Global Information Assurance Certification Paper

Auditing the Wireless environment: A mobile wireless LAN used for training in multiple sites on a corporate WAN- An Auditor's perspective

GSNA v. 2.0
SANS Conference 2002 – Orlando

Submitted by
Angela Loomis

September 2002

Abstract/Summary

This paper is submitted as the requirement for a practical in the GSNA certification track. It examines in detail an audit of a small wireless network that will be used for a training site on a company's wide area network. The auditor's objective is to secure this training LAN for a specific location; later, the auditor will use the same methods and tests to certify other locations on the corporate WAN. The goal of the practical is to address specific wireless vulnerabilities and tighten up this small network so that unauthorized access via the wireless link is not going to occur.
The auditor examines not only the wireless access point, but also the laptops used for training. The risks of wireless are many, so the auditor wants to secure the small LAN so that the risks to the corporate WAN will be mitigated.

Contents

Assignment 1

Identify the system to be audited

This audit is an auditor's perspective of a wireless LAN used for training only. The training wLAN consists of a Cisco Aironet 1200 (System Firmware v. 11.42, Radio Firmware v. 4.99.38) and ten HP Omnibook XE 4100 laptop systems. The laptops connect to the AP via the Cisco 350 wireless card; and are allowed to access the Internet over the corporate WAN. Any Internet access passes over the corporate network infrastructure and through the corporate firewall. This mobile training network enables training to take place in various rooms in numerous buildings throughout the WAN, but primarily from "Location A." This audit of "Location A" will provide a framework for testing and certifying other possible training locations in various buildings as training requests arise. This audit will outline the method used to "certify" a location on the corporate campus for use as a training area.

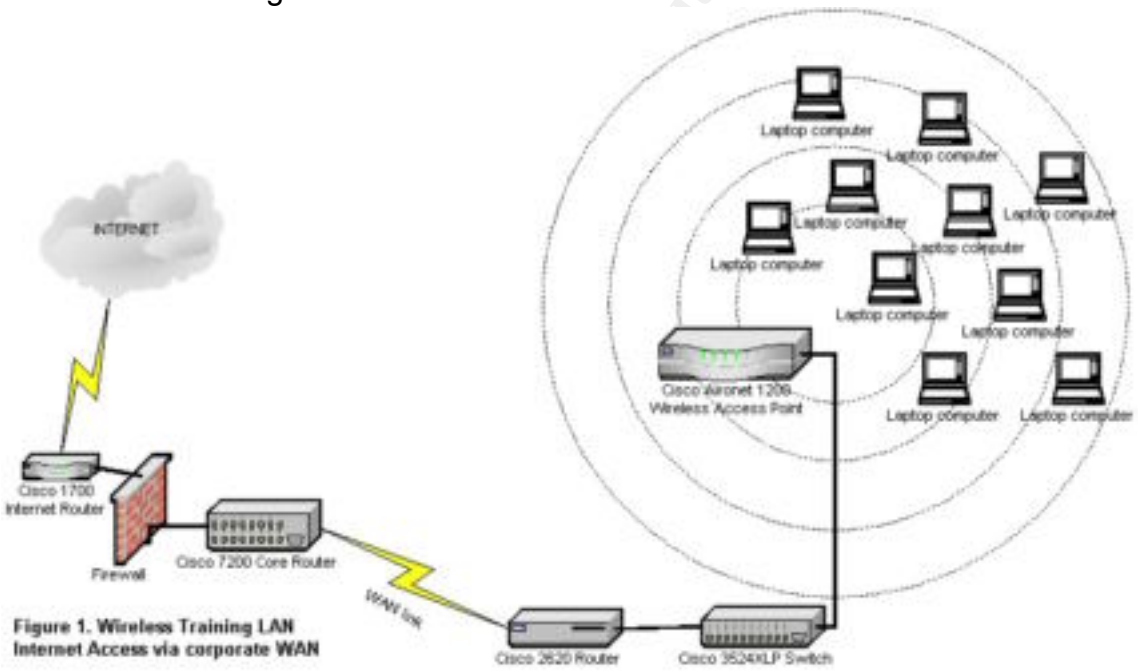


Figure 1. Wireless Training LAN Internet Access via corporate WAN

Figure 1 provides a view of the path the wLAN traffic will travel from "Location A" to the Internet. Most other locations provide similar paths across the corporate WAN. The wireless AP will connect to a switch and/or a router. That router connects back to the central office via a private T1. The central office connects to the Internet through a firewall. While not specifically depicted in the diagram (for simplicity's sake), the corporate WAN includes servers and workstations at both the satellite office and central office.

