



AN AIRMAGNET TECHNICAL WHITE PAPER

Supplied by:

Phoenix Datacom Ltd  
Phoenix House  
Smeaton Close  
Rabans Lane  
Aylesbury  
Bucks HP19 8UW

[www.phoenixdatacom.com/airmagnet](http://www.phoenixdatacom.com/airmagnet)

email: [info@phoenixdatacom.com](mailto:info@phoenixdatacom.com)

tel: 01296 397711

## Managing WLAN Risks With Vulnerability Assessment

By Lisa Phifer, Core Competence Inc.

[WWW.AIRMAGNET.COM](http://WWW.AIRMAGNET.COM)

©2005 AirMagnet Inc, All rights reserved.

AirMagnet, AirWISE, PocketNOC, the AirMagnet logo are trademarks of AirMagnet Inc.

All other product names mentioned herein may be trademarks of their respective companies.

## Table of Contents

Summary .....	5
Managing WLAN Risks With Vulnerability Assessment .....	6
Understanding WLAN Vulnerabilities .....	6
Inability to Control Access .....	6
Lack of Confidentiality .....	7
Unauthorized Network Use .....	8
Forged Messages .....	9
Denial of Service .....	9
Putting Attacks Into Perspective: Risk Analysis .....	13
Conducting A Vulnerability Assessment .....	15
Using Portable Tools for WLAN Discovery .....	17
Using Penetration Tests to find Vulnerabilities .....	18
Using WIPS to Monitor Attacks .....	20
Using Wireless Analyzers for Investigation .....	21
Putting Assessment Results To Work .....	22

©2005 AirMagnet Inc, All rights reserved.

AirMagnet, AirWISE, PocketNOC, the AirMagnet logo are trademarks of AirMagnet Inc.

All other product names mentioned herein may be trademarks of their respective companies.

How AirMagnet Can Help.....25

Appendix A: Example Worksheet ..... 28

©2004 AirMagnet Inc, All rights reserved.

AirMagnet, AirWISE, PocketNOC, the AirMagnet logo are trademarks of AirMagnet Inc.  
All other product names mentioned herein may be trademarks of their respective companies.

## Summary

Many options are available to safeguard wireless LANs, but which security measures should your company deploy, and how can you tell whether your network is sufficiently hardened against 802.11 and 802.1X attacks? This paper describes an iterative process for business risk analysis, vulnerability identification, and threat remediation. It explains how to conduct your own WLAN vulnerability assessment and apply results to manage your risk.

## Managing WLAN Risks With Vulnerability Assessment

With completion of 802.11i and maturation of Wi-Fi products, businesses now have the tools needed to safeguard wireless LANs, deflecting and reacting to intrusions. But enabling a few security options may not be enough. How can you really know whether your network is sufficiently hardened against 802.11 and 802.1X attacks?

A proven-effective defense requires systematic identification and elimination of vulnerabilities that could be exploited to penetrate your network and compromise business assets. This paper categorizes WLAN attacks and defines an iterative process for risk analysis. It explains how to conduct a vulnerability assessment and use results to mitigate high-priority threats. By finding and fixing your own vulnerabilities before intruders do, you can tap wireless benefits without creating unacceptable business risk.

### Understanding WLAN Vulnerabilities

All networks are somewhat vulnerable, but in wired networks, physical barriers reduce risk by limiting media access. Ethernet ports can be locked away in closets and offices, and unused ports can be disabled. In wireless networks, the medium is the air. Walls, doors, and floors reduce signal strength, but do not stop attacks launched from stairwells, lobbies, parking lots, or nearby buildings. These new vectors can be used to exploit 802.11 and 802.1X vulnerabilities.

### Inability to Control Access

War drivers use shareware Stumblers and high-gain antennas to discover APs. Intruders frequently penetrate company networks by exploiting unauthorized "rogue" APs, installed by naïve employees inside the firewall. They also look for promiscuous wireless devices that are willing to associate

with any station. Once connected, intruders can use traditional network attacks to probe clients, servers, and datastores and find open ports and exploitable services.

Careful AP placement can reduce RF signal leakage, but it won't stop outsiders from transmitting or receiving on channels used by your WLAN. Many APs support MAC access control lists, but intruders can easily bypass them by using a legitimate address. Since access to the air cannot be reliably controlled, you must assume that attackers are present and "harden" wireless-connected devices to prevent compromise.

### Lack of Confidentiality

Intruders that discover your WLAN can easily eavesdrop on wireless traffic. Shareware or commercial capture tools can record packets and extract TCP/IP headers, usernames, passwords, email messages, files, and other data sent over the air. To inhibit eavesdropping, WLANs can encrypt 802.11 data using standards like Wired Equivalent Privacy (WEP), the Temporal Key Integrity Protocol (TKIP), or the Advanced Encryption Standard (AES).

Unfortunately, WEP keys are easily cracked by analyzing captured traffic, letting intruders decrypt all data sent until the key is updated. TKIP and AES provide more robust encryption, particularly when used with 802.1X key delivery. However, 802.11 management and control frames cannot be encrypted, nor can values like ESSID and MAC address. It is therefore important to know what attackers can see and assess the damage they can do with those values.

