CHAPTER

9

Securing Wireless Systems

Ever hear the saying ‘‘the more things change the more thing stay the same?’’ Consider the not-too-distant past when people used modems and dialup accounts. During this time, wardialing became very popular. Programs like ToneLoc and Scan were popular. Hackers of the time would call ranges of phone numbers looking for systems with modems tied to them. Administrators fought back by limiting the hours that modems were on, started using callback systems, and added caller ID.

Then came the move to the early Internet. The same methodology of wardialing was carried over to port scanning. The attacker used this newer technology as a way to search for access to a vulnerable system. Administrators were forced to add firewalls, intrusion detection, and filter access to unneeded ports at the edge of the network. Today, many networks have switched to wireless. After all, it’s an inexpensive method to add connectivity for local users. Attackers see wireless in the same way that the previous technologies were viewed. Wireless wardriving tools can be used to connect to unsecured networks or tools can be used in an attempt to break weak encryption. Again, administrators must be ready to respond to the threat.

This chapter discusses attacking and securing wireless. I start by discussing some wireless basics, and then move on to methods used to attack and secure wireless systems. Wireless communication plays a big role in most people’s lives, from cell phones and satellite TV to data communication. Most of you probably use a cordless phone at your house or wireless Internet at the local coffee shop. Do you ever think about the security of these systems once the information leaves the local device? You next-door neighbor may be listening to your cordless phone calls with a UHF scanner, or the person next to you at the coffee shop may be sniffing your wireless connection to steal credit card numbers, passwords, or other information. Securing wireless communication is an important aspect of any security professional's duties.

Wi-Fi Basics

The term *wireless* can apply to many things, such as cell phones, cordless phones, global positioning systems (GPS), AM/FM radio, LAN wireless systems, or WAN wireless systems, to name a few. For the purpose of this book, I am discussing IEEE 802.11 LAN wireless systems, or Wi-Fi. Wireless Fidelity (Wi-Fi) is the consumer-friendly name given to the 802.11 family of wireless networking protocols. The idea was to give consumers a more market-friendly name than the technical-sounding 802.11. This family of protocols was created by the Institute of Electrical and Electronics Engineers (IEEE).

The IEEE also oversees wired versions of Ethernet such as 802.3. From an equipment standpoint, wireless costs are similar to those of their wired counterparts. The big difference is that there are none of the cable plant costs associated with wired LANs. The cable plant is the physical wires that make up your network infrastructure. Therefore, a business can move into a new or existing facility with cabling and incur none of the usual costs of running a LAN drop to each end user. Although wireless does have its advantages, you need to consider some issues before deciding that wireless is the perfect connectivity solution, including the following:

- Wired Ethernet is typically faster than most versions of wireless.
- Obstacles and interference don't affect wired Ethernet the same way they affect wireless.
- Wired Ethernet doesn't have a drop in performance the way that wireless does, as long as maximum cable lengths are not exceeded.
- Wired Ethernet is more secure than wireless in that the attacker must gain access to the physical cable plant. A denial of service attack is also harder to launch in a wired system.

Just consider the fact that wireless networks broadcast data through the public airwaves rather than over network cable. To intercept data on a wired LAN, an intruder must have physical access to the network either by physically connecting over the local Ethernet LAN or by logically connecting over the Internet. Wireless systems make it possible for the attacker to sit in the parking lot across the street and receive the signal. Even if you encrypt the data on your wireless network, the attacker can still sniff it. Before we get too far into the ways in which wireless can be attacked, let's start by discussing some wireless fundamentals, and then we will move on to wireless attacks, hacking tools, and finally some ways to secure wireless networks.

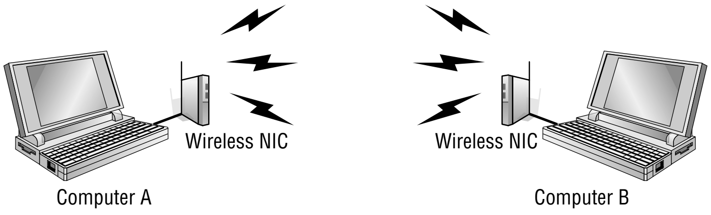


Figure 9-1 Wireless ad hoc mode.

Wireless Clients and NICs

Wireless networks require the client to use a wireless adapter or wireless network interface card (NIC) to connect to the network and communicate with other computers. An access point (wireless router) can provide Internet connectivity to multiple users. A simple wireless LAN consists of two or more computers connected via a wireless connection. No cables or wired connections are required. The computers are connected via wireless NICs that transmit the data over the airwaves. Figure 9-1 shows an example of this.

Actually, Figure 9-1 shows two computers operating via wireless in *ad hoc* mode. Wireless systems can operate in either *ad hoc* or *infrastructure mode*. Ad hoc mode doesn't need any equipment except wireless network adapters. Ad hoc mode allows a point-to-point type of communication that works well for small networks, and is based on a peer-to-peer style of communication. Infrastructure mode makes use of a wireless access point (WAP). A WAP is a centralized wireless device that controls the traffic in the wireless medium. Figure 9-2 shows an example of a wireless LAN (WLAN) setup with a WAP.

In infrastructure mode, the wireless device communicates with the WAP. The WAP then forwards the packets to the appropriate computer. If you want to use your wireless-equipped device with a specific WAP, it must be configured to use the same *service set ID* (SSID). The SSID distinguishes one wireless network from another. The SSID can be up to 32 bits and is case-sensitive. It is easily sniffed if it is being broadcast. Overall, if we compare ad hoc wireless networks to infrastructure mode networks, you will see that infrastructure mode is much more scalable.

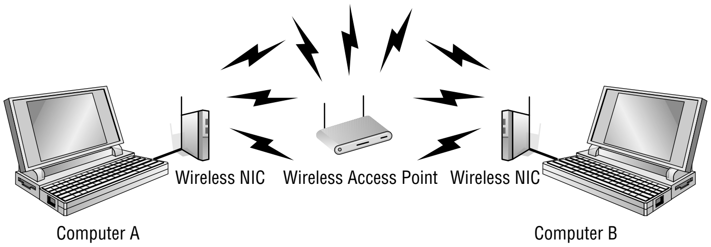


Figure 9-2 Wireless infrastructure mode.

There are some issues with wireless networks that wired networks do not have to worry about. As an example, in a wired network, it's easy for any one of the devices to detect whether another device is transmitting. In a wireless network, the WAP hears all the wireless devices, but individual wireless devices cannot hear other wireless devices. This is described as the hidden-node problem. To get around this problem, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is used. It functions by having the wireless device listen before it sends a packet. If the wireless device detects that another device is transmitting, it waits for a random period and tries again. If the first wireless device listens and discovers no other device is transmitting, it sends a short message known as the ready-to- send (RTS).

Wireless Access Points

So far, we have primarily discussed wireless devices and how they can communicate with each other or with the WAP. Let's look now at the WAP. WAPs can operate in several different modes depending on what you buy and how much money you spend. These modes are as follows:

- **Normal mode** — Provides a central point of connection for client wireless devices
- **Bridge mode** — Enables the access point (AP) to communicate directly with another AP. This requires that both APs be capable of point-to-point bridging. This technology is useful for extending a WLAN between buildings
- **Client mode** — Enables the AP to operate as a network client, communicating with other APs, not with other clients
- **Repeater mode** — Provides a method to repeat another access point's signal and extends its range

Wireless Communication Standards

Next let's take a look at some of the popular wireless standards for use with WLANs. Table 9-1 lists the specifications for these standards.

The first of these protocols to be released was actually 802.11b. The IEEE does not always release these standards in alphabetic order. The 2.4GHz band is unlicensed and is known as the Industrial, Scientific, and Medical (ISM) band. When operating, these devices may interfere with 802.11b, 802.11g, or 802.11n communications.

The 802.11 family of protocols defines the physical layer standards by which the protocols work. These standards describe the frequency, band, and

Table 9-1 IEEE WLAN Standards

IEEE STANDARD	ESTIMATED SPEED	FREQUENCIES
802.11a	54Mbps	5.725 to 5.825
802.11b	11Mbps	2.400 to 2.2835
802.11 g	54Mbps	2.400 to 2.2835
802.11n	540Mbps	2.400 to 2.2835

the transmission technology used to access the network and communicate in the defined band. The 802.11b, 802.11 g, and 802.11n systems divide the usable spectrum into 14 overlapping staggered channels whose frequencies are 5 MHz apart. The channels that are available for use in a particular country differ according to the regulations of that country. As an example, in North America 11 channels are supported, whereas most European countries support 13 channels.

Most wireless devices broadcast by using spread-spectrum technology. This method of transmission transmits data over a wide range of radio frequencies (RFs). Spread spectrum lessens noise interference and allows data rates to speed up or slow down, depending on the quality of the signal. Spread spectrum is an RF communications system in which the baseband signal bandwidth is intentionally spread over a larger bandwidth by injecting a higher-frequency signal. Thus, energy used in transmitting the signal is spread over a wider bandwidth and appears as noise. This technology was pioneered by the military to make *eavesdropping* difficult and increase the difficulty of signal jamming. Currently, the following types of spread-spectrum technology exist: direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), and orthogonal division multiplexing (ODM).

- **DSSS** — This method of transmission divides the stream of information to be transmitted into small bits. These bits of data are mapped to a pattern of ratios called a spreading code. The higher the spreading code, the more the signal is resistant to interference, but the less bandwidth is available. The transmitter and the receiver must be synchronized to the same spreading code.
- **FHSS** — This method of transmission operates by taking a broad slice of the bandwidth spectrum and dividing it into smaller subchannels of about 1MHz. The transmitter then hops between subchannels, sending out short bursts of data on each subchannel for a short period of time.

This is known as the dwell time. For FHSS to work, all communicating devices must know the dwell time and must use the same hopping pattern.

Because FHSS uses more subchannels than DHSS, it can support more wireless devices. FHSS devices also typically use less power and are the cheaper of the two types.

