GIVING A SNIFFER CONGESTION

The best way to defend against sniffers is three fold. First, don't visit anything important while on a con's Wi-Fi. This includes your email, financial institutions (credit card company and bank user information pages) or any place where you have to submit confidential information like your social security or credit card numbers. Do your online shopping at home, not at the con.

Second, when possible only use encrypted protocols (https, SSH, etc) when you are on a public network. For example, if you have to access a web page with confidential information make sure that the URL is preceded by https://. This indicates that the site is using SSL/TLS and that the data being transmitted between you and the server is encrypted (in theory, someone could be pulling a MITM attack as explained before). Not all protocols support encryption so you may want to look into using a service that allows you to "tunnel" through unsecured networks. Tunneling works by encrypting all of the data you are sending and routing it to an intermediate server (the exit point) on a network you trust (more or less) where it is unencrypted and sent on to its intended destination. A few examples of these systems are VPNs, Tor, Hamachi or SSH tunneling (all of which are topics too involved to cover here, but a quick Google search should tell you what you need to know). Using Torpark (a portable version of the Firefox web browser which can be run off of a USB thumbdrive) is a convenient way to use the Tor encrypted proxy network for those too lazy to set it up on their own Windows based laptop. For those that don't want to touch an icky Microsoft Windows box try the OpenBSD based Anonym.OS LiveCD. I feel I should also make you aware that while the previously mentioned technologies will protect you from attackers at your local hotspot, deviant computer users at the exit point of the encrypted tunnel may still be able to sniff your data.

And finally, use different passwords for different sites. To illustrate why it's a bad idea to use the same password everywhere, let me give you a little theoretical scenario. Let's say you use the same password on a social network site like MySpace or Facebook (which don't use SSL for encryption, and trust me, they are easy to sniff with Cain or Ethereal) as you do on your bank's web page (which more than likely does use SSL). If someone sniffs your Facebook or MySpace password they may then try to use it on your bank's website, or maybe see if you use the same password for your email account.

TOOLS DESCRIBED

Softperfect's NetScan
http://www.softperfect.com/

Ethereal
http://www.ethereal.com/

Cain
http://www.oxid.it/cain.html

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

Ettercap
http://ettercap.sourceforge.net/

TCPDump
http://www.tcpdump.org/

Hotspotter
http://www.remote-exploit.org/

Karma
http://www.theta44.org/karma/

Tor
http://tor.eff.org/

Hamachi
http://www.hamachi.cc/

Torpark
http://www.freehaven.net/~arrakis/torpark.html

Anonym.OS
http://theory.kaos.to/projects.html

For further information on sniffers visit:
http://www.irongeek.com/i.php?page=security/AQuickIntrotoSniffers
http://www.irongeek.com/i.php?page=security/arpspoof

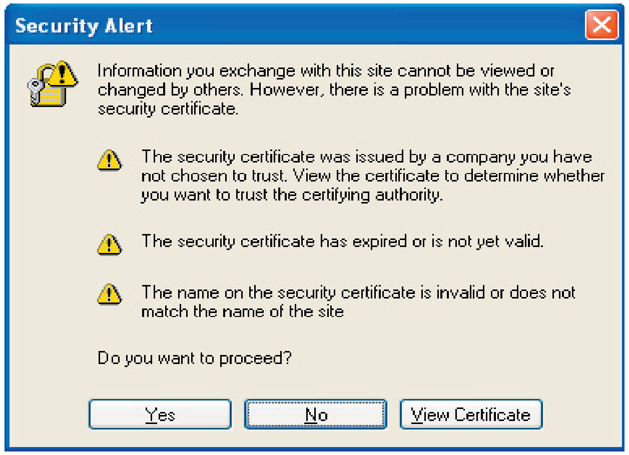
With a little work and knowledge you can stay relatively safe on the open Wi-Fi network at the con. If this article has you paranoid, or scratching your head like a monkey doing a math problem, ask a geeky friend for help. Enjoy the con.

