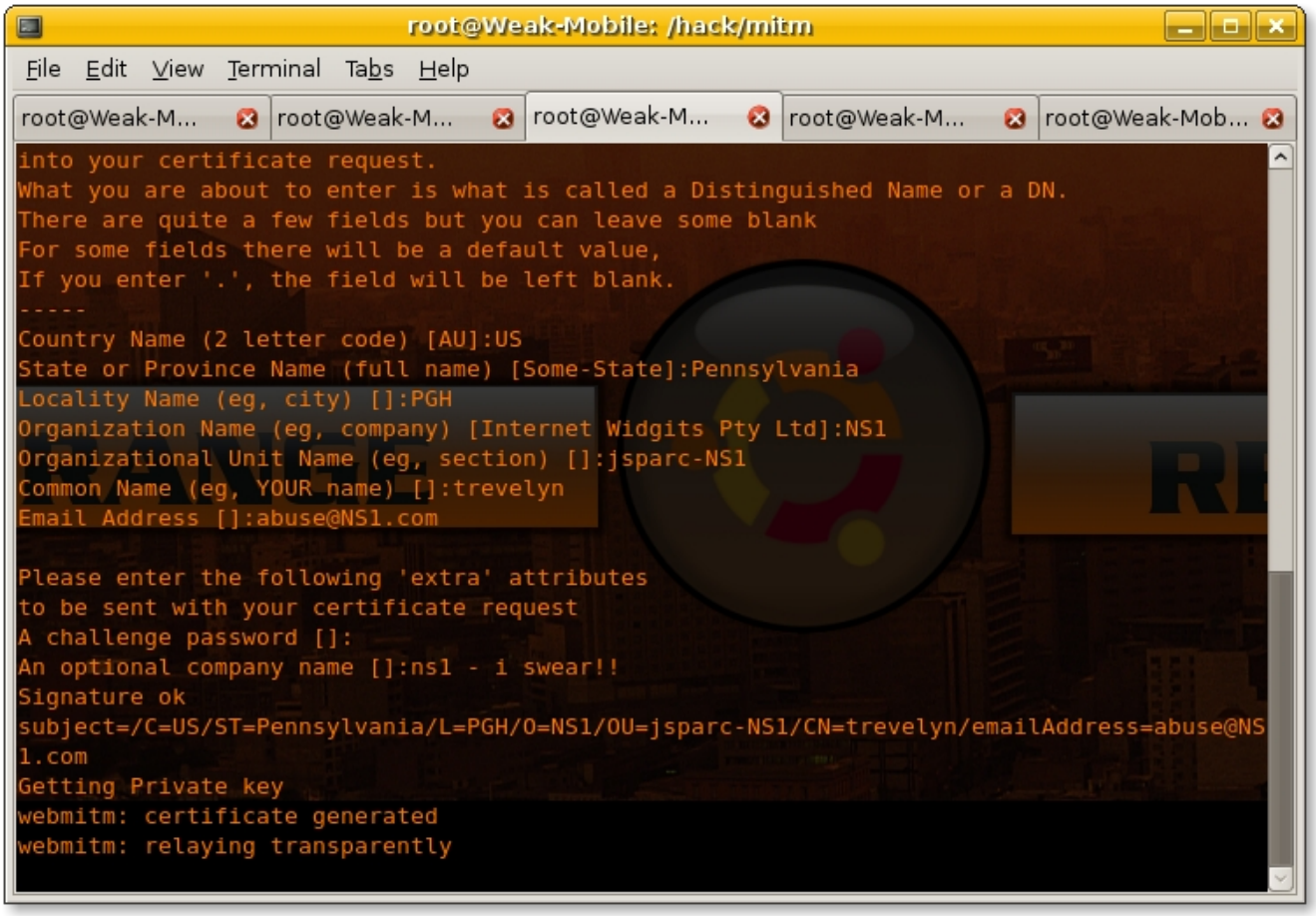
Then you want to run ARPspoof against your target. ARPspoof simply keeps telling your victim that *you* are the router and not the router itself. This way, all traffic must go through *you* first before even touching the gateway!



Now we want to start up DNSspoof, so we can provide names to correspond to the IP's your victim will be searching for...



And we can see that the victims machine has already tried to reach Google. ;) Then, we want to start Webmitm, a tool that allows you to create *fake* web certificates for using the SSL protocol. If you create a fake certificate you can decrypt the captured traffic that goes by port 443 on machines. SSL is used to "secure" connections to online banking, gmail, hotmail, yahoo, online web applications for mobile phone activations, ... the list will forever go on. So basically everything someone *would not* want you to see goes by that port. You can create a hostsfile for dnspoof co recreate certain sites as well, but I won't get too far into this, for this is a "Quick Introduction."



With the “-dd” switch webMITM becomes more verbose, and would display passwords and user names that the victim tries to use.

Any information about the victim is vital, and you must use any means necessary to gain it. You could even jump into their dustbins at night outside of the place, and maybe search for bags with paper in them that might contain vital info. Believe it or not, I have found screen shots of peoples bank accounts this way!

Spoofing your ID (to make the victim comfortable)

You could also easily spoof your caller-id to say whatever you want with online caller id spoofing services. Spoof the Caller ID to that of the corporation HQ. Call up the victim company and say you are a technician and you need to confirm a few things with the network administrator. Or you could spoof emails from anyone@anywhere. It's all to easily done.

To spoof an email create a free web page from a free host such as Homestead.com or Geocities or even Myspace. Then type out the email address of the victim and save it. Open a terminal and type "lynx http://address2pagehere.com" and after accepting the billions of cookies, highlight the address you typed out, and press enter. Lynx will prompt you for a return address – put whatever you want. The rest is up to you.

All of these examples are vital in gaining axx on a network. The more information you obtain, the clearer the picture becomes.

I hoped this helped anyone interested in the subject of pen testing get a slightly better understanding of what a quick sweep of the area could become.

Vital information is wasted in entropy everyday, from lost wifi packets, to unread voice mails, even dropped cellphone calls. Don't let anymore vital information be wasted.

References

[1] Back|track>> Linux - http://www.offensive-security.com/

[2] NavyNos Linux - http://navynos.linux.pl/

[3] Operator Linux - http://www.ussysadmin.com/operator/

[4] PHLAK Linux - http://www.phlak.org/modules/news/

[5] Tcpdump - http://en.wikipedia.org/wiki/Tcpdump

[6] Wire Shark - http://www.wireshark.org/

[7] Etherape - http://etherape.sourceforge.net/

[8] Ettercap - http://ettercap.sourceforge.net/

[9] Nmap - http://insecure.org/

[10] Slang, for “access” used commonly by a member of our staff here at Weak-Net Labs.

[11] man page for Iwconfig - http://www.linuxcommand.org/man_pages/iwconfig8.html

[12] Remote-Exploit forums, the creators of Back|Track>> Linux - http://www.remote-exploit.org/

[13] Aircrack-ng Suite - http://www.aircrack-ng.org/doku.php

[13.5] Aircrack-ptw – a much more efficient algorithm to crack WEP encryption - http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/

[14] Hydra Network password buteforce - http://www.thc.org/thc-hydra/

[15] Metasploit's exploit framework - http://www.metasploit.com/

[16] Dsniff – MITM tools for getting valuable info from other machines

http://www.monkey.org/~dugsong/dsniff/

Thanks to everyone who has every taught me anything, I promise I will pass on the knowledge cheerfully. - Trevelyn