Users can also be tricked into associating with a phony AP that advertises the ESSID of a hotspot ("tmobile"), home WLAN ("linksys"), or your corporate WLAN. This "Evil Twin" relays user traffic to the Internet or a legitimate AP, leveraging this vantage point to solicit credit card numbers, inject viruses, or intercept data "hidden" by SSL or SSH. These Man-in-the-Middle attacks are not unique to wireless, but promiscuous stations make these attacks easy.

### Unauthorized Network Use

An attacker with your shared WEP key can use your WLAN just like any legitimate user. To close this loophole, the 802.11i Enhanced Security standard adds two more options: PreShared Keys (PSKs) for personal use, and 802.1X for enterprise use.

With PSKs, users must supply a group password before they can reach the upstream (wired) network. Simple PSKs are even easier to crack than WEP keys, so using strong values is crucial. If you need to authorize individual access to selected resources, use 802.1X instead.

802.1X port access control supports many kinds of authentication, including passwords, tokens, and certificates. Vulnerabilities depend upon the Extensible Authentication Protocol (EAP) type carried by 802.1X. For example, Lightweight EAP (LEAP) can be dictionary-attacked to expose passwords that enable network access. Assessing your WLAN's 802.1X vulnerabilities can help you make safer EAP implementation choices.

Most businesses also employ server, domain, and VPN authentication. But WLANs – particularly hotspots – offer ample opportunity to capture or crack

user credentials like email logins, PPTP passwords, and weak IPsec shared secrets. Finding and mitigating these vulnerabilities can help you deter unauthorized use of wireless-connected assets.

### Forged Messages

802.11 uses a Cyclic Redundancy Check to detect transmission errors, but can't stop someone from sending a forged frame with a valid CRC. This leaves WLANs vulnerable to data replay and injection attacks.

TKIP and AES can detect and discard forged 802.11 data by applying a cryptographic Message Integrity Check (MIC). However, there is no standard to prevent modification or insertion of 802.11 management or control frames, or 802.1X/EAP messages exchanged when connections are established. These forged messages are used in many attacks -- especially DoS attacks.

### Denial of Service

Cordless phones, Bluetooth, microwave ovens, and neighbor APs can all interfere with your WLAN's ability to deliver service. Worse, attackers can intentionally flood your WLAN with 802.11 or 802.1X frames to impede legitimate use. A DoS attack can transmit continuously to prevent others from transmitting, flood the air with thousands of bogus AP Beacons, or send forged Deauthenticate or Disassociate frames to prevent other stations from staying connected. You cannot stop outsiders from transmitting, but you can spot and react to such attacks.

Some DoS attacks try to cripple wireless devices. For example, receiving a few bad TKIP data frames can trip an AP's MIC threshold, suspending WLAN service for one minute. A malformed EAP-Identity response can

crash APs which are vulnerable to this EAP-of-Death attack. Wireless devices are often new products that warrant hardening against these and other DoS attacks.

Table 1 (below) summarizes common 802.11 and 802.1X attacks, giving examples of freely available tools used by wireless intruders. As we shall see, many of these tools can be used during an assessment to find your own vulnerabilities -- preferably before they can be exploited by others.

Category	Attack	Example Tools
Authentication Attacks  Steal credentials to penetrate wired network and services	WPA PSK Cracking	Wpa_crack, coWPAtty
	LEAP Cracking	Anwrap, Asleep, LEAPcracker
	Password Capture	Dsniff, WinSniffer
	VPN Login Cracking	ike_crack, pptp_bruter
Access Control Attacks  Circumvent filters and firewalls to obtain unauthorized access	War Driving	NetStumbler, KisMac
	MAC Spoofing	SMAC, Wellenreiter
	Rogue AP Backdoor	Any AP (including HostAP)
	Rogue Ad Hoc	Any Station
Confidentiality Attacks  Intercept sensitive or private data sent over wireless associations	Eavesdropping	Ethereal, Ettercap, BSD-Tools
	WEP Key Cracking	Aircrack, Aircsnort, dwepecrack
	Evil Twin	HostAP, SoftAP
	AP Phishing	Airsnarf, Hotspotter
Integrity Attacks	802.11 Replay	Airpwn, wnet reinject

Modify packets sent over wireless to mislead sender or receiver	802.11 Injection	void11, wnet dinject
	EAP Replay / Injection	Same as above
	DNS Poisoning	Dsniff dnsspoof
Denial-of-Service Attacks  Inhibit or prevent legitimate use of WLAN services	RF Jamming	Alchemy, HyperWRT
	Queensland DoS	Prism Test Utility
	Beacon Flood	FakeAP
	Deauth Flood	Airjack, Omerta
	MIC Exploit	File2air
	EAP-of-Death	libradiate

Table 1: Wireless LAN Attacks and Example Tools

### Putting Attacks Into Perspective: Risk Analysis

Defending your WLAN from attack is best accomplished by using risk analysis to drive security policy definition and implementation. On-going monitoring and periodic testing can then be used to verify that a deployed WLAN meets defined objectives. Any discovered vulnerabilities are (re)analyzed so that policies can be refined and/or fixes can be applied. An iterative process like this (Figure 1) creates a concrete, measurable foundation for effective WLAN threat management.

