Chapter 1

Introduction to Wireless Hacking

In This Chapter

- Understanding the need to test your wireless systems
- Wireless vulnerabilities
- Thinking like a hacker
- Preparing for your ethical hacks
- Important security tests to carry out
- What to do when you're done testing

Wireless local-area networks — often referred to as WLANs or Wi-Fi networks — are all the rage these days. People are installing them in their offices, hotels, coffee shops, and homes. Seeking to fulfill the wireless demands, Wi-Fi product vendors and service providers are popping up just about as fast as the dot-coms of the late 1990s. Wireless networks offer convenience, mobility, and can even be less expensive to implement than wired networks in many cases. Given the consumer demand, vendor solutions, and industry standards, wireless-network technology is real and is here to stay. But how safe is this technology?

Wireless networks are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 set of standards for WLANs. In case you've ever wondered, the IEEE 802 standards got their name from the year and month this group was formed — February 1980. The ".11" that refers to the wireless LAN working group is simply a subset of the 802 group. There's a whole slew of industry groups involved with wireless networking, but the two main players are the IEEE 802.11 working group and the Wi-Fi Alliance.

Years ago, wireless networks were only a niche technology used for very specialized applications. These days, Wi-Fi systems have created a multibillion-dollar market and are being used in practically every industry — and in every size organization from small architectural firms to the local zoo. But with this increased exposure comes increased risk: The widespread use of wireless systems has helped make them a bigger target than the IEEE ever bargained for. (Some widely publicized flaws such as the Wired Equivalent Privacy (WEP) weaknesses in the 802.11 wireless-network protocol haven't helped things, either.) And, as Microsoft has demonstrated, the bigger and more popular you are, the more attacks you're going to receive.

With the convenience, cost savings, and productivity gains of wireless networks come a whole slew of security risks. These aren't the common security issues, such as spyware, weak passwords, and missing patches. Those weaknesses still exist; however, networking without wires introduces a whole new set of vulnerabilities from an entirely different perspective.

This brings us to the concept of ethical hacking. *Ethical hacking* — sometimes referred to as *white-hat hacking* — means the use of hacking to test and improve defenses against *un*ethical hackers. It's often compared to penetration testing and vulnerability testing, but it goes even deeper. Ethical hacking involves using the same tools and techniques the bad guys use, but it also involves extensive up-front planning, a group of specific tools, complex testing methodologies, and sufficient follow-up to fix any problems before the bad guys — the black- and gray-hat hackers — find and exploit them.

Understanding the various threats and vulnerabilities associated with 802.11-based wireless networks — and ethically hacking them to make them more secure — is what this book is all about. Please join in on the fun.

In this chapter, we'll take a look at common threats and vulnerabilities associated with wireless networks. We'll also introduce you to some essential wireless security tools and tests you should run in order to strengthen your airwaves.

Why You Need to Test Your Wireless Systems

Wireless networks have been notoriously insecure since the early days of the 802.11b standard of the late 1990s. Since the standard's inception, major 802.11 weaknesses, such as physical security weaknesses, encryption flaws, and authentication problems, have been discovered. Wireless attacks have been on the rise ever since. The problem has gotten so bad that two wireless security standards have emerged to help fight back at the attackers:

- **Wi-Fi Protected Access (WPA):** This standard, which was developed by the Wi-Fi Alliance, served as an interim fix to the well-known WEP vulnerabilities until the IEEE came out with the 802.11i standard.
- **IEEE 802.11i (referred to as WPA2):** This is the official IEEE standard, which incorporates the WPA fixes for WEP along with other encryption and authentication mechanisms to further secure wireless networks.

These standards have resolved many known security vulnerabilities of the 802.11a/b/g protocols. As with most security standards, the problem with these wireless security solutions is not that the solutions don't work — it's that many network administrators are resistant to change and don't fully implement them. Many administrators don't want to reconfigure their existing wireless systems

and don't want to have to implement new security mechanisms for fear of making their networks more difficult to manage. These are legitimate concerns, but they leave many wireless networks vulnerable and waiting to be compromised.

Even after you have implemented WPA, WPA2, and the various other wireless protection techniques described in this book, your network may still be at risk. This can happen when (for example) employees install unsecured wireless access points or gateways on your network without you knowing about it. In our experience — even with all the wireless security standards and vendor solutions available — the majority of systems are still wide open to attack. Bottom line: Ethical hacking isn't a do-it-once-and-forget-it measure. It's like an antivirus upgrade — you have to do it again from time to time.

