Chapter 10

Wireless LANs

In This Chapter

- Understanding risks of wireless LANs
- Selecting wireless LAN hacking tools
- Hacking against wireless LANs
- Minimizing wireless network security risks

Wireless local area networks (WLANs) — specifically, the ones based on the IEEE 802.11 standard — are increasingly being deployed into both business and home networks. Next to instant messaging and personal video recorders, WLANs are the neatest technology I've used in quite a while. Of course, with any new technology come security issues, and WLANs are no exception. In fact, the 802.11b wireless technology has been the poster child for weak security and network hack attacks for several years running.

WLANs offer a ton of business value, from convenience to reduced network deployment time. Whether your organization allows wireless network access or not, testing for WLAN security vulnerabilities is critical. In this chapter, I cover some common wireless network security vulnerabilities that you should test for. And I discuss some cheap and easy countermeasures you can implement to help ensure that WLANs are not more of a risk to your organization than they're worth.

Understanding the Implications of Wireless Network Vulnerabilities

WLANs are very susceptible to hacker attacks — even more so than wired networks are (discussed in Chapter 9). They have vulnerabilities that can allow a hacker to bring your network to its knees and allow your information to be gleaned right out of thin air. If a hacker comprises your WLAN, you can experience the following problems:

- Loss of network access, including e-mail, Web, and other services that can cause business downtime
- Loss of confidential information, including passwords, customer data, intellectual property, and more
- Legal liabilities associated with unauthorized users

Most of the wireless vulnerabilities are in the 802.11 protocol and within wireless *access points* (APs) — the central hublike devices that allow wireless clients to connect to the network. Wireless clients have some vulnerabilities as well.

Various fixes have come along in recent years to address these vulnerabilities, but most of these fixes have not been applied or are not enabled by default. You may also have employees installing rogue WLAN equipment on your network without your knowledge; this is the most serious threat to your wireless security and a difficult one to fight off. Even when WLANs are hardened and all the latest patches have been applied, you still may have some serious security problems, such as DoS and man-in-the-middle attacks (like you have on wired networks), that will likely be around for a while.

Choosing Your Tools

Several great WLAN security tools are available for both the Windows and UNIX platforms. The UNIX tools — which mostly run on Linux and BSD — can be a bear to configure and run properly if the planets and stars are not properly aligned. The PC Card services in Linux are the trickiest to set up, depending on your type of WLAN card and your Linux version.

Don't get me wrong — the UNIX-based tools are excellent at what they do. Programs such as Kismet (`www.kismetwireless.net`), AirSnort (`airsnort.shmoo.com`), AirJack (`802.11ninja.net/airjack`), and Wellenreiter (`www.wellenreiter.net`) offer many features that most Windows-based applications don't have. These programs run really well if you have all the Linux dependencies installed. They also offer many features that you don't need when assessing the security of your WLAN.

In the spirit of keeping things simple, the tests I outline in this chapter require only Windows-based utilities. My favorite tools for assessing wireless tools in Windows are as follows:

- NetStumbler (`www.netstumbler.com`) for AP discovery and enumeration
- Wireless client management software — such as Orinoco's Client Manager software — for AP discovery and enumeration

- WildPackets' AiroPeek (www.wildpackets.com) or your favorite WLAN analyzer for detailed information on wireless hosts, decryption of encrypted traffic, and more
- LANguard Network Security Scanner (www.gfi.com) for WLAN enumeration and vulnerability scanning

A case study with Matt Caldwell on hacking wireless networks

Matt Caldwell, shared with me a wild story of a wireless warflying experience — yes, it's wardriving, but in an airplane! Here's his account of what happened.

The Situation

Mr. Caldwell's employer — the state of Georgia — wanted to have the state's wireless networks assessed. The problem with terrestrial wardriving is that it's very slow, so Mr. Caldwell and his team conducted an experiment to determine the most economical way to assess the access points across the state of Georgia, which comprised 47,000 employees and 70 agencies. They knew the location of the buildings and knew they had to visit all of them. As a test, they drove around one building to count the number of access points they detected and concluded that it would take almost six months to assess all the state buildings.