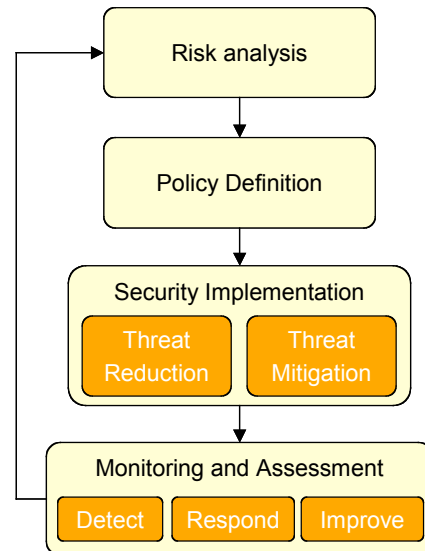


Figure 1:  
Security As A Process

Understanding the attacks that *can* occur is crucial. However, some attacks are less likely or more damaging than others. Furthermore, it is not practical or possible to defend any network against *all* possible attacks.

A more realistic goal is to *reduce* associated risk to an *acceptable level*. Put potential WLAN attacks into perspective by identifying your WLAN's vulnerabilities, the probability that attacker will exploit them, and the business impact should compromise occur. For example:

- Stumblers, MAC spoofing, and WEP crackers all help intruders gain wireless access to upstream networks. Wi-Fi enthusiasts often use these techniques simply to obtain free Internet access. In fact, most users accidentally associate with the wrong AP at some point. The *probability* that wireless service theft will be attempted is thus high. If your WLAN is open or lightly-secured, the *level of difficulty* is low. But what is the *business impact*? Stolen Internet access may be relatively benign --

unless used to launch more-damaging attacks. As a result, many companies ignore war drivers and low-grade reconnaissance activities, focusing instead on rogues that actually attempt to penetrate the corporate network.

- An Evil Twin attack requires more interest and persistence than cleartext data capture. On the other hand, most users are very willing to connect to unknown APs, and business traffic at hotspots represents a lucrative target. One might therefore rank Evil Twin attack as medium difficulty and probability. Consumers can take some comfort from credit card liability limits, but businesses must take steps to protect company assets from Evil Twins -- for example, by requiring VPN tunnels at hotspots and mutual 802.1X authentication at the workplace.
- Point-and-click 802.11 injection tools make wireless DoS attacks trivial, but what are the odds that one will be aimed at your WLAN? That depends on what the attacker gains; this may in turn be related to business impact. Taking a conference room AP offline may result in little gain or harm, but disabling a wireless surveillance camera could have direct benefit for the attacker, and serious consequences for the owner. This simple example demonstrates why companies should spend more securing and monitoring their highest-priority WLAN assets.

To perform a wireless risk analysis, start by defining your business needs. Ultimately, security is not just about keeping intruders out – it's about letting legitimate users reach authorized services. Document who needs WLAN access, where. Identify users or groups permitted to use wireless at the office, on the road, and at home. Determine resources to be accessed over wireless, like destinations on the Internet or servers and segments inside your company Intranet. Which application protocols, ports, databases, and shares must be opened to wireless users, and when?

Next, quantify new business risks caused by adding wireless access to your network. List the assets that you will be putting in harm's way, including devices on wireless and upstream wired networks. What information do those services and databases contain? Also consider data that resides on wireless stations and flows over wireless links – this is also an asset to be protected. For each asset, estimate the likelihood of compromise and potential cost to your business, using quantifiable metrics like downtime, cost of recovery, legal liability, etc..

When this process is complete, you will have a prioritized list of at-risk assets. Use this foundation to write a security policy that defends your assets from wireless-borne attack, balancing cost/benefit and residual risk. Then select, install, and configure counter-measures that implement and enforce your security policy. Finally, test your secure WLAN implementation to verify policy compliance and identify remaining vulnerabilities.

### Conducting A Vulnerability Assessment

A vulnerability assessment is a systematic evaluation that uses penetration testing and monitoring to identify security weaknesses that could be exploited, and the consequences of doing so (e.g., attack tools that run successfully, information they can obtain, systems they can compromise). These results must be reviewed to determine severity and identify steps that reduce or eliminate threats -- for example, update AP software, reconfigure a WLAN client, add a firewall.

To be truly effective, assessments should be repeated. For example, conduct an assessment before and after WLAN deployment so that you can spot vulnerabilities introduced by wireless and verify that newly-installed security measures are working as intended. Also conduct assessments after

significant network or policy changes are made, and at regular intervals, to prevent vulnerabilities from creeping into your WLAN over time.

