Covers all Exam Objectives for CEHv6

Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CEH™

Certified Ethical Hacker

STUDY GUIDE

Exam 312-50
Exam EC0-350

Kimberly Graves

SYBEX SERIOUS SKILLS.

Table of Contents

Wireless Network Hacking

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Overview of WEP, WPA authentication mechanisms, and cracking techniques
- ✓ Overview of wireless sniffers and locating SSIDs, MAC spoofing
- ✓ Understand rogue access points
- ✓ Understand wireless hacking techniques
- ✓ Describe the methods used to secure wireless networks

Wireless networks add another entry point into a network for hackers. Much has been written about wireless security and hacking because wireless is a relatively new technology and rife with security vulnerabilities. From the increase of Wi-Fi hotspots to the rising number of cell phones, PDAs, and laptops equipped with Wi-Fi radios, wireless security is an ever increasing issue for many organizations.

Because of the broadcast nature of radio frequency (RF) wireless networks and the rapid adoption of wireless technologies for home and business networks, many hacking opportunities exist in wireless networking. Even for organizations with a "no wireless" policy—meaning they do not support any Wi-Fi connectivity—rogue wireless access points placed on the LAN are an increasing threat. The cost of Wi-Fi equipment is dropping and many organizations are pressing the IT staff to install wireless networks to complement or replace existing wired networks.

Wi-Fi and Ethernet

It is important to recognize that Wi-Fi networks are fundamentally different from Ethernet networks. Whereas in an Ethernet network the data is carried in frames on copper or fiber-optic cabling, in a Wi-Fi network the data travels across open air. Additionally, any encryption applied to wireless networks only encrypts the data itself, leaving the header potion of the wireless frame open to many types of attacks. The details of wireless attacks and countermeasures will be covered later in this chapter, but first you need to understand the fundamentals of the 802.11 standards and protocols.

802.11 Wireless LANs operate at layer 1 and 2 of the OSI Model. This means that the protocols in use on a WLAN are the same from Layer 3 (usually IP) on up to Layer 7 (the application layer). See Figure 10.1.

Many people call 802.11 WLANs "wireless Ethernet," which is a big misnomer. 802.11 has a completely different frame format at Layer 2 than does 802.3 (Ethernet). For example, Ethernet Layer 2 frames carry only two MAC addresses, while 802.11 frames have fields for four MAC addresses. Ethernet just defines source and destination addresses, while an 802.11 frame can define source, destination, transmitter and receiver. 802.11 frames also carry a frame control field in the MAC header used to indicate information about the frame, such as if the frame is encrypted. See Figure 10.2.

FIGURE 10.1 Wireless LANs in the OSI Model

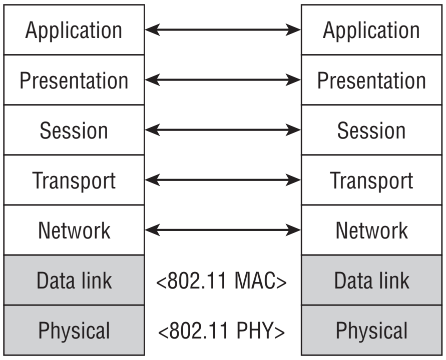
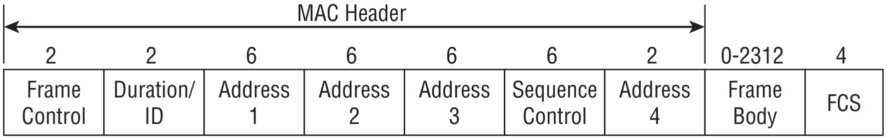


FIGURE 10.2 802.11 MAC Header



2	2	6	6	6	6	2	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

There are three types of 802.11 frames:

- Management—Used for notification, connection, disconnection, and information.
- Control—Used to control which station has access to the wireless network media.
- Data—Used to carry upper layer data.

Most wireless LANs (WLANs) are based on the IEEE 802.11 standards and amendments, such as 802.11a, 802.11b, 802.11g, and 802.11n. The lettered amendments have been rolled up into a final 802.11 standard and are now referred to by the clause or section number within the 802.11 standard. However, since the lettered amendments are still frequently used when differentiating between the sections of the 802.11 standard, they will be used here in this chapter as well. Table 10.1 shows a comparison of the 802.11 standard amendments.

TABLE 10.1 802.11 comparison

IEEE Standard	Frequency	Speed	Transmission Range	Spread Spectrum
802.11	2.4 GHz	Up to 2 Mbps	Depends on spread spectrum type	DSSS and FHSS
802.11a	5 GHz	Up to 54 Mbps	25 to 75 feet indoors; range can be affected by building materials	OFDM
802.11b	2.4 GHz	Up to 11 Mbps	Up to 150 feet indoors; range can be affected by building materials	DSSS
802.11g	2.4 GHz	Up to 54 Mbps	Up to 150 feet indoors; range can be affected by building materials	DSSS
802.11n	2.4 and 5 GHz	Up to 600 Mbps	At least as far as b, g, and a—and possibly much further	OFDM

The initial 802.11 standard included only rudimentary security features and was fraught with vulnerabilities. The 802.11i amendment is the latest security solution that addresses the 802.11 weaknesses. The Wi-Fi Alliance created additional security certifications known as *Wi-Fi Protected Access* (WPA) and WPA2 to fill the gap between the original 802.11 standard and the latest 802.11i amendment. The security vulnerabilities and security solutions discussed in this chapter are all based on these IEEE and Wi-Fi Alliance standards.