In his spare time, Mr. Caldwell flies single-engine aircraft, and he decided that if the military could gather intelligence via aircraft, so could he! After getting through some political red tape, he and a fellow aviator used duct tape to mount an antenna on a Cessna 172RG (he thanks MacGyver for this idea!). He mounted the antenna at a 90-degree angle from the plane's nose so that he could make notes on the direction of the plot point. By doing some simple math, plus 90 degrees gave them radial on the approximate bearing of the target access point.

The Outcome

As Mr. Caldwell and his colleague climbed above 500 feet, NetStumbler (the wireless assessment software they were using) began chiming over the engine noise with its "bongs." It seemed like every second, a new wireless AP was being discovered. They made their way around downtown Atlanta and detected over 300 unique APs at about 2,000 feet AGL. They proved that warflying can be an effective method of detecting access points and a great statistical-gathering activity. They collected data on 382 APs in less than one hour in the air!

Matt Caldwell's Lessons Learned

- Don't eat a McDonald's double cheeseburger before flying — or at least carry a barf bag!
- Use extra duct tape and a safety rope, or put the antenna in the aircraft.
- Use good software to do triangulation so you don't have to calculate the position manually.
- Seventy percent of the APs detected had no WEP encryption!
- Almost 50 percent of the APs detected had default SSIDs.

Matt Caldwell, CISSP, is founder of and chief security officer for GuardedNet, Inc.

You also need the proper hardware. A good setup I've used is a laptop PC with an Orinoco (formerly made by Lucent, now Proxim) 802.11b PC Card. This card is not only compatible with NetStumbler, but also has an antenna connector that allows you to connect an external antenna. Another bonus is that most wireless security tools are very friendly with the Orinoco card. A lot of security tool support is available for the Prism2 chipset found in wireless cards by Belkin, D-Link, Linksys, and more. Before you purchase a wireless PC Card or PCI adapter, verify what chipset it has to ensure compatibility with the majority of security tools. The SeattleWireless HardwareComparison page (`www.seattlewireless.net/index.cgi/HardwareComparison`) is a good reference for this type of information.

You can also use a handheld wireless security testing device such as an AirMagnet (`www.airmagnet.com`) or the Fluke WaveRunner (`www.flukenetworks.com`). Both devices have their own built-in programs that are great for testing security settings on your WLAN.

An external antenna is also something to consider as part of your arsenal. I have had good luck running tests without an antenna, but your mileage may vary. If you're performing a walk-through of your facilities to test for wireless signals, for example, adding an additional antenna increases your odds of finding legitimate — and, more important, unauthorized APs. You can choose among three main types of wireless antennas:

- **Omnidirectional:** Transmits and receives wireless signals 360 degrees over shorter distances, such as in boardrooms or reception areas. These antennas, also known as dipoles, typically come installed on APs from the factory.
- **Semidirectional:** Transmits and receives directionally focused wireless signals over medium distances, such as down corridors and across one side of an office.
- **Directional:** Transmits and receives highly focused wireless signals over long distances, such as between buildings. This antenna, also known as a high-gain antenna, is the antenna of choice for wireless hackers driving around cities looking for vulnerable APs — an act also known as *wardriving*.

As an alternative to the antennas described in the preceding list, you can use a nifty Pringles-can design. If you're interested in trying this, check out the article at `www.oreillynet.com/cs/weblog/view/wlg/448` for details. You can even try other alternatives, such as a pork-and-beans can! A simple Internet search turns up a lot of information on this subject, if you're interested. One site in particular sells a Cantenna kit pretty cheaply at `mywebpages.comcast.net/hughpep`.

Wireless LAN Discovery

After you have an Internet connection, wireless hardware (a wireless card, at a minimum), and wireless testing software (NetStumbler or similar client management software, at a minimum), you're ready to roll.

Checking for worldwide recognition

The first test requires only the MAC address of your AP and access to the Internet. You're testing to see if someone has discovered your WLAN and posted information about it for the world to see. If you're not sure what your AP's MAC address is, you should be able to view it by using the `arp -a` command in DOS. You may have to ping the access point's IP address first so the MAC address is loaded into your ARP cache. Figure 10-1 shows what this may look like.

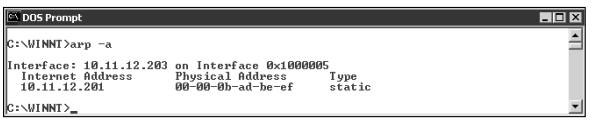

Figure 10-1: Finding the MAC address of an AP using `arp`.