Assessments may be performed by in-house or third-party staff, starting with full, partial, or zero knowledge of your network and security implementation. Most companies use in-house staff to find and fix well-known vulnerabilities, then tap outside expertise to spot unforeseen problems. All assessments should be conducted with consent of the network owner, considering potential impact on business activities and network resources. For example, you may wish to conduct DoS testing off-hours, but monitor WLAN activity 24/7 during the entire assessment period.

If you are responsible for conducting a WLAN vulnerability assessment, start by defining objectives, methodology, and expected outputs. Tests vary, depending upon available tools, the topology of the network being assessed, that network's security policy, etc.. However, it is critical that the methods used, the tests run, and all results be documented to enable fix verification and consistent evaluation of the entire network.

Begin with a prototype assessment on a few WLAN resources, refining your methods and outputs until you are comfortable applying them on a larger scale. Use prototype results to revisit your objectives -- are you exercising the policy you intended to verify, or providing answers to the questions originally posed? This up-front "sanity check" can avoid wasting time on unnecessary or inappropriate tests, or return site visits for test repetition to collect missing results.

The following sections discuss techniques and tools that can be useful when conducting a WLAN vulnerability assessment, from wireless device discovery and penetration testing, to security event monitoring and spectrum analysis. A sample worksheet, provided in Appendix A, illustrates how assessment results can be documented for review and remediation.

### Using Portable Tools for WLAN Discovery

The first step in any vulnerability assessment is to identify all wireless devices near the site(s) under test. Authorized devices will be subjected to further assessment; the rest will be scrutinized to determine ownership and threat. Discovery is part of the site survey conducted when planning a new WLAN, but the information needed for risk analysis is a subset of that required for RF network design. Here, we describe WLAN discovery for security purposes only.

War drivers and IT staff often use Stumblers for WLAN discovery. These tools are free, easy to use for simple tasks, and available for most OS's, including handhelds. But they are also limited. Most Stumblers can find APs, but not Stations. Many interface with GPS, but latitude/longitude is not that useful indoors. Stumblers are handy for ad hoc AP discovery, but a complete vulnerability assessment requires a portable WLAN Analyzer that can scan *all* RF channels, export details about *all* wireless devices, and help you easily notice and locate unknown devices.

To discover wireless devices, work from a floorplan to methodically scan at intervals, covering the entire site, inside and out, above and below. Scan all channels, in both RF bands, repeating the survey at least twice, at different times of day. Generate a list of discovered APs, noting ESSID, MAC address, IP address, channel, SNR, and observed 802.11/802.1X security protocols. Generate a similar list of discovered Stations, noting whether

they are associated to an Ad Hoc node, probing for multiple ESSIDs, and/or actively associated with specific AP(s).

Next, use the site's WLAN inventory (if one already exists) to isolate previously unknown devices. For efficiency, you may wish to list but otherwise ignore APs with weak SNR (distant neighbors) or transient unassociated Stations (guests). For the rest, use a "find" tool (or a WIPS with rogue mapping) to locate each device and identify the equipment and owner. Finding all stations may not be practical, but continue until you have found all APs above a defined SNR.

Save scan results, using your assessment worksheet to consolidate what you have learned thus far. Discovery output is the foundation for penetration testing, inventory update, and Access Control Lists. For example, configure your WLAN Analyzer with meaningful names and categorize devices to easily differentiate between neighbors, rogues, and known authorized devices.

### Using Penetration Tests to find Vulnerabilities

Intruders use wireless, TCP/IP, and server attack tools to compromise your WLAN. Fight fire with fire by using these tools to "penetration test" your own wireless devices and network infrastructure. Aiming simulated attacks at your WLAN determines whether intruders could successfully exploit common vulnerabilities, and helps you understand immediate consequences (e.g., visible data, networks breached, systems crashed).

Network-borne attacks usually scan devices and ports, using tools like Nmap or Superscan. Devices that appear to be active are "fingerprinted" to identify

operating systems, server programs, accounts, and shares, using tools like Winfingerprint and Xprobe. A Common Vulnerabilities and Exposures (CVE) database is then consulted for flaws in the target's software and tools that can exploit them. During a WLAN assessment, aim these tools at your wireless gateways/switches, APs, hosts, and other systems exposed to wireless, like DHCP and DNS servers. Run tests while associated to different APs to spot subnet-specific vulnerabilities. If your WLAN uses VPN or portal authentication, run tests both before and after authentication.

Intruders exploit active APs and open ports to connect to your network and services. Management ports (Telnet, SSH, SNMP, TFTP) may be probed, using default logins. WEP traffic may be analyzed with AirSnort or WEPcrack. In WLANs using WPA-PSK, authentication messages may be analyzed with coWPAtty or wpa\_crack. In WLANs using 802.1X, EAP IDs may be recorded for each station. For password-based EAPs, cracking may be attempted. During an assessment, use these tests to identify weak controls and credentials for every device/port and ESSID. To test off-hours, you may need to generate traffic. Because WEP cracking depends on weak IVs, time-to-crack can vary, and you should note which devices generate them.