Authentication and Cracking Techniques

Two methods exist in the 802.11 standard for authenticating wireless LAN clients to an access point: open system or shared-key authentication. Open system does not provide any security mechanisms but is simply a request to make a connection to the network. Shared-key authentication has the wireless client hash a string of challenge text with the Wired Equivalent Privacy (WEP) key to authenticate the client to the network. Table 10.2 compares the Wi-Fi security standards type of authentication and encryption.

WEP was the first security option for 802.11 WLANs. WEP is used to encrypt data on the WLAN and can optionally be paired with shared-key authentication to authenticate WLAN clients. WEP uses an RC4 64-bit or 128-bit encryption key to encrypt the Layer 2 data payload. This WEP key comprises a 40-bit or 104-bit user-defined key combined with a 24-bit Initialization Vector (IV), making the WEP key either 64 or 128 bit.

TABLE 10.2 Wi-Fi security comparison

Wi-Fi Security	Authentication	Cipher	Encryption
WPA-Personal	Preshared Key	TKIP	RC4
WPA-Enterprise	802.1X/EAP	TKIP	RC4
WPA2-Personal	Preshared Key	CCMP (default), TKIP (optional)	AES (default), RC4 (optional)
WPA2-Enterprise	802.1X/EAP	CCMP (default), TKIP (optional)	AES (default), RC4 (optional)

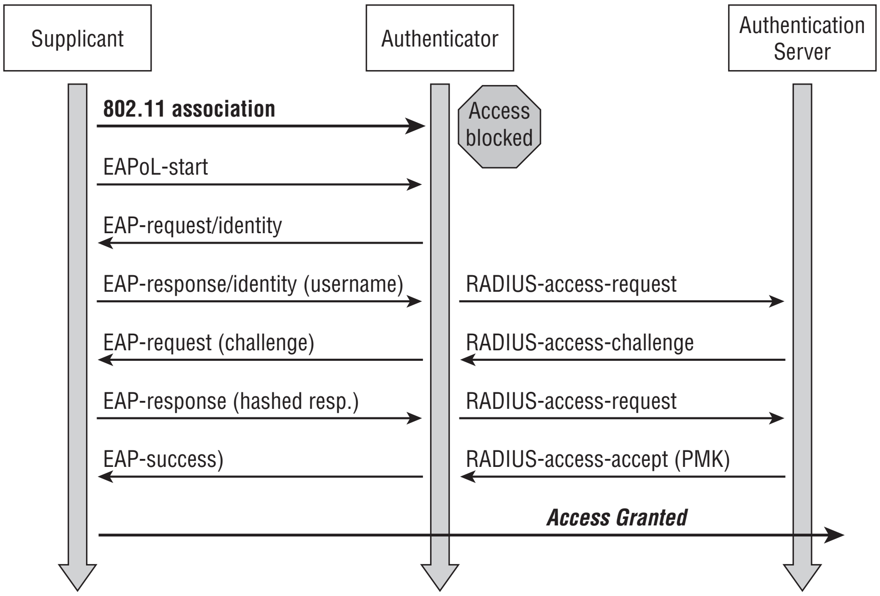
The process by which RC4 uses IVs is the real weakness of WEP: it gives a hacker the opportunity to crack the WEP key. The method, knows as the *Fluhrer, Mantin, and Shamir (FMS) attack*, uses encrypted output bytes to determine the most probable key bytes. The ability to exploit the WEP vulnerability was incorporated into products like AirSnort, WEPCrack, and Aircrack. Although a hacker can attempt to crack WEP by brute force, the most common technique is the FMS attack.

WPA employs the Temporal Key Integrity Protocol (TKIP)—which is a safer RC4 implementation—for data encryption and either WPA Personal or WPA Enterprise for authentication. WPA Personal uses an ASCII passphrase for authentication whereas WPA Enterprise uses a RADIUS server to authenticate users. WPA Enterprise is a more secure robust security option but relies on the creation and more complex setup of a RADIUS server. TKIP rotates the data encryption key to prevent the vulnerabilities of WEP and, consequently, cracking attacks.

WPA2 is similar to 802.11i and uses the Advanced Encryption Standard (AES) to encrypt the data payload. AES is considered an uncrackable encryption algorithm. WPA2 also allows for the use of TKIP during a transitional period called *mixed mode security*. This transitional mode means both TKIP and AES can be used to encrypt data. AES requires a faster processor, which means low-end devices like PDAs may only support TKIP.

