WEP is turned off. If strong encryption and authentication techniques are in use, you'll likely not find a way in.

Analyze Security Gaps

The information you gather during the assessment provides a basis for understanding the security posture of a company or organization. After collecting information, spend some time thinking about potential gaps in security. This includes issues with policy, network architecture, operational support, and other items that weaken security, such as presence of unauthorized base stations and abilities to penetrate the network. This requires you to think like a hacker and uncover any and all methods that make it easier for someone to penetrate and access (or control) company resources through the wireless network.

Recommend Improvements

As you spot weaknesses, research and describe methods that will counter the issues. Start by recommending improvements to the policies, which dictate what the company requires in terms of security for the wireless networks. This provides a basis for defining technical and procedural solutions that strengthen the system's security to a level that protects the company's interests.

Common Security Policies

With any wireless network, consider policies that will protect resources from unauthorized people. Here's a look at what you should include.

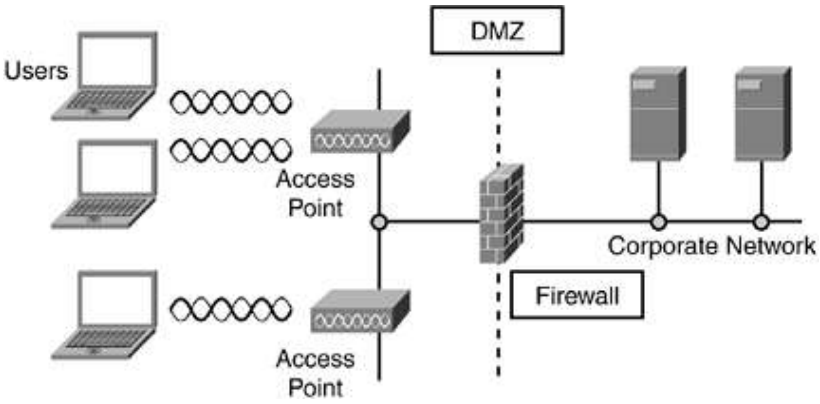
Place Wireless Users Outside a Firewall

Consider implementing a wireless demilitarized zone (DMZ) by placing a firewall between the wireless network and the corporate network. (See **Figure 8-8**.) With this approach, equip each client device with a virtual private network (VPN) that the protected network will

Exhibit 1010
Page 253 of 292

accept. As a result, a hacker would need to utilize a correctly configured VPN—which is difficult to do— to gain access to company resources.

Figure 8-8. Firewalls Offer Additional Security to Wireless Networks



The problem with a VPN solution for all users is that it's difficult to manage and sometimes slows performance. As a result, mainly consider VPNs if users will roam into public areas.

Use Effective Encryption

Skilled hackers can crack into a WEP-protected network using freely available tools. However, WEP does a good job of protecting many home and business networks from the general public. To crack WEP, you need to know how to use complicated tools and capture a lot of network packets, something that most people won't bother with unless the network resources are extremely valuable and they have infinite patience. The use of standard 802.11 WEP for networks with low attack risk is a minimum for any security policy.

If your wireless network hardware supports a form of encryption (such as WPA) that changes keys often, use it. This offers a much more

Exhibit 1010
Page 254 of 292

secure solution than using static methods such as WEP. If extremely high security is necessary, utilize superior standards, such as AES.

Ensure Firmware Is Up-to-Date

Vendors often implement patches to firmware in base stations and radio NICs that fix security issues. Start by upgrading the firmware in the base station soon after pulling it out of the box. Make it a habit to periodically check that all devices have the most recent firmware releases to cover up all known security holes. This is why it's a good idea to make certain you can easily upgrade the firmware in the base stations that you purchase.

Physically Secure Base Stations

Some base stations will revert to factory default settings, which do not provide any security, when someone pushes a reset. This makes the base station a fragile entry point. As a result, provide adequate physical security for the base station hardware.

For example, don't place a base station within easy reach on a table in the office. Instead, mount them out of view above ceiling tiles. Some base stations don't have reset buttons, but they allow you to reset through an RS-232 cable via a console connection. To prevent this, be sure to disable the console port.

Also, don't leave base stations within reach of a hacker who can replace a legitimate safeguarded base station with an unsecured, rogue base station that accepts access from any user. In fact, it's a good idea to conceal the base station as much as possible to make it more difficult for a hacker to find. Be sure, however, to note the location of the wireless hardware; otherwise, you'll have a difficult time finding them yourself.