After you have the AP's MAC address, browse to the WiGLE database of WLANs (`www.wigle.net`) to see if your AP is listed. You have to register with the site to perform a database query, but it's worth it. After you select the Query link and login, you see a screen similar to Figure 10-2. You can enter such AP information as geographical coordinates, but the simplest thing to do is enter your MAC address in the format shown.

If your AP is listed, that means that someone has discovered it — most likely via wardriving — and has posted the information for others to see. You need to start implementing the security countermeasures listed in this chapter as soon as possible to keep others from using this information against you! You can also check `www.wifimaps.com` to see if your AP is listed at another WLAN lookup site.

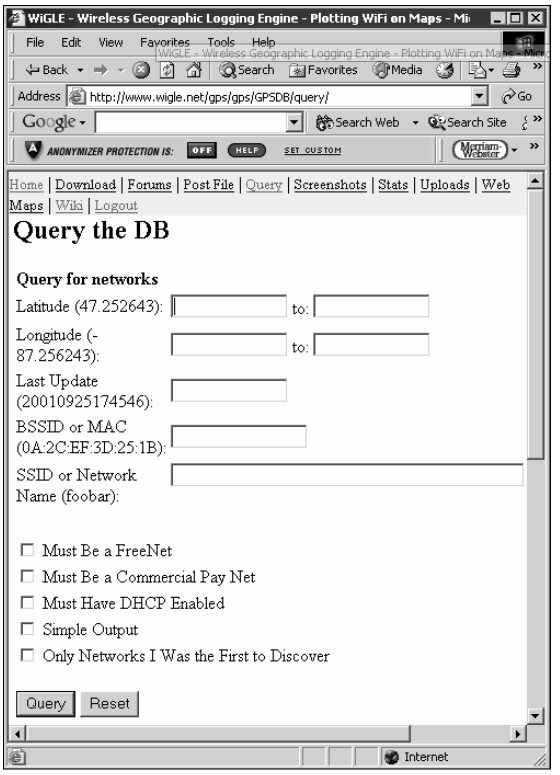

Figure 10-2: Searching for your wireless APs using the WiGLE database.

Scanning your local airwaves

Monitor the airwaves around your building to see what authorized and unauthorized APs you can find. You're looking for the SSID (service set identifier), which is your WLAN's name. If you have multiple WLANs, each one has a network SSID associated with it.

Here's where NetStumbler comes into play. NetStumbler can discover SSIDs and other detailed information about wireless APs, including the following:

- MAC address
- Name
- Radio channel in use
- Vendor name
- Whether encryption is on or off
- RF signal strength (signal-to-noise ratio)

Figure 10-3 shows an example of what you might see when running NetStumbler in your environment. The information that you see here is what others can see. NetStumbler and most other tools work by sending a probe-request signal from the client. Any APs within signal range must respond to with their SSIDs — that is, if they're configured to broadcast their SSIDs.

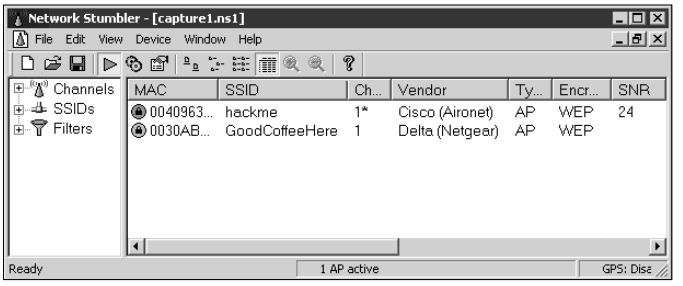

Figure 10-3: NetStumbler displays detailed data on APs.

Kismet — the popular wireless sniffer (network analyzer) for Linux and BSD UNIX — looks not only for probe responses from APs like NetStumbler does, but also for other 802.11 management packets, such as association responses and beacons. This allows Kismet to detect the presence of a WLAN even when probe-response packets are disabled in the AP — something that NetStumbler can't do.

When you're using certain wireless security assessment tools, including NetStumbler and AiroPeek, your adapter may be put in passive monitoring mode. This means you can no longer communicate with other wireless hosts or APs while the program is loaded. Also, some programs require a specialized driver for your wireless card that often disables normal WLAN functionality. If this is the case, you need to roll back (reinstall) the original adapter's driver (supplied by the vendor) to restore the standard functions of your adapter.