WPA Personal and WPA2 Personal use a passphrase to authentication WLAN clients. WPA Enterprise and WPA2 Enterprise authenticate WLAN users via a RADIUS server using the 802.1X/Extensible Authentication Protocol (EAP) standards. Figure 10.3 shows the 802.1x/EAP process and the communication process used to authenticate a client using 802.1x/EAP.

FIGURE 10.3 802.1X authentication process



802.11i and WPA use the same encryption and authentication mechanisms as WPA2. However, WPA2 doesn't require vendors to implement preauthorization. Preauthorization enables fast, secure roaming, which is necessary in very mobile environments with time-sensitive applications such as wireless VoIP.

Table 10.3 summarizes the authentication and encryption options for WLANs and associated weaknesses.

TABLE 10.3 802.11 and WPA security solutions and weaknesses

	Encryption	Authentication	Weakness
Original IEEE 802.11 standard	WEP	WEP	IV weakness allows the WEP key to be cracked. The same key is used for encryption and authentication of all clients to the WLAN.
WPA	TKIP	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.
WPA2	AES (can use TKIP while in mixed mode)	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.
IEEE 802.11i	AES (can use TKIP while in mixed mode)	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.

Hacking Tools

Aircrack is a WEP-cracking software tool. It doesn't capture packets; it's used to perform the cracking after another tool has captured the encrypted packets. Aircrack runs on Windows or Linux.

WEPCrack and AirSnort are Linux-based WEP-cracking tools.

NetStumbler and Kismet are WLAN discovery tools. They both discover the Media Access Control (MAC) address, Service Set Identifier (SSID), security mode, and channel of the WLAN. Additionally, Kismet can discover WLANs whose SSIDs are hidden, collect packets, and provide IDS functionality.

Real World Scenario

Be Careful Where You War Drive

In 2003, hackers used a wireless network at home-improvement retailer Lowe's in an attempt to steal credit card numbers. The three hackers discovered a vulnerable WLAN at a Lowe's store in Southfield, Michigan while scanning for open connections, or "war driving" in the area. The hackers then used the open access point to compromise the entire corporate network of the North Carolina–based home improvement store company, hacking into stores in California, Kansas, South Dakota, and other states over the course of several weeks. They accessed a credit processing program called tcpcredit that skimmed credit account information for every transaction processed at a particular Lowe's store. The hacker's plan was thought to be a way to siphon off millions of credit card numbers through a backdoor installed in the proprietary Lowe's program.

One of the men involved in the hacking attempt pleaded guilty to four counts of wire fraud and unauthorized access to a computer after he and two accomplices hacked into the Lowe's network. In 2004 he was convicted and is currently serving a nine-year prison term even though there is no evidence that he gathered any credit card numbers. During the investigation only six credit card numbers were found in the file that was created from the modified tcpcredit program. This story goes to show that even harmless war driving could draw unwanted attention, so be careful about the WLAN to which you are connecting.

Using Wireless Sniffers to Locate SSIDs

A common attack on a WLAN involves eavesdropping or sniffing. This is an easy attack to perform and usually occurs at hotspots or with any default installation access point (AP), because packets are generally sent unencrypted across the WLAN. Passwords for network access protocols such as FTP, POP3, and SMTP can be captured in cleartext (unencrypted) by a hacker on an unencrypted WLAN.

The *Service Set Identifier (SSID)* is the name of the WLAN and can be located in beacon frames and probe response frames. If two wireless networks are physically close, the SSIDs are used to identify and differentiate the respective networks. The SSID is usually sent in the clear in a beacon frame as well as other frames, such as probe response frames. Most APs allow the WLAN administrator to hide the SSID. However, this isn't a robust security mechanism because some tools can read the SSID from other packets, such as probe requests and other client-side packets.

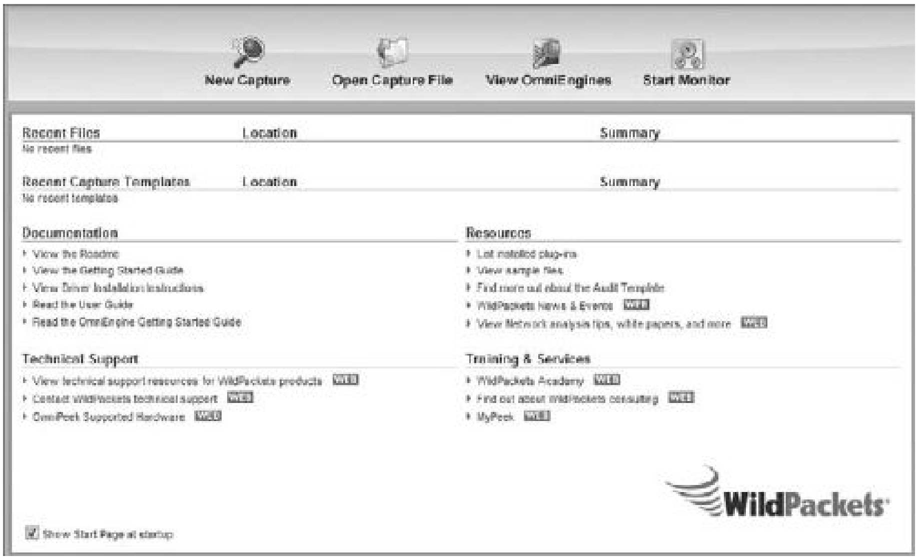
Exercise 10.1 walks you through installing and using a WLAN sniffer tool called Omnipeek.