- **ODM** — This spread-spectrum technique uses frequency division multiplexing and distributes data over carriers that are spaced apart at precise frequencies. The spacing provides the ''orthogonality'' and prevents demodulators from seeing frequencies other than their own. The benefits of this technology include resiliency to RF interference and lower multi-path distortion; the technology is sometimes called multi-carrier or discrete multi-tone modulation. The technique is used for digital TV in Europe, Japan, and Australia.

Bluetooth Basics

A review of wireless basics would not be complete without some mention of *Bluetooth*. This is another technology you will most likely come in contact with. Bluetooth is a wireless personal area network (PAN) technology developed by the Bluetooth Special Interest Group. The Bluetooth technology was originally conceived by Ericsson to be a standard for small, cheap radio-type devices that would replace cables and allow for short-range communication. Bluetooth technology enables users to connect many different devices simply and easily without cables. It is named after Harald Bluetooth, King of Denmark in the late 900s, and is used specifically to provide a peer-to-peer service to cellular phones, laptops, handheld computers, digital cameras, printers, and the like. It uses FHSS technology and hops 1,600 times per second among 79 RF channels. By the mid 1990s, the technology started to grow, and by 2000 its usage had become much more widespread. The three classifications of Bluetooth are as follows:

- **Class 1** — Has the longest range, up to 100 meters, and has 100mW of power.
- **Class 2** — Although not the most popular, it allows transmission up to 20 meters and has 2.5mW of power.
- **Class 3** — This is the most widely implemented and supports a transmission distance of 10 meters and has 1mW of power.

The IEEE group for Bluetooth is 802.15.1. Bluetooth operates at the 2.45GHz frequency. Bluetooth divides the bandwidth into narrow channels to avoid interference with other devices that utilize the same frequency.

THE REAL RANGE OF BLUETOOTH

One reason why Bluetooth did not originally have strong security controls built in was that it was believed that Bluetooth could be targeted only from a very close range. That theory didn't last long; in 2005, a presentation at Black Hat demonstrated that Bluetooth could be targeted from up to about a mile away. If the attacker was targeting a high-rise or office building, several antennas could be used to track a specific individual as he moved around the building. The actual device used to sniff Bluetooth at these ranges was little more than a modified antenna, duct tape, a gun stock, cable, and tie wraps. Anyone could build such a device in an afternoon. If you would like to learn more about this hack or might even want to build your own Bluetooth long-range antenna, take some time to review the information at the following URL: `www.tomsnetworking.com/2005/03/08/how_to_bluesniper_pt1`.

Wi-Fi Security

Wired and wireless networks are very different from a security standpoint. First, on a wired network the user must gain some access to the physical wire or connector. Second, the network card must be connected to the network. Finally, there is the issue of authentication. Most networks require a user to authenticate himself or herself with a password, token, or biometric (or combination of these). On a wireless network, these issues were initially overlooked in the first wireless security standard, Wired Equivalent Privacy (WEP).

Wired Equivalent Privacy

WEP was designed to provide the same privacy that a user would have on a wired network. WEP is based on the RC4 symmetric encryption standard and uses either a 64-bit or 128-bit key. WEP's security issue actually begins here, because the entire 64- or 128-bit key is not used for encryption, and 24 bits of this key are actually pealed off for use as an initialization vector (IV). The purpose of the IV is to encrypt each packet with a different key. This is accomplished by adding the IV to the 40-bit or 104-bit preshared key (PSK). The result is IV + PSK. This also has reduced the effective key strength of the process because the effective lengths of the keys are now only 40 or 104 bits.

There are two ways to generate and use the PSK:

- First, the default key method shares a set of up to four default keys with all the WAPs.

- Second is the key-mapping method, which sets up a key-mapping relationship for each wireless station with another individual station. Although slightly more secure, this method is more work; it adds overhead and reduces throughput somewhat. This overhead means many systems that use WEP opt to use a single shared key on all stations.

To better understand the WEP process, you need to understand the basics of Boolean logic. Specifically, you need to understand how XORing (exclusive OR) works. XORing is just a simple binary comparison between 2 bits that produce another bit as a result of the XORing process. When the 2 bits are compared, XORing looks to see whether they differ. If the answer is yes, the resulting output is a 1. If the 2 bits are the same, the result is a 0. Table 9-2 shows an example of this.

Table 9-2 XOR Functions

VALUE				
DATA BIT	1	0	1	0
KEY BIT	1	0	0	1
RESULTING VALUE	0	1	1	0

To better understand this process and to understand how WEP functions, let's look at the seven steps for encrypting a message:

1. The transmitting and receiving stations are initialized with the secret key. This secret key must be distributed by using an out-of-band mechanism such as email, posting it on a web site, or giving it to you on a piece of paper (as many hotels do).
2. The transmitting station produces a seed, which is obtained by appending the 40-bit secret key to the 24-bit IV, for input into a pseudo-random number generator (PRNG).
3. The transmitting station inputs the seed to the WEP PRNG to generate a key stream of random bytes.
4. The key stream is XOR'd with plaintext to obtain the ciphertext.
5. The transmitting station appends the ciphertext to the IV and sets a bit that indicates that it is a WEP-encrypted packet. This completes WEP encapsulation, and the results are transmitted as a frame of data.
   WEP encrypts only the data. The header and trailer are sent in clear text.
6. The receiving station checks to see whether the encrypted bit of the frame it received is set. If so, the receiving station extracts the IV from the frame and appends the IV to the secret key.

7. The receiver generates a key stream that must match the transmitting station's key. This key stream is XOR'd with the ciphertext to obtain the sent plaintext.

The big problem with WEP is that the IVs are not exclusive and are reused. This results in a big vulnerability in that reused IVs expose the PSK. To demonstrate this better, consider the following. Let's assume that our PSK is 8765309. This value would be merged with qrs to create the secret key of qrs8765309. This value would be used to encrypt a packet. The next packet would require a new IV. Therefore it would still use the PSK 8765309 but this time it would concatenate it with the value mno to create a new secret key of mno8765309. This would continue for each packet of data created. This should help you realize the changing part of the secret key is the IV, and that's what WEP cracking is interested in. A busy AP that sends a constant flow of traffic will actually use up all possible IVs after five to six hours. Once someone can capture enough packets so that he has reused keys, WEP can be cracked. Tools such as WEP Crack and AirSnort were created for just this purpose.

While wireless vendors did work to remove weak IVs, attackers were looking for other ways to crack the encryption standard. In August 2004, a hacker named KoreK released a new piece of attack code that sped up WEP key recovery by nearly two orders of magnitude. Instead of using the passive approach of collecting millions of packets to crack the WEP key, his concept was to actively inject packets into the network. The idea is to solicit a response from legitimate devices on the WLAN. Even though the hacker can't decipher these packets in their encrypted form, he can guess what they are and use them in a way to provoke additional traffic-generating responses. This makes it possible to crack WEP in less than 10 minutes on many wireless networks. With these issues on everyone's mind, IEEE knew that a new encryption standard would be needed. After all, WEP did not even ensure the authenticity of the data packets.

Wi-Fi Protected Access

The task force assigned to address the growing security needs of wireless users is 802.11i. They were challenged not only to develop a long-term standard but also to develop something that could be used to secure wireless systems quickly. To meet these two demands, Wi-Fi Protected Access (WPA) was developed as a short-term solution.

WPA delivers a level of security way beyond what WEP offers. WPA uses Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and adds an integrity-checking feature that verifies that the keys haven't been tampered with. WPA improves on WEP by increasing the IV from 24 bits to 48. Rollover has also been eliminated, which means key reuse is less likely to occur. WPA also avoids another weakness of WEP by using a different secret key for each packet. Another improvement in WPA is message integrity. WPA addressed a message integrity check (MIC) that is known as Michael. Michael is designed to detect invalid packets and can even take measures to prevent attacks. Best of all, WPA is backward compatible and can work with the RC4 algorithm. This enables users to upgrade existing hardware that may not be able to work with more intense cryptographic algorithms.

In 2004, the long-term solution to wireless security was approved with the release of WPA2. This is the standard that the 802.11i group had been working toward. It was designed to use Advanced Encryption Standard (AES). AES requires much more processing power than RC4, which was included with the original 802.11 design. Key sizes of up to 256 bits are now available, which is a vast improvement over the original 40-bit encryption WEP used. Table 9-3 shows the common modes and types of WPA and WPA2.

WPA and WPA2 can use a variety of security protocols such as Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP is based on the AES encryption algorithm. It expands the IV to 48 bits to prevent rollover and detects replayed traffic. Another WPA authentication protocol is *Extensible Authentication Protocol* (EAP), defined in RFC 3758. EAP is an authentication framework, not an authentication mechanism. EAP rides on top of the Ethernet protocol to facilitate authentication between the client requesting to be authenticated and the server performing the authenticating. There is also EAP over LAN (EAPOL), which the IEEE approved as a transmission method to move packets from the client to an authentication server. There are four basic types of EAPOL packets:

- **The EAPOL packet —** This message type is simply a container for transporting EAP packets across a LAN.
- **The EAPOL start —** This message is used by the client to inform the authenticator it wants to authenticate to the network.

Table 9-3 WPA and WPA2 Differences

MODE	WPA	WPA2
ENTERPRISE MODE	Authentication: IEEE 802.1x EAP	Authentication: IEEE 802.1x EAP
	Encryption: TKIP/MIC	Encryption: AES/CCMP
PERSONAL MODE	Authentication: PSK	Authentication: IEEE 802.1x EAP
	Encryption: TKIP/MIC	Encryption: TKIP/MIC

- **The EAPOL logoff —** The message informs the authenticator that the client is leaving the network.
- **The EAPOL key —** This message type is used with 802.1x for key distribution.

Finally, there is Temporal Key Integrity Protocol (TKIP). TKIP is used to address the known cipher attack vulnerability that WEP was vulnerable to. TKIP's role is to ensure each data packet is sent with its own unique encryption key. TKIP uses the RC4 algorithm.

