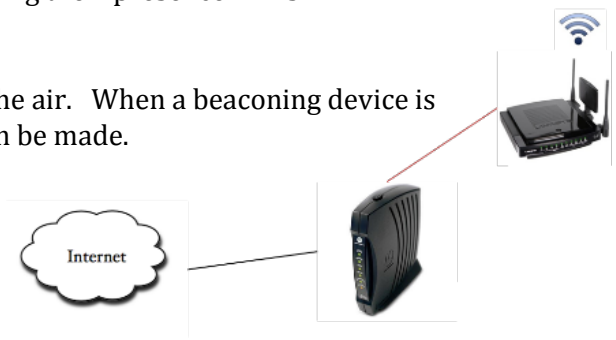
Attacks on Wireless Networks

DISCOVERY

The first step in attacking a wireless network is to discover it.

Wireless access points enable wireless network devices such as laptops, desktops and smart phones to get out to the Internet and access network resources in a wireless local area network. Wireless access points make themselves known by sending signals out to the air announcing their presence. This is known as **beaconing**.

Wireless devices detect this signal by scanning the air. When a beaconing device is located, a connection to the beaconing device can be made.



DISCOVERING THRU LOCATION MAPPING

When hackers want to find open wireless networks they try to locate wireless access points. These wireless access points can be located by **War Driving**. This is the process of finding wireless access points by driving (or walking) around cities or business centers locating and mapping these access points. Once these wireless access points are discovered, connections can be made to the wireless networks logically contained by these access points; quite often these connections are not authorized connections.

Click on the image or link below to see an example of Wireless Access Point mapping.

http://upload.wikimedia.org/wikipedia/commons/1/15/Seattle_Wi-Fi_map_UW-300-letter-3.png

PROFESSIONAL WAR DRIVING TOOLS

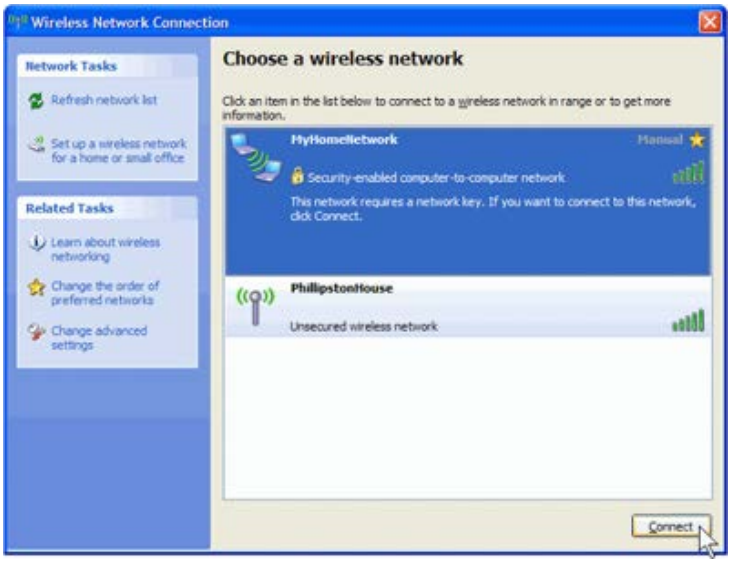
You need at least a portable wireless computer to detect wireless access points, such as a smart phone, tablet or a laptop. To actually map the signals so that you can revisit them at a later date use a GPS and GPS mapping software.

Click on the image or link below to view an example of war driving software using a GPS.

http://www.gpsvisualizer.com/map_input?form=wifi

CONNECTING

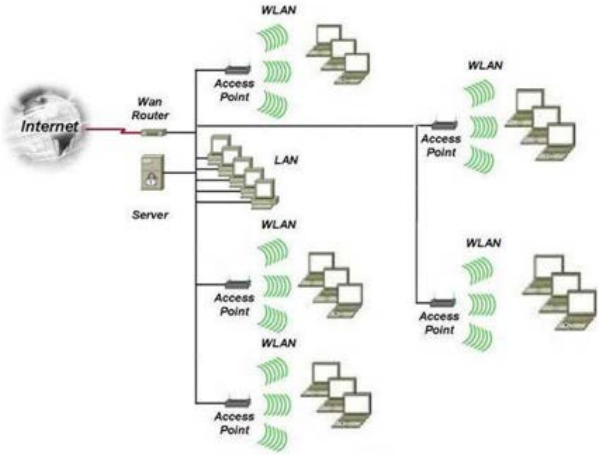
By default, when a wireless access point beacons, it includes a **Service Set Identifier** (SSID) with the beacon. This way, when a wireless device detects the beacon, it can display the wireless access point with its' SSID (or network name). In the image below both wireless access points shown come from wireless access points that beacon the SSID.



