A WildPackets Academy Tutorial

AiroPeek and Wireless Security: 802.11 Security Audits

This tutorial will demonstrate how to set up a Security Audit using WildPackets’ 802.11 wireless LAN analyzers, AiroPeek standard and AiroPeek NX. (“AiroPeek” in this paper will refer to both our expert AiroPeek NX and our standard AiroPeek.)

Despite the explosion of wireless technology in the marketplace, concerns about 802.11 security remain. The fact is that it isn't secure. This doesn't mean, however, that the technology can't or shouldn't be used in your enterprise.

Understanding the limitations of wireless LAN security is the first step towards ensuring that important and confidential data is not made available to prying antennae. The next steps are to:

• Establish corporate policy regarding an appropriate level of security given the state of the technology;
• Determine what corporate information is allowed to be transmitted over the airwaves given the chosen level of security;
• Implement the level of security required;
• Verify the implementation;
• Monitor the airwaves for traffic that violates either of the first two tenets.

AiroPeek is the most comprehensive wireless LAN management tool available on the market today. Significant among the many uses of AiroPeek is its use as a security audit tool. AiroPeek gives you the ability to quickly and easily verify security implementations and monitor traffic for security violations. And AiroPeek security features are easily tailored to your network.

Here are some practical ways to use AiroPeek to secure your wireless LAN:

1. Security Audit Template

AiroPeek ships with a Security Audit Template. This Template, located in the Security Audit Template folder, creates a capture window that triggers a notification when a packet matches any of a number of custom security filters. Before using the template, you must load the Security Audit Filters file.

![Filters view in AiroPeek, showing imported Security Audit filters.](image)
The security template includes many pre-defined filters that look for common wireless LAN security issues, including:

- An unfamiliar host requesting a DHCP address assignment
- Access points using a default ESSID
- SNMP traffic going across the WLAN
- Spanning Tree Algorithm operating across the WLAN
- TELNET being used on the WLAN
- Contention Free mode in use on the network
- OSPF operating across the WLAN
- The “Request To Send” mechanism implemented on your network
- Non-WEP (unencrypted) data present on the WLAN
- HSRP or IGRP operating across the WLAN

By default, a "severe" notification is used when any of these security-related events has been identified. The actual severity depends upon your network, e.g., what applications are running. You can change the severity used in the Start Trigger action and use notification options to email you when the event occurs. Since the Security Audit Template has set filters to allow ONLY the security-related issues, the presence of one packet in the buffer indicates that an event has occurred. Turn on the "filter" column in the packet list display to see which security exposure was identified.

![Start Trigger Event](image)

**Figure 2.** The Start Trigger Event shows what a particular Capture window is waiting for.

### 2. Alarms

AiroPeek ships with a number of pre-configured, wireless security-related alarms, including:

- Wireless distribution system in use
- Excessive 1 Mbit/s packet transmission
- Excessive 802.11 Management traffic
- WEP ICV Errors
Again, the actual relevance of a specific alarm is dependent upon your network. You can also modify the sensitivity of the alarms.

Figure 3. Alarms window, showing Security Audit alarms

### 3. Create your own Security Audit Template

Many security-related items are specific to your network, so a pre-defined template cannot encompass all the security risks. With AiroPeek, it is easy to define your own filters and alarms and tailor them to your network. Examples of relevant filters include:

- SSID beacons enabled
- Attempt to associate by user with blank ESSID.
- Traffic from MAC address of a stolen wireless card/laptop - create an advanced filter to look for the MAC addresses.
- Rogue Access Point filter - This filter is created by capturing normal network traffic and determining the data offset in an 802.11 frame corresponding to the ESSID or BSSID.
- Filter for SNMP community words.
4. Visual Cues

AiroPeek includes a Nodes tab that breaks down your network traffic in several ways via a pull-down menu next to the nodes count. One choice in the menu is "802.11." This option lists the wireless nodes with specific wireless data, much of which can be monitored for wireless security issues, including:

- SSID column - view all BSSIDs seen on the network to quickly establish whether rogue access points exist.
- WEP column - see who is talking WEP and who isn't.
- WEP ICV errors - see who is transmitting WEP ICV errors.
- WEP Key - see which WEP key (1-4) is in use.
- Signal strength and packets sent/received statistics.

![Figure 4. Nodes view, showing Nodes stats](image)

5. 802.1x Implementations

AiroPeek decodes several new protocols, including some used in 802.1x security implementations. By decoding the EAP and Kerberos protocols, AiroPeek helps troubleshoot client authentications and verify that the end result is encrypted traffic.

6. Tracking Excessive Server Type Activity

Excessive traffic of specific application types may indicate that a rogue client is attempting to gain access to the network. These can be seen as excessive packets of a particular type, such as:

- Excessive broadcasts
- Excessive Wireless retries
- Excessive EAP/LEAP handshaking
- Excessive DHCP requests
7. Interference

Occurrence of high wireless retry packets or high CRC errors while signal strength remains strong is an indication that there may be RF interference. Interference can be caused by other devices operating in the 2.4 GHz frequency, such as Bluetooth or cordless phones, or perhaps by someone flooding the frequency, thereby making the network unusable.

Summary

The AiroPeek Security Audit Template is a great starting place for your own network security scans. With a special set of security audit filters and a capture template designed to use them, the Security Audit Template scans network traffic in the background, looking for indications of a security breach. When it finds one, it captures the packets that meet its criteria and sends a notification, keeping you informed of suspicious activity on your wireless LAN. With its easily customizable features, the Security Audit Template can be modified precisely to fit your wireless security needs. Here we have demonstrated a number of practical ways to ensure the security of your wireless network.
WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

WildPackets Academy

WildPackets Academy provides the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for Ethernet and 802.11 wireless LANs.

In addition to classroom-taught Network Analysis Courses, WildPackets Academy also offers:

- Web-Delivered Training
- On-site and Custom Courseware Delivery
- The Technology, Engineering, and Networking Video Workshop Series
- On-site and Remote Consulting Services
- Instruction and testing for the Network Analysis Expert (NAX™) Certification

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit www.wildpackets.com/academy. NAX examination and certification details are available at www.nax2000.com.

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek NX/EtherPeek and AiroPeek NX/AiroPeek, led by a WildPackets Academy Instructor. Please visit www.wildpackets.com for complete details and scheduling information.

About WildPackets, Inc.

WildPackets, a privately-held corporation, was founded in 1990 with a mission to create software-based tools to simplify the complex tasks associated with maintaining, troubleshooting, and optimizing evolving computer networks. WildPackets' patented, core "Peek" technology is the development base for EtherPeek™, TokenPeek™, AiroPeek™, and the NX™ family of expert packet analyzers. All are recognized as the analysis tools of choice for small, medium, and large enterprise customers, allowing IT Professionals to easily maximize network productivity. Information on WildPackets, WildPackets Academy, Professional Services, products, and partners is available at www.wildpackets.com.