Disable base stations during outage periods. If possible, shut down the base stations when users don't need them. This limits the window of

Exhibit 1010
Page 255 of 292

opportunity. You could pull the power plug on each base station; however, consider deploying power-over-Ethernet equipment that provides this feature through centralized operational support tools.

Assign Strong Passwords to Base Stations

Don't use default passwords for base stations. Default passwords are well known, making it easy for someone to change configuration parameters on the base station to her advantage. Instead, use passwords that are difficult to guess. In fact, it's a good idea to use a mix of uppercase and lowercase letters, as well as special symbols. Be sure to alter these passwords periodically. Also, ensure that passwords are encrypted before being sent over the network.

Don't Broadcast SSIDs

If this feature is available, you can avoid having user devices automatically sniff the SSID being used by the wireless LAN access point. Windows XP and other monitoring tools will automatically sniff the 802.11 beacon frames to obtain the SSID. With SSID broadcasting turned off, the base station will not include the SSID in the beacon frame, making most sniffing tools useless. In addition, Windows and XP users will not see that the wireless LAN exists.

The disabling of SSIDs isn't foolproof, however, because someone can still monitor 802.11 association frames and recover the SSID. Shutting off the broadcast mechanism, however, will limit access.

Reduce Propagation of Radio Waves

Through the use of directional antennae, it's possible to confine the propagation of radio waves within an area where hackers are not able to physically access. For example, a wireless network design could specify antenna gain and orientation to reduce the spillage of radio waves outside the perimeter of the facility. This not only optimizes coverage, it also minimizes the ability for a snooper to eavesdrop on

user signal transmissions or interface with the corporate network through an access point.

Implement Personal Firewalls

If a hacker is able to associate with a base station, the hacker can easily access files on other users' devices through the Windows operating system that are associated with an access point connected to the same wireless LAN. As a result, it's crucial that all users disable file sharing for all folders and utilize personal firewalls. This is crucial when users are operating in public locations.

Monitor Base Station Configuration

Utilize operational support tools to continually monitor the network and check for base stations that don't conform to configuration policies. A base station that doesn't match specific security settings has likely been reset or is possibly a rogue base station.

If base stations are found with improper settings, restore the settings as soon as possible. Be sure to encrypt management traffic, however, through the use of secure Simple Network Management Protocol (SNMP). SNMP Version 1, for example, sends everything in the clear. You can also deploy intrusion detection sensors, available in some operational support tools, to identify the presence of hackers based on invalid MAC addresses. The main idea is to provide alerts if suspicious behavior is occurring.

Control Deployments

Ensure that all employees and organizations within the company coordinate the installation of wireless networks with the appropriate IT group. For example, forbid the use of unauthorized access points. Mandate the use of approved vendor products after you've had a chance to verify appropriate security safeguards.

Exhibit 1010
Page 257 of 292

Maintain a list of authorized radio NIC and base station MAC addresses that you can use as the basis for identifying rogue base stations during surveys. In addition, deploy management tools that force base stations to comply with corporate security policies.

With these recommendations in mind, you have a basis for forming a solid security policy. When deciding on which techniques to implement, however, consider the actual security needs. For example, WEP might be good enough for home and small business wireless LANs. If you work for a financial institution or retail store transmitting sensitive data, concentrate on using something stronger, such as WPA or AES.

Exhibit 1010
Page 258 of 292

Chapter Summary

Security is one of the most important and complex elements of wireless networks. The ability of a hacker to monitor traffic, gain unauthorized access to valuable resources, and deny the service of a wireless network are issues that you must consider. Through the use of effective encryption and authentication, it's possible to significantly minimize threats. Keep in mind, however, that the necessary level of security depends on requirements. An acceptable level of security for a home application is much lower than what's needed for an enterprise.

Exhibit 1010
Page 259 of 292

Chapter Review Questions

You can find the answers to the following questions in **Appendix A**, "Answers to Chapter Review Questions."

1: What are the three major security threats of a wireless network?

2: What is the primary means for guarding against traffic monitoring?

3: How do you keep hackers from gaining access to company resources through the wireless network?

4: What method will help alleviate the implications of a successful DoS attack?

5: Why is WEP not acceptable for protecting sensitive information?

6: How is TKIP different than WEP?

