13.1.11 Wireless Hacking Countermeasures Tool Facts

To secure your wireless network, it's important to implement and adopt appropriate countermeasures.

This lesson covers the following topics:

- Wi-Fi predictive planning tools
- WPA/WPA2 cracking
- RF scanning and rogue access points (APs)
- Vulnerability scanning
- Wireless penetration testing

Wi-Fi Predictive Planning Tools

Proper planning and implementation of network security is essential to creating hack-resistent Wi-Fi. Predictive planning tools can assist you. Although all tools won't have the same features, Wi-Fi predictive planning tools can assist you with:

- AP Placement
- Cable length calculations
- Signal strength predictions
- Floor plans and blueprints
- Building material impact
- Simulation of network performance
- Centralized wireless network management
- Expansion options

Defend Against WPA/WPA2 Cracking

When working with a wireless network, always upgrade to WPA2 with AES/CCMP (or newer) encryption whenever possible. WPA2 provides per-frame or per-packet authentication. This means that each packet includes its own unique authentication. Despite the increase of security offered by WPA2, it can still be hacked if additional countermeasures are not taken. These countermeasures are described in the following table.

Countermeasure	Description
Software updates and patches	A simple yet effective countermeasure is to ensure that the WPA2 devices are using the latest patches.
Passphrase protection	A passphrase is a combination of letters, numbers, spaces, and punctuation symbols used as a security key for network connections. When working with WPA and WPA2, the passphrase's security is critical. A wireless device and the AP use a pre-shared key (PSK) to authenticate and, once authenticated, to create a Pairwise Key Master (PKM) to secure communications. They initiate communications using a process known as the four-way handshake to prove that they independently know the pre-shared key passphrase. During this handshaking process, the following occurs: ▪ The AP sends a random value with a Key Replay Counter (KRC) to the wireless device. ▪ The wireless device creates the Pairwise Transient Key (PTK) from the information sent from the AP. The wireless device returns a different random value to the AP, a Message Integrity Code (MIC), and the KRP with the same value the AP sent. ▪ The AP creates a PTK and verifies the message, creates a Group Temporal Key (GTK), and sends the GTK to the wireless device. ▪ The wireless device verifies the message and, if valid, sends confirmation to the AP. Even though capturing the packets used during the handshaking process is relatively easy using a sniffing tool, you can make cracking the PMK nearly impossible (or, at least, very difficult) by following a few simple guidelines: ▪ Use passphrases that are a combination of letters, numbers, symbols, and spaces. ▪ Use passphrases that are long enough to be hard to guess (typically at least 20 characters or more), but easy to remember. ▪ Do not use famous quotes from movies, books, or other similar sources. ▪ Ensure that your passphrases are not reused between sites, applications, or other sources. ▪ Change passphrases often.
Client-level protections	You should also be proactive and provide countermeasures at the client level. This includes the following steps: ▪ Properly configure the firewall to prevent a hacker from installing a rogue AP on the network. ▪ Ensure that all clients are using only WPA2 with AES and CCMP encryption.

	▪ Ensure that the other client settings, such as the server and address, are correct, and that clients will not be prompted to connect to new servers.
Virtual Private Networks (VPNs)	Another method of defending against WPA/WPA2 cracking is to use VPN technology to protect client data when connecting from a remote system.
Network Access Protection (NAP) and Network Access Control (NAC)	Two solutions to improve security are Network Access Protection and Network Access Control. ▪ NAC is an approach to computer security that attempts to unify endpoint security technology, user or system authentication, and network security enforcement. ▪ NAP is a Microsoft technology for controlling network access to a computer based on the computer's health. With NAP, system administrators can define policies for system health requirements.