Intruders may also aim 802.11, 802.1X, and TCP/IP DoS tools at devices on your WLAN. An assessment should exercise your DoS defenses, including configurable thresholds on wireless gateways, switches, and firewalls, and Wireless Intrusion Prevention System coverage. For example, go systematically from floor to floor, flooding a test target with Deauthenticate frames long enough to reliably find sensor coverage holes. Flood every AP model/version in your WLAN with several 802.11 and 802.1X messages to spot product-specific DoS vulnerabilities. Aim TCP, UDP, and ICMP floods at your WLAN gateway/firewall to find the rate at which failure (if

any) occurs. Because DoS testing is disruptive -- and potentially destructive -- exercise caution about which tests you run, when, and where.

Finally, run your own Evil Twin AP to assess how wireless stations react and evaluate the effectiveness of deployed countermeasures. For example, try various ESSIDs to lure stations that are vulnerable to Hotspotter attack. Run password capture tools on the Evil Twin to identify application credentials that are easily intercepted/cracked. If your WIPS is configured to auto-block rogue APs, verify that your Evil Twin is effectively contained in this manner.

Pen-test tools like these can be downloaded from websites or run from a bootable CD like the Auditor Security Collection. Use pen-test results to flesh out your assessment worksheet, highlighting attacks that were easy, missed by sensors, or had major impact. Include observations that may be helpful when determining recommended fixes (e.g., visible RF obstructions).

### Using WIPS to Monitor Attacks

WLAN discovery and pen-tests find vulnerabilities, but do not tell us if those vulnerabilities have been exploited. Portable WLAN Analyzers can "spot check" wireless activity in one location -- in fact, running an analyzer next to your pen-test system can be helpful to eyeball simulated attacks. But for full-time monitoring of your entire WLAN, devices therein, and actual user traffic, use a Wireless Intrusion Prevention System (WIPS).

Like wired network IPS, a wireless IPS uses traffic analysis to watch for attack signatures, protocol errors, atypical behavior, and policy violations, generating alerts and defensive actions. But WIPS sensors listen to the air,

decoding 802.11 and 802.1X protocols. WIPS servers understand wireless attacks and can enforce wireless security policies -- for example, automatically deauthenticating rogue devices. Intrusion alerts are recorded to a central database to enable historical reporting, accessible from any WIPS console.

Although not its primary goal, a WIPS can be extremely helpful during a WLAN vulnerability assessment. A WIPS can help "fill in the blanks" during WLAN discovery -- a full-time monitor will hear more than ad hoc sampling. By combining observations from multiple sensors, a WIPS can triangulate a discovered device's location on a floorplan to make searches more efficient. By generating policy-based alerts, a WIPS can help you spot misconfigured devices, actual attacks that may have occurred recently, problem-prone locations and devices that may warrant additional scrutiny, and on-going risky user behavior.

Finally, during pen-testing, a WIPS can confirm that tests are working as expected. They can teach you how to recognize signs of attack. They can even suggest how to mitigate them. In return, pen-test results may help you decide how to fine-tune your WIPS; for example, adjusting sensor placement, channel scan settings, DoS thresholds, and alert policies.

### Using Wireless Analyzers for Investigation

The broad insights delivered by WIPS can be complemented by drill-down investigation, using WLAN traffic and spectrum analyzers. These portable tools are instrumental during vulnerability assessment, from start to finish. They provide a mobile platform for WLAN discovery, an as-needed vehicle for traffic capture, and a "wireless dashboard" for viewing pen-test effects. In addition, analyzers help you dig deeper to investigate potential vulnerabilities.

For example, suppose that a WIPS report identifies an AP that seems to be experiencing frequent DoS attacks. When testing that site, you use a WLAN traffic analyzer to capture and decode live 802.11 packets near that AP. By examining channel utilization, you determine the "DoS attack" looks like RF interference. You then use a WLAN spectrum analyzer to identify the non-802.11 culprit (e.g., microwave oven) and pinpoint that device's location.

Alternatively, if the attack is carried by 802.11 packets, you apply a filter to focus on suspicious traffic -- for example, watching all 802.11 management packets with a given SSID. If the source appears to be a competing AP, you try to associate with it and trace network connectivity. If the source is an intruder station, you track attempts to associate with your APs.

In other words, leverage the tools in your toolbox to learn what you can about the intrusion. A live attack source may be long gone by the time your assessment report is reviewed, but the information learned can be put to good use: understanding how attacks progress and the vulnerabilities they exploit can be just as important as knowing that they happened.

### Putting Assessment Results To Work

Wireless vulnerability assessments are a means to an end. To reduce business risk, results must be applied to eliminate vulnerabilities through station and AP hardening, rogue detection and elimination, and deployment of 802.11/802.1X security measures. To facilitate this, assessment reports may rank identified vulnerabilities by severity and recommend countermeasures.

**Rogue Management:** Most vulnerability assessments find at least some previously-unknown wireless devices. Assessment results enumerate discovered devices ("rogues") and observed properties to enable threat assessment, classification, and elimination. For example, a report might recommend classifying low-SNR APs as Neighbors so that ACLs be used to block unauthorized associations. It may recommend that high-SNR APs connected without permission to the corporate network be physically removed, using location information in the report.