Evaluate the risk to the system

The wLAN needs to be secured from both outside access via unauthorized wireless connections and separated from the corporate WAN. While the information contained on the wLAN itself is insignificant because it is strictly used for training purposes, the access provided through the corporate infrastructure includes a measure of risk to the corporate WAN. The risks provided to the training center and corporate data include standard security risks that exist for any network, with the addition of the vulnerabilities provided by wireless access. The matrix below includes specific risks, as well as the probability of occurrence, and possible outcomes of those risks.

Risk	Probability and Risk Rating	Outcome
Unauthorized wireless access-Intrusion via wireless LANjacking	High	Compromise of Corporate and/or customer data Reputation, customer confidence damaged.
Unauthorized WAN access-Intrusion via training center laptop end user	High	Compromise of Corporate and/or customer data
Sniffing of plaintext data between laptops and AP.	Low	Compromise of training center data only
Compromise of WEP-decryption of WEP encrypted data	Medium	Compromise of training center data, leading to unauthorized access via wireless access point authentication compromise. Compromise of Corporate and/or customer data.
Disruption of wireless network via radio interference	Low	Decreased efficiency of training center—denial of service.
Obsolescence of purchased wireless technology	Medium	Possibility that hardware cannot be upgraded to address newly discovered vulnerabilities
Virus, Trojan, or Malware exploited on training center laptops	Medium	Virus infection of the training LAN and WAN wired network, compromise of Corporate and/or customer data.
Misconfigured Wireless Access Point	High	Could provide access to Corporate and/or customer data leading to compromise of that data. Reputation, customer confidence damaged.
Unauthorized setup and use of wireless training center by employees	High	Could provide access to corporate and/or customer data via unsecured setup of wLAN in unsecured area. High level of customer confidence shaken. Reputation damaged.

Theft or tampering with AP and training laptops.	Medium	Damage or loss of hardware

Current State of Practice
It seems everyone is discussing wireless network vulnerabilities. Many articles have recently come out describing the numerous vulnerabilities presented in wireless networking, even in mainstream press. In July, Doonesbury featured a wireless network "cowboy" accessing the Internet through another man's home wireless network. (http://www.doonesbury.com/strip/dailydose/index.cfm?uc_full_date=20020721&uc_comic=db&uc_daction=X)

Many of these articles outline vulnerabilities without giving much advice for mitigating risk. Wireless standards for security (802.11i, 802.1x) are still under development by IEEE and IETF. Wireless security standards have been documented and outlined by some government agencies to provide guidance for wireless implementation. One of the best resources for wireless network implementation guidelines was released by NIST (Nation Institute of Standards and Technology) in a draft report in July 2002. (http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf)

The NIST report includes a checklist for secure wireless LAN implementation. While I am basing my checklist on many of the NIST points, I am also expanding it to include guidance provided by the FDIC regarding wireless. And, I am breaking it into sections that relate specifically to the wireless LAN training network that we will be implementing in the near future. (http://www.fdic.gov/news/news/financial/2002/fil0208.html) As an FDIC insured institution, any technology we implement is examined for compliance with known standards as well as evaluated as to its fitness in our regulated environment. The privacy of customer data is of primary importance in order to comply with regulations like Gramm-Leach-Bliley.

Because the emerging and current state of wireless security is both vulnerable and evolving, NIST is finalizing a report recommending to government that wireless LANs not be implemented at all. (http://maccentral.macworld.com/news/0208/19.wirelesslans.php)

Improvement of current methods and techniques
Specific checklists for the Cisco Aironet 1200 don't exist for auditing purposes. In order for me to develop the checklist for the wireless training LAN, I needed to evaluate the wireless access point coupled with laptop evaluation. I also needed to audit to ensure that the training users were segregated from our corporate WAN. The checklists, which follow, and the methodology used, can certainly be modified and used to certify any location within a corporate WAN environment for the installation and use of wireless. The NIST checklist that has been out in draft form and will soon be released provides an excellent starting point for developing checklists for wireless LANs. It is very granular with its recommendations so

that even people without a thorough technical understanding of wireless can identify settings and parameters that secure the wireless environment. Again, with this wireless training LAN, I need to evaluate the AP, the wireless card setup, and how the training users are segregated or separated from our regular network.

Assignment 2

Create an Audit Checklist

Cisco Aironet 1200 Access Point Checklist

Step 1 - Policy for wireless training LAN

Reference	Security basics, NIST document
Control Objective	Outlines standards for wireless implementation company-wide.
Risk	This step provides for an overlaying policy and standard for the company outlining "certified" training scenarios. Clearly stated policies regarding wireless access leave nothing open to interpretation company-wide. With a known policy in place, management has more leverage in the case of an information security incident.
Compliance	Does the company have a clearly stated policy on wireless access in general as well as a clearly stated policy on the specific wireless training LAN? Either the policy exists, or it doesn't. However, some policies include vague language that addresses new installation of systems like the wireless AP—what does this company have in place for policy?
Testing	Review existing policies for language relevant to wireless. Review any newly developed or implemented policies for language relevant to wireless.
Objective/Subjective	Subjective-policy language generally has room for interpretation.