The best way to search for APs that are not broadcasting their SSIDs from within Windows is to use a WLAN analyzer such as AiroPeek (my favorite) — which is the sister product of the excellent wired network analyzer EtherPeek — or TamoSoft's CommView for Wi-Fi (`www.tamos.com/products/commwifi`), which I've heard great things about. You can do this by enabling a capture filter on 802.11 management packets, as shown in AiroPeek's options in Figure 10-4.

An ad-hoc mode — a peer-to-peer type setup — in WLANs can allow wireless clients to communicate directly with one another without having to pass through an AP. These types of WLANs operate outside the normal wireless security controls and, thus, can cause serious security issues above and beyond the normal 802.11 vulnerabilities. The best way to detect these rogue networks is to use NetStumbler. You can also use a WLAN analyzer or wireless IDS and search for beacon packets where the ESS field is not equal to 1.

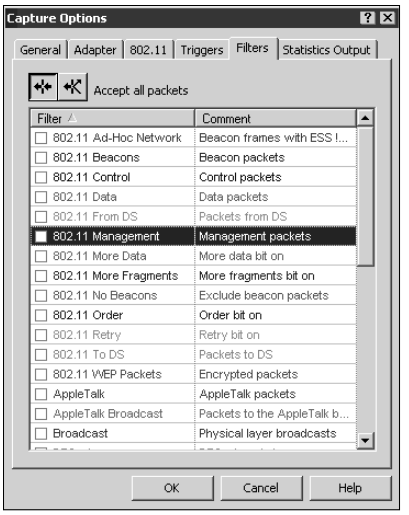

Figure 10-4: AiroPeek detects APs that don't broadcast SSIDs.

Wireless Network Attacks

Various malicious hacks — including various DoS attacks — can be carried out against your WLAN. This includes APs that are forced to reveal their SSIDs during the process of being disassociated from the network and rejoining. In addition, hackers can literally jam the RF signal of an AP — especially in 802.11b and 802.11g systems — and force the wireless clients to reassociate to a rogue AP masquerading as the victim AP. Hackers can create man-in-the-middle attacks by maliciously using tools such as ESSID-jack and monkey-jack and can flood your network with thousands of packets per second by maliciously using packet-generation tools such as Gspoof or LANforge — enough to bring the network to its knees. Even more so than with wired networks, this type of DoS attack is practically impossible to prevent on WLANs.

Various hacking tools for the UNIX platform can perform these types of hacks, including Cqure AP, HostAP, and AirJack. After hackers carry out these types of attacks against your WLAN, they can attempt to capture traffic and penetrate into any systems that attach to it.

You can carry out several — nonmalicious — attacks against your WLAN. The associated countermeasures help protect your network from these vulnerabilities, as well as from the malicious attacks previously mentioned. When testing your WLAN security, look out for the following weaknesses:

- Unencrypted wireless traffic
- Unauthorized APs

- RF signals that are too strong
- Wireless equipment that's easy to access physically
- Default configuration settings

A good starting point for testing is to attempt to attach to your WLAN as an outsider and run a vulnerability-assessment tool, such as LANguard Network Security Scanner. This test enables you to see what others can see on your network, including information on the OS version, open ports on your AP, and even network shares on wireless clients. Figure 10-5 shows the type of information that can be revealed about an AP on your network.

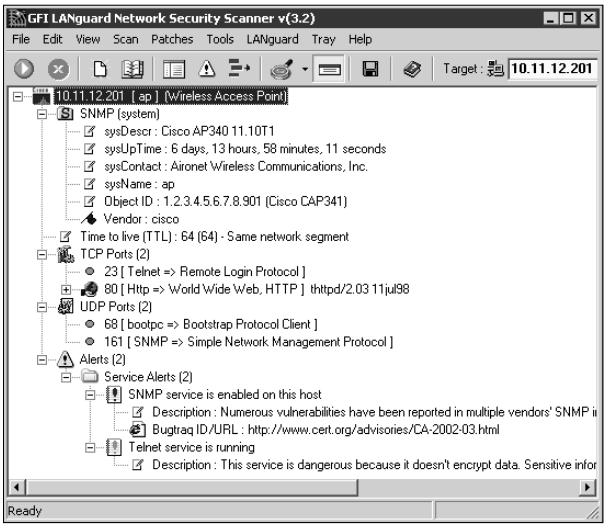

Figure 10-5: A LANguard scan of a potentially vulnerable AP.

