



Wireless Vulnerability Assessment

For: ABC

From: Apr 17, 2008 12:55 PM

To: Apr 17, 2008 4:55 PM

Location: \\ABC Corp

A Report by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043

www.airtightnetworks.net



Table of Contents






About This Report	3
Result Summary	4
Recommended Actions	6
Detailed Results	8
Critical Vulnerabilities.....	8
High Severity Vulnerabilities.....	10
Medium Severity Vulnerabilities.....	11
Low Severity Vulnerabilities.....	13
Probable Vulnerabilities.....	14
Appendix A: Categorized List of Access Points	16
Appendix B: Categorized List of Clients	17
Appendix C: List of Wireless Scanners	19
Appendix D: Severity of Vulnerabilities	20

About This Report

This report is an assessment of your network's wireless security posture. It lists the number and type of wireless devices detected in your environment, records the presence of vulnerabilities and threats they pose to your network. The report contains: (1) *Summary of Results*, (2) *Detailed Results* for all vulnerabilities that were detected, and (3) Recommended Actions that you need to take for remediation and for improving your network's security posture.

The results are based on your airspace scanned using AirTight Networks' preconfigured wireless scanners. Wireless vulnerability assessment is done by comparing the scanned data with an up-to-date vulnerability database maintained by AirTight Networks. The Common Vulnerability Scoring System (CVSS) standard has been adapted to assess wireless vulnerabilities.

The table below classifies vulnerabilities based on their severity levels. A detailed description of each severity level follows.





Severity level	Type	Description
 5	Critical	Security breach or wireless malpractice detected! An intruder may have entered your network; sensitive data is exposed; or your users are bypassing your security policy control (e.g., firewalls, and URL, spam, and malware filters).
 4	High	Known vulnerabilities those ignore basic security measures and naturally expose your network and data assets even to inadvertent unauthorized access.
 3	Medium	Vulnerabilities that violate best practices and can lead to unauthorized usage of your network resources or hackers with medium expertise and knowledge of published exploits can exploit these vulnerabilities in minutes.
 2	Low	Hackers can collect information about your network and may use it to discover other vulnerabilities; high expertise needed to exploit these vulnerabilities.
 1	Probable	Potential vulnerabilities that may pose a threat.

NOTE:

You should not ignore vulnerabilities with severity levels 3, 4, and 5 in your airspace. Compliance to legislative regulations may require you to also address severity level 2 vulnerabilities. We highly recommend that appropriate remedial action be taken to protect your network and data assets against these threats.

Result Summary

Vulnerabilities Total: 19 **Overall Security Risk:**  **5** **Status:** Critical

Severity Level	Count of Vulnerabilities
 5	5
 4	4
 3	8
 2	2

Wireless Scanners Summary

Total number of wireless scanners: 2

Approximate area scanned for wireless vulnerabilities: 40000 sq. ft

Add more scanners for covering additional airspace if necessary.

Wireless Devices Summary

Total number of access points (APs) detected: 17

Total number of clients detected: 45

NOTE: A detailed list of all detected wireless devices is shown in the Appendices.

Categorized Vulnerabilities Summary

Severity Level:  **5** **Type:** Critical **Vulnerabilities:** 5

Vulnerabilities	Count
Non-authorized Client Connections	1
Misbehaving Clients	1
Ad-hoc Network	2
Mac Spoofing	1

Severity Level:  **4** **Type:** High **Vulnerabilities:** 4

Vulnerabilities	Count
Ad-hoc Mode	2
Rogue AP	2

Severity Level:  **3** **Type:** Medium **Vulnerabilities:** 8

Vulnerabilities	Count
Potential Victim of Wi-Phishing Attack	4
Open External AP	3
WEP Authorized AP	1

Severity Level:  **2** **Type:** Low **Vulnerabilities:** 2

Vulnerabilities	Count
Policy Compliant Rogue AP	2

Severity Level:  **1** **Type:** Probable **Vulnerabilities:** 0

Vulnerabilities with Severity Level 1 were not found.

Recommended Actions

Wireless vulnerability assessment is an iterative process. It is important to review your network's wireless security posture periodically due to the inherently dynamic and sudden nature of wireless vulnerabilities. Wireless vulnerabilities occur as:

- New wireless devices are added to your airspace
- Configuration of devices changes
- New vulnerabilities are discovered
- New exploits and hacking tools are developed

Usually, when companies first subscribe to wireless vulnerability assessment, they cycle through the process several times to accurately identify wireless vulnerabilities, remediate those vulnerabilities, and see their network's security posture improve. This cycle of frequent assessment is recommended until your network has unacknowledged or unaddressed vulnerabilities with severity level 3, 4, or 5.

