The Art of casual WiFi hacking

Jeremy Martin, CISSP-ISSAP, NSA-IAM/IEM, CEH – jeremy@infosecwriter.com

It is a cloudy Friday night and I am in the listening to another episode of 2600's "Off the hook" radio when the interruption of the phone catches my attention. I had been expecting the call from my colleague, because I needed help with some new proof-of-concept ideas for a penetration test I have the following week. During the conversation, we eagerly decided to head out for the night to Wardrive in the area. Wardriving is always a good excuse to test new programs and ideas. We position both laptops for optimal WiFi signal, easy access to the GPS devices, and secure them for the least amount of movement while driving. Right before we leave, we make sure the power converter is turned on, and the systems are plugged in. To cover all our bases, one laptop runs Windows XP Pro, NetStumbler, and Cain&Able while the second system has Suse 9.2 Linux with Kismet, Airsnort, Aircrack, and Void11. Using two devices with such different environments improves success while surveying WiFi in an area or "footprinting" them.

Here is where the fun begins. After driving for a few miles, we enter a well lit street in the business section of town, and hear the ping of live access points every few seconds. Even though we have been doing this for years, we are both amazed at the percentage of companies that employ WiFi that do not implement any sort of encryption. This allows us to park and let Kismet do what it does best... passively listen to network traffic running over the 802.11 signal. We are able to map several subnets and gather other interesting information being broadcast to the public. At the end of the night, we were able to gather over 127 WiFi hotspots after only driving seventeen miles round trip. With this type of information gathered, playtime for hackers begins.

Wardriving

Also referred to as *"Geek's catch and release fishing"*, is the act of driving around and scanning for open WiFi hotspots. This is considered a sport in many circles and is growing in popularity across the globe.

Warwalking

Is similar to Wardriving, but on foot. There are many PDA devices that will allow you to install wireless and network auditing tools.

Wardrive is done for many reasons. Some do it for a social activity with friends. Others Wardrive as a community service to increase awareness, as a business model to secure for profit, or even the cause the dreaded criminal acts of spreading viruses, hack, or commit fraud.

The Gear

Windows system:

- Acer Aspire 1520 laptop
- Riklen GPS
- FM Modulator
- Windows XP Pro
- NetStumbler
- Cain & Able
- MS Streets & Trips

Linux system:

- Acer Travelmate
- Microsoft MN-520
- Suse Linux 9.2
- Kismet
- AirSnort
- Void11

Wardriving does not take a long list of special tools and equipment. Above is a list of equipment I use and have found to work, it is not a requirements list. Almost any WiFi enabled Windows machine can scan for hotspots right out of the box by installing either Cain or NetStumbler. Linux is another story. Since the Linux environment allows for more direct access to the hardware, there are more items to consider. These include Linux compatibility, correct drivers, and knowledge of iwconfig or similar configuration utility for using the card in promiscuous mode. Many "Live Linux" distributions take care of most the work for you if the WiFi card has compatible chipsets. The most common and well known WiFi chipset for Linux use is the PRISM 2. The Orinoco Gold card became very popular because of it's easy of use and ability to work with most Linux environments out of the box. You can use most Windows based cards in a Linux environment by using an NDIS driver, but they will not work for scanning purposes because of the inability to access the hardware directly.

The problem you may come across is that most Windows based scanning utilities use a method of scanning called "Active scanning" because of the limited access to the hardware. When scanning for WiFi using an active scanning method, your device sends out a request on every channel and logs all replies. The traffic produced can be immense and is also noisy. Anyone setup to listen for incoming connections will instantly know you are scanning because of this.

NetStumbler is an active Windows based scanner that produces the information you need for mapping WiFi hotspots including SSID, Encryption, and GPS coordinates. Since the program constantly screams out "ARE THERE ANY ACCESS POINTS OUT THERE", the responses are more abundant. One of the issues you may come across is that the traffic is so chatty that other devices scanning may get spammed by fake access points. NetStumbler is not self contained and it uses Windows drivers to access the WiFi card, causing the Wireless Zero Configuration to shut down when run. Wireless Zero Configuration in WinXP allows the operating system to find available WiFi networks. This is a problem for connecting to an access point while Wardriving. The easiest way to resolve this is to save the NetStumbler data, close the program, and refresh the available networks.