Encrypted traffic

Wireless traffic can be captured directly out of the airwaves, making this communications medium susceptible to malicious eavesdropping. Unless the traffic is encrypted, it's sent and received in cleartext just like on a standard wired network. On top of that, the 802.11 encryption protocol, Wired Equivalent Privacy (WEP), has its own weakness that allows hackers to crack the encryption keys and decrypt the captured traffic. This vulnerability has helped put WLANs on the map — so to speak.

WEP, in a certain sense, actually lives up to its name: It provides the privacy equivalent to that of a wired network and then some. However, it was not intended to be cracked so easily. WEP uses a fairly strong symmetric (shared-key) encryption algorithm called RC4. Hackers can observe encrypted wireless traffic and recover the WEP key due to a flaw in how the RC4 initialization

vector (IV) is implemented in the protocol. This weakness is due to the fact that the IV is only 24 bits long, which causes it to be repeated every 16.7 million packets — even sooner in many cases, based on the amount of wireless clients entering and leaving the network.

Most WEP implementations initialize WLAN hardware with an IV of 0 and increment it by one for each packet sent. This can lead to the IV's being reinitialized — started over at 0 — approximately every five hours. Given this, WLANs that have a small number of clients transmitting a relatively small rate of wireless packets are normally more secure than large WLANs that transmit a lot of wireless data.

Using various UNIX-based tools such as WEPCrack (`wepcrack.sourceforge.net`), AirSnort (`airsnort.shmoo.com`), and WepAttack (`wepattack.sourceforge.net`), hackers need to collect only a few hours' up to a few days' (depending on how much wireless traffic is on the network) worth of packets to be able to break the WEP key.

A longer key length, such as 128 bit or 192 bit, doesn't make WEP exponentially more difficult to crack. This is because WEP's static key scheduling algorithm requires only that about 20,000 or so additional packets be captured to crack a key for every extra bit in the key length.

Although WEP is crackable, it's still much better than no encryption at all. Similar to the effect that home-security-system signs have on would-be home intruders, a wireless LAN running WEP is not nearly as attractive to a hacker as one without it. The hacker is likely to just move on to easier targets.

You can carry out this attack against your network, but it probably won't prove anything other than WEP is vulnerable. After you implement the WEP countermeasures mentioned in the next section, you can always run some of the WEP cracking tools to ensure that the countermeasures are working.

If you need to use your WLAN analyzer to view traffic as part of your security assessment, you won't be able to see any traffic if WEP is enabled unless you know your WEP key. You can enter your key into your analyzer, but just remember that hackers can do the same thing if they're able to crack your WEP key using one of the tools I mention earlier!

Figure 10-6 shows an example of how you can view protocols on your WLAN by entering your WEP key into AiroPeek via the 802.11 tab in the Capture Options window before you start your packet capture.

Countermeasures

The simplest solution to the WEP problem is to use a VPN for all wireless communications. You can easily implement this in a Windows environment — for

free — by enabling PPTP for client communications. You can also use the IPSec support built into Windows, as well as SSH, SSL/TLS, and other proprietary vendor solutions, to keep your traffic secure.

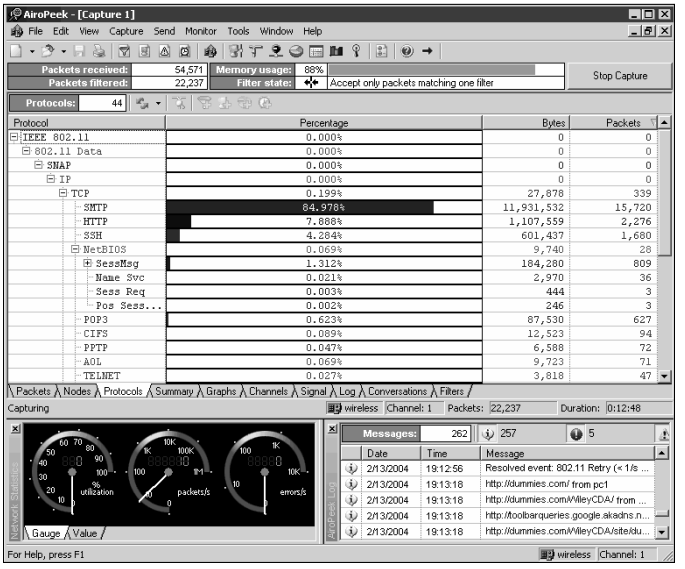

Figure 10-6: Using AiroPeek Client Manager to search for rogue APs.