You can configure a wireless access point to **NOT** include the SSID with its beacon. This, however, will only stop the casual, unauthorized users.

Here are some things to consider before turning off the SSID:

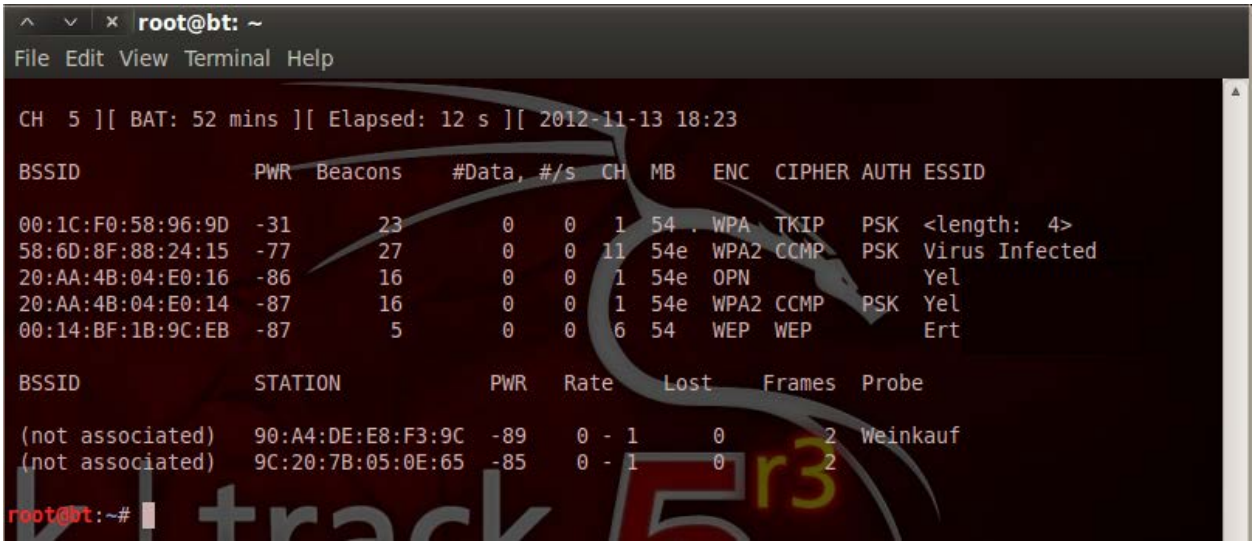
1. The SSID can be discovered using programs like **Air Snort** or **Net Stumbler** even when the SSID is not included in the beacon.
2. Turning off the SSID may cause some inconvenience to legitimate users such as those that roam around through multiple wireless access zones.
3. Some operating systems make it difficult to connect to wireless access points that don't broadcast the SSID, especially when there are wireless networks in the area that do.



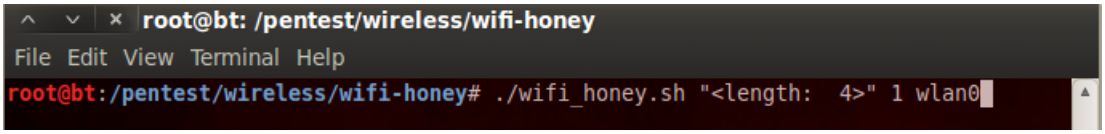
Check out this YouTube video: http://www.youtube.com/watch?v=kIaZ8lvVl3g

Phases of discovery/cracking wireless access point passwords (please note, this is for educational purposes only):