Knowing the dangers your systems face

Before we get too deep into the ethical-hacking process, it will help to define a couple of terms that we'll be using throughout this book. They are as follows:

- **Threat:** A *threat* is an indication of intent to cause disruption within an information system. Some examples of threat agents are hackers, disgruntled employees, and malicious software (malware) such as viruses or spyware that can wreak havoc on a wireless network.
- **Vulnerability:** A *vulnerability* is a weakness within an information system that can be exploited by a threat. Some examples are wireless networks not using encryption, weak passwords on wireless access points or APs (which is the central hub for a set of wireless computers), and an AP sending wireless signals outside the building. Wireless-network vulnerabilities are what we'll be seeking out in this book.

Beyond these basics, quite a few things can happen when a threat actually exploits the vulnerabilities of a various wireless network. This situation is called *risk.* Even when you think there's nothing going across your wireless network that a hacker would want — or you figure the likelihood of something bad happening is very low — there's still ample opportunity for trouble. Risks associated with vulnerable wireless networks include

- Full access to files being transmitted or even sitting on the server
- Stolen passwords
- Intercepted e-mails
- Back-door entry points into your wired network
- Denial-of-service attacks causing downtime and productivity losses
- Violations of state, federal, or international laws and regulations relating to privacy, corporate financial reporting, and more

- "Zombies" — A hacker using your system to attack other networks making you look like the bad guy
- Spamming — A spammer using your e-mail server or workstations to send out spam, spyware, viruses, and other nonsense e-mails

We could go on and on, but you get the idea. The risks on wireless networks are not much different from those on wired ones. Wireless risks just have a greater likelihood of occurring — that's because wireless networks normally have a larger number of vulnerabilities.

The really bad thing about all this is that without the right equipment and vigilant network monitoring, it can be impossible to detect someone hacking your airwaves — even from a couple of miles away! Wireless-network compromises can include a nosy neighbor using a frequency scanner to listen in on your cordless phone conversations — or nosy co-workers overhearing private boardroom conversations. Without the physical layer of protection we've grown so accustomed to with our wired networks, anything is possible.

Understanding the enemy

The wireless network's inherent vulnerabilities, in and of themselves, aren't necessarily bad. The true problem lies with all the malicious hackers out there just waiting to exploit these vulnerabilities and make your job — and life — more difficult. In order to better protect your systems, it helps to understand what you're up against — in effect, to think like a hacker. Although it may be impossible to achieve the same malicious mindset as the cyberpunks, you can at least see where they're coming from technically and how they work.

For starters, hackers are likely to attack systems that require the least amount of effort to break into. A prime target is an organization that has just one or two wireless APs. Our findings show that these smaller wireless networks help stack the odds in the hackers' favor, for several reasons:

- Smaller organizations are less likely to have a full-time network administrator keeping tabs on things.
- Small networks are also more likely to leave the default settings on their wireless devices unchanged, making them easier to crack into.
- Smaller networks are less likely to have any type of network monitoring, in-depth security controls such as WPA or WPA2, or a wireless intrusion-detection system (WIDS). These are exactly the sorts of things that smart hackers take into consideration.

However, small networks aren't the only vulnerable ones. There are various other weaknesses hackers can exploit in networks of all sizes, such as the following:

- The larger the wireless network, the easier it may be to crack Wired Equivalent Privacy (WEP) encryption keys. This is because larger networks likely receive more traffic, and an increased volume of packets to be captured thus leads to quicker WEP cracking times. We cover WEP in-depth in Chapter 14.
- Most network administrators don't have the time or interest in monitoring their networks for malicious behavior.
- Network snooping will be easier if there's a good place such as a crowded parking lot or deck to park and work without attracting attention.
- Most organizations use the omnidirectional antennae that come standard on APs — without even thinking about how these spread RF signals around outside the building.
- Because wireless networks are often an extension of a wired network, where there's an AP, there's likely a *wired* network behind it. Given this, there are often just as many treasures as the wireless network, if not more.
- Many organizations attempt to secure their wireless networks with routine security measures — say, disabling service-set-identifier (SSID) broadcasts (which basically broadcasts the name of the wireless network to any wireless device in range) and enabling media-access control (MAC) address filtering (which can limit the wireless hosts that can attach to your network) — without knowing that these controls are easily circumvented.
- SSIDs are often set to obvious company or department names that can give the intruders an idea which systems to attack first.