802.1x Authentication

802.1x provides port-based access control. When used in conjunction with EAP, it can be used as a means to authenticate devices that attempt to connect to a specific LAN port. Although EAP was designed for the wired world, it is being bundled with WPA as a means of communicating authentication information and encryption keys between a client or supplicant and an access control server such as RADIUS. In wireless networks, EAP works as follows:

1. The WAP requests authentication information from the client.
2. The user then supplies the requested authentication information.
3. The WAP then forwards the client-supplied authentication information to a standard RADIUS server for authentication and authorization.
4. The client is allowed to connect and transmit data upon authorization from the RADIUS server.

There are other ways the EAP can be used depending on its implementation: password, digital certificates, and token cards are the most common forms of authentication used. EAP can be deployed as EAP-MD5, Cisco Lightweight EAP (LEAP), EAP with Transport Layer Security (EAP-TLS), or EAP with Tunneled TLS (EAP-TTLS).

IN THE LAB

All this talk of wireless may have you thinking of how to apply this to your network security lab. The best place to start is by observing some wireless traffic with and without encryption. You will need a WAP, wireless card, and a sniffer to complete this task. You will find Wireshark already installed in the BackTrack distribution. Use your Windows client to connect to your WAP, and make sure that all encryption is turned off. This primarily includes WEP and WPA, as those are the two most commonly found protocols. Once the WAP has been reconfigured, start BackTrack and connect through a wireless card to the

(continued)

IN THE LAB *(continued)*

Internet. Now start Wireshark and ensure that it is capturing traffic. Browse several pages on the Internet and then stop Wireshark. If you look at any one individual frame from the wireless client, you will notice that everything is in clear text.

Next, you will want to reconfigure the access point to use WEP or WPA. Again, start capturing traffic with Wireshark and browse several random pages on the Internet. Stop the capture; notice how the traffic is now encrypted? Even with the encryption, you might notice that the media access control (MAC) addresses (physical addresses) are still in the clear. WEP and WPA protect the contents of the packet and not the physical frame. When finished verify the WAP has encryption turned on.

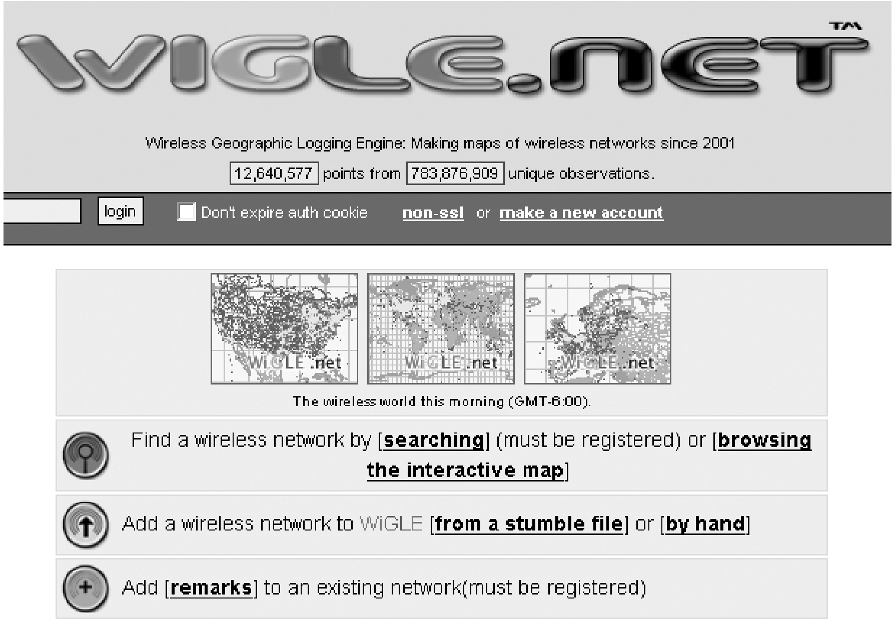
Wireless LAN Threats

Wireless networks are open to a number of threats that you may not ever even consider on a wired network. This section discusses some of the attacks that can be launched against a wireless LAN. These include wardriving, eavesdropping, rogue APs, and denial of service attacks.

Wardriving

As you learned in Chapter 3, ''Passive Information Gathering,'' *wardriving* is the term used to describe someone who uses a laptop and a wireless NIC to look for wireless networks. The entire act of searching for wireless networks has created some unique activities such as the following:

- **Wardriving** — The act of finding and marking the locations and status of wireless networks. This activity is usually performed by automobile. The wardriver typically uses a Global Positioning System (GPS) device to record the location, and a discovery tool such as NetStumbler.
- **Warchalking** — The act of marking buildings or sidewalks with chalk to show others where it's possible to access an exposed company wireless network.
- **War flying** — Similar to wardriving, except that a plane is used rather than a car. One of the first publicized acts occurred in the San Francisco area.



Wireless Geographic Logging Engine: Making maps of wireless networks since 2001

12,640,577 points from 783,876,909 unique observations.

The wireless world this morning (GMT-6:00).

Find a wireless network by [searching] (must be registered) or [browsing the interactive map]

Add a wireless network to WiGLE [from a stumble file] or [by hand]

Add [remarks] to an existing network(must be registered)

Figure 9-3 www.wigle.net wireless LAN tracking.

As you can see, the concept is simple: move from place to place and look for wireless networks. If the wardriver has a GPS attached to his laptop or handheld device, all he needs to do is log this data, and over time he can start to assemble a database of networks and their location. Some web sites have even been set up for just this purpose. Figure 9-3 show one such site, `www.wigle.net`.

On the surface, there may not be anything illegal with someone searching for and finding wireless networks. The real concern is what comes next. Piggybacking is the first issue that comes to mind. Just like addicts need a fix, some people *need* Internet access. It might be the guy across the hall at the apartment building who just doesn't have the cash for his own Internet access, or it could be the road warrior who needs to check his email and feels he just can't wait till he gets home or back to the office.

BLACKBERRYS AND EMAIL ADDICTION

On April 19 2007, Research in Motion, makers of the BlackBerry handheld devices, suffered an outage in the push technology they use to deliver email to their handheld devices. The reaction from many users was similar to what is

(continued)

BLACKBERRYS AND EMAIL ADDICTION *(continued)*

seen in individuals that suffer from addiction. This included craving, stress, emotional upset, and the desire to quickly get the addictive substance back. So much was actually made of the outage that some have even gone as far as to describe BlackBerrys as "CrackBerrys" because of the device's supposed addictive nature. According to `http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=401646&in_page_id=1770`, a study performed claims the BlackBerry is fuelling a rise in email addiction that can be identified by the fact that sufferers must check their email every few minutes. Whether this is a real addiction is yet to be proven. But what is known is that people will go to great lengths to check email or get Internet access to do so.

The second group of people to be concerned with are wireless hackers who would like to use an organization's wireless connection to gain access to its resources. These individuals want to access sensitive information, gain top-secret data, or crash a critical system. Although not everyone scanning for wireless networks is trying to cause damage or harm to your company's computers, it is something to be concerned about.

IN THE LAB

With wireless security being such an important topic, you may be wondering how to plug all these potential security holes. In the lab, you can start by turning on encryption. You will also want to practice defense in depth. Therefore, you should apply more than just this one defensive measure. For example, you might want change the SSID and not broadcast it, turn off DHCP for wireless clients, and limit or filter which MAC addresses can connect to the network. While it is true that some of these defenses may be overcome by an attacker, the idea is to raise enough barriers that they move on to other targets. Practice implementing each of the controls in the lab environment and consider ways in which security can be applied in layers.

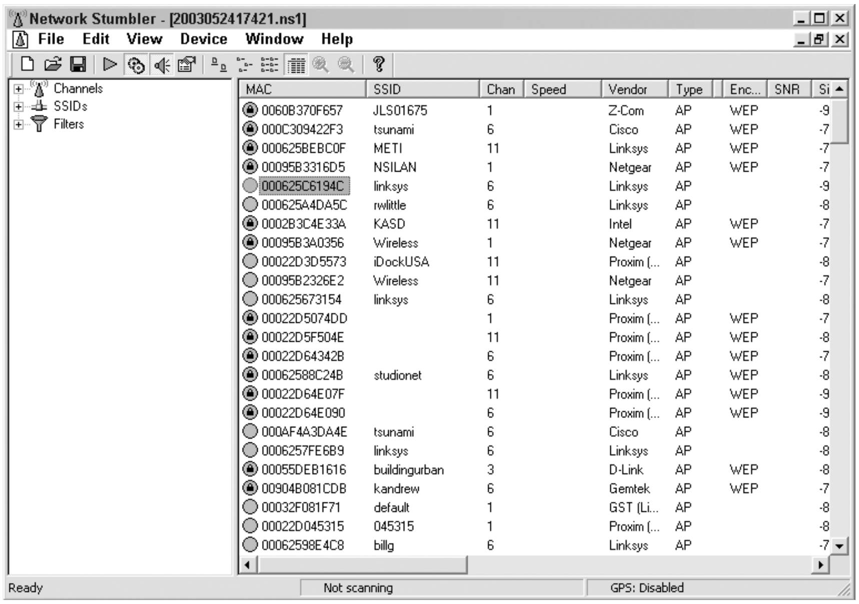
NetStumbler

One of the primary tools used to locate wireless networks is NetStumbler. You can download the program from `www.netstumbler.com`. NetStumbler is a Windows-based GUI tool that you can use as a wireless scanner. It operates by sending out a steady stream of broadcast packets on all channels. It's useful for checking the coverage of an organization's wireless LAN. Figure 9-4 shows a screenshot of NetStumbler.

Netstumbler can provide the user with a wealth of information such as:

- MAC address
- SSID
- Access point name
- Channel
- Vendor
- Security (WEP on or off)
- Signal strength
- GPS coordinates (if GPS device is attached)

MiniStumbler is a version of the software that is available for handheld devices.