EXERCISE 10.1

Installing and Using a WLAN Sniffer Tool

1. Download a trial version of Omnipeek from `www.wildpackets.com`. You will need to have a wireless LAN adapter that is supported by Omnipeek in promiscuous mode for Omnipeek to properly capture all the traffic on a wireless LAN. Check for the supported wireless LAN adapters and supporting drivers from `www.wildpackets.com`.

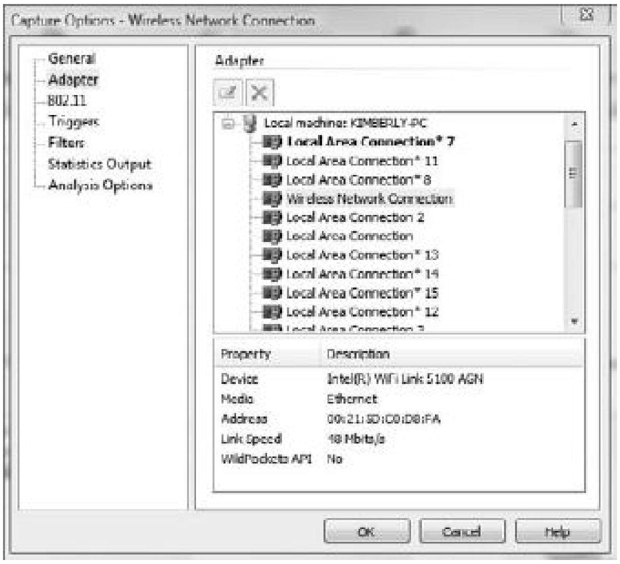
2. Start a new capture by clicking the New Capture button on the Omnipeek start screen.


New Capture
Open Capture File
View OmniEngines
Start Monitor
Recent Files
Location
Summary
No recent files
Recent Capture Templates
Location
Summary
No recent templates
Documentation
View the Readme
View the Getting Started Guide
View Driver Installation Instructions
Read the User Guide
Read the OmniEngine Getting Started Guide
Resources
List installed plug-ins
View sample files
Find more out about the Audit Template
WildPackets News & Events WEB
View Network analysis tips, white papers, and more WEB
Technical Support
View technical support resources for WildPackets products WEB
Contact WildPackets technical support WEB
OmniPeek Supported Hardware WEB
Training & Services
WildPackets Academy WEB
Find out about WildPackets consulting WEB
MyPeek WEB
WildPackets
☑ Show Start Page at startup

EXERCISE 10.1 ***(continued)***

3. Select the wireless adapter from the capture options.

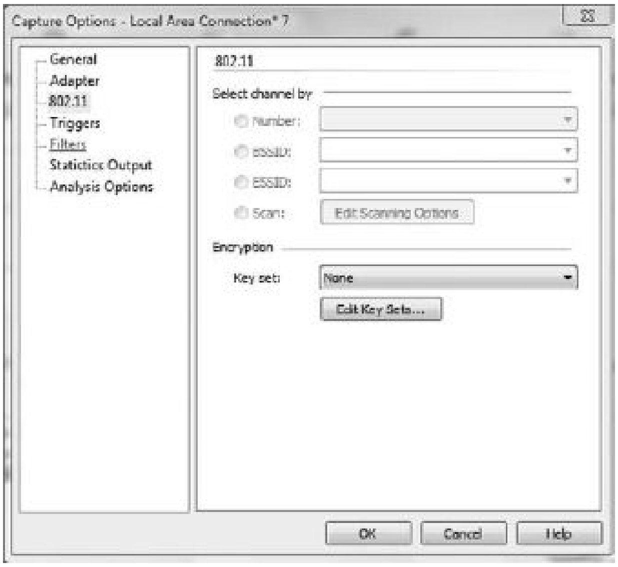
   Note: On the Adapter tab, the WildPackets API must list a description of Yes or the adapter will not work properly in Omnipeek, as shown here:



Local machine: KIMBERLY-PC
- Local Area Connection* 7
- Local Area Connection* 11
- Local Area Connection* 8
- Wireless Network Connection
- Local Area Connection 2
- Local Area Connection
- Local Area Connection* 13
- Local Area Connection* 14
- Local Area Connection* 15
- Local Area Connection* 12
- Local Area Connection 3

Property	Description
Device	Intel(R) WiFi Link 5100 AGN
Media	Ethernet
Address	00:21:5D:C0:D8:FA
Link Speed	48 Mbits/s
WildPackets API	No

4. Click the 802.11 tab and choose initially to scan all channels. Later, once you have identified a specific WLAN to monitor, you can choose to only capture traffic on that one channel.