Proactive measures can also be recommended to prevent rogue damage in the future. For example, suspicious stations may be added to a WIPS "watch list" to escalate any future alerts pertaining to them. Automated actions may be configured for malicious rogues that lie off-premises but within RF range, like network connectivity checks and temporary wireless blocking. After such measures are deployed, repeat assessments can be used to verify their effectiveness.

**WLAN Infrastructure Hardening:** APs, switches, gateways, web portals, DNS/DHCP servers, and other devices connected to WLANs often require hardening to resist network-borne attacks. Pen-test results may be accompanied by recommended countermeasures, like changing AP defaults, disabling unnecessary services, using stronger admin passwords or authentication methods, disabling wireless-side management and restricting wired-side to specific IP addresses and/or VLANs, adding AP filters to prevent route updates or LAN broadcasts from being relayed onto the wired network, tuning anti-DoS thresholds, and upgrading device firmware/patches to fix CVEs. It may not be possible to eliminate all discovered vulnerabilities and meet business needs, but applied fixes should be verified through repeat testing until residual risk is acceptable.

**Station Hardening:** Wireless-enabled desktops, laptops, PDAs, handheld scanners, VoWiFi phones, and field terminals also require hardening. Countermeasures and best practices typically used to defend Internet-connected hosts, like personal firewalls, are generally recommended for WLAN hosts. Pen-test results may also identify WLAN-specific vulnerabilities that warrant further recommendations, like configuring WLAN clients to accept only Infrastructure associations, from company-specified ESSIDs, using company-mandated 802.1X credentials. Finally, recommend that any wireless NIC sending weak IVs be upgraded or retired. If Evil Twin associations or unsafe user behavior is seen, recommend user education and surveillance.

**Securing Data In Transit:** Assessments verify compliance with the WLAN's defined security policy and identify weaknesses in that policy. For example, if policy mandates WEP on employee WLANs, test results should enumerate those stations/APs willing to associate without WEP. The mean time required to crack WEP keys and sensitive data captured/decrypted with those keys may also be documented to support risk analysis. If risk is too high, WEP keys may be rotated more often, 802.1X may be adopted to deliver keys, or the WLAN may be migrated to TKIP or AES or VPN tunneling. An assessment report may recommend data security alternatives to reduce vulnerabilities, and also measures to detect and prevent future policy violations.

**Controlling Network Use:** Finally, assessments exercise the WLAN's Access Control and Authentication mechanisms to determine whether and where and how breach can occur. Results may enumerate visible user identities and crackable credentials that should be strengthened. They may demonstrate unexpected consequences of compromise -- for example, other systems that can be accessed with cracked user credentials, or products with authentication-related CVEs. Here again, recommendations can be made to

---

mitigate vulnerabilities, based on the WLAN's defined security policy. For example, if policy mandates WPA-PSK, test results should enumerate ESSIDs with weak PSKs, recommending replacement with random values longer than 20 characters, or perhaps 802.1X. Tests should be repeated to verify changes and detect introduction of new vulnerabilities -- this is particularly true when upgrading to a relatively complex solution like 802.1X or adds a new EAP Type.

### How AirMagnet Can Help

AirMagnet provides a comprehensive tool suite that supports WLAN Vulnerability assessment. From site surveys and spectrum analysis to security monitoring and traffic analysis, AirMagnet products can help you conduct efficient, effective assessments to manage wireless risk.

**AirMagnet Surveyor** supports WLAN planning, simulation, verification, and optimization, delivering results that make it easy to visualize your network and RF behavior in meaningful terms. Surveyor provides a solid foundation for mapping the location of wireless devices discovered during site surveys, sharing this data easily with other AirMagnet products.

**AirMagnet Spectrum Analyzer** proactively identifies, classifies, and graphs sources of RF interference in all 802.11 bands. It can detect devices that are adversely impacting your WLAN in real time, including Bluetooth, cordless phones, microwave ovens and video cameras, pinpointing their location to speed investigation and elimination.



Figure 3: AirMagnet Spectrum Analyzer

**AirMagnet Laptop and Handheld Analyzers** are portable platforms for WLAN traffic observation, capture, and analysis. They provide an extensive set of 802.11 monitoring and diagnostic tools to spot-check activity, security policy compliance, connection problems, and conduct site surveys. They can record discovered device data, exporting ACLs for use by AirMagnet Enterprise and third-party systems. They can scan 802.11a/b/g channels, filtering and decoding traffic, using expert analysis to identify attacks and weak configurations. Using an AirMagnet Analyzer, you can track down wireless devices and associate with specific APs to check connectivity and run targeted penetration tests.