Network Stumbler - [2003052417421.ns1]
File Edit View Device Window Help
Channels
SSIDs
Filters
Ready
Not scanning
GPS: Disabled

MAC	SSID	Chan	Speed	Vendor	Type	Enc...	SNR	Si
0060B370F657	JLS01675	1		Z-Com	AP	WEP		-9
000C309422F3	tsunami	6		Cisco	AP	WEP		-7
000625BEBC0F	METI	11		Linksys	AP	WEP		-7
00095B3316D5	NSILAN	1		Netgear	AP	WEP		-7
000625C6194C	linksys	6		Linksys	AP			-9
000625A4DA5C	rwlittle	6		Linksys	AP			-8
0002B3C4E33A	KASD	11		Intel	AP	WEP		-7
00095B3A0356	Wireless	1		Netgear	AP	WEP		-7
00022D3D5573	iDockUSA	11		Proxim (...	AP			-8
00095B2326E2	Wireless	11		Netgear	AP			-7
000625673154	linksys	6		Linksys	AP			-8
00022D5074DD		1		Proxim (...	AP	WEP		-7
00022D5F504E		11		Proxim (...	AP	WEP		-8
00022D64342B		6		Proxim (...	AP	WEP		-7
00062588C24B	studionet	6		Linksys	AP	WEP		-8
00022D64E07F		11		Proxim (...	AP	WEP		-9
00022D64E090		6		Proxim (...	AP	WEP		-9
000AF4A3DA4E	tsunami	6		Cisco	AP			-8
0006257FE6B9	linksys	6		Linksys	AP			-8
00055DEB1616	buildingurban	3		D-Link	AP	WEP		-8
00904B081CDB	kandrew	6		Gemtek	AP	WEP		-7
00032F081F71	default	1		GST (Li...	AP			-8
00022D045315	045315	1		Proxim (...	AP			-8
00062598E4C8	billg	6		Linksys	AP			-7

Figure 9-4 NetStumbler.

Using NetStumbler is rather straightforward. Just download and install the program onto a laptop computer that has a wireless NIC. The most common type of wireless card that is used is one that has an attachment for an external antenna. Cards such as the Proxim and Cisco are popular because both have jacks for external antennas. Using an external antenna allows the attacker to extend the range and to either use a focused directional antenna or an omnidirectional magnetic-based antenna that can be easily mounted to the roof of a car. This allows the wardriver to easily move around looking for WAPs. Figure 9-5 shows an example of this.

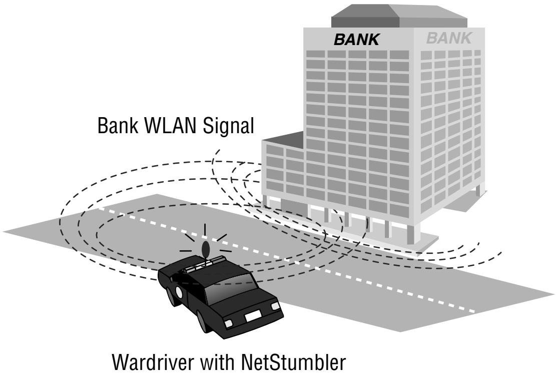


Figure 9-5 Wardriving with NetStumbler.

IN THE LAB

Since you are building your own security lab, NetStumbler is a good tool to perform site surveys. It enables you to examine your organization's wireless infrastructure and coverage. NetStumbler can also be used to look for rogue APs. You never know when an employee may have illegally added a WAP without the organization's permission. Finally, just because you don't find any rogue APs, don't be fooled into thinking the organization is 100 percent clear, because NetStumbler does not look at the 900MHZ or 5GHz frequencies.

NetStumbler works by sending probe request frames that cause APs to respond with information about themselves. The normal operation of a WAP is for it to transmit beacons about 10 times a second. The beacons provide information on time, capabilities, supported rates, and the SSID. If the WAP supports the closed network feature, NetStumbler will not get a response, provided that the WAP does not respond to probe request frames using broadcast SSIDs.

Even if the WAP is in a hidden mode, there are still ways for the attacker to get the SSID. All the attacker has to do is to send a spoofed disassociate message. The message simply tells the WAP to dissociate an active station. The spoofed client will then be forced to reassociate with the WAP. To do this, the client cycles through probe requests within a second after the disassociation attack. BackTrack contains the Void11 tool, which will accomplish just such an attack. It can also be downloaded from `www.wirelessdefence.org/Contents/Void11Main.htm`. (Note that the URL is case sensitive.) This method forces a hidden WAP to reveal its SSID.

Kismet

Kismet is an 802.11 Layer 2 wireless network detector that runs on the Linux OS. It is also available on BackTrack or can be downloaded from `www.kismetwireless.net`. Kismet works with many wireless cards and has a similar functionality to NetStumbler's. Kismet has the following features:

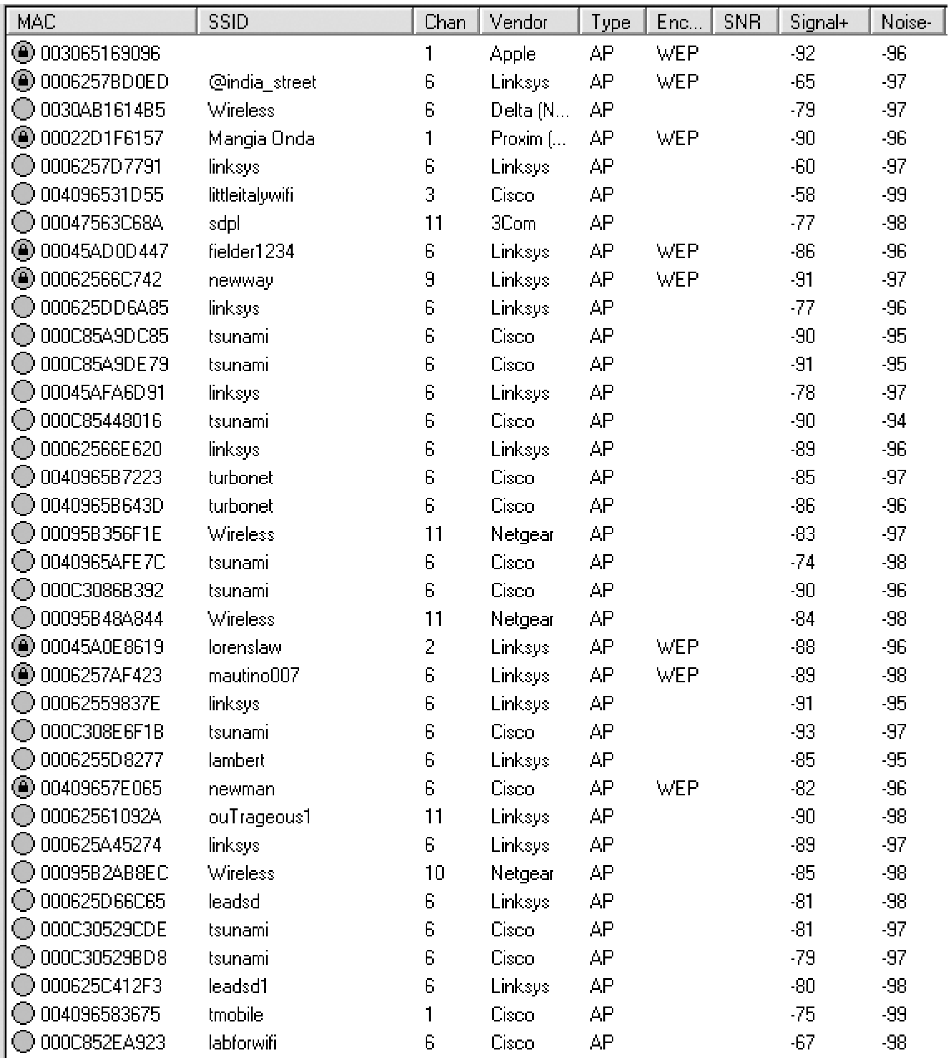
- Detection of NetStumbler clients
- Cisco product detection via CDP
- IP block detection
- Hidden SSID decloaking
- Ethereal file logging
- Airsnort-compatible weak key logging
- Run-time decoding of WEP packets
- Grouping and custom naming of SSIDs
- Multiple clients viewing a single capture stream
- Graphical mapping of data
- Manufacturer identification
- Detection of default WAP configurations

NetStumbler and Kismet are just two of the tools available for site surveys and wardriving activities.

Eavesdropping

Eavesdropping is another WLAN threat. If a hacker can use NetStumbler or Kismet and find an WAP that is configured with the manufacturer's default configuration, it will likely be a target for the attacker. A WAP with even WEP installed is much less appealing for the person doing a random drive-by. Why spend the time hacking it when so many WAPs are open? Even today, WAPs are still open everywhere. As an example of this, consider the following. On a recent trip to a large West Coast city, I placed my laptop in my backpack and walked about 8 to 10 blocks. Figure 9-6 shows the results of my war walk.