Text by Irongeek. http://irongeek.com
Layout by riscphree. http://riscit.info
Shouts to the Infonomicon.org crew!

HACKER CON WI-FI HIJINX

Knowing the rules of the game

So, you are at the con and you want to use the open Wi-Fi (802.11a,b,g,n) network to surf the web and communicate with distant friends. All fine and dandy, but keep in mind there are a lot of playful folks sharing the hacker con's network with you. There will be more sniffers running at a hacker con than at a bloodhound convention. This pamphlet should help you be somewhat safer while using your wireless devices on the con's network and hopefully keep you off of the Wall of Shame (Ask at the con for its location).



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate has expired or is not yet valid.

The name on the security certificate is invalid or does not match the name of the site

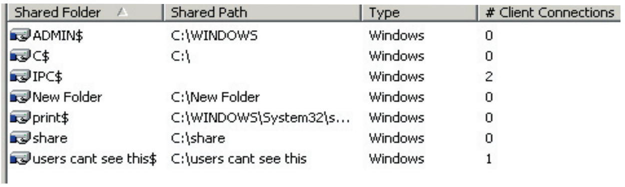
Do you want to proceed?

Open File Shares

One of the first things you should be aware of is open file shares. I'm just going to cover Microsoft Windows computers in this section, but similar problems can exist for *nix systems too (check your Samba and NFS configs). While at the con some deviant folks may run a tool like Softperfect's NetScan to find all open Windows file shares on the local network and see which ones they can read or write to. Less technical attackers may just look in "Network Places" and see what shows up. This could be kind of embarrassing if someone happens to find a little file share on your box that has some oh-so-private pictures (It's a con for tech geeks, look around you, do you really want to see these people naked?). Another threat is that other computers on the hotspot's network infected with malware could be looking for a place to spread to and happen to find shares on your laptop with write permissions.

The quickest way to find out what file shares may be available on your Windows box to outsiders is to go to the run bar, type "compmgmt.msc", hit enter and check under the "Shared Folders" section to see what's there (*nix guys check your smb.conf file). If you see any shares without a $ on the end of their names (normally these are just "hidden" admin shares that only system administrators can get to) you may want to check the permissions on them. However, even if you find these shares, they may not be available to everyone. A local firewall may be in place that will block access to them unless the firewall is configured to allow "File and Printer Sharing". A more thorough way to find out what shares you may have open is to have a friend take his Windows laptop, go to the run bar and type in something along the lines of \\your-computer-name

Obviously, change the "your-computer-name" to whatever your laptops name is. You can find your computer's name by right-clicking on "My Computer", choosing "Properties" and then selecting the "Computer Name" tab. Your safest bet is to turn off file sharing if you don't use it. Click Start->Control Panel->Network Connections, then right click on your wireless connection, choose properties and uncheck "File and Printer Sharing for Microsoft Networks" to disable it.



Shared Folder	Shared Path	Type	# Client Connections
ADMIN$	C:\WINDOWS	Windows	0
C$	C:\	Windows	0
IPC$		Windows	2
New Folder	C:\New Folder	Windows	0
print$	C:\WINDOWS\System32\s...	Windows	0
share	C:\share	Windows	0
users cant see this$	C:\users cant see this	Windows	1

For more information on rogue file share visit this URL:
http://www.irongeek.com/i.php?page=security/roguefileshares

Sniffers

Probably the biggest threat when using open Wi-Fi networks are deviant users running sniffers on the network. Pay special attention to this section if you're interested in avoiding identity theft where attackers use your credentials to access bank, credit and other sorts of personal accounts. Sniffers (also known as Network Analyzers) are a category of software that can look at network traffic, decode it, and give meaningful information about what kind of data is crossing a network. While sniffers have a lot of legitimate uses they are also useful tools for deviant computer users since they can be used to pull plain text passwords off a network (Basic authentication HTTP, POP3, SMTP, TELNET, FTP, etc), watch instant message conversations (AIM, Yahoo, MSN, etc), read e-mail messages or view web sites that other hotspot users are visiting. A few popular general purpose sniffers are NAI Sniffer (commercial), Ethereal (an Open Source GUI Sniffer for Linux, Windows and other platforms), TCPDump (Open Source command line sniffer for *nix - any Unix like operating system like Linux or FreeBSD-) and its Windows version called WinDump. A bigger concern for users on open wireless networks would be special purpose sniffers like Cain, Ettercap and the Dsniff package that allow users to easily parse out passwords from network traffic.