After that, wireless vulnerability assessment can be scheduled periodically (e.g., monthly or quarterly) to maintain a good wireless security posture.

Refer to the Detailed Results section to learn about remedial actions corresponding to specific wireless vulnerabilities in your network. Remedial actions can be broadly classified into:


- **Manual:** These solutions require human intervention, e.g., changing device configuration, upgrading the firmware.
- **Automatic:** These solutions lessen the burden on the system administrators by providing 24x7 monitoring, intrusion detection and prevention capabilities, e.g., using software on wireless clients to manage how they behave and connect, wireless network security solutions that detect and automatically block anomalous activities or attacks.



Detailed Results

Detailed Results

Severity 5 Vulnerabilities

Severity Level:  5 Type: Critical Vulnerabilities: 5

Unauthorized Client Connections

Count: 1

Threat: An unauthorized client connecting to your authorized AP indicates a potential malicious attempt to break into your corporate network by wireless access.

Remediation: Manually check if the SSID of APs on your network is not the same as the one used on your neighbors' networks. Also, configure and enforce an authentication policy between authorized APs and authorized clients.

For automatically blocking any unauthorized connections to your network, consider using a wireless security solution.

Device(s) Involved:

Location	Device Name	MAC Address	Protocol	SSID	Security
ABC Corp	Buffalo_2B:0C:1B	00:0D:0B:2B:0C:1B	802.11b/g	Elektra	WEP

Misbehaving Clients

Count: 1

Threat: Authorized clients that associate with an external or a threat posing AP (e.g., rogue AP) are likely bypassing your firewalls and content (URL, malware, spam) filter policies. Such misbehaving clients can lead to reduced productivity, liability for illegal content flowing through your network, or leak sensitive data.

Remediation: Check the wireless settings on your authorized clients and ensure they are configured to connect only to your authorized SSID. A wireless client management software can help in enforcing your security policies and regulating how your clients connect wirelessly.

If you do not want to touch your clients, consider using a wireless security solution for automatically blocking authorized clients from connecting to external or threat-posing APs

Device(s) Involved:

Location	Device Name	MAC Address
ABC Corp	Intel_25:B8:48	00:13:CE:25:B8:48

Ad-hoc Network

Count: 2

Threat: Authorized clients directly connecting to unauthorized clients is a major security threat; such connections open a backdoor to your network and your authorized devices may be infected with viral SSIDs.

Ad-hoc connections even between authorized clients should be discouraged as these connections can bypass your corporate security policies.

Remediation: You should locate the clients and before redeploying them, manually change the configuration of your clients to prevent them from participating in ad-hoc networks.

A wireless security solution can be used to locate ad-hoc networks on your premises and automatically block authorized clients from participating in ad-hoc networks.

Consider using a wireless client management software for enforcing your security policies and controlling networks to which your clients can connect.

Device(s) Involved:

Location	Device Name	MAC Address
ABC Corp	Cisco-Linksys_78:FF:D2	00:12:17:78:FF:D2
ABC Corp	Intel_25:B8:48	00:13:CE:25:B8:48

Mac Spoofing

Count: 1

Threat: Detection of MAC spoofing indicates that a hacker has knowledge about the MAC addresses of your authorized devices and is using it maliciously. Your network security is potentially breached or prone to a denial-of-service attack.

Remediation: Use wireless security solutions for automatically blocking malicious devices that can use spoofed MAC addresses to enter your network or launch other attacks.

Device(s) Involved:

Event Location	Date And Time	Event Details
ABC Corp	Apr 28, 2008 3:52 PM	Client RF signature anomaly detected for Client [Intel_25:B8:48]

Severity 4 Vulnerabilities

Severity Level:  4

Type: High

Vulnerabilities: 4

Ad-hoc Mode

Count: 2

Threat: Authorized clients in ad hoc connection mode are likely infected with viral SSIDs and can inadvertently compromise your entire network's security by accepting direct connections. Unauthorized clients can enter your network through such connections, while authorized clients can bypass your security policy control (e.g., firewalls, and URL, spam, and malware filters).

Remediation: You should locate the clients and before redeploying them, manually change the configuration of your clients to prevent them from operating in ad-hoc mode.

Consider using a wireless client management software for enforcing your security policies and ensuring that clients only connect in the infrastructure mode to authorized APs.

Device(s) Involved:

Location	Device Name	MAC Address
ABC Corp	Cisco-Linksys_01:4C:18	00:18:39:01:4C:18
ABC Corp	Intel_25:B8:48	00:13:CE:25:B8:48

Rogue AP

Count: 2

Threat: Rogue APs are unauthorized APs connected to your corporate network in violation of your security policies. Outsiders can enter the corporate network using these Rogue APs as wireless backdoors.