Notice how only a few of those shown had encryption turned on. Out of the 140 WAPs I picked up, fewer than half had any form of encryption turned on. Now, although my war walk was just for statistical purposes, an attacker within range can take the next step and intercept the radio signals from these open WAPs and decode the data being transmitted. Nothing more than a



MAC	SSID	Chan	Vendor	Type	Enc...	SNR	Signal+	Noise-
🔒 003065169096		1	Apple	AP	WEP		-92	-96
🔒 0006257BD0ED	@india_street	6	Linksys	AP	WEP		-65	-97
○ 0030AB1614B5	Wireless	6	Delta (N...	AP			-79	-97
🔒 00022D1F6157	Mangia Onda	1	Proxim (...	AP	WEP		-90	-96
○ 0006257D7791	linksys	6	Linksys	AP			-60	-97
○ 004096531D55	littleitalywifi	3	Cisco	AP			-58	-99
○ 00047563C68A	sdpl	11	3Com	AP			-77	-98
🔒 00045AD0D447	fielder1234	6	Linksys	AP	WEP		-86	-96
🔒 00062566C742	newway	9	Linksys	AP	WEP		-91	-97
○ 000625DD6A85	linksys	6	Linksys	AP			-77	-96
○ 000C85A9DC85	tsunami	6	Cisco	AP			-90	-95
○ 000C85A9DE79	tsunami	6	Cisco	AP			-91	-95
○ 00045AFA6D91	linksys	6	Linksys	AP			-78	-97
○ 000C85448016	tsunami	6	Cisco	AP			-90	-94
○ 00062566E620	linksys	6	Linksys	AP			-89	-96
○ 0040965B7223	turbonet	6	Cisco	AP			-85	-97
○ 0040965B643D	turbonet	6	Cisco	AP			-86	-96
○ 00095B356F1E	Wireless	11	Netgear	AP			-83	-97
○ 0040965AFE7C	tsunami	6	Cisco	AP			-74	-98
○ 000C3086B392	tsunami	6	Cisco	AP			-90	-96
○ 00095B48A844	Wireless	11	Netgear	AP			-84	-98
🔒 00045A0E8619	lorenslaw	2	Linksys	AP	WEP		-88	-96
🔒 0006257AF423	mautino007	6	Linksys	AP	WEP		-89	-98
○ 00062559837E	linksys	6	Linksys	AP			-91	-95
○ 000C308E6F1B	tsunami	6	Cisco	AP			-93	-97
○ 0006255D8277	lambert	6	Linksys	AP			-85	-95
🔒 00409657E065	newman	6	Cisco	AP	WEP		-82	-96
○ 00062561092A	ouTrageous1	11	Linksys	AP			-90	-98
○ 000625A45274	linksys	6	Linksys	AP			-89	-97
○ 00095B2AB8EC	Wireless	10	Netgear	AP			-85	-98
○ 000625D66C65	leadsd	6	Linksys	AP			-81	-98
○ 000C30529CDE	tsunami	6	Cisco	AP			-81	-97
○ 000C30529BD8	tsunami	6	Cisco	AP			-79	-97
○ 000625C412F3	leadsd1	6	Linksys	AP			-80	-98
○ 004096583675	tmobile	1	Cisco	AP			-75	-99
○ 000C852EA923	labforwifi	6	Cisco	AP			-67	-98

Figure 9-6 War walking results.

wireless sniffer and the ability to place the wireless NIC into *promiscuous* mode is required. If the attacker is using an antenna, he can be even farther away, which makes these attacks hard to detect and prevent.

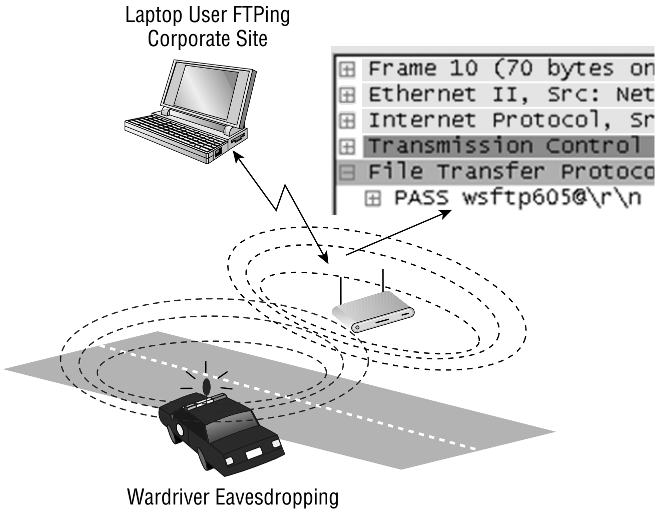
Anything that is not encrypted is vulnerable to attack. Most computer security is based on passwords. Protocols such as File Transfer Protocol (FTP), Telnet, and Simple Mail Transport Protocol (SMTP) transmit username and passwords in clear text. These protocols are highly vulnerable. Wireless equipment can be configured for open systems authentication or shared key authentication. Open systems authentication means no authentication is used.

A large portion of the wireless equipment sold defaults to this setting. If used in this state, hackers are not only free to sniff traffic on the network, they are free to connect to it and use it as they see fit. If there is a path to the Internet, the hacker may use the victim's network as the base of attack. Anyone tracing the IP address will be led back to the victim, not the hacker.

Many hotels, business centers, coffee shops, and restaurants provide wireless access with open authentication. In these situations, it is excessively easy for a hacker to gain unauthorized information, hijack resources, and even introduce back doors onto other systems. Just think about it: one of the first things most users do is check their email. This means that usernames and passwords are being passed over a totally insecure network. Tools such as Dsniff, Win Sniffer, and Cain & Abel can be used to eavesdrop and capture passwords being passed on an insecure network. Figure 9-7 shows an example of this.

Dsniff allow the attacker to focus on one specific type of traffic. Dsniff is included with BackTrack and can also be downloaded from `http://monkey.org/~dugsong/dsniff/`. Dsniff is actually a collection of tools that includes Dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy. These tools allow the attacker to passively monitor a network for interesting data such as passwords, email, and file transfers. The Windows port is available at `www.datanerds.net/~mike/dsniff`. An example capture of Dsniff is shown here:

```
C:\>dsniff
User: James
Password: Pil@t77
```



```
⊞ Frame 10 (70 bytes on
⊞ Ethernet II, Src: Net
⊞ Internet Protocol, Sr
⊞ Transmission Control
⊟ File Transfer Protoco
   ⊞ PASS wsftp605@\r\n
```

Figure 9-7 Password eavesdropping.

Win Sniffer is a password-capture utility that enables network administrators to capture passwords of any network user. Win Sniffer can capture and decode FTP, POP3, HTTP, ICQ, SMTP, Telnet, IMAP, and NNTP usernames and passwords.

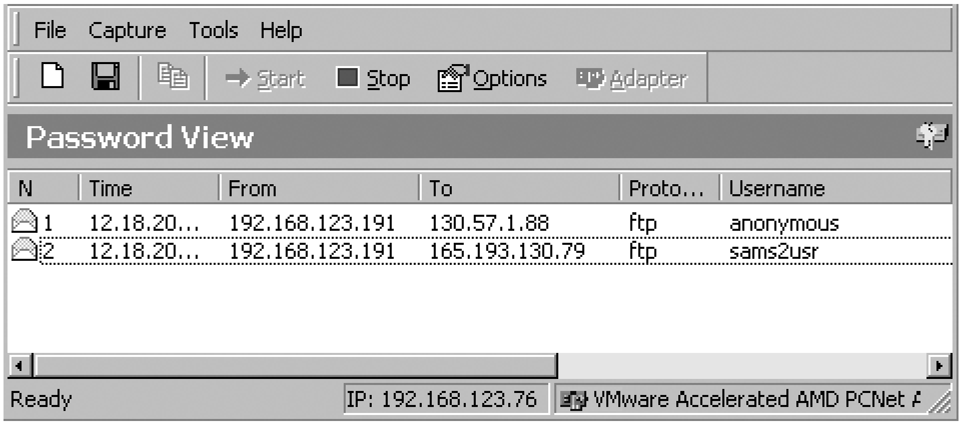
Win Sniffer is a Windows utility that is typically installed on a laptop. It can be used by security professionals to audit the network or by attackers to access sensitive information. Win Sniffer can be downloaded from `www.winsniffer.com`. Figure 9-8 shows a sample capture from the program.

Cain is a multipurpose tool that can perform a variety of tasks, including Windows enumeration, sniffing, and password cracking. Cain & Abel is shown in Figure 9-9 and is available from `www.oxid.it`. Cain & Abel will perform password sniffing and password cracking. The password-cracking portion of the program can perform dictionary and brute-force cracking, and can use precomputed hash tables.

LCP is available from `www.lcpsoft.com` and is designed to audit passwords and password strength. LCP can perform the following functions:

- Accounts information import
- Passwords recovery
- Brute-force password cracking in single or distributed more
- Hashes computing

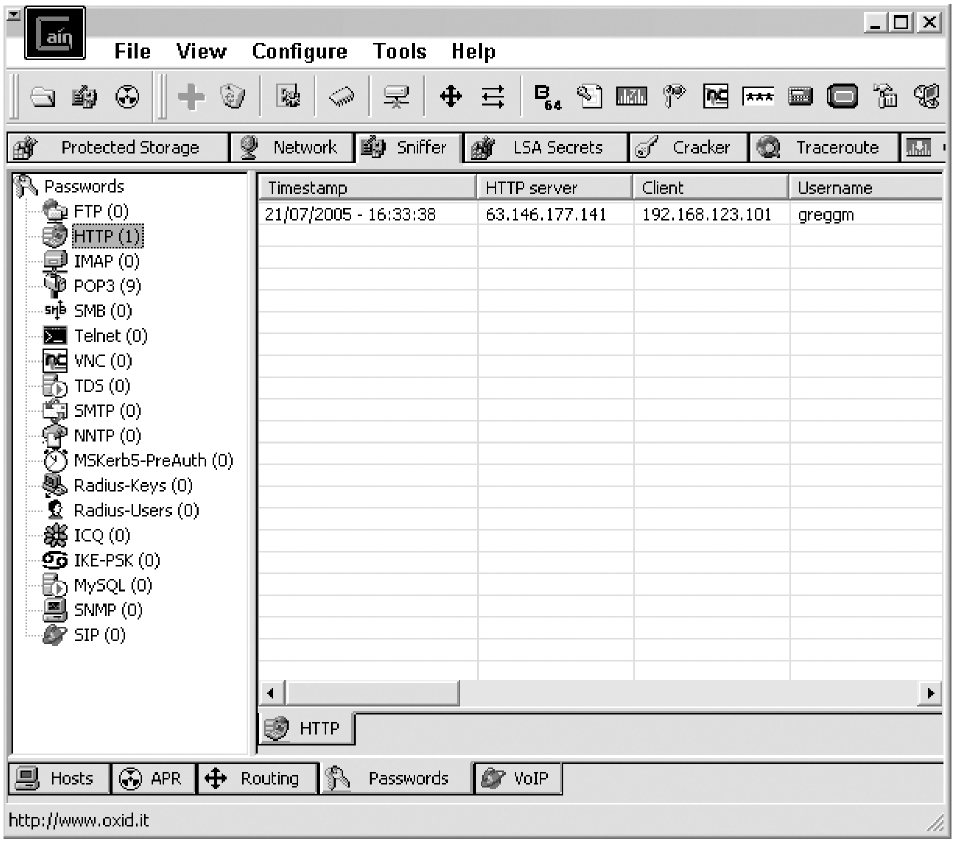
Even if encryption is being used, the Ethernet frame is still transmitted in the clear. Even the WLANs using WEP are vulnerable. Tools discussed throughout this chapter can be used to crack WEP. While the deficiencies of WEP were corrected with the WPA protocol, those WAPs still running WEP are vulnerable.