Select channel by
○ Number:
○ BSSID:
○ ESSID:
○ Scan:

Encryption
Key set: None

EXERCISE 10.1 ***(continued)***

5. Click OK to start the capture. The capture window will show frames being captured. Double-click a frame to see more detail.
6. Click the stop capture button to stop capturing. Select the Display filter drop down button (it looks like a funnel) from the toolbar just above the frames. Select POP from the filter drop down list. Only POP email frames will be displayed. You can use a display filter to show only certain types of frames. POP, SMTP, FTP, TELNET, and HTTP frames all carry clear text data. Passwords and other information can be gathered from those frames.
7. To find Access Points (AP) and Stations that are connected, click on the WLAN menu on the left side of the screen. The APs BSSID, STA MAC, Channel, and SSID can all be located on the WLAN screen of Omnipeek. APs not broadcasting the SSID will show 0x00 for the SSID until a station connects and Omnipeek can determine the SSID from the probe frames. Once Omnipeek can determine the SSID, it will be displayed on the WLAN screen.

MAC Filters and MAC Spoofing

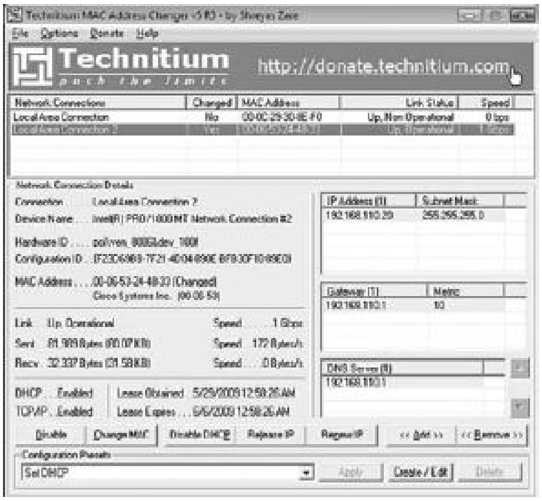
An early security solution in WLAN technology used MAC address filters: a network administrator entered a list of valid MAC addresses for the systems allowed to associate with the AP. MAC filters are cumbersome to configure and aren't scalable for an enterprise network because they must be configured on each AP. MAC spoofing is easy to perform (as you'll see in Exercise 10.2) and negates the effort required to implement MAC filters. A hacker can identify a valid MAC address because the MAC headers are never encrypted.

EXERCISE 10.2

MAC Address Spoofing

1. Download and install TMAC from `www.technitium.com`.
2. Select the wireless adapter from the list of network connections in TMAC. Click the Change MAC button.

EXERCISE 10.2 *(continued)*



Technitium MAC Address Changer v5 R3 - by Shreyas Zare

Network Connections	Changed	MAC Address	Link Status	Speed
Local Area Connection	No	00-0C-29-30-8E-F0	Up, Non Operational	0 bps
Local Area Connection 2	Yes	[illegible]	Up, Operational	1 Gbps

Network Connection Details

Connection . . . Local Area Connection 2
Device Name . . . Intel(R) PRO/1000 MT Network Connection #2
Hardware ID . . . . pci\ven_8086&dev_100f
Configuration ID . . {F23D6989-7F21-4D04-890E-BFB30F10[illegible]}
MAC Address . . . . 00-06-53-24-48-33 (Changed)
Cisco Systems Inc. (00-06-53)

Link . . Up, Operational Speed . . . . 1 Gbps
Sent . . 81,909 Bytes (80.07 KB) Speed . . 172 Bytes/s
Recv . . 32,337 Bytes (31.58 KB) Speed . . . 0 Bytes/s

DHCP . . Enabled Lease Obtained . . 5/29/2009 12:58:26 AM
TCP/IP . . Enabled Lease Expires . . . 6/6/2009 12:58:26 AM

IP Address (1)	Subnet Mask
192.168.110.20	255.255.255.0

Gateway (1)	Metric
192.168.110.1	10

DNS Server (1)
192.168.110.1

Configuration Presets: Set DHCP

3. Type **00:11:22:33:44:55** as the MAC address; click the Change Now button and confirm the changes to be made to the MAC address.

4. Open a command prompt and type `IPCONFIG /ALL` to confirm the MAC address of the wireless adapter has been changed to 00:11:22:33:44:55.

5. To restore the original MAC address of the network adapter, select the adapter within TMAC, click the Change MAC button, and click the Original MAC button.

6. Configure an access point to allow only the MAC address 00:11:22:33:44:55 to connect to the WLAN. (This step will vary depending on the type of access point—refer to the user guide for your access point to configure the MAC address filtering.)

7. Test the wireless client connecting using the original MAC address. The client should not connect to the AP with the MAC filtering applied. Change the MAC to 00:11:22:33:44:55 using TMAC and attempt to connect again to the AP. It should be able to connect to the AP using the Spoofed MAC address.

\

Hacking Tool

SMAC is a MAC spoofing tool that a hacker can use to spoof a valid user's address and gain access to the network.