Cain & Able is one of the best FREE all-around auditing programs out there for the windows platform. It sports ARP poisoning, password crackers, a VoIP logger, and has a WiFi scanner built in. This application does not have the same downfall as NetStumbler because it uses a Third-Party driver called WinPcap (used for most low level network programs like the sniffer Ethereal). Cain & Able doesn't seem to detect the volume of Access points as NetStumbler does, so the choice is mainly a preference one

Kismet is popular because it uses "Passive scanning" methods and does not interfere with network traffic or WiFi signals. When using a passive scanner, data is logged only when an access point transmits. It is almost impossible to detect while giving you even more information then the previously mentioned counterparts. If enough traffic is generated or active traffic passes through, you can grab the IP address range of the access point without having to log in. Knowing the access point's IP address can come in handy if the network does not use DHCP. If you use a second computer running Cain to Arp poison the access point, Kismet can gather a lot more then just the SSID.

If you do not want to install a Linux distribution on your system, you can download a live Linux distribution with all of the required tools already installed on a CD. Live Linux distributions are used to allow even a Windows installed system to boot into a Linux environment that is not installed on the hard drive. Most Live Linux distributions do not mount the hard drive and leave little to no trace evidence that they were ever used in an attack. These distributions can also be used to gather information from a target system without compromising the evidence.

Last but not least, you need a means of transportation of some sort. I like to use a vehicle because I'm too lazy to carry around a "desktop replacement" laptop and have not invested money into a good PDA yet. It's much more efficient to sit, relax, and Wardrive. I drive a good old American gas guzzling SUV to seat all of the people comfortably. One of the most important items you can purchase besides the computer equipment would have to be the power converter. I use a three 700 watt AC converters because there is usually 1-6 people needing power. I also have a spare battery because I tend to drain more power then most people.

Now that you have chosen your gear, you can start to Wardrive. One of the most common questions people ask when they are new to the scene is "what should I expect"? When you drive, most areas will usually have a concentration of noticeable signals in business districts and residential areas. I know it doesn't take a genius to deduct these obvious facts, but there are different reasons why the hotspots are available.

Small to medium sized businesses are more likely to have unsecured wireless access points then large companies, publicly traded businesses, financial institutions, or health organizations. The later are covered under many regulations in most countries and are required to encrypt wireless communications if they are allowed to use them at all. Many small to medium sized businesses either do not have the budget to hire competent IT staff or do not feel that the security is important and do not bother to lock down straying signals. Yet there is another reason this section may have open WiFi. They want it… Some people feel adding open internet access adds another level of service and quality of life to their environment. These companies welcome your patronage.

Residential WiFi is the most common signal you will pick up. Some open access points are open to develop adhoc Metropolitan Area Networks for file sharing, underground internet media, and to help make society. SeattleWireless.net is a prime example of a portion of the community working together to bring WiFi to a larger crowd. This Seattle based group even produced several online videos to help increase awareness. Not all residential service is open to sharing though. Many ISPs have service agreements that make sharing the Internet access against the rules, subjecting the owner to fines and/or cancellation of service. If the resident does not give you the proverbial "ok" to use the Internet or network connection, you may be breaking many laws including theft of service, unauthorized access to a computer network, criminal trespass, or even federal anti-wiretapping laws.

Now that you have the data, what do you do with it? This section will discuss using a program on the Microsoft Windows platform with NetStumbler data to survey an area. Below, figure 1 shows a sample of data that may resemble the data you will also find. Keep in mind that the percentage of Encrypted Vs. Non-encrypted networks will vary from location to location. In the area where these tests have been conducted, 65.78% of the networks have no encryption scheme implemented. Scary part is the business districts had a higher percentage of vulnerable systems then residential areas. Another very important thing to look at is the list of SSID names… Many of them are using the default name. Broadband routers with default name will probably still have the default passwords on them as well, and are far more interesting targets then a hidden SSID. Now, back to work…