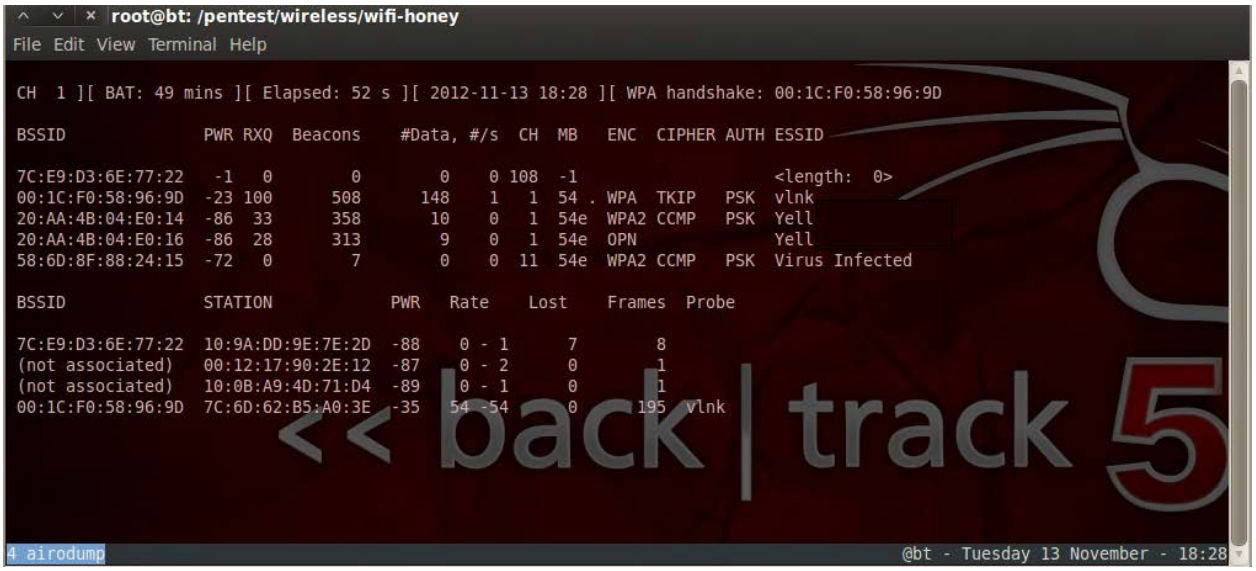
1. Locate a victim and make note of the victims ESSID and channel number.



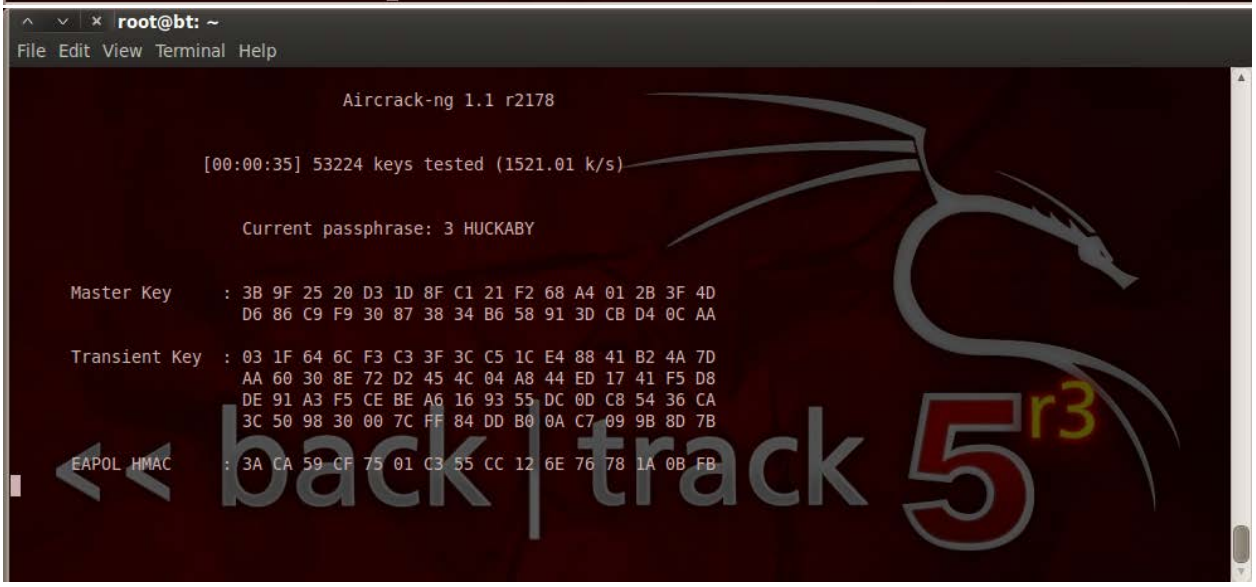
2. Monitor the victim and look for a connection (handshake) to the access point.