Rogue Access Points

Rogue access points are WLAN access points that aren't authorized to connect to a network. Rogue APs open a wireless hole into the network. A hacker can plant a rogue AP, or an employee may unknowingly create a security hole by plugging an access point into the network. The resulting rogue AP can be used by anyone who can connect to the AP, including a hacker, giving them access to the wired LAN. This is why it's critical for organizations to scan for rogue access points. Even organizations that have a "no wireless" policy need to perform wireless scanning to ensure no rogue APs are connected to the network.

Rogue APs are probably the most dangerous wireless threat that exists because they give a potential hacker direct access to the wired LAN. Clients connecting to rogue access points will usually receive an IP address directly from the network or from the AP and then the traffic is bridged directly on the wired LAN. From there a hacker can perform scanning, enumeration, and system hacking against targets on the wired LAN. Countermeasures to detect and remove rogue access points exist and should be implemented by all organizations.

Many enterprise WLAN controller–based management solutions have the ability to perform rogue access point detection. These controller-based solutions include the ability to monitor the air using either access points or sensors/monitors, or both. Access points by nature must remain on a channel while clients are connected in order to service those clients, whereas sensors and monitors are able to continually scan the air on all channels in the frequency band to capture possible rogue access point wireless transmissions. These wireless MAC addresses are compared to addresses received on the wire to determine if the AP is connected to the same LAN as the wireless intrusion detection system (WIDS) or wireless intrusion prevention system (WIPS). Some WIPSs can also keep clients from connecting to rogue access points by sending spoofed deauthentication frames to any client attempting to connect to the rogue AP—thus keeping clients from sending data through the rogue AP. Overlay WIDS/WIPS systems can also be helpful in detecting rogue access points by triangulating the position of the rogue AP.

Enterprise WLAN WIPS and overlay WIPS are only temporary detection and containment options. The primary goal should be to locate the rogue AP and remove it from the network.

Evil Twin or AP Masquerading

Hackers can use a software-based AP to create an AP that looks like a real Access Point. This is known as the Evil Twin attack or AP Masquerading.

Wireless Hacking Techniques

Most wireless hacking attacks can be categorized as follows:

Cracking Encryption and Authentication Mechanisms These mechanisms include cracking WEP, WPA preshared key authentication passphrases, and Cisco's Lightweight EAP authentication (LEAP). Hackers can use these mechanisms to connect to the WLAN using stolen credentials or can capture other users' data and decrypt or encrypt it. A protection against this attack is to implement a stronger type of encryption, such as AES.

Eavesdropping or Sniffing This type of attack involves capturing passwords or other confidential information from an unencrypted WLAN or hotspot. A protection against this attack is to use SSL application-layer encryption or a VPN to secure user data.

Denial of Service DoS can be performed at the physical layer by creating a louder RF signature than the AP with an RF transmitter, causing an approved AP to fail so users connect to a rogue AP. DoS can be performed at the Logical Link Control (LLC) layer by generating deauthentication frames (deauth attacks), by continuously generating bogus frames, or by having a wireless NIC send a constant stream of raw RF (Queensland attack). A countermeasure is to enforce a security perimeter around your WLAN and detect and remove sources of DoS attacks using an IDS.

AP Masquerading or Spoofing Rogue APs pretend to be legitimate APs by using the same configuration SSID settings or network name. A countermeasure to AP masquerading is to use a WIDS to detect and locate spoofed APs.

MAC Spoofing The hacker pretends to be a legitimate WLAN client and bypasses MAC filters by spoofing another user's MAC address. WIDSs can detect MAC spoofing, and not using MAC filtering is a way to avoid MAC spoofing attacks.

Planting Rogue Access Points The most dangerous attack is a rogue AP that has been planted to allow a hacker access to the target LAN. A countermeasure is to use a WIPS to detect and locate rogue APs.

Wireless networks give a hacker an easy way into the network if the AP isn't secured properly. There are many ways to hack or exploit the vulnerabilities of a WLAN. There are also effective countermeasures to many of these attacks. The next section will detail the best methods to secure wireless network.

Securing Wireless Networks

Because wireless networking is a relatively new technology compared to wired networking technologies, fewer security options are available. Security methods can be categorized by the applicable layer of the OSI model.

Layer 2, or MAC layer, security options are as follows:

- Static WEP (not recommended)
- WPA
- WPA2/802.11i

Layer 3, or Network layer, security options are as follows:

- IPSec
- SSL VPN

Layer 7, or Application layer, security options are as follows:

- Secure applications such as Secure Shell (SSH), HTTP over SSL (HTTPS), and FTP/SSL (FTPS)

NOTE Because of its numerous weaknesses, WEP shouldn't be used as the sole security mechanism for a WLAN.

Securing Home Wireless Networks

Many people setting up wireless home networks rush through the job to get their Internet connectivity working as quickly as possible. The small office, home office (SOHO) networking products on the market make setup quick and easy but not necessarily secure. Configuring additional security features can be time consuming and nonintuitive for some home users, and therefore they may not implement any security mechanism at all.