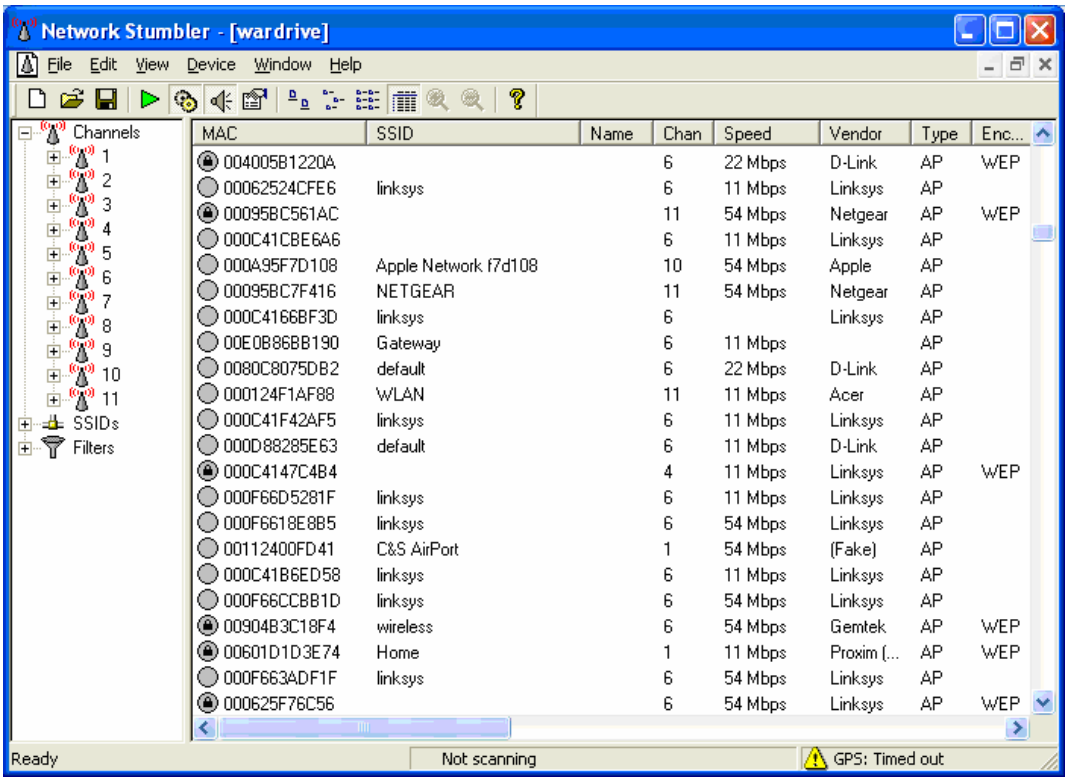

Figure 1 (NetStumbler data gathered during an area scan)

The native NetStumbler file (NS1), can be uploaded to most of the online WiFi public depositories for the rest of the community to view such as wifimaps.com and wigle.net. For example:

Wigle.net quotes Types supported:

- NetStumbler: native (.ns1), text, wiscan, summary
- DStumbler: text output
- Kismet: CSV (.csv), XML (.xml), GPS (.gps), CWGD output
- MacStumbler: plist XML, wiscan format
- Pocket Warrior: Text output

However, if you want to import it into many of the commercial map programs like Microsoft's Streets & Trips or Map Point, you will need to convert the data into a more universally read file such as a CSV formatted file. This is easily done by opening NetStumbler, left clicking on file, Left click on export, and then on Summary. Save the file with a ".CSV" extension and then close NetStumbler. Converting data in general is not that difficult, you just need to be aware of the end format. The exported file is most of the way done, but just needs to go through a little clean up before importing to another program. As illustrated in figures 2 and 2, by opening the file in a basic text editor, you can see how clean the file already is. You will just need to remove a couple lines. If you have programming skills, you can automate the process in very little time.