Newer 802.11-based solutions exist as well. If you can configure your wireless hosts to regenerate a new key dynamically after a certain number of packets have been sent, the WEP vulnerability can't be exploited. Many AP vendors have already implemented this fix as a separate configuration option, so check for the latest firmware with features to manage key rotation. For instance, the proprietary Cisco LEAP protocol uses per-user WEP keys that offer a layer of protection if you're running Cisco hardware.

The wireless industry has come up with a solution to the WEP problem called Wi-Fi Protected Access (WPA). WPA uses the Temporal Key Integrity Protocol (TKIP) encryption system, which fixes all the known WEP issues. WPA requires an 802.1x authentication server, such as a RADIUS server, to manage user accounts for the WLAN. Check with your vendor for WPA updates.

A forthcoming 802.11i standard from the IEEE integrates the WPA fixes and more. This standard is an improvement over WPA but is not compatible with older 802.11b hardware, due to its implementation of the Advanced Encryption Standard (AES) for encryption. The workaround for this is to use TKIP, which is backward-compatible with older hardware because it uses the RC4 encryption scheme. Keep an eye out for 802.11i support for your wireless hardware.

Rogue networks

Watch out for unauthorized APs and wireless clients attached to your network that are running in ad-hoc mode.

Using NetStumbler or your client manager software, you can test for APs that don't belong on your network. You can also use the network monitoring features in a WLAN analyzer such as AiroPeek.

Look for the following rogue AP characteristics:

- Odd SSIDs, including the popular default ones *linksys, tsunami, comcomcom,* and *wireless.*
- Odd AP system names — that is, the name of the AP if your hardware supports this feature — not to be confused with the SSID.
- MAC addresses that don't belong on your network. Look at the first three bytes of the MAC address (the first six numbers), which specify the vendor name. You can perform a MAC-address vendor lookup at `coffer.com/mac_find` to find information on APs you're unsure of.
- Weak radio signals, which can indicate that an AP has been hidden away or is on the outside of your building.
- Communications across a different radio channel than what your network communicates on.
- A degradation in network throughput for any WLAN client.

Figure 10-7 shows how you can use AiroPeek's Monitor utility to spot an odd network host (the NETGEAR system) when you have a Cisco Aironet-only network, or vice versa.

My test network for this example is small compared to what you might see, but you get the idea of how an odd system can stand out.

Don't rely solely on this method. Hackers can spoof their MAC addresses, making them look like Cisco Aironet systems that belong on your network.

Walk around your building or campus to perform this test to see what you can find. Physically look for devices that don't belong — a well-placed AP or WLAN client that's turned off won't show up in your network analysis tools. Search near the outskirts of the building or near any publicly accessible areas. Scope out boardrooms and the offices of upper-level managers for any unauthorized devices. These are places that are typically off-limits but often are used as locations for hackers to set up rogue APs.

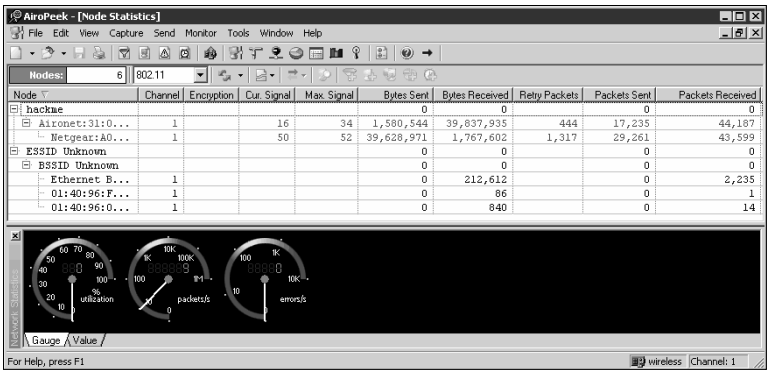

Figure 10-7: Using AiroPeek's Monitor to spot a product that doesn't belong.