3. Handshake was made, cracking can begin. Notice how the **Extended Service Set Identifier** (ESSID) was discovered for the vlnk router, even though that router did not beacon the ESSID.



4. Scan the captured network packets to crack the password. If the encryption was nonexistent or WEP, then this process would not take long. If the password was complex (with numbers, special characters, letters, length) and if the encryption was WPA or WPA2, this cracking process would have to run for years before the password is cracked. Please note, if you change your access point's password often, any password that may be cracked by a hacker would be obsolete by the time the hacker is able to use it.



LAUNCHING ASSAULTS

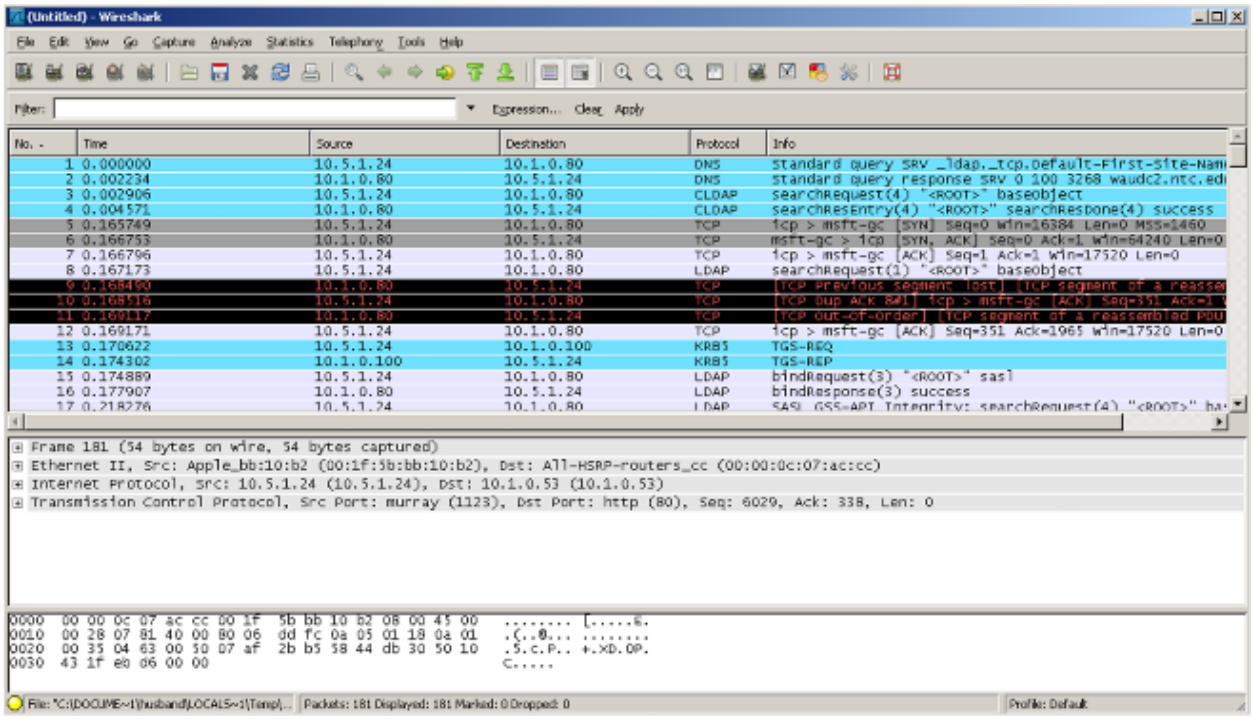
Once an attacker discovers a wireless network and connects to it, an attack can happen. Here are a few attacks that can be made against a wireless network:

1. Eavesdropping
2. Stealing data

3. Injecting malware
4. Storing illegal content
5. Launching denial of service attacks
6. Impersonating a legitimate network
7. Stealing DNS traffic