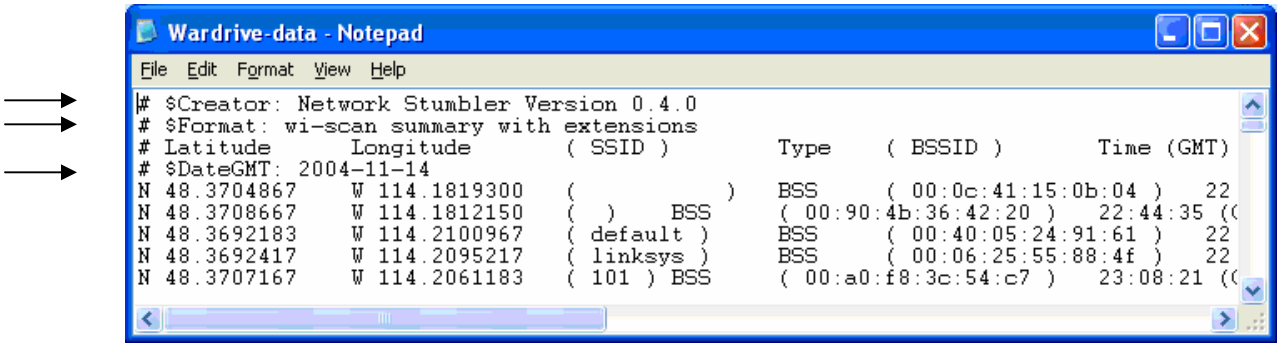

Figure 2 (NetStumbler data export containing proprietary header information)

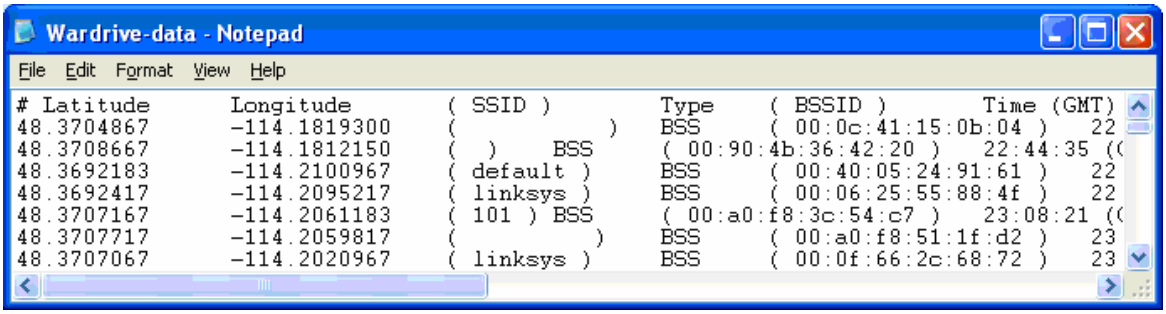

Figure 3 (NetStumbler data export after header information has been cleaned)

Now that you have used Cain, NetStumbler, or Kismet to gather the information, you can start your quest to crack the WEP. The important portion of the data that you will need to start with is the targets SSID, MAC address, and Channel.

Gathering the information

With the needed information, criminals will now start to attack the WEP, or install a Warcracker (small computer designed to automate information gathering and cracking process) that can be either accessed remotely or picked up at a later time. Information Security professionals will sometimes install these devices during a penetration tests or espionage simulations to sniff traffic and archive it for future analysis.

To stay legal while practicing "proof-of-concept", it is a good idea to create a lab environment with several WiFi access points as targets and several systems with WiFi cards to increase the amount of "interesting" traffic. Interesting traffic contains the key negotiation packets and will allow you to gather enough information by sniffing to crack the WEP key in a short period of time. This traffic can be generated by running programs like Aireplay and Void11. This will generate the required WEP initialization vectors for the cracking to take place. Airodump is easy to use and helps with this process.

For this example, the target WiFi Access Point has the SSID of WLAN, MAC address of XX:XX:XX:XX:XX:XX, and the channel of 9. We will use Airodump to capture the weak IV packets and start the passive packet capture to the file named keygen. The command should look like this from the a root level command line shell:

root@home[\]# airodump wlan0 keygen XX:XX:XX:XX:XX:XX

This will save all of the interesting packets in a file called keygen.txt that we will use shortly. However, unless you have a lot of time on your hands, you may want to speed up the process a little. Void11 is a common tool that deauthenticates the wireless clients. This works great in a lab environment, but will set off triggers in a business setting and is a symptom of a possible attack of your system. During a Kismet scan, we have found a client system with the MAC address of YY:YY:YY:YY:YY:YY. This is important because we are going to target that MAC address along with the Wireless Access Point to help generate the information we need. Using Void11, the command should look like this from the a root level command line shell:

root@home[\]# void11_penetration -D -s YY:YY:YY:YY:YY:YY -B XX:XX:XX:XX:XX:XX wlan0