Remediation: Use wireless security solutions for automatically blocking wireless access to Rogue APs. Locate the Rogue AP and physically disconnect it from your corporate network.

Device(s) Involved:

Location	MAC Address	Protocol	SSID	Security
ABC Corp	00:09:5B:FD:73:30	802.11b/g	Alice	WEP
ABC Corp	00:11:95:18:1A:AF	802.11b/g	Malice	Open

Severity 3 Vulnerabilities

Severity Level:  3

Type: Medium

Vulnerabilities: 8

Potential Victim of Wi-Phishing Attack

Count: 4

Threat: In Wi-Phishing, hackers use common or factory-default SSIDs to lure clients to unwittingly connect to their AP instead of the authorized WLAN. Clients probing for these common SSIDs are prime candidates for a Wi-Phishing attack.

Remediation: Locate the client and remove entries of vulnerable SSIDs from the client's preferred networks list, so it does not probe for those networks. A wireless client management software can help in enforcing your security policies and regulating how your clients behave and connect wirelessly.

Device(s) Involved:

Location	Device Name	MAC Address
ABC Corp	Cisco-Linksys_01:4C:18	00:18:39:01:4C:18
ABC Corp	Intel_25:B8:48	00:13:CE:25:B8:48
ABC Corp	Intel_2B:EC:05	00:13:02:2B:EC:05
ABC Corp	Intel_92:0B:A6	00:19:D2:92:0B:A6

Open External AP

Count: 3

Threat: External APs are not connected to your corporate network, but are in the wireless vicinity of your facility. Your authorized client devices are likely to connect to open external APs bypassing your security policy control (e.g., firewalls, and URL, spam and malware filters). This in turn can lead to reduced productivity, liability for illegal content flowing through your network, or leak sensitive data.

Remediation: Check the wireless settings on your authorized clients and ensure they are configured to connect only to your authorized SSID. A wireless client management software can help in enforcing your security policies and regulating how your clients connect wirelessly.

If you do not want to touch your clients, consider using a wireless security solution for automatically blocking authorized clients from connecting to external APs.

Device(s) Involved:

Location	MAC Address	Protocol	SSID
ABC Corp	00:15:E9:61:63:CA	802.11b/g	Carib4
ABC Corp	00:19:5B:8C:A8:0C	802.11b/g	Load-Guest
ABC Corp	00:1E:58:23:BF:27	802.11b/g	blueguest

WEP Authorized AP

Count: 1

Threat: It is well known that the Wired Equivalent Privacy (WEP) encryption is broken and can be easily exploited to steal sensitive data and possibly to enter your network.

Remediation: Upgrade the encryption capabilities of all your WiFi APs and clients to use strong encryption like WPA2 and protect your WiFi traffic from eavesdropping. At least upgrade the devices using WEP to filter out weak IVs.

Device(s) Involved:

Location	Device Name	MAC Address	Protocol	SSID
ABC Corp	Buffalo_2B:0C:1B	00:0D:0B: 2B:0C:1B	802.11b/g	Elektra

Severity 2 Vulnerabilities

Severity Level:  2

Type: Low

Vulnerabilities: 2

Policy Compliant Rogue AP

Count: 2

Threat: A rogue AP on the network is masquerading as an authorized AP with policy compliant settings. If this is in fact an authorized AP, then move it manually to the "Authorized AP" folder.

Remediation: Locate the rogue AP and physically disconnect it from your network if it is indeed a rogue AP. If it is an authorized AP, then manually classify it as authorized to mitigate this alert.

Device(s) Involved:

Event Location	Date And Time	Event Details
ABC Corp	Apr 28, 2008 1:01 PM	New settings on Rogue AP [Proxim_53:4D:1C] are policy compliant
ABC Corp	Apr 28, 2008 1:01 PM	New settings on Rogue AP [Proxim_53:4D:1B] are policy compliant

Severity 1 Vulnerabilities

Severity Level:  1

Type: Probable

Vulnerabilities: 0

Vulnerabilities with severity level 1 were not found.

Appendices

Categorized List of Access Points

This is a list of wireless access points (APs)—classified as authorized, rogue, external, or uncategorized—detected in your airspace during the reporting interval. You should verify if all your APs have been correctly classified as authorized. This list will serve as a wireless AP inventory and can be useful for more detailed analysis or forensics if anomalous wireless activity is detected.