7: WPA uses TKIP and is a subset of the 802.11i standard. True or false?

8: Why is the use of MAC address filters not effective?

9: What is a rogue access point, and why does it pose a problem?

Exhibit 1010
Page 260 of 292

10: What should you install on a laptop that a user will utilize on a public wireless LAN to avoid unauthorized people from accessing files on the laptop?

Exhibit 1010
Page 261 of 292

Appendix A. Answers to Chapter Review Questions

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Exhibit 1010
Page 262 of 292

Chapter 1

1: What is a distinguishing attribute of a wireless network as compared to a general wireless communication system?

A1: Answer: In a wireless network, communications takes place between computer devices.

2: What types of information does a wireless network support?

A2: Answer: E-mails, messages, web pages, database records, streaming video, and voice.

3: What are the four types of wireless networks?

A3: Answer: Wireless PAN, LAN, MAN, and WAN.

4: What is the typical maximum range of a wireless PAN?

A4: Answer: 50 feet.

5: True or false: A wireless PAN consumes little power from small handheld computer devices.

A5: Answer: True.

6: What is a common standard for wireless LANs?

A6: Answer: IEEE 802.11 or Wi-Fi.

7: What relatively new standard applies to wireless MANs?

A7: Answer: IEEE 802.16.

8: Why do wireless WANs not effectively satisfy requirements for indoor wireless networks?

A8: Answer: Wireless WAN systems are generally installed outdoors, and the signals lose strength before reaching the inside of the facility.

9: What is a common application of wireless networks in homes and small offices?

A9: Answer: Sharing Internet connections among multiple, mobile computers is a common application.

10: What are examples of applications for wireless WANs?

A10: Answer: Access to Internet applications from outdoor locations, realestate transactions, field-service and sales calls, vending-machine status, and utility-meter reading are a few examples.

Exhibit 1010
Page 264 of 292

Chapter 2

1: Which wireless NIC form factors are best for small wireless computer devices?

A1: Answer: PC Card, Mini-PCI, and CompactFlash.

2: What are examples of elements that impair the propagation of wireless communications signals through the air medium?

A2: Answer: Rain, snow, smog, and smoke.

3: What is the primary purpose of a base station?

A3: Answer: Interfaces the wireless communications signals traveling through the air medium to a wired network.

4: What are common features of wireless middleware?

A4: Answer: Optimization techniques, intelligent restarts, data bundling, screen shaping and reshaping, and end-system support.

5: On what layers of the OSI reference model do wireless networks operate?

A5: Answer: Physical layer and data link layer.

Exhibit 1010
Page 265 of 292

6: How is throughput different from data rate?

A6: Answer: Throughput doesn't include overhead of protocols.

7: True or false: A computer device stores data in analog form.

A7: Answer: False.

8: A wireless NIC must convert the information into what type of signal before transmission through the air medium?

A8: Answer: Analog.

9: Which medium access protocol is common with wireless networks?

A9: Answer: CSMA.

10: Explain how the ARQ form of error control works.

A10: Answer: The receiving wireless NIC performs error checking and sends a request to the sending wireless NIC to retransmit the frame if errors are found.

Exhibit 1010
Page 266 of 292

Chapter 3

1: RF signals offer relatively short range as compared to light signals. True or false?

A1: Answer: False.

2: What type of weather impacts RF signals the most?

A2: Answer: Heavy rain.

3: Why does interference cause errors in wireless networks?

A3: Answer: The interference causes the receiver to misunderstand the signal because two signals are present at the same time.

4: What are sources of RF interference?

A4: Answer: General examples include cordless phones, microwave ovens, and Bluetooth devices.

5: Multipath affects higher data rates more than lower data rates for 2.4 GHz systems. True or false?

A5: Answer: True. The receiver has difficulties with differentiating one bit from another when demodulating high data rate signals because the bits are close together.

Exhibit 1010
Page 267 of 292

6: What is meant by a diffused infrared light system?

A6: Answer: A system that emits light in all directions that reflects off of the ceiling and walls.

7: Approximately up to what range do direct infrared systems operate?

A7: Answer: 1 mile.

8: How does modulation make it possible to transmit information through the air?

A8: Answer: Modulation superimposes an information signal onto a carrier signal that has a frequency suitable for propagating through the air.

9: What attributes of a signal does QAM change in order to represent information?

A9: Answer: Amplitude and phase.

10: Spread spectrum generally requires user licenses. True or false?