N	Time	From	To	Proto...	Username
1	12.18.20...	192.168.123.191	130.57.1.88	ftp	anonymous
2	12.18.20...	192.168.123.191	165.193.130.79	ftp	sams2usr

Ready | IP: 192.168.123.76 | VMware Accelerated AMD PCNet A

Figure 9-8 Win Sniffer.



Timestamp	HTTP server	Client	Username
21/07/2005 - 16:33:38	63.146.177.141	192.168.123.101	greggm

Figure 9-9 Cain & Abel.

Rogue and Unauthorized Access Points

A *rogue access point* is an unauthorized connection to the corporate network. A Gartner group report found that 20 percent of networks have rogue WAPs attached. Two primary threats can occur from rogue and unauthorized WAPs:

- The employee’s ability to install unmanaged APs. The ease of use of wireless equipment and the lure of freedom is just too much for some employees to resist.
- The ability to perform WAP spoofing.

The way to prevent and deter rogue WAPs installed by insiders is by building strong policies that dictate harsh punishments for individuals found to have installed rogue WAPs and by performing periodic *site surveys*.

Rogue WAPs may also be installed by outsiders seeking access. These devices pose a serious threat. Many times these devices are placed near the outside of the building. As an example, the attacker may seek to place

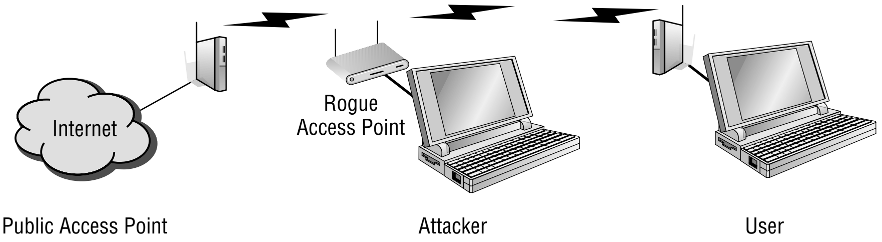


Figure 9-10 Access point spoofing.

the rogue WAP near a window or in a location close to the outside of the building so that he can sit in a parking lot or unsecured outside location and attack the network. The attacker will not want to arouse suspicion, so picking a place that he can sit and not look out of place is important. The attacker will also typically use a low-cost device, because the possibility of loss is high. If encryption is already being used on the network, the attacker will most likely also turn encryption on (because he doesn't want to arouse suspicion). Site surveys would most likely be looking for unencrypted traffic or anything that looks out of the ordinary.

Access point spoofing occurs when the hacker sets up their own rogue WAP near the victim's network or in a public place where the victim might try and connect. If the spoofed WAP has the stronger signal, the victim's computer will choose the spoofed WAP. This puts the attacker right in the middle of all subsequent transmissions. From this man-in-the-middle position, the attacker may attempt to steal usernames and passwords or simply monitor traffic. When performed in an open hot spot, this attack is sometimes referred to as the evil twin attack. Figure 9-10 shows an example of this.

Host routing is also a potential problem for wireless clients. Both Windows and Linux provide IP-forwarding capabilities. Therefore, if a wireless client is connected to both a wired and wireless networks at the same time, this may expose the hosts on the trusted wired network to all any hosts that connect via the wireless network. Just by a simple misconfiguration, an authorized client may be connected to the wired network while unknowingly having its wireless adapter enabled and connected to an unknown WLAN. If hackers can compromise the host machine via the open WLAN adapter, they are then positioned to mount an attack against the hosts on the wired network.

Denial of Service

If all else fails, an attacker can always target a wireless network for a denial of service (DoS) attack. Although a DoS attack does not get the attacker access, it does render the network unusable or degrade service for legitimate users.

These attacks can target a single device or the entire wireless network, or can attempt to render wireless equipment useless. Some common types of wireless DoS attacks are covered here:

- **Authentication flood attack** — This type of DoS attack generates a flood of EAPOL messages requesting 802.1X authentication. As a result, the authentication server cannot respond to the flood of authentication requests and consequently fails to return successful connections to valid clients.
- **Deauthentication flood attack** — This type of DoS targets an individual client and works by spoofing a deauthentication frame from the WAP to the victim. The victim's wireless device would attempt to reconnect, so the attack would need to send a stream of deauthentication packets to keep the client out of service.
- **Network jamming attack** — This type of DoS targets the entire wireless network. The attacker simply builds or purchases a transmitter to flood the airwaves in the vicinity of the wireless network. A 1,000-watt jammer 300 feet away from a building can jam 50 to 100 feet into the office area. Where would a hacker get such a device? If could be built from a microwave oven. At the heart of a microwave oven is a magnetron. Normally, a microwave oven doesn't emit radio signals beyond its shielded cabinet. The magnetron must be modified to be useful, but very little skill is required to make this modification. This type of attack would be dangerous to anyone in the general area of the transmitter, as at high level it would be like placing yourself in a microwave oven. You can also opt to buy a ready-made jammer. Here is an example for your review: `www.engadget.com/2005/07/27/spymodex-900mhz-2-5ghz-wireless-jammer`.
- **Equipment destruction attack** — This type of DoS targets the AP. The hacker uses a high-output transmitter with a directional high-gain antenna to pulse the AP. High-energy RF power will damage electronics in the WAP, resulting in its being permanently out of service. Such high-energy RF guns have been demonstrated to work, and cost little to build.

Exploiting Wireless Networks

Wireless networks can be exploited in many different ways. Previous sections of this chapter have demonstrated some of the ways in which wireless systems are vulnerable. Now let's looks at some specific tools and techniques used to exploit wireless networks.

Finding and Assessing the Network

The first thing that must be done is to find the network. The BackTrack disc included with this book has Kismet included. For the Windows user, NetStumbler can also be used. Unless you plan to hold your laptop out the window of your car as you drive around, you also want to make sure to get a good external antenna. Antennas come in two basic types: directional and omnidirectional. A directional antenna can be used in a single direction only, whereas an omnidirectional antenna can receive signals from all directions. If you want to pick up a good directional antenna, check out `www.cantenna.com` or take a look at `www.turnpoint.net/wireless/cantennahowto.html` for instructions on how to build your own. If you are unsure of the target's location, an omnidirectional antenna may be a better choice.

After locating the target network, you might want to initially use a tool such as Wireshark just to get an idea of whether the network is actually using encryption. You should be able to tell this by using Kismet or NetStumbler, but Wireshark may help you determine whether the organization is using *MAC filtering*. If that is the case, MAC-spoofing tools are needed. Change-Mac is a MAC-spoofing tool that can be used to change your computer's MAC address and bypass MAC address filtering. Change-MAC can be downloaded from `http://www.softpedia.com/get/Security/Security-Related/Change-MAC.shtml`. After you have determined whether MAC filtering is being used and what, if any, encryption is present, you can take advantage of several different tools to crack various encryption mechanisms.

Setting Up Aerodump

WEP cracking can be done from a single system or from two systems (with one injecting traffic and the second sniffing traffic). Either way, the primary tool discussed here is Aircrack. Aircrack is actually a suite of tools that provides everything you need to crack WEP. Aircrack includes the following:

- **Airodump** — Captures wireless packets
- **Aireplay** — Performs injection attacks
- **Aircrack** — Cracks the WEP key

The Aircrack suite can be started from the command line, or if you are using BackTrack it can be found at Kmenu ➪ BackTrack ➪ Wireless Tools ➪ Cracking ➪ Aircrack.

The first thing that must be done is to configure the wireless card to capture an ARP packet. The following command should be used:

```
airodump CARD dump CHANNEL 1
```

Let's look at what this command means. `CARD` is the name of the wireless card you are using, and `CHANNEL` is the channel of the AP. Common channels are 1, 6, and 11. The `1` at the end of the command line instructs Airodump to only save IVs to the file. This will also change the suffix for the capture file from `.cap` to `.ivs`.

Configuring Aireplay

Aireplay is used to inject packets to increase the selection of crackable data. Aireplay has several options that make it a powerful tool. These are listed here:

```
Attack 0: Deauthentication
Attack 1: Fake authentication
Attack 2: Interactive packet replay
Attack 3: ARP request replay attack
Attack 4: KoreK chopchop attack
Attack 5: Fragmentation attack
Attack 9: Injection test
```

Let's spend some time now getting interactive so that I can show you step by step specifically how this tool can be used. For this example, I use the deauthentication and ARP request replay attacks. For some background, ARP's (Address Resolution Protocol) purpose is to map known IP addresses to unknown MAC addresses. The first step in this two-step process is to send a broadcast message requesting the target's physical address. If a device recognizes the address as its own, it issues an ARP reply containing its MAC address to the original sender. The MAC address is then placed in the ARP cache and used to address subsequent frames. This same process holds true for wireless clients. When a wireless client attempts to communicate through an AP, it sends an ARP request. Because a wireless network does not have the reliability of a wired network, several ARPs are actually transmitted. If encryption is being used, the response is sent as encrypted traffic. Unless limits have been implemented, it might be possible to generate several hundred ARP replies per second.