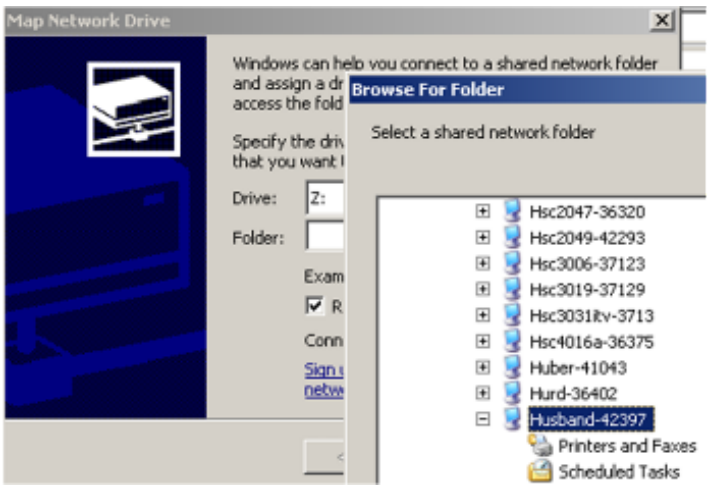
EAVESDROPPING

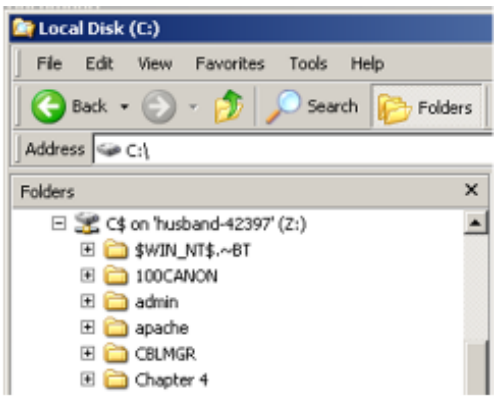
Transmissions can be captured using a protocol analyzer/sniffer like Wireshark. If the captured transmissions (packets) are not securely encrypted with the latest encryption algorithm such as WPA2, personal information can be obtained relatively easy. See image below.



STEALING DATA

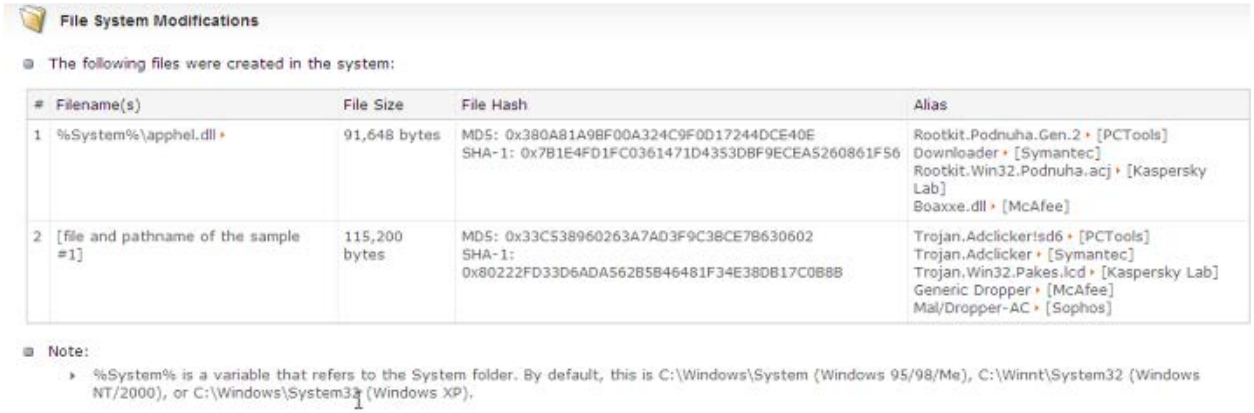
Once you successfully connect to a wireless network you are essentially on that network. If the network is not secured with pre-established trust relationships, network sharing can become available to you, thus enabling you to access network resources such as shared folders. Even the C: drive is shared by default.





INJECTING MALWARE

Once you are on a wireless network you are behind enemy lines (the firewall). This allows you to inject malware such as worms onto other network devices such as servers or workstations. From there, the worms can crawl to other devices in the network.