Location	MAC Address	Protocol	Device Folder	Security	Vendor
ABC Corp	00:09:5B:FD:73:30	802.11b/g	Rogue AP	WEP	Netgear
ABC Corp	00:0D:0B:2B:0C:1B	802.11b/g	Authorized AP	WEP	Buffalo
ABC Corp	00:0D:97:04:83:AD	802.11b/g	External AP	Unknown	Tropos
ABC Corp	00:0D:97:04:84:5E	802.11b only	External AP	Unknown	Tropos
ABC Corp	00:11:24:A6:B1:1C	802.11b/g	External AP	WEP	Apple
ABC Corp	00:11:93:34:BE:90	802.11b/g	External AP	WEP	Cisco
ABC Corp	00:11:95:18:1A:AF	802.11b/g	Rogue AP	Open	D-Link
ABC Corp	00:11:95:53:4E:65	802.11b/g	Uncategorized AP	Open	D-Link
ABC Corp	00:11:95:53:4E:67	802.11a	Uncategorized AP	Open	D-Link
ABC Corp	00:11:95:E0:F2:D0	802.11a	External AP	802.11i	D-Link
ABC Corp	00:11:95:E0:F2:D8	802.11b/g	External AP	802.11i	D-Link
ABC Corp	00:15:E9:61:63:CA	802.11b/g	External AP	Open	D-Link
ABC Corp	00:19:5B:8C:A8:0C	802.11b/g	External AP	Open	D-Link
ABC Corp	00:1E:58:23:BF:27	802.11b/g	External AP	Open	Unknown
ABC Corp	00:20:A6:53:4D:1B	802.11a	Authorized AP	802.11i	Proxim
ABC Corp	00:20:A6:53:4D:1C	802.11b/g	Authorized AP	802.11i	Proxim
ABC Corp	00:40:05:BE:CC:17	802.11b/g	External AP	WEP	Unknown

Categorized List of Clients

This is a list of wireless clients—classified as authorized, unauthorized, or uncategorized—detected during the reporting interval. Use this wireless client inventory to quickly verify if all your clients have been correctly classified as authorized. If you have a “no-WiFi” policy, then this list can help you identify authorized clients that are violating the policy. You can also gauge the level of potential risk in your airspace in the form of non-authorized clients.

Location	MAC Address	Device Folder	Vendor
ABC Corp	00:05:4E:4D:49:2F	Unauthorized Client	Philips
ABC Corp	00:0E:35:52:C6:CC	Unauthorized Client	Intel
ABC Corp	00:0E:35:E1:40:46	Uncategorized Client	Intel
ABC Corp	00:0E:35:FF:54:DF	Uncategorized Client	Intel
ABC Corp	00:12:17:78:FF:D2	Authorized Client	Cisco-Linksys
ABC Corp	00:12:F0:7E:7D:73	Unauthorized Client	Intel
ABC Corp	00:12:F0:AC:AC:CF	Unauthorized Client	Intel
ABC Corp	00:13:02:2B:EC:05	Authorized Client	Intel
ABC Corp	00:13:CE:25:AD:63	Authorized Client	Intel
ABC Corp	00:13:CE:25:B8:48	Authorized Client	Intel
ABC Corp	00:13:CE:29:F0:3E	Uncategorized Client	Intel
ABC Corp	00:13:CE:3F:67:1E	Authorized Client	Intel
ABC Corp	00:13:CE:79:10:13	Uncategorized Client	Intel
ABC Corp	00:13:CE:82:50:10	Unauthorized Client	Intel
ABC Corp	00:13:CE:86:79:49	Unauthorized Client	Intel
ABC Corp	00:13:E8:1E:E0:19	Unauthorized Client	Intel
ABC Corp	00:16:44:9D:7F:82	Unauthorized Client	Unknown
ABC Corp	00:16:44:9E:AC:17	Uncategorized Client	Unknown
ABC Corp	00:16:6F:09:CF:3C	Unauthorized Client	Intel
ABC Corp	00:16:6F:6D:43:E2	Authorized Client	Intel
ABC Corp	00:16:6F:6F:25:B6	Uncategorized Client	Intel
ABC Corp	00:16:6F:79:4C:84	Uncategorized Client	Intel
ABC Corp	00:16:6F:95:B6:65	Uncategorized Client	Intel
ABC Corp	00:16:CF:63:30:A4	Uncategorized Client	Unknown
ABC Corp	00:17:F2:3F:AE:5D	Unauthorized Client	Apple
ABC Corp	00:18:39:01:4C:18	Authorized Client	Cisco-Linksys
ABC Corp	00:18:DE:45:9F:48	Uncategorized Client	Intel
ABC Corp	00:19:7D:A7:E7:72	Unauthorized Client	Unknown
ABC Corp	00:19:7E:4D:FC:DE	Uncategorized Client	Unknown
ABC Corp	00:19:D2:6D:3E:AF	Uncategorized Client	Intel
ABC Corp	00:19:D2:92:09:26	Uncategorized Client	Intel
ABC Corp	00:19:D2:92:0B:A6	Authorized Client	Intel