WLANs authenticate the wireless devices, not the users. Hackers can use this to their advantage by gaining access to a wireless client via remote-access software such as telnet or SSH or by exploiting a known application or OS vulnerability. After they're able to do that, they potentially have full access to your network.

Countermeasures

The only way to detect rogue APs and hosts on your network is to monitor your WLAN proactively, looking for indicators that wireless clients or rogue APs might exist. But if rogue APs or clients don't show up in NetStumbler or in your client manager software, that doesn't mean you're off the hook. You may also need to break out the WLAN analyzer, wireless IDS, or other network management application.

You can enable MAC-address filtering controls on your AP so that wireless clients must have an authorized MAC address before being allowed to connect. The problem with this countermeasure is that hackers can easily spoof MAC addresses in UNIX by using the `ifconfig` command and in Windows with the SMAC utility, as I describe in Chapter 9. However like WEP, MAC-address-based access controls are another layer of protection and better than nothing at all. If a hacker spoofs one of your MAC addresses, the only way to detect malicious behavior is to spot the same MAC address being used in two or more places on the WLAN.

You may be able to make a couple of configuration changes — depending on your AP — to keep hackers from carrying out these tests against you:

- If possible, increase your wireless beacon broadcast interval to the maximum setting, which is around 65,535 milliseconds (roughly 66 seconds). This can help hide the AP from hackers who are wardriving or walking by your building quickly.

- Disable probe responses to prevent your AP from responding to NetStumbler requests.

Use personal firewall software such as BlackICE — my favorite — (`blackice.iss.net`) or ZoneAlarm (`www.zonelabs.com`) on all client computers to prevent unauthorized remote access to your network.

Physical-security problems

Various physical-security vulnerabilities can result in physical theft, the reconfiguration of wireless devices, and the capturing of confidential information. You should look for the following security vulnerabilities when testing your systems:

- APs mounted on the outside of a building and accessible to the public.
- Poorly mounted antennas — or the wrong types of antennas — that broadcast too strong a signal and that are accessible to the public. You can view the signal strength in NetStumbler or your wireless client manager.

These issues are often overlooked due to rushed installations, improper planning, and lack of technical knowledge, but they can come back to haunt you later.

Countermeasures

Secure APs, antennas, and other equipment in secure closets, ceilings, or other places that are difficult for a would-be intruder to access physically. Terminate your APs outside any firewall or other network perimeter security devices — or at least in a DMZ — whenever possible. If you place the wireless equipment inside your secure network, it can negate any benefits you would get out of your perimeter security devices.

If wireless signals are propagating outside your building where they don't belong, either

- Turn down the transmit power setting of your AP.
- Use a smaller or different antenna (semidirectional or directional) to decrease the signal.

Some basic planning helps prevent these vulnerabilities.

Vulnerable wireless workstations

Wireless workstations have tons of security vulnerabilities — from weak passwords to unpatched security holes to the storage of WEP keys locally. One serious vulnerability is for wireless clients using the Orinoco wireless card. The Orinoco Client Manager software stores encrypted WEP keys in the Windows Registry — even for multiple networks — as shown in Figure 10-8.

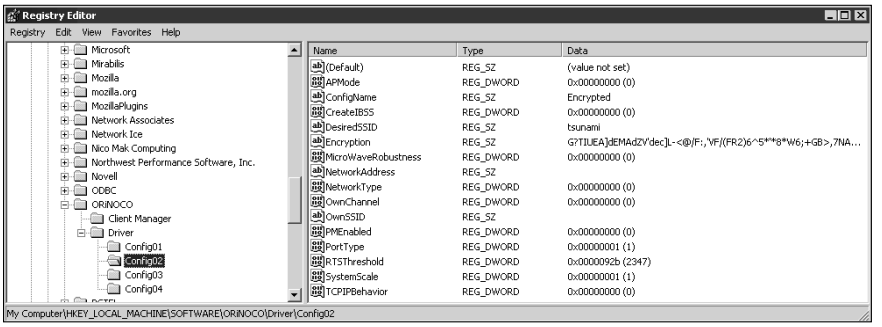

Figure 10-8: Encrypted WEP key of a wireless card.

You can crack the key by using the Lucent Orinoco Registry Encryption/Decryption program found at `www.cqure.net/tools.jsp?id=3`. Make sure that you use the `-d` command-line switch and put quotes around the encrypted key, as shown in Figure 10-9. This program comes in handy if you forget what your key is, but it can be used against you as well.