File System Modifications

The following files were created in the system:

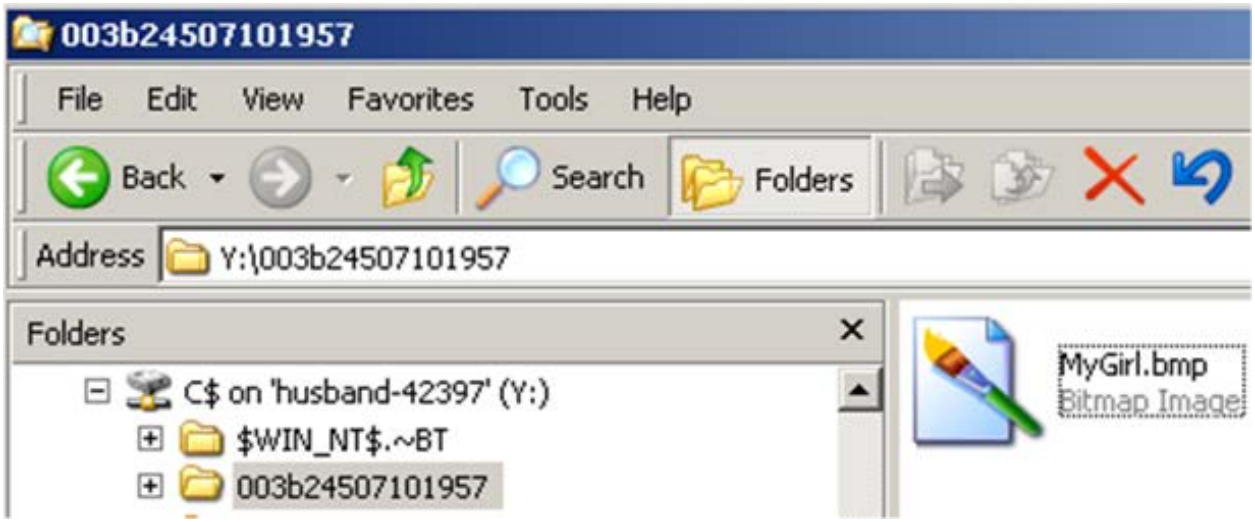
#	Filename(s)	File Size	File Hash	Alias
1	%System%\apphel.dll	91,648 bytes	MD5: 0x380A81A98F00A324C9F0D17244DCE40E SHA-1: 0x7B1E4FD1FC0361471D4353D8F9ECEA5260861F56	Rootkit.Podnuha.Gen.2 [PCTools] Downloader [Symantec] Rootkit.Win32.Podnuha.acj [Kaspersky Lab] Boaxxe.dll [McAfee]
2	[file and pathname of the sample #1]	115,200 bytes	MD5: 0x33C538960263A7AD3F9C38CE7B630602 SHA-1: 0x80222FD33D6ADA562B5B46481F34E38DB17C0B8B	Trojan.Adclicker!sd6 [PCTools] Trojan.Adclicker [Symantec] Trojan.Win32.Pakes.lcd [Kaspersky Lab] Generic Dropper [McAfee] Mal/Dropper-AC [Sophos]

Note:

- %System% is a variable that refers to the System folder. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