Since people have a tendency to ignore threats until they have been directly confronted with them I'm going to explain the background of some of the common attacks. Test these on your own home network if you like, BUT NOT ON SOMEONE ELSE'S! There are a few ways attackers can sniff a wireless network, depending on their hardware. Computers on a wireless LAN act a lot like they are on an Ethernet LAN using hubs. Every computer on the LAN can see the traffic destined to others but normally they just choose to ignore it. (In reality it's a little more complicated than that, but I want this to be an article and not a book on the intricacies of 802.11 networks) However, if a network card is put into what is known as promiscuous mode, it will not ignore traffic going to other computers and will instead look at it, allowing the user of the computer running the sniffer to see the data traveling to other computers attached to the same access point. Promiscuous mode works on pretty much any wired network card in Windows and Linux (or other Unix like Operating System), but not all wireless cards support it properly (like Intel's Centrino 802.11g chipset know as IPW2200). If the sniffer's card does support promiscuous mode it will have to be attached to the wireless networks WAP (Wireless Access Point) to be able to see anything.

If the attacker is using Linux (or another Unix like Operating System) the attacker may be able to use what is known as monitor mode if their card supports it. In monitor mode, the wireless network card listens to the raw packets in the radio waves without ever having to attach to a WAP. The nice thing about monitor mode from the attacker's perspective is that they leave no logs of their activities since they don't have to attach to the WAP and don't have to send any packets on the network.

Man in the Middle

A third way is to use what is known as ARP poisoning to route traffic through the attackers laptop, allowing them to see all of the traffic passed as well as giving them a chance to modify it (I've seen an Ettercap script that was programmed to replace the images in web page with the image from lemonparty.org. If you don't know what that is don't ask). Tools like Arpspoof, Ettercap and Cain all have ARP poisoning functionality built in. The downside to ARP poisoning from the attackers perspective is that it's noisy (Intrusion Detection Systems [IDS] packages and ARPWatch can easily detect it) and has a tendency to screw up a network if it's not done right or if someone decides to ARP poison the entire network at one time. ARP poisoning's advantages for the attacker are that it can be done in both Windows and *nix and it allows what is know as a Man-in-the-middle (MITM) attack. A Man-in-the-middle attack is where an attacker gets two or more other network members to send traffic through his computer first, then passes it on to its intended recipients. Man-in-the-middle attacks allow the attacker to "proxy" some protocols that are normally encrypted and secure (like SSL/TLS or SSH) and sniff the connection by pretending to be someone they're not. Depending on the protocol, the user may get a warning message letting them know that the keys have changed. For example, if someone MITMs an SSL connection the user might see a message pop up from their browser something like:

Firefox:
Website Certified by an Unknown Authority
Unable to verify the identity of server as a trusted site

Microsoft Internet Explorer:
Security Alert
Information you exchange with this site cannot be viewed of changed by others. However, there is a problem with the sites security certificate.

Notice the message from Microsoft is dead wrong. Another way you might notice that an ARP poisoning attack is going on would be if the network slows down to a crawl and you have intermittent networking problems. However there is no guarantee that an ARP poisoning attack will noticeably affect a network from a usability stand point. The most sure fire way to detect one is with an IDS in the right location on the network (Unfortunately, it's doubtful you have one running on your laptop).

A fourth way is for the attacker to set up their own laptop as a rogue access point using a tool like Hotspotter or Karma, wait for victims to unwittingly attach to it, and sniff to their little heart's content.