Figure 10-9: Cracking a WEP key with Lucent Orinoco.

If hackers remotely access a workstation via the Connect Network Registry in regedit, they can obtain these keys, crack them, and be on your network in a jiffy.

Countermeasures

You can implement the following countermeasures on your workstations to keep them from used as entry points into your WLAN.

- Regularly perform vulnerability assessments on your wireless workstations, as well as your other network hosts.
- Apply the latest vendor security patches and enforce strong user passwords.
- Use personal firewalls on these systems to keep malicious intruders off of those systems and out of your network.
- Install antivirus software.
- Consider installing an antispyware application such as PestPatrol.

Default configuration settings

Similar to wireless workstations, wireless APs have many known vulnerabilities. The most common ones are default SSIDs and admin passwords. The more specific ones occur only on certain hardware and software versions that are posted in vulnerability databases and vendor Web sites.

The one vulnerability that stands out above all others is that certain APs, including Linksys, D-Link, and more, are susceptible to a vulnerability that exposes any WEP key(s), MAC-address filters, and even the admin password! All that hackers have to do to exploit this is to send a broadcast packet on UDP port 27155 with a string of `gstsearch`.

To test for this vulnerability, you can use a program called pong. This program sends the broadcast packet automatically and returns any information it discovers. To run pong, follow these steps:

1. **Download the program from** `www.mobileaccess.de/wlan/dl.php/pong_v1.1.zip`**.**
2. **Unzip the program to** `c:\wireless` **(or a similar directory).**
3. **Drop out to a DOS prompt, and enter** pong**.**

If pong returns *no answer,* as shown in Figure 10-10, you're safe. Otherwise, look out!

Figure 10-10: The results you *should* get from pong.

Countermeasures

You can implement some of the simplest and effective security countermeasures for WLANs — and they're all free:

- Make sure that you change default admin passwords, AP names, and SSIDs.
- Disable SSID broadcasting if you don't need this feature. Figure 10-11 shows the SSID setting for a Cisco Aironet AP.
- Disable SNMP if you're not using it.
- Apply the latest firmware patches for your APs and WLAN cards. This countermeasure helps to prevent various vulnerabilities, including the UDP broadcast exploit. If you find that it doesn't, consider using another vendor's wireless products.

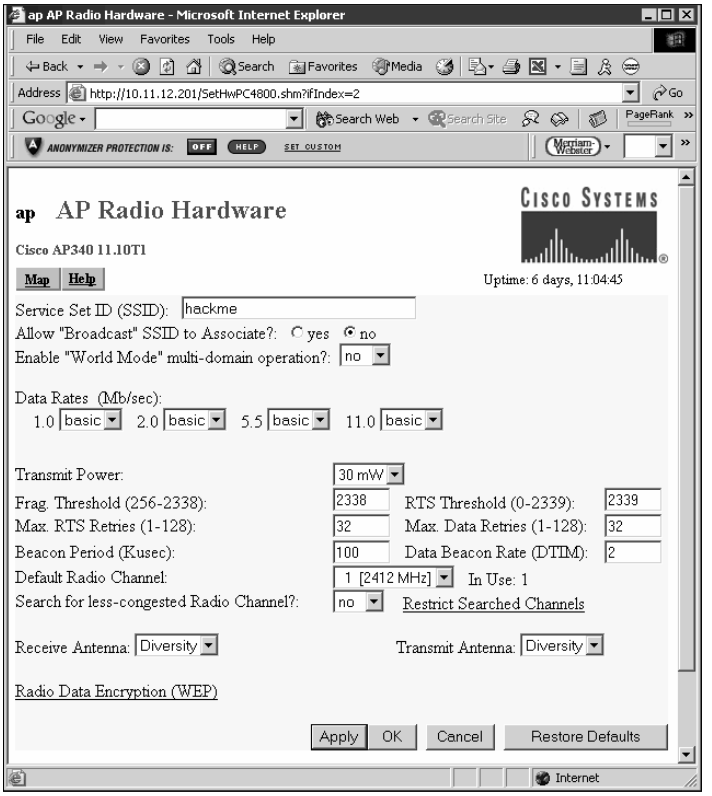

Figure 10-11: Cisco Aironet setting to disable SSID broadcasts.