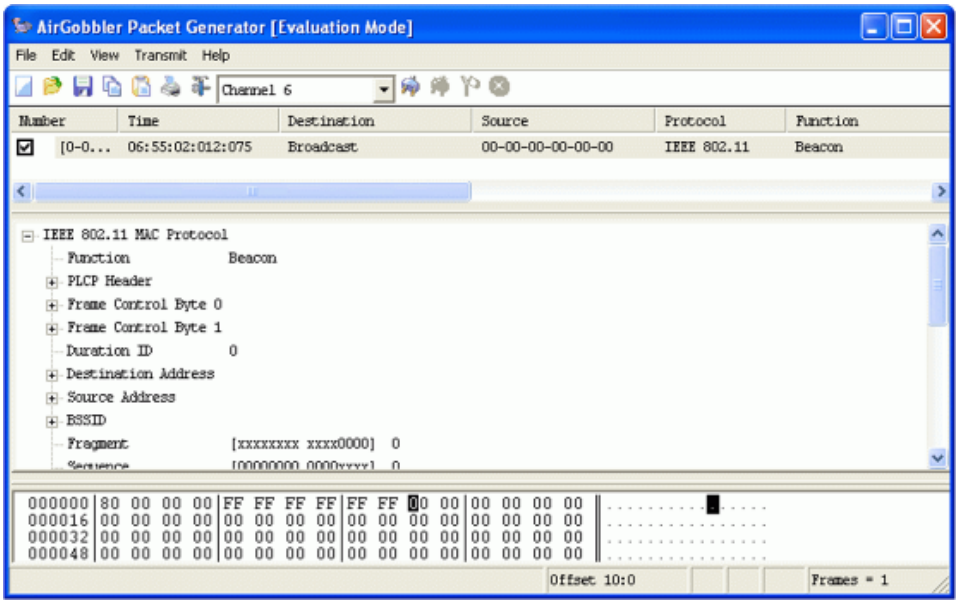
STORING ILLEGAL CONTENT

Criminals use the Internet and their computer for illegal purposes. The smart ones know that if illegal content is stored on their own personal computer, it can be used as evidence against them if a forensic investigation is ever made against them. To avoid being caught, criminals will store illegal content on someone else's computer without the owner of that computer knowing it. Once a criminal can access a wireless network and be able to access a network share (with "write" access), this process is relatively easy.

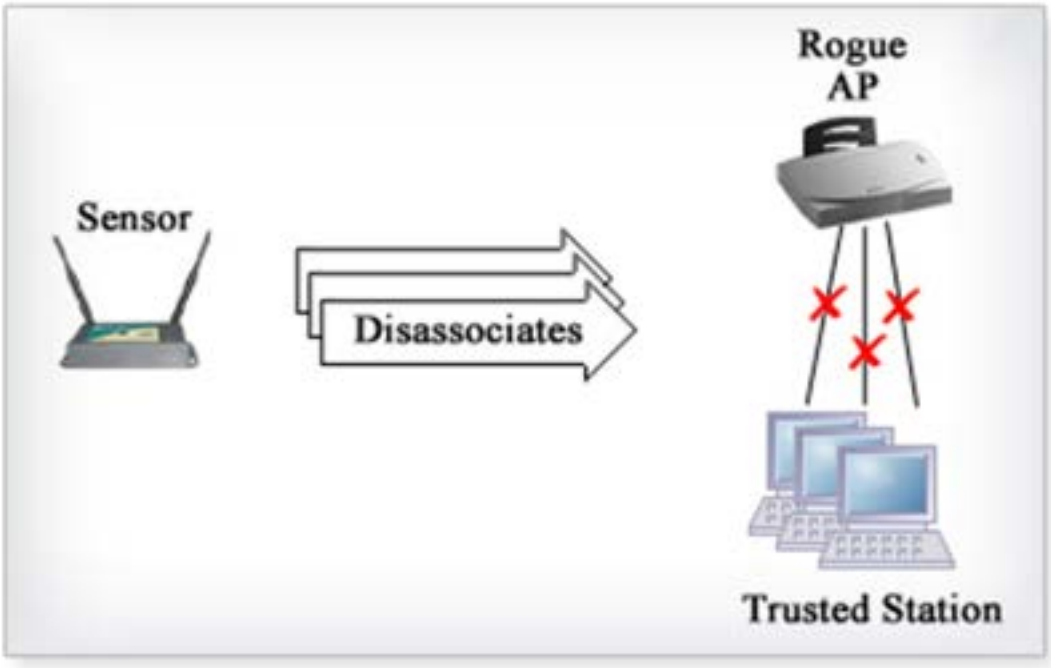


LAUNCHING DENIAL OF SERVICE (DOS) ATTACKS

The intention of a DoS attack is to saturate a network (either wired or wireless) or a device (such as a web server) with traffic (network packets) to the point that the network or device becomes useless to anyone trying to access it. If a criminal is connected to a wireless network, they can flood the wireless network with traffic that will bring the wireless access points to a crawl.