Location	MAC Address	Device Folder	Vendor
ABC Corp	00:1A:92:B1:F3:B8	Uncategorized Client	Unknown
ABC Corp	00:1B:77:28:E5:C1	Authorized Client	Intel
ABC Corp	00:1B:77:81:29:5A	Authorized Client	Intel
ABC Corp	00:1B:77:81:47:9C	Authorized Client	Intel
ABC Corp	00:1B:77:A3:A6:6E	Unauthorized Client	Intel
ABC Corp	00:1B:77:A4:A8:7A	Unauthorized Client	Intel
ABC Corp	00:1B:77:D1:28:1C	Authorized Client	Intel
ABC Corp	00:1D:4F:EB:0A:83	Unauthorized Client	Unknown
ABC Corp	00:1F:3A:12:D3:41	Uncategorized Client	Unknown
ABC Corp	00:1F:3A:1F:01:3D	Uncategorized Client	Unknown
ABC Corp	00:1F:3A:4C:5F:4F	Uncategorized Client	Unknown
ABC Corp	00:1F:3A:4C:5F:58	Uncategorized Client	Unknown
ABC Corp	00:1F:3A:4C:64:64	Unauthorized Client	Unknown

List of Wireless Scanners

This is a list of wireless scanners that were connected to the server during the reporting interval. Verify if all deployed wireless scanners are listed.

Location	Device Name	MAC Address	IP Address
ABC Corp	AirTight_00:6D:90	00:11:74:00:6D:90	192.168.201.74
ABC Corp	AirTight_10:84:F4	00:11:74:10:84:F4	192.168.201.84

Severity of Vulnerabilities

Severity level	Type	Description
 5	Critical	Security breach or wireless malpractice detected! An intruder may have entered your network; sensitive data is exposed; or your users are bypassing your security policy control (e.g., firewalls, and URL, spam, and malware filters).
 4	High	Known vulnerabilities those ignore basic security measures and naturally expose your network and data assets even to inadvertent unauthorized access.
 3	Medium	Vulnerabilities that violate best practices and can lead to unauthorized usage of your network resources or hackers with medium expertise and knowledge of published exploits can exploit these vulnerabilities in minutes.
 2	Low	Hackers can collect information about your network and may use it to discover other vulnerabilities; high expertise needed to exploit these vulnerabilities.
 1	Probable	Potential vulnerabilities that may pose a threat.

Critical severity: Occurrence of a critical severity demands your urgent attention. It is raised when malpractices in wireless usage, anomalous activities or attacks are detected in your airspace and your entire network's security is potentially at risk. Few examples of instances with critical severity: authorized users connecting to external or rogue APs, outsiders connecting to your authorized APs, authorized users participating in ad hoc networks, network and data exposed by open or WEP connections, MAC spoofing, honeypot attack, denial of service (DoS) attack.

High severity: Ignoring basics of wireless security leads to these vulnerabilities that give outsiders easy access to your network and data assets and a security breach is imminent; deliberate effort to hack into your network is not necessary. Few examples of high severity vulnerabilities are: using "out-of-box" settings (e.g., no security, default password) on your WiFi devices, rogue APs installed on your network, your authorized devices are in ad hoc mode.

Medium severity: Violating WLAN best practices usually results in these vulnerabilities. Few examples are: using the broken Wired Equivalent Privacy (WEP) encryption standard on your WiFi devices, and lack of policies to control how and to which WLANs your WiFi clients can connect. Hackers can break through your weak security settings, or lure users to connect to them (e.g., honeypots) gaining access to sensitive data or backdoor entry into your network.

Low severity: These vulnerabilities leak information about your WLAN configuration and attract unwarranted attention from outsiders to your network, or attract your authorized users to connect to external WLANs, e.g., APs using vulnerable or hotspot SSIDs. Hackers can use such information to discover and exploit other vulnerabilities in your network.

Probable: These are potential vulnerabilities that may pose limited threat to security or performance of your network. You should manually verify the existence and credibility of these probable threats. For instance: an extraordinary number of wireless frame errors indicate a potential jamming attack or inadvertent interference from another RF source; a large number of broadcast messages indicate a potential attack or misconfiguration.