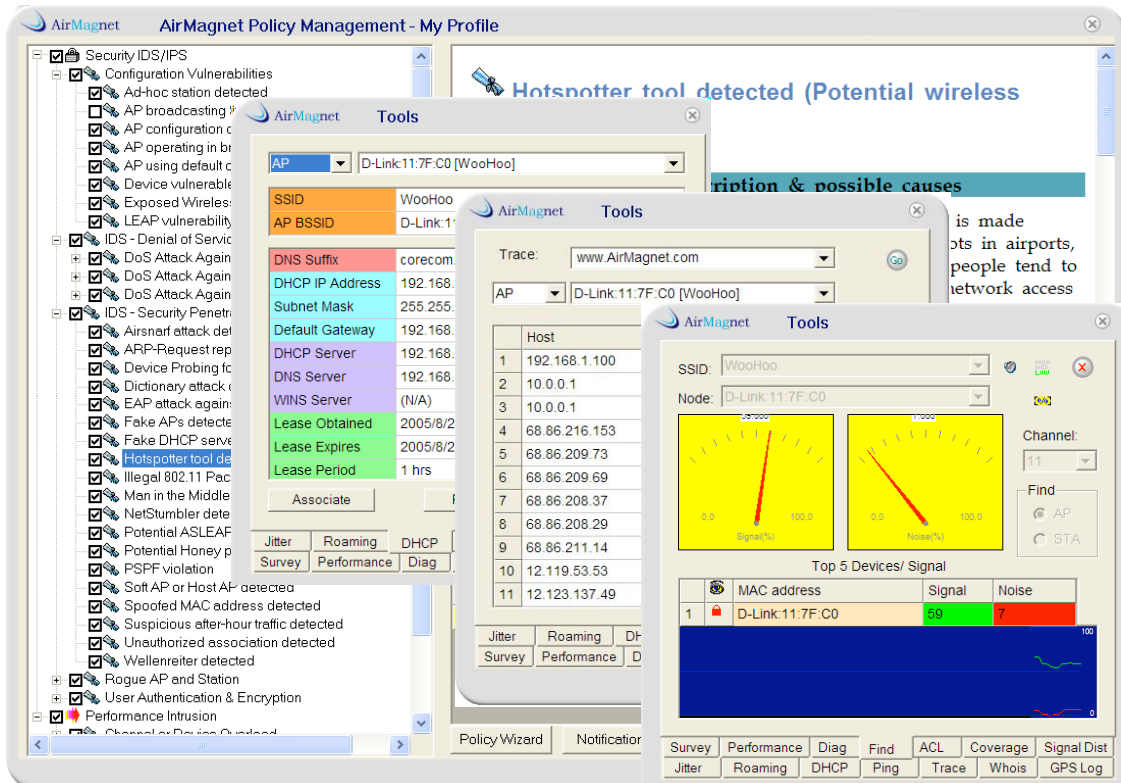


Figure 4: AirMagnet Laptop Analyzer

**AirMagnet Enterprise** delivers robust, scalable 24/7 wireless intrusion detection and prevention. By combining distributed sensors with a central server engine, Enterprise can spot well over one hundred wireless security, performance, and operational problems, and automatically defend the network in real-time as threats arise. Pre-configured, customizable policies simplify analysis of violations in terms of location, time, hardware, and policy type. When a potential attack or weak configuration is found, Enterprise can launch active wired and wireless traces to determine whether the affected device is attached to the network, and map its approximate location.

**About AirMagnet**

Founded in 2001, AirMagnet, Inc. provides the most trusted WLAN management and security software systems in handheld, laptop and enterprise configurations. Used by IT professionals at more than 4,000 companies worldwide—including 66 of the Fortune 100—in manufacturing, financial, retail, service, health care, utility, transportation, education and government sectors, AirMagnet solves Wi-Fi connection problems, tracks down unauthorized access, simplifies site surveys, and locks in unprecedented levels of network performance, security and reliability. Additional information about AirMagnet and its products is available at [www.AirMagnet.com](http://www.AirMagnet.com).

**Appendix A: Example Worksheet**

The following worksheet illustrates how results gathered during a vulnerability assessment can be recorded. Just as there is no "one size fits all" testing process, there is no standard documentation to record these results. Use this example to create your own worksheet that reflects what you plan to test and monitor during your own vulnerability assessment. We highly recommend taking your worksheet on a "test drive" to ensure that documented results are complete and meet your assessment objectives.

Test Date	
Tester MAC(s)	
Tester Adapter(s)	

### Intended / Deployed WLAN Characteristics

AP Type	Number	Station Type	Number	Other	Number	Assigned ESSIDs
802.11b		802.11b		Bridges		Employee Intranet =
802.11g		802.11g		Ad Hoc Peers		Guest Intranet =
802.11,bg		802.11bg				Other =
802.11a		802.11a				

### Site Survey Floorplan and Locations

1.	Insert Floorplan Here  Mark Testing Locations on Floorplan  Describe Testing Locations at left
2.	
3.	
4.	
5.	

### AP Inventory

AP MAC	ESSID	Channel	IP Address	SNR	Owner	Location	Classification
: : : : :							
: : : : :							
: : : : :							

AP MAC	SSID Beaconed	802.11 Auth	802.11 Encrypt	WPA PSK	802.1X	EAP Types	Other
: : : : :							
: : : : :							
: : : : :							

### Station Inventory

STA MAC	Last ESSID	Last Channel	SNR	Owner	Location	Adapter	Classification
: : : : :							
: : : : :							
: : : : :							