Throughout this book, we point out ways the bad guys work when they're carrying out specific hacks. The more cognizant you are of the hacker mindset, the deeper and broader your security testing will be — which leads to increased wireless security.

Many hackers don't necessarily want to steal your information or crash your systems. They often just want to prove to themselves and their buddies that they can break in. This likely creates a warm fuzzy feeling that makes them feel like they're contributing to society somehow. On the other hand, sometimes they attack simply to get under the administrator's skin. Sometimes they are seeking revenge. Hackers may want to use a system so they can attack other people's networks under disguise. Or maybe they're bored, and just want to see what information is flying through the airwaves, there for the taking.

The "high-end" *uber*hackers go where the money is — literally. These are the guys who break into online banks, e-commerce sites, and internal corporate databases for financial gain. What better way to break into these systems than through a vulnerable wireless network, making the real culprit harder to trace? One AP or vulnerable wireless client is all it takes to get the ball rolling.

For more in-depth insight into hackers — who they are, why they do it, and so on — check out Kevin's book *Hacking For Dummies* (Wiley) where he dedicated an entire chapter to this subject. Whatever the reasons are behind all of these hacker shenanigans, the fact is that your network, your information, and (heaven forbid) your job are at risk.

There's no such thing as absolute security on any network — wireless or not. It's basically impossible to be completely proactive in securing your systems since you cannot defend against an attack that hasn't already happened. Although you may not be able to prevent every type of attack, you can prepare, prepare, and prepare some more — to deal with attacks more effectively and minimize losses when they do occur.

Information security is like an arms race — the attacks and countermeasures are always one-upping each other. The good thing is that for every new attack, there will likely be a new defense developed. It's just a matter of timing. Even though we'll never be able to put an end to the predatory behavior of unethical cyber thugs, it's comforting to know that there are just as many ethical security professionals working hard every day to combat the threats.

Wireless-network complexities

In addition to the various security vulnerabilities we mentioned above, one of the biggest obstacles to secure wireless networks is their complexity. It's not enough to just install a firewall, set strong passwords, and have detailed access control settings. No, wireless networks are a completely different beast than their wired counterparts. These days, a plain old AP and wireless network interface card (NIC) might not seem too complex, but there's a lot going on behind the scenes.

The big issues revolve around the 802.11 protocol. This protocol doesn't just send and receive information with minimal management overhead (as does, say, plain old Ethernet). Rather, 802.11 is highly complex — it not only has to send and receive radio frequency (RF) signals that carry packets of network data, it also has to perform a raft of other functions such as

- Timing message packets to ensure client synchronization and help avoid data-transmission collisions
- Authenticating clients to make sure only authorized personnel connect to the network
- Encrypting data to enhance data privacy
- Checking data integrity to ensure that the data remains uncorrupted or unmodified

For a lot of great information on wireless-network fundamentals, check out the book that Peter co-authored — *Wireless Networks For Dummies*.

In addition to 802.11-protocol issues, there are also complexities associated with wireless-network design. Try these on for size:

- Placement of APs relative to existing network infrastructure devices, such as routers, firewalls, and switches
- What type of antennae to use and where to locate them
- How to adjust signal-power settings to prevent RF signals from leaking outside your building
- Keeping track of your wireless devices — such as APs, laptops, and personal digital assistants (PDAs)
- Knowing which device types are allowed on your network and which ones don't belong

These wireless-network complexities can lead to a multitude of security weaknesses that simply aren't present in traditional wired networks.

Getting Your Ducks in a Row

Before going down the ethical-hacking road, it's critical that you plan everything in advance. This includes:

- Obtaining permission to perform your tests from your boss, project sponsor, or client
- Outlining your testing goals
- Deciding what tests to run
- Grasping the ethical-hacking methodology (what tests to run, what to look for, how to follow-up, etc.) before you carry out your tests

For more on the ethical-hacking methodology, see Chapter 3.

All the up-front work and formal steps to follow may seem like a lot of hassle at first. However, we believe that if you're going to go to all the effort to perform ethical hacking on your wireless network as a true IT professional, do it right the first time around. It's the only way to go.