Deauthentication and ARP Injection

If for some reason a client device becomes deauthenticated, it will try to reauthenticate itself with the WAP. During this process, several ARP requests will take place. To attack the WAP I can use Aireplay and the -0 attack shown above. This will effectively deauthenticate the client and force it to reauthenticate itself. Before you perform the attack, Aireplay needs to be set up on a separate system or in a different terminal window to capture the ARP request so that it can rebroadcast the packet and generate additional traffic. This is accomplished by typing the following command into a new terminal window and launching the capture:

```
aireplay -3 -b APMAC -h CLIENTMAC -x 500 DEVICE
```

This preceding command tells Aireplay to listen for an ARP request coming from the client's MAC address and directed at the WAP's MAC address, then broadcast that request 500 times per second from your wireless NIC. Now the deauthentication attack may also be run:

```
aireplay -0 10 -a APMAC -c CLIENTMAC DEVICE
```

This command specifies the `APMAC`, which is your WAP MAC address, `CLIENTMAC`, which is the client MAC address, and the `DEVICE`, which is the device name.

Capturing IVs and Cracking the WEP KEY

When the attack is launched, a steady stream of packets will be received. It might take up to approximately 300,000 packets to break 64-bit WEP and approximately 1,000,000 packets to break 128-bit WEP. To crack the key, Aircrack will be used. Aircrack can be run while packets are being captured. Aircrack common options include the following:

```
-a [mode 1 or 2] 1=WEP, 2=WPA-PSK
-e [essid] target selection network ID
-b [bssid] target access point's MAC
-q enable quiet mode
-w [path] path to a dictionary word list (WPA only)
-n [no. bits] WEP key length (64, 128, 152 or 256)
-f [fudge no.] defaults are 5 for 64 bit WEP and 2 for 128 bit WEP
```

Next, I launch the crack with the following syntax:

```
aircrack -a 1 -b APMAC dump.ivs
```

This command starts Aircrack and reads the required data from the `dump.ivs` file. In this example, Aircrack had to run about 35 minutes to finally return the following:

```
64-bit WEP key "3be6ae1345."
```

If your organization still uses WEP, you may want to use your own network security lab and a WAP to attempt this technique. Once you are comfortable with repeating this process, bring other networking team members and management into the lab so that they can see how vulnerable WEP is, and use this demonstration to tighten security. This also is effective at demonstrating why money was well spent in constructing the lab.

Other Wireless Attack Tools

There is no shortage of wireless tools for someone building a network security lab. Some of these tools include the following:

- **Mognet** — An open source, Java-based wireless sniffer that was designed for handhelds but will run on other platforms, too. It performs real-time frame captures and can save and load frames in common formats such as Ethereal, Libpcap, and TCPdump.
- **WaveStumbler** — Another sniffing tool that was designed for Linux. It reports basic information about APs such as channel, SSID, and MAC.
- **AiroPeek** — A Windows-based commercial WLAN analyzer that is designed to help security professionals deploy, secure, and troubleshoot WLANs. AiroPeek has the functionality to perform site surveys, security assessments, client troubleshooting, WLAN monitoring, remote WLAN analysis, and application layer protocol analysis.
- **Airsnort** — A Linux-based WLAN WEP-cracking tool that recovers encryption keys. Airsnort operates by passively monitoring transmissions and then computing the encryption key when the program captures enough packets.
- **THC-wardrive** — A Linux tool for mapping WAPs; works with a GPS.
- **AirTraf** — A packet-capture decoding tool for 802.11b wireless networks. This Linux tool gathers and organizes packets and performs bandwidth calculations as well as signal-strength analysis on a per-wireless-node basis.
- **Airsnarf** — Airsnarf is a simple rogue WAP setup utility designed to demonstrate how a rogue AP can steal usernames and passwords from public wireless hot spots. Airsnarf was developed and released to demonstrate an inherent vulnerability of public 802.11b hot spots — snarfing usernames and passwords by confusing users with DNS and HTTP redirects from a competing AP.

Exploiting Bluetooth

Bluetooth has also been shown to be vulnerable to attack. One early exploit is *Bluejacking*. Although not a true attack, Bluejacking allows an individual to send unsolicited messages over Bluetooth to other Bluetooth devices. This can include text, images, or sounds. A second, more damaging, type of attack is known as *Bluesnarfing*. Bluesnarfing is the theft of data, calendar information, or phone book entries. Tools used to attack Bluetooth include these:

- **RedFang** — A small proof-of-concept application used to find undiscoverable Bluetooth devices.
- **Bluesniff** — A proof-of-concept tool for a Bluetooth wardriving.
- **Btscanner** — A Bluetooth-scanning program that can perform inquiry and brute-force scans, identify Bluetooth devices that are within range, and export the scan results to a text file and sort the findings.
- **BlueBug** — A tool that exploits a Bluetooth security loophole on some Bluetooth-enabled cell phones. It allows the unauthorized downloading of phone books and call lists, and the sending and reading of SMS messages from the attacked phone.

Securing Wireless Networks

Securing wireless is a challenge, but it can be accomplished. Wireless signals don't stop at the outer walls of the facility. Wireless is accessible by many more individuals than have access to your wired network. Although we look at some specific tools and techniques used to secure wireless, the general principle is the same as those used in wired networks. It is the principle of defense in depth.

Defense in Depth

Defense in depth is about building many layers of protection, such as the following:

- Encrypting data so that it is hidden from unauthorized individuals
- Limiting access based on least privilege
- Providing physical protection and security to the hardware
- Using strong authentication to verify the identity of the users who access the network
- Employing layers of security controls to limit the damage should one layer of security be overcome

- Deploying many layers of security to make it much harder for an attacker to overcome the combined security mechanisms

Changing the default value of the SSID is a good place to start. Another potential security measure that may work, depending on the organization, is to limit access to the wireless network to specific network adapters. Some switches and WAPs can perform MAC filtering. MAC filtering uses the MAC address assigned to each network adapter to enable or block access to the network.

Probably one of the easiest ways to increase the security of the network is to retire your WEP devices. No matter what the key length is, WEP is vulnerable. Moving to WPA2 will make a big improvement in the security of your wireless network. If you're serious about building your own network security lab, you also want to be proficient at performing site surveys. The goal of a site survey is to gather enough information to determine whether the client has the right number and placement of APs to provide adequate coverage throughout the facility.

It is also important to check and see how far the signal radiates outside of the facility. Finally, you're going to want to do a thorough check for rogue APs. I can't tell you the number of times I have seen APs show up in locations where they should not have been. These are as big a threat as, and perhaps even bigger than, the weak encryption you may have found. A site survey is also useful in detecting interference coming from other sources that could degrade the performance of the wireless network. The six basic steps of a site survey are as follows:

1. Obtain a facility diagram.
2. Visually inspect the facility.
3. Identify user areas.
4. Use site-survey tools to determine primary access locations and check that no rogue APs are in use.
5. After the installation of APs, verify their signal strength and range.
6. Document your findings, update the policy, and inform users of rules regarding wireless connectivity.

Misuse Detection

Intrusion detection systems (IDSs) have a long history of use in wired networks to detect misuse and flag possible intrusions and attacks. Because of the increased numbers of wireless networks, more options are becoming available for wireless intrusion detection.

A wireless IDS works much like wired intrusion detection in that it monitors traffic and can alert the administrator when traffic is found that doesn't match normal usage patterns or when traffic matches a predefined pattern of attack. A wireless IDS can be centralized or decentralized and should have a combination of sensors that collect and forward 802.11 data. Wireless attacks are unlike wired attacks in that the hacker is often physically located at or close to the local premise.

Some wireless IDS systems can provide a general estimate of the hacker's physical location. Therefore, if alert data is provided quickly, security professionals can catch the hackers while launching the attack. A couple of commercial wireless IDS products are AirDefense RogueWatch and IBM RealSecure Server Sensor and wireless scanner. Those who lack the budget to purchase a commercial product have a number of open source solutions available, including the following:

- **AirSnare** — Will alert you to unfriendly MAC addresses on your network and will also alert you to DHCP requests taking place. If AirSnare detects an unfriendly MAC address, you have the option of tracking the MAC address's access to IP addresses and ports or launching Ethereal upon detection.
- **WIDZ Intrusion detection** — Designed to be integrated with SNORT or RealSecure, this is used to guard WAPs, and monitors for scanning, association floods, and bogus WAPs.
- **Snort-Wireless** — Designed to integrate with Snort. It is used to detect rogue APs, ad hoc devices, and NetStumbler activity.

Summary

This chapter examined wireless technologies, wireless vulnerabilities, and wireless exploits. Wireless is a technology that is here to stay, so anyone working in IT or IT security should have a good understanding of how it functions. Every technology typically goes through growing pains and tends to become more secure as it matures. Consider early cordless phones. Most shared a few channels, so anyone could take his or her phone ''mobile'' and pick up a neighbor's conversation or listen in to someone else from down the block. Modern cordless phones are much more secure. Cell phones have a similar history. Early analog phones were vulnerable to tumbling, cloning, and numerous attacks. These attacks continued until modern digital phones gained market share. Their level of security is much greater than their analog predecessors. WLAN technologies have already made significant strides. Replacing WEP with WPA was a good start. WPA2 is an even better technology. In the future, expect further advances to improve security even more.

Key Terms

- **Access point spoofing** — The act of pretending to be a legitimate AP for the purpose of tricking individuals to pass traffic by the fake connection so that it can be captured and analyzed.
- **Ad hoc mode** — An individual computer in ad hoc operation mode can communicate directly to other client units. No AP is required. Ad hoc operation is ideal for small networks of no more than two to four computers.
- **Bluejacking** — The act of sending unsolicited messages, pictures, or information to a Bluetooth user.
- **Bluesnarfing** — The theft of information from a wireless device through a Bluetooth connection.
- **Bluetooth** — An open standard for short-range wireless communication of data and voice between both mobile and stationary devices. Used in cell phones, PDA, laptops, and other devices.
- **Defense in depth** — The process of implementing multilayered security. The layers may be administrative, technical, or logical.
- **Eavesdropping** — The unauthorized capture and reading of network traffic.
- **Extensible Authentication Protocol** — A method of authentication that can support multiple authentication methods such as tokens, smart cards, certificates, and one-time passwords.
- **Infrastructure mode** — A form of wireless networking in which wireless stations communicate with each other by first going through an access point.
- **Intrusion detection systems** — A key component of security that is used to detect anomalies or known patterns of attack.
- **MAC filtering** — A method of controlling access on a wired or wireless network by denying access to a device if the device's MAC address does not match one on a preapproved list.
- **Promiscuous mode** — A mode in which your network adapter is set to examine all traffic, in contrast to its normal mode, in which it examines only traffic matching its address. Promiscuous mode allows a network device to intercept and read all network packets that arrive at its interface in their entirety.
- **Rogue APs** — A 802.11 AP that has been set up by an attacker for the purpose of diverting legitimate users so that their traffic can be sniffed or manipulated.