RF Scanning and Rogue APs

An unauthorized or rogue AP is a constant threat for wireless networks. Therefore, you should actively perform radio frequency (RF) scanning to monitoring the RF spectrum for these types of devices. A Wireless Intrusion Prevention System (WIPS) and a Wireless Intrusion Detection System (WIDS) are two types of tools that can perform RF scanning. WIPS and WIDS can be implemented as either a software application or a hardware device. Their primary purpose is to detect and prevent unauthorized network access to your wireless network in real time. These systems often include some type of management software that is used to configure, view, and log intrusions.

The following table identifies additional key characteristics of WIPS and WIDS.

Characteristic	Description
MAC address filtering	In many cases, WIPS and WIDS accomplish their function, in part, by comparing the MAC addresses of all wireless APs on a network against a known MAC filtering list. When a device not on the list attempts to connect to the network, it is denied, and an alert is sent to an administrator. This is particularly true of WIDS.
Disable/block attacks	In addition to detecting a threat, a higher-end WIPS can also analyze the unique radio frequency signatures that the wireless devices generate. Using predefined rules, it disables or blocks these types of attacks. For example, devices such as the AirTight WIPS and the WatchGuard WIPS will automatically detect and prevent: ▪ Rogue APs ▪ Misconfigured APs ▪ Rogue clients ▪ Ad hoc networks In addition, WatchGuard, as well as other intrusion prevention tools, can differentiate between authorized, external, and rogue APs.
Evil twin detection	Many WIPS tools can protect your network from what is referred to as an evil twin. An evil twin is a rogue AP that appears to be legitimate but is set up to eavesdrop on wireless communications. It's known as an evil twin because, in most cases, the rogue AP is configured to use the same SSID and BSSID used by a legitimate AP. Since the evil twin is often configured to pass internet traffic through to the legitimate AP, users are unaware that data is being monitored and captured.

Some network management software has the ability to use wired side inputs. This means that the management software running on a computer that is physically connected to the LAN can detect APs connected through the wire. The advantage of this method is that it may find rogue APs that were not detected using the other methods. However, be aware that if the rogue AP doesn't support the technology used by the network management software, it may still go undetected.

When a rogue AP is detected, it must be eliminated. In most cases, this attack is as simple as removing the physical AP. However, if the rogue AP is inaccessible, you can ensure that no clients can connect to it by initiating a denial-of-service attack on it.

Vulnerability Scanning

Vulnerability scanning is a security technique used to identify security weaknesses in your Wi-Fi network. With the software and hardware available today, vulnerability testing can and should be run continuously. Vulnerability scanning tools typically identify:

- Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.
- Misconfiguration, such as missing patches and open mail relays.
- Issues with passwords, such as using the default passwords, common passwords, and blank or absent passwords on some system accounts.
- Denials-of-service attacks.

Wireless Penetration Testing

A wireless penetration test attempts to break into your wireless network. If your network has been adequately protected, the penetration test will only trigger alarms. If done correctly, penetration tests can help you analyze your design weaknesses and find technical flaws and

vulnerabilities. Although vulnerability testing is ongoing, penetration testing is recommended at least once per year.

A wireless penetration test helps you:

- Identify any wireless threats that may still need to be addressed.
- Find any required upgrades for the network design, hardware, or software.
- Identify if any sensitive data can be captured. The penetration tester uses packet analysis or sniffing tools to do this.
- Define the steps that are needed and should be followed to prevent successful attacks and exploitation. These steps should include the specific procedures that should be followed when a breach is detected.
- Collect and document information about the devices connected, as well as the security protocols being used.

General steps for wireless penetration testing include:

1. Discover the devices connected to your wireless networks and document all of the devices found.
2. Perform common Wi-Fi attacks on the wireless devices and check the devices for the various encryptions (for example WEP, WPA/WPA2, and PEAP).
3. Conduct specific penetration tests to break the encryption for each encryption type found.
4. Detect unencrypted data transmission on wireless LANs. If the network is not encrypted, perform common Wi-Fi attacks and document the risk.
5. Ensure that no damage was caused during any of the penetration tests.
6. Document all results and generate a report.