The law of sowing and reaping applies to the ethical-hacking planning phase. The more time and effort you put in up front, the more it pays off in the long run — you'll be better prepared, have the means to perform a more thorough

wireless-security assessment, and (odds are) you'll end up with a more secure wireless network.

Planning everything in advance saves you a ton of time and work in the long-term; you won't regret it. Your boss or your client will be impressed to boot!

Gathering the Right Tools

Every job requires the right tools. Selecting and preparing the proper security testing tools is a critical component of the ethical-hacking process. If you're not prepared, you'll most likely spin your wheels and not get the desired results.

Just because a wireless hacking tool is designed to perform a certain test, that doesn't mean it will. You may have to tweak your settings or find another tool altogether. Also keep in mind that you sometimes have to take the output of your tools with a grain of salt. There's always the potential for *false positives* (showing there's a vulnerability when there's not) and even *false negatives* (showing there's no vulnerability when there *is*).

The following tools are some of our favorites for testing wireless networks and are essential for performing wireless hacking tests:

- Google — yep, this Web site is a great tool
- Laptop computer
- Global Positioning System (GPS) satellite receiver
- Network Stumbler network stumbling software
- AiroPeek network-analysis software
- QualysGuard vulnerability-assessment software
- WEPcrack encryption cracking software

Starting in Chapter 6, we get to work with these tools in more detail later on in this book, when we lay out specific wireless hacks.

You can't do without good security-testing tools, but no one of them is "the" silver bullet for finding and killing off all your wireless network's vulnerabilities. A trained eye and a good mix of tools is the best combination for finding the greatest number of weaknesses in your systems.

It's critical that you understand how to use your various tools for the specific tests you'll be running. This may include something as informal as playing around with the tools or something as formal as taking a training class. Don't worry, we'll show you how to work the basics when we walk you through specific tests in Chapters 5 through 16.

To Protect, You Must Inspect

After you get everything prepared, it's time to roll up your sleeves and get your hands dirty by performing various ethical hacks against your wireless network. There are dozens of security tests you can run to see just how vulnerable your wireless systems are to attack — and Chapters 5 through 16 of this book walk you through the most practical and important ones. The outcomes of these tests will show you what security holes can — or cannot — be fixed to make your wireless network more secure. Not to worry, we won't leave you hanging with a bunch of vulnerabilities to fix. We'll outline various countermeasures you can use to fix the weaknesses you find.

In the next few sections, we outline the various types of security attacks to establish the basis for the vulnerability tests you'll be running against your wireless network.

Non-technical attacks

These types of attacks exploit various human weaknesses, such as lack of awareness, carelessness, and being too trusting of strangers. There are also physical vulnerabilities that can give an attacker a leg up on firsthand access to your wireless devices. These are often the easiest types of vulnerabilities to take advantage of — and they can even happen to you if you're not careful. These attacks include

- Breaking into wireless devices that users installed on their own and left unsecured
- *Social engineering* attacks whereby a hacker poses as someone else and coaxes users into giving out too much information about your network
- Physically accessing APs, antennae, and other wireless infrastructure equipment to reconfigure it — or (worse) capture data off it

Network attacks

When it comes to the nitty-gritty bits and bytes, there are a lot of techniques the bad guys can use to break inside your wireless realm or at least leave it limping along in a nonworking state. Network-based attacks include

- Installing rogue wireless APs and "tricking" wireless clients into connecting to them
- Capturing data off the network from a distance by walking around, driving by, or flying overhead
- Attacking the networking transactions by spoofing MAC addresses (masquerading as a legitimate wireless user), setting up man-in-the-middle (inserting a wireless system between an AP and wireless client) attacks, and more
- Exploiting network protocols such as SNMP
- Performing denial-of-service (DoS) attacks
- Jamming RF signals

Software attacks

As if the security problems with the 802.11 protocol weren't enough, we now have to worry about the operating systems and applications on wireless-client machines being vulnerable to attack. Here are some examples of software attacks:

- Hacking the operating system and other applications on wireless-client machines
- Breaking in via default settings such as passwords and SSIDs that are easily determined
- Cracking WEP keys and tapping into the network's encryption system
- Gaining access by exploiting weak network-authentication systems