For shorten the time it takes even more, many people use Void11 in conjunction with Aireplay. This program captures valid traffic and replays the traffic and sends it to the Access Point to generate more of the right traffic.

root@home[\]# aireplay -i wlan0 -b XX:XX:XX:XX:XX:XX -m 68 -n 68 -d YY:YY:YY:YY:YY:YY

The entire time the programs Void11 and Aireplay are running, Airodump is capturing packets that will be used in the cryptanalysis process. With multiple systems generating the traffic, a sniffer can record data faster and increase the time it takes to uncover the key. Aerodump can be used to save the traffic to a file, and aircrack can then take that file to attack the key. The whole trick is to force the WiFi device to generate the right traffic.

Cracking the WEP

Now we have a file ready to be sent to the butcher. This is where Aircrack comes in. It will use the Airodump data and start the cracking process to generate the correct key. To break 128 bit WEP, the file will need to have 200,000 to 700,000 unique IV packets. Assuming that we have a good enough file, we attack the file to get the key. Using Aircrack, the command should look like this from the root level command line shell:

root@home[\]# aircrack -f 2 -m XX:XX:XX:XX:XX:XX -n 128 -q 3 keygen.cap*

When the key has been discovered, you should see "KEY FOUND!". At this point, the Wireless Access Point has been compromised and can be accessed. You have now cracked WiFi encryption!

A similar method was use at an ISSA meeting in Los Angeles, a local team of FBI special agents cracked a 128 bit WEP key in three minutes using commonly found tools available off the Internet. This demonstration was done to prove that even WEP 128 is a vulnerable encryption and should no longer be used when securing WiFi hotspots. Keep in mind, the more computers generating interesting packets, the faster you can break the WEP.

In this article, we have discussed the entire process of cracking WEP encryption from the initial search during Wardriving or Warwalking. It is important to become familiar with scanning tools like Cain, Kismet, NetStumbler, and MiniStumbler to help survey the area. The either tools that have been covered should give you the ability to crack your own WEP key and may now have the extra push you need to convince those with WiFi to move to the next level of security, WPA. WPA or WPA2 encryption is the new commercial standard and is more difficult to break.

* Disclaimer: *Do not connect to Wireless networks that you do not have authorization to use. Many businesses are more then happy to share their WiFi signal with you if you are a customer. On the other side of the coin, private parties such as home users are usually not as friendly when they see someone parked outside their house in the middle of the night and may call the police. Depending on the laws and regulations in your area, this may be considered illegal. Just remember, Wardriving is the catch and release for geeks. Be safe, be smart, and happy Wardriving.*

About the author:

Jeremy Martin has been in the Information Security field for many years as both an instructor and consultant specializing in penetration testing and espionage simulations.

Resources:

Windows WiFi

- http://www.NetStumbler.com (NetStumbler & MiniStumbler)
- http://www.oxid.it (Cain & Able)

Linux WiFi (Some of these applications have a port to Windows)

- http://freshmeat.net/projects/aircrack (Aircrack, Aireplay, Airodump)
- http://sourceforge.net/projects/airpwn (Airpwn)
- http://sourceforge.net/projects/airsnort (Airsnort)
- http://www.kismetwireless.net/ (Kismet)
- http://wepcrack.sourceforge.net/ (WEPCrack)

WiFi Hotspot online maps

- http://www.wifimaps.com/
- http://wigle.net/

Other good resources

- http://www.cwnp.com (Planet3 Wireless)
- http://www.infosecwriter.com (More articles and artwork by this author)
- http://www.oissg.org (Open Information Systems Security Group)
- http://www.revision3.com (Home of Several Hack/Computer ezines)
- http://www.seattlewireless.net (Seattle Wireless)
- http://www.tomsnetworking.com/Sections-article111-page1.php (FBI Cracks WEP)