- **Site survey** — The process of determining the optimum placement of WAPs. The objective of the site survey is to create an accurate wireless system design/layout and budgetary quote.
- **Wardriving** — The process of driving around a neighborhood or area to identify WAPs.

Exercises

This section presents several hands-on exercises to help reinforce your knowledge and understanding of the chapter. The author selected the tools and utilities used in these exercises because they are easily obtainable. Our goal is to provide you with *real* hands-on experience.

Using NetStumbler

In this exercise, you use NetStumbler to scan for available WAPs. You need a laptop and wireless card to complete the exercise.

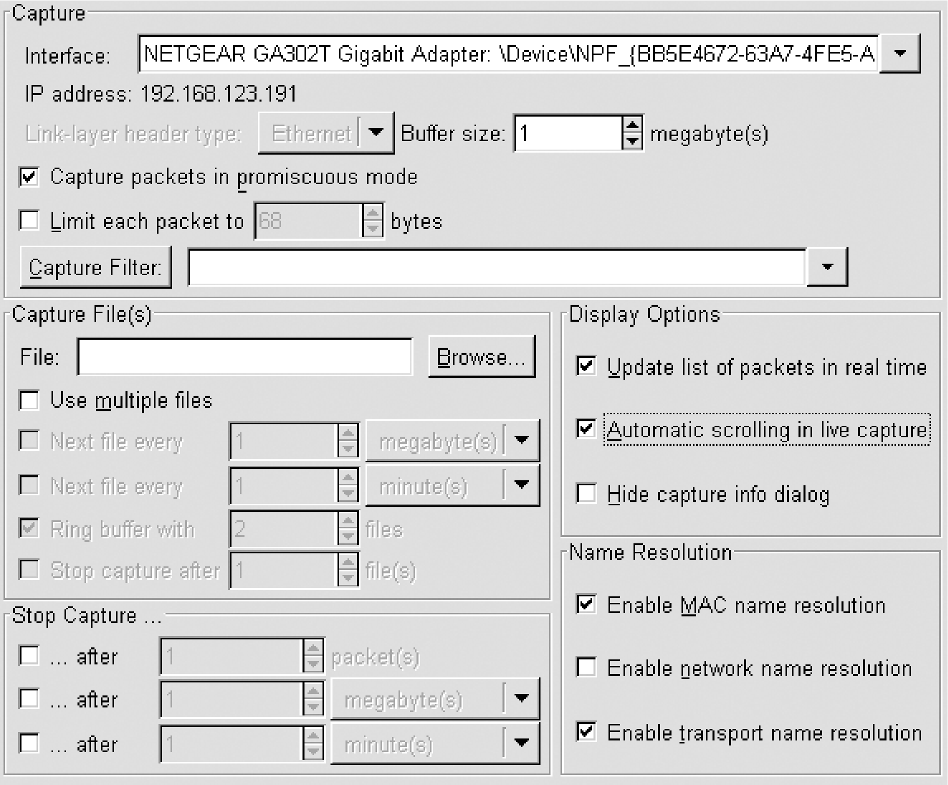
1. You will be using the NetStumbler program for this exercise. Download the program from `www.netstumbler.com/downloads`.
2. After installing the program on a Windows-based PC, make sure that you have loaded the appropriate wireless card. The NetStumbler site has a list of the types and brands of cards that work with the application.
3. To help prevent the chance of accidentally accessing someone's WAP, it is best to unbind all your TCP/IP properties. This can be done by unchecking the TCP/IP properties under Settings/Dialup and Network Connections.
4. Now you should start NetStumbler. By default, it places an icon on your desktop. Once the program is open, click File/Enable Scan. This should start the scanning process. If you are unable to pick up any WAPs, you may want to move around or consider taking your laptop outside. In most urban areas, you should not have much trouble picking up a few stray signals.

Detected signals display as green, yellow, or red to denote the signal strength. Other fields of information the program provides includes signal strength, SSID, name, channel, speed, vendor, and encryption status. If you hook up a GPS, your NetStumbler will also provide longitude and latitude.

Using Wireshark to Capture Wireless Traffic

In this exercise, you will set up Wireshark so that you will be able to capture and examine encrypted and unencrypted wireless traffic. You can use the Wireshark program that is preinstalled in BackTrack, or you can download the Windows version from `www.wireshark.org`.

1. After loading Wireshark, you will see several options across the top of the program. Select Capture ➪ Options to configure the program. Make sure to choose the correct interface (NIC) adapter and set the program to update packets in real time and for automatic scrolling. An example is shown in Figure 9-11.
2. Choose the Start Capture option.
3. After a few packets have been captured, stop Wireshark. You will see information displayed in three different views. The top window shows all packets that were captured. Clicking one of these will display that frame's contents in the middle frame, as shown in Figure 9-12. You may



Capture

Interface: NETGEAR GA302T Gigabit Adapter: \Device\NPF_{BB5E4672-63A7-4FE5-A

IP address: 192.168.123.191

Link-layer header type: Ethernet Buffer size: 1 megabyte(s)

☑ Capture packets in promiscuous mode

☐ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File:

☐ Use multiple files

☐ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☐ Hide capture info dialog

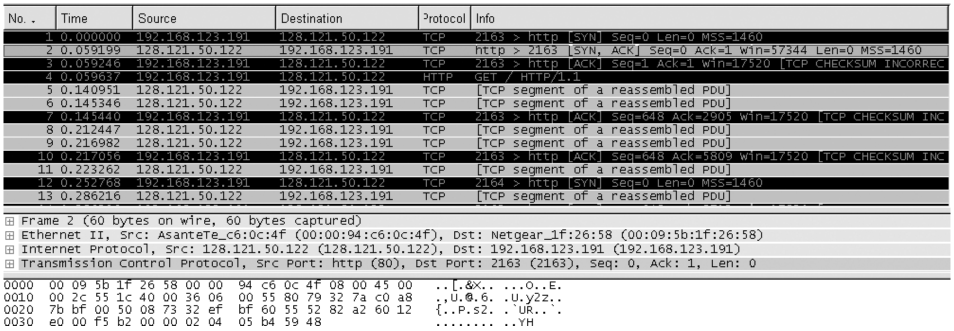
Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution

Figure 9-11 Wireshark capture options.



```
No. .  Time      Source           Destination      Protocol Info
     1 0.000000  192.168.123.191  128.121.50.122   TCP      2163 > http [SYN] Seq=0 Len=0 MSS=1460
     2 0.059199  128.121.50.122   192.168.123.191  TCP      http > 2163 [SYN, ACK] Seq=0 Ack=1 Win=57344 Len=0 MSS=1460
     3 0.059246  192.168.123.191  128.121.50.122   TCP      2163 > http [ACK] Seq=1 Ack=1 Win=17520 [TCP CHECKSUM INCORREC
     4 0.059637  192.168.123.191  128.121.50.122   HTTP     GET / HTTP/1.1
     5 0.140951  128.121.50.122   192.168.123.191  TCP      [TCP segment of a reassembled PDU]
     6 0.145346  128.121.50.122   192.168.123.191  TCP      [TCP segment of a reassembled PDU]
     7 0.145440  192.168.123.191  128.121.50.122   TCP      2163 > http [ACK] Seq=648 Ack=2905 Win=17520 [TCP CHECKSUM INC
     8 0.212447  128.121.50.122   192.168.123.191  TCP      [TCP segment of a reassembled PDU]
     9 0.216982  128.121.50.122   192.168.123.191  TCP      [TCP segment of a reassembled PDU]
    10 0.217056  192.168.123.191  128.121.50.122   TCP      2163 > http [ACK] Seq=648 Ack=5809 Win=17520 [TCP CHECKSUM INC
    11 0.223262  128.121.50.122   192.168.123.191  TCP      [TCP segment of a reassembled PDU]
    12 0.252768  192.168.123.191  128.121.50.122   TCP      2164 > http [SYN] Seq=0 Len=0 MSS=1460
    13 0.286216  128.121.50.122   192.168.123.191  TCP      [TCP segment of a reassembled PDU]

⊞ Frame 2 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: AsanteTe_c6:0c:4f (00:00:94:c6:0c:4f), Dst: Netgear_1f:26:58 (00:09:5b:1f:26:58)
⊞ Internet Protocol, Src: 128.121.50.122 (128.121.50.122), Dst: 192.168.123.191 (192.168.123.191)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 2163 (2163), Seq: 0, Ack: 1, Len: 0

0000   00 09 5b 1f 26 58 00 00  94 c6 0c 4f 08 00 45 00   ..[.&X.. ...O..E.
0010   00 2c 55 1c 40 00 36 06  00 55 80 79 32 7a c0 a8   .,U.@.6. .U.y2z..
0020   7b bf 00 50 08 73 32 ef  bf 60 55 52 82 a2 60 12   {..P.s2. .`UR..`.
0030   e0 00 f5 b2 00 00 02 04  05 b4 59 48               ........ ..YH
```

Figure 9-12 Wireshark capture.

also note that the bottom frame displays the actually hex dump. While reading hex is not mandatory, notice the first 16 bytes of the frame. The first 8 bytes are the destination MAC and the second 8 bytes are the source MAC.

4. Now use Wireshark to capture and analyze some wireless traffic with and without encryption. Note that the MAC addresses will be visible in both.