A10: Answer: False.

Exhibit 1010
Page 268 of 292

Chapter 4

1: What form factors are common for wireless PAN radio cards?

A1: Answer: PC Card and CF.

2: What application can strongly benefit through the use of a wireless USB adapter (also referred to as a wireless dongle)?

A2: Answer: Any application that can benefit from interfacing with a PC or laptop through the USB port, such as PDA, wireless mouse, and wireless digital camera for synchronization purposes.

3: When would the use of a wireless PAN router make sense?

A3: Answer: For applications limited to the size of a room, such as in homes and small offices.

4: What is the general maximum coverage area of a wireless PAN?

A4: Answer: Within 30 feet, such as within a room.

5: Which IEEE standards group uses Bluetooth as the basis for the standard?

Exhibit 1010
Page 269 of 292

A5:	Answer: 802.15.
6:	In what frequency band does Bluetooth operate?
A6:	Answer: 2.4 GHz.
7:	What is the primary issue of using Bluetooth around 802.11 wireless LANs?
A7:	Answer: They both operate in the same 2.4 GHz frequency band, which can result in interference and degradation in performance.
8:	A Bluetooth-enabled device is always transmitting. True or false?
A8:	Answer: False.
9:	What is the highest possible data rate of an IrDA device?
A9:	Answer: 4 Mbps.
10:	What is a benefit of IrDA as compared to Bluetooth?
A10:	Answer: IrDA is immune from RF interference with wireless LANs.

Exhibit 1010
Page 270 of 292

Chapter 5

1: Which wireless LAN component is most commonly used in home and small offices?

A1: Answer: Wireless LAN router.

2: What is the primary difference between an access point and a wireless LAN router?

A2: Answer: A wireless LAN router actually routes packets to their destination. Access points don't implement DHCP and NAT. Routers do implement DHCP and NAT.

3: When would the use of a wireless LAN repeater make sense?

A3: Answer: When extending the range of an access point or router to an area where wires can't be run feasibly.

4: How does a wireless LAN radio NIC identify with which access point to associate?

A4: Answer: The radio NIC listens for beacons being sent periodically by each access point and associates with the access point having the strongest beacon signal.

5: WEP is a mandatory encryption mechanism. True or false?

Exhibit 1010
Page 271 of 292

A5: Answer: False.

6: In what frequency band does 802.11a operate in?

A6: Answer: 5 GHz.

7: How many non-overlapping channels are available with 802.11b wireless LANs?

A7: Answer: Three.

8: True of false: 802.11g operates at up to 54 Mbps and interoperates with 802.11b.

A8: Answer: True.

9: Which 802.11 frequencies are available almost worldwide?

A9: Answer: 2.4 GHz (802.11b and 802.11g).

10: What does Wi-Fi provide?

A10: Answer: A product having Wi-Fi certification will interoperate with other products that have Wi-Fi certification, regardless of the manufacturer.

Exhibit 1010
Page 272 of 292

Chapter 6

1: Why does a wireless MAN offer good return on investment?

A1: Answer: Wireless MANs eliminate the need to install expensive cabling or lease communications circuits.

2: A learning bridge forwards all packets. True or false?

A2: Answer: False.

3: What is the primary difference between a bridge and an access point?

A3: Answer: A bridge connects networks together. An access point connects end users.

4: What are examples of semidirectional antennae?

A4: Answer: Patch and Yagi.

5: In regards to beamwidth, what is the primary difference between a semidirectional and highly directional antenna?

A5: Answer: A highly directional antenna has a much narrower beamwidth, which increases range if the power remains constant.

Exhibit 1010
Page 273 of 292

6: What is an example of a highly directional antenna?

A6: Answer: Dish antenna.

7: What polarization would be most effective at a receiver if the transmitter were using vertical polarization?

A7: Answer: Vertical polarization.

8: What are the advantages of using point-to-multipoint systems versus point-to-point for interconnecting multiple sites?

A8: Answer: Point-to-multipoint can be less expensive and easier to add more sites.

9: What are the advantages of using packet radio for wireless MANs?

A9: Answer: Packet radio routers don't require any cabling between them, and the system is relatively survivable because packets can take a different route if a router becomes inoperative.

10: Which standards do wireless MANs employ?

A10: Answer: 802.11, Wi-Fi, and 802.16.

Exhibit 1010
Page 274 of 292