These days wireless networking products are so ubiquitous and inexpensive that just about anyone can set up a WLAN in a matter of minutes with less than $100 worth of equipment. This widespread use of wireless networks means that there may be dozens of potential network intruders within range of your home or office WLAN. Most WLAN hardware has gotten easy enough to set up that many users simply plug it in and start using the network without giving much thought to security. Nevertheless, taking a few extra minutes to configure the security features of your wireless router or access point is time well spent. The following recommendations will improve the security of your home wireless network:

Change default administrator passwords and usernames. When configuring your home access point, you usually use a web browser to access the configuration interface. Almost all routers and access points have an administrator password that's needed to log into the device and modify any configuration settings. To set up these pieces of equipment, manufacturers provide a default username and password. Many of the default logins are simple (such as username=admin and password=admin) and very well known to hackers on the Internet. Most devices use a weak default password like "password" or the manufacturer's name, and some don't have a default password at all. You should change the default password on your home AP as soon as possible. As soon as you set up a new WLAN router or access point, your first step should be to change the default administrative password to something else.

Use WEP/WPA encryption. Most Wi-Fi equipment supports some form of *encryption*. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by hackers. You should configure the strongest form of encryption that works with your wireless clients. 802.11's WEP (Wired Equivalency Privacy) encryption has well-known weaknesses that make it relatively easy for a determined user with the right equipment to crack the encryption and access the wireless network. A better way to protect your WLAN is with WPA (Wi-Fi Protected Access). WPA provides much better protection and is also easier to use, since your password characters aren't limited to 0–9 and A–F as they are with WEP. (Note: WEP can also use ASCII keys.)

Change the default SSID. Access points use a network name called an SSID to advertise the network to wireless users. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "Linksys." Just knowing the SSID does not by itself allow your neighbors to break into your network, but it is a start. More importantly, when someone finds a default SSID, it is usually an indication of a poorly configured network. You should change the default SSID immediately when configuring wireless security on your network.

Do not auto-connect to open Wi-Fi networks. Connecting to an open Wi-Fi network such as a free wireless hotspot or an unknown WLAN exposes your computer to security risks. Most computers have a setting available allowing these connections to happen automatically without notifying you. Most versions of Windows will reconnect to a previously connected SSID. This setting should not be enabled except in temporary situations.

Enable firewall settings on your laptop and home access point. Most network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. You should always install and configure personal firewall software on each computer connected to the router.

Reduce your WLAN transmitter power. You won't find this feature on all wireless routers and access points, but some allow you to lower the power of your WLAN transmitter and thus reduce the range of the signal. (Normally this feature is only available with enterprise-class access points.) Although it's usually impossible to fine-tune a signal so precisely that it won't leak outside your home or business, with some trial and error you can often limit how far outside your premises the signal reaches, minimizing the opportunity for outsiders to access your WLAN. This will also improve your throughput on your access point by limiting the wireless cell to just your premise.

Disable remote administration. Most WLAN routers have the ability to be remotely administered via the Internet. Ideally, you should use this feature only if it lets you define a specific IP address or limited range of addresses that will be able to access the router. Otherwise, almost anyone anywhere could potentially find and access your router. As a rule, unless you absolutely need this capability, it's best to keep remote administration turned off.

Summary

The growth of wireless networks has been fueled by convenience and an ever-increasing mobile workforce. More employees are working from home or on the road, and organizations are building larger enterprise WLANs to support greater mobility of the workforce. In the past, many organizations have avoided WLANs because of the inherent lack of security and immature technologies.

The ratification of 802.11n promises greater speeds on wireless LANs, making them comparable to existing Ethernet LANs. This enhanced speed will only increase the number of organizations using wireless for business applications and consequently increase the security risks.

More recently, WLAN security mechanisms have matured to the point that businesses and government offices are beginning to adopt WLAN technology. With proper security mechanisms and implementation, WLANs can be secured to a high standard. By carefully following the security recommendations and countermeasures, you can secure your WLAN against attack.

Exam Essentials

Understand the inherent security vulnerabilities of using a WLAN. RF is a broadcast medium, like a hub environment, and therefore all traffic is able to be captured by a hacker.

Understand the security solutions implemented in the IEEE 802.11 standard. WEP, shared key, and MAC filters are security solutions offered in the original IEEE 802.11 standard.

Understand the security solutions offered by the Wi-Fi Alliance. WPA and WPA2 are Wi-Fi Alliance equipment security certifications.

Know what an SSID is used for on a WLAN. The SSID identifies the network name and shouldn't be used as a security mechanism.

Know what security mechanisms should not be used for WLAN security. WEP and MAC filters shouldn't be used as the sole means to secure the WLAN.