## WLAN Vulnerability Assessment

STA MAC	Assoc ESSIDs	802.11 Auth	802.11 Encrypt	WPA PSK	802.1X	EAP Types	EAP User ID
: : : : :							
: : : : :							
: : : : :							

### Network Scan Results: Discovered Devices (complete for each WLAN subnet)

Role	MAC Address	IP Address	Owner	Notes
WLAN Gateway	: : : : :			
DHCP Server	: : : : :			
DNS Server	: : : : :			
RADIUS Server	: : : : :			
Access Points	: : : : :			
Stations	: : : : :			
Other	: : : : :			

**AP Test Results (complete for each tested AP)**

AP MAC	: : : : :	AP IP Address	
Operating System		Discovered Version	
Open TCP Ports		Service Banners Returned	
Open UDP Ports		Service Banners Returned	
SNMP Admin Used?		SNMP Community Strings	
Telnet Admin Used?		Telnet Login / Password	
Web Admin Used?		Web Login / Password	
Blocks Broadcasts?		Blocks Station-to-Station?	
Blocks WLAN SNMP?		Blocks WLAN Routing?	
Accepts Spoofed ARP?		Physically Secured?	
Encryption Off?		Observed Encryption Types	
WEP Weak IVs?		Cracked WEP Keys	
MAC ACL Used?		Valid Station MACs	
PSK Guessable?		Cracked PSK	
802.1x Required?		Observed EAP Types	
AP DoS Test Results			

### Station Test Results (complete for each tested Station)

Station MAC	: : : : :	Static IP Address?	
Operating System		Discovered Version	
Open TCP Ports		Service Banners Returned	
Open UDP Ports		Service Banners Returned	
NetBIOS Name		NetBIOS Shares	
NetBIOS Service List		NetBIOS User/Group List	
Assoc with ANY AP?		Assoc with Ad Hoc Peer?	
Encryption Off?		Observed Encryption Types	
WEP Weak IVs?		PSK Guessable?	
802.1x Used?		Observed EAP Types	
802.1x IDs Exposed?		Observed 802.1x User ID	
LEAP Used?		Cracked User Password	
Applications Protocols		Observed Servers & Logins	

### WLAN Infrastructure Test Results (complete for each tested gateway/switch/server)

Device MAC	: : : : :	Device IP Address	
Operating System		Discovered Version	
Open TCP Ports		Service Banners Returned	
Open UDP Ports		Service Banners Returned	
SNMP Admin Used?		SNMP Community Strings	
Telnet Admin Used?		Telnet Login / Password	
Web Admin Used?		Web Login / Password	
Accepts Spoofed ARP?		Physically Secured?	
Uses RADIUS Server?		RADIUS Test Results	
Acts as DNS Server?		DNS Test Results	
Acts as DHCP Server?		DHCP Test Results	
Acts as VPN Gateway?		VPN Test Results	
Acts as Web Portal?		Web Server Test Results	

### Detected Attacks and Anomalies

Type of Event	Source MAC/IPs	Destination MAC/IPs	Time	Location	Observations and Details
<b>Network DoS Attacks</b>  - CTS Flood  - Queensland DoS  - RF Jamming  - Spectrum Interference					
<b>AP DoS Attacks</b>  - 802.11 Association Flood  - 802.11 Authenticate Flood  - 802.11 MIC DoS Attack  - 802.1X EAP Start Flood  - 802.1X EAP of Death					
<b>Station DoS Attacks</b>  - 802.11 Deauthenticate Flood  - 802.11 Disassociate Flood					

<b>Type of Event</b>	<b>Source MAC/IPs</b>	<b>Destination MAC/IPs</b>	<b>Time</b>	<b>Location</b>	<b>Observations and Details</b>
<ul style="list-style-type: none"> <li>- 802.1X EAP Failure</li> <li>- 802.1X EAP Logoff Flood</li> </ul>					
<b>Reconnaissance Activities</b> <ul style="list-style-type: none"> <li>- NetStumbler</li> <li>- Wellenreiter</li> <li>- MAC Address Spoofing</li> </ul>					
<b>Evil Twin Activities</b> <ul style="list-style-type: none"> <li>- Fake DHCP Server</li> <li>- Hotspotter</li> <li>- Honeypot AP</li> <li>- SoftAP or HostAP</li> <li>- AP in Bridged Mode</li> </ul>					
<b>MitM Attacks</b> <ul style="list-style-type: none"> <li>- AirSnarf</li> <li>- ARP Replay</li> </ul>					

<b>Type of Event</b>	<b>Source MAC/IPs</b>	<b>Destination MAC/IPs</b>	<b>Time</b>	<b>Location</b>	<b>Observations and Details</b>
<b>Spoofing / Cracking</b>  - MAC Spoofing  - ASLEAP Attack  - EAP Dictionary Attack  - EAP Type Attack					

This table summarizes Wireless IPS and WLAN analyzer security alerts corresponding to attacks and anomalies observed during the assessment period. Note: deviations from defined security policy and rogue devices should be recorded in the AP or Station List.