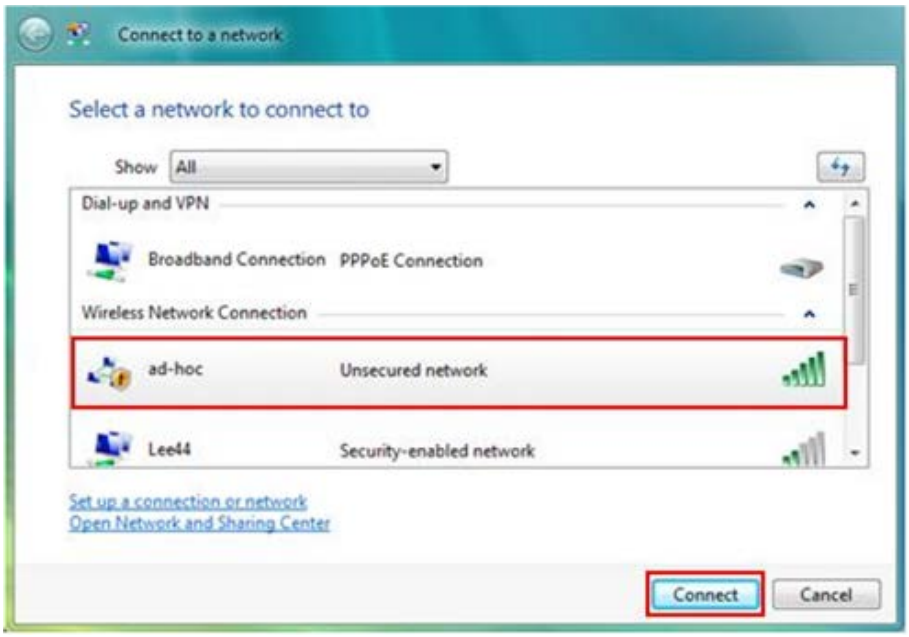


An even more effective means of disabling a wireless network is by establishing a **disassociation network frame** (packet) to disconnect legitimate wireless devices from the network.



IMPERSONATING A LEGITIMATE NETWORK

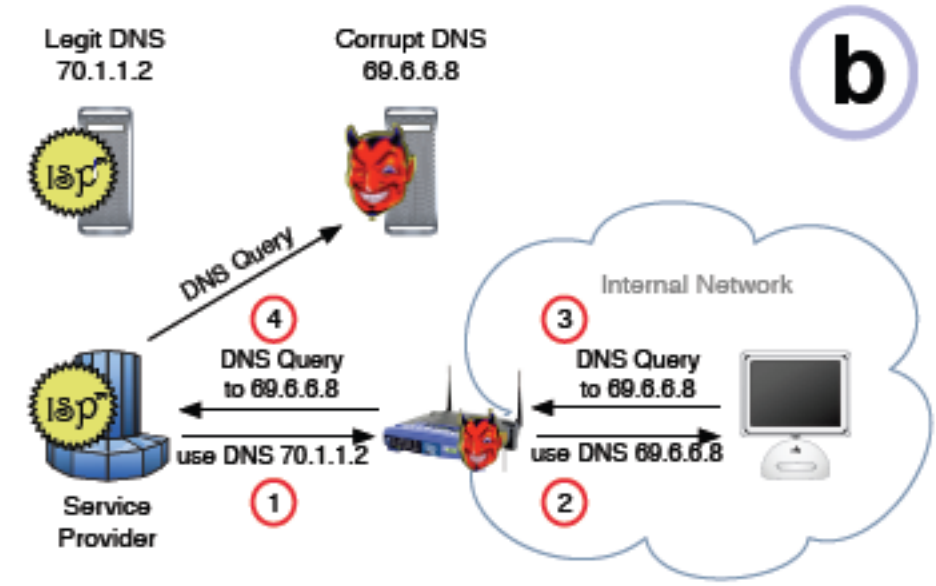
If you were an attacker, wouldn't it be nice if you could get people to connect to you instead of you connecting to them? This can actually be done from a wireless PC that is configured to be an ad hoc wireless network that allows other PCs to connect to it as if it were a real network. Once the connection is made, the attacker might be able to inject malware or steal data.



STEAL DOMAIN NAME SERVICE (DNS) TRAFFIC

Through a relatively simple Java script that you unknowingly download from a compromised web server somewhere on the Internet, your wireless access point, if left at the default settings, can have its' internal settings changed to reroute your name resolution requests to a corrupt DNS server.

The way this works is simple. Once you get compromised, the addresses (URLs) that you type in your browser such as **www.paypal.com**, will likely route you to an attacker's computer. When this happens, the attacker's computer will quickly Phish for personal information.


b
Legit DNS
70.1.1.2
Corrupt DNS
69.6.6.8
DNS Query
Internal Network
4
3
DNS Query
to 69.6.6.8
DNS Query
to 69.6.6.8
use DNS 70.1.1.2
use DNS 69.6.6.8
1
2
Service
Provider