Review Questions

1. Which of the following security solutions uses the same key for both encryption and authentication?

   A. WPA

   B. WPA2

   C. WEP

   D. 802.11i

2. What does WEP stands for?

   A. Wireless Encryption Protocol

   B. Wired Equivalent Privacy

   C. Wireless Encryption Privacy

   D. Wired Encryption Protocol

3. What makes WEP crackable?

   A. Same key used for encryption and authentication

   B. Length of the key

   C. Weakness of IV

   D. RC4

4. Which form of encryption does WPA use?

   A. AES

   B. TKIP

   C. LEAP

   D. Shared key

5. Which form of authentication does WPA2 use?

   A. Passphrase only

   B. 802.1x/EAP/RADIUS

   C. Passphrase or 802.1x/EAP/RADIUS

   D. AES

6. 802.11i is most similar to which wireless security standard?

   A. WPA2

   B. WPA

   C. TKIP

   D. AES

7. Which of the following is a Layer 3 security solution for WLANs?
   - **A.** MAC filter
   - **B.** WEP
   - **C.** WPA
   - **D.** VPN

8. A device that sends deauth frames is performing which type of attack against the WLAN?
   - **A.** Denial of service
   - **B.** Cracking
   - **C.** Sniffing
   - **D.** MAC spoofing

9. What is the most dangerous type of attack against a WLAN?
   - **A.** WEP cracking
   - **B.** Rogue access point
   - **C.** Eavesdropping
   - **D.** MAC spoofing

10. 802.11i is implemented at which layer of the OSI model?
    - **A.** Layer 1
    - **B.** Layer 2
    - **C.** Layer 3
    - **D.** Layer 7

11. Which of the following is the best option for securing a home wireless network?
    - **A.** WEP
    - **B.** Shared-key authentication
    - **C.** WPA-Personal
    - **D.** WPA-Enterprise

12. You just installed a new wireless access point for your home office. Which of the following steps should you take immediately to secure your WLAN?
    - **A.** Spoof your clients MAC address.
    - **B.** Change the Admin password on the AP.
    - **C.** Change the channel on the AP to Channel 11.
    - **D.** Set the SSID to SECURE.

13. What can be done on a wireless laptop to increase security when connecting to any WLAN? (Choose two.)

A. Install and configure personal firewall software.

B. Disable auto-connect features.

C. Use WEP.

D. Use MAC filtering.

14. What is an SSID used for on a WLAN?

A. To secure the WLAN

B. To manage the WLAN settings

C. To identify the WLAN

D. To configure the WLAN AP

15. What is the best way to enforce a "no wireless" policy?

A. Install a personal firewall.

B. Disable WLAN client adapters.

C. Use a WIDS/WIPS.

D. Only connect to open APs.

16. Which of the following is a program used to spoof a MAC address?

A. MAC Again

B. Big MAC

C. TMAC

D. WZC

17. Which of the following are Layer 7 application-secure protocols used to secure data on WLAN hotspots?

A. HTTPS

B. HTTP

C. FTP

D. VPN

18. Which type of frame is used by a WIPS to prevent WLAN users from connecting to rogue access points?

A. Disconnect

B. Deauthentication

C. Disable

D. Reject

19. WPA passphrases can consist of which of the following character sets?

    A. Only a–z and A–Z

    B. Only a–z

    C. Only a–z, A–Z, and 0–9

    D. Only 0–9

20. Which of the following is a countermeasure to using WEP?

    A. Use a strong WEP key of at least 20 characters.

    B. Use a WEP key that does not repeat any of the same characters.

    C. Use WPA instead of WEP.

    D. Implement a preshared key with WEP.

Answers to Review Questions

1. C. WEP uses the same key for encryption and authentication.
2. B. WEP is an acronym for Wired Equivalent Privacy.
3. C. WEP is crackable because of the lack of sophistication in using the IV when deploying RC4.
4. B. WPA uses TKIP.
5. C. WPA2 uses either a passphrase in personal mode or 802.1x/EAP/RADIUS in enterprise mode.
6. A. 802.11i is almost the same as WPA2.
7. D. A VPN is a Layer 3 security solution for WLANs.
8. A. A DoS can be performed by a device sending constant deauth frames.
9. B. A rogue AP is the most dangerous attack against a WLAN because it gives a hacker an open door into the network.
10. B. 802.11i is a Layer 2 technology.
11. C. WPA-Personal has the strongest authentication and encryption usable on a home network. WPA-Enterprise requires a RADIUS server, which most home users would not have the ability to set up and configure.
12. B. You should immediately change the Admin password on an AP's web interface when installing a new AP.
13. A, B. Installing and configuring personal firewall software and disabling auto-connect features are two ways to increase the security of WLAN connections.
14. C. A Service Set Identifier (SSID) is used to identify the WLAN to wireless users.
15. C. Using a wireless intrusion detection system or protection system is the best way to enforce a "no wireless" policy.
16. C. TMAC is a program used to spoof a MAC address.
17. A. HTTPS is a secure version of HTTP commonly used to secure data on WLAN hotspots.
18. B. Deauthentication frames are used by a WIPS to prevent users from connecting to rogue APs.
19. C. WPA passphrases can be alphanumeric and include a–z, A–Z, and 0–9.
20. C. Using WPA is a countermeasure to the weakness of WEP.