Step 2 - Administrative access to AP

Reference	Security basics – password protect access to systems, change default password, etc.
Control Objective	Control unauthorized administrative level system access; deny unauthorized administrator access.
Risk	AP compromise leading to system and network access to an unauthorized end user. This is a high level risk in that it could lead to compromise of customer data by allowing unauthorized access to the corporate network.
Compliance	There must be a strong password for administrative access. There must also be strong passwords in place for other users to ensure the integrity of the running configuration of the AP.
Testing	Evaluate admin and other username/pw for system. (In this particular case this may be accomplished by simply asking the administrator for this information—since the admin and audit have a great rapport!)
Objective/Subjective	Objective

Step 3 - AP Security settings

Reference	Cisco Aironet 1200 Configuration Guide, NIST standards
Control Objective	Control unauthorized wireless access to AP and the corporate WAN with the most secure configuration. Ensure the AP configuration is as secure as technically possible in the existing network environment.
Risk	System and network compromise by unauthorized persons leading to compromise of corporate and customer private data. This is a very high risk for a wireless network.
Compliance	Implement most secure configuration outlined in product literature. Cisco literature describes these levels of security for the access point (listed from least secure to most secure configuration)- A. Default settings B. Unique SSID with Broadcast SSID disabled C. Shared Key authentication with WEP D. Open authentication with WEP E. MAC-based authentication with WEP F. EAP authentication with WEP G. EAP authentication with MIC, broadcast key rotation, and WEP

Testing	1. Confirm unique SSID with Broadcast SSID disabled, AND 2. Confirm shared key authentication, OR 3. Open authentication, OR 4. MAC-based authentication with WEP, OR 5. EAP authentication with WEP, OR 6. EAP authentication with MIC, broadcast key rotation, and WEP Obviously, the choice of authentication method is directly related to the security of the wireless LAN. A better score would be the highest level of security, with lower scores for any other methods of authentication. Take into consideration network resources available: for instance, in order to implement EAP, a RADIUS server must be available to authenticate clients. In this particular case, no RADIUS server exists on the WAN, and the added expense for the RADIUS implementation is not endorsed for the protection of a small training LAN. So, for this case, the highest level afforded is MAC-based authentication with WEP. These settings can be confirmed by examining the configuration; and testing MAC authentication.
Objective/Subjective	Objective

Step 4 - Key length and use

Reference	Common security knowledge, NIST standards
Control Objective	Larger keys take exponentially longer to break—therefore, key size should be set to the highest level the system will afford. Also, keys should be changed periodically, especially when using shared key authentication. This provides a level of security by limiting the timeframe a key is in use so that the key is less likely to be broken.
Risk	Key may be broken, compromising the security of the encrypted corporate and customer data.
Compliance	Ensure 128 bit keys (or higher, if system settings allow) are used. Verify that keys are changed, and what timeframe key change occurs.
Testing	Verify within the AP configuration settings. Verify key change by looking for policies, and with interviews of the AP administrator.
Objective/Subjective	Subjective

Step 5 - Physical access to AP

Reference	NIST standards, common security practice.
Control Objective	Ensure only authorized personnel have physical access to the AP.
Risk	Theft of AP. Also, unauthorized setup and use by employees. This is a high level risk, and those responsible need to be aware of the chain of responsibility regarding the access point. This could lead to AP compromise, and correlated risk to the corporate network, and customer data.
Compliance	Ensure the physical security of the AP when in use, and not in use. Are there procedures that address the storage of the AP when not in use? Are there specific "sign-out" procedures for use of the systems? Who holds the keys to the locked area where these systems are stored?
Testing	Review IT internal documentation about securing access point. Review IT procedures for use of AP. Verify who has the keys to remove the AP from locked storage. Review and verify available secure storage and use areas for AP. Check AP storage during and after training sessions.
Objective/Subjective	Objective

Step 6 - Wireless "perimeter" site survey-signal strength and security

Reference	NIST standards, Cisco documentation,
Control Objective	Control the "perimeter" of the wireless reception by using the least possible MhZ so that the wireless signal is significantly degraded outside the physical training area.
Risk	Wireless signal may be hijacked if it is available to the outside world indiscriminately. This is a high level risk with an outcome of the compromise of corporate and customer private data.
Compliance	To exhibit compliance in this area, signal strength must be as low as it can go in public areas of the building. Additionally, there should be NO signal picked up outside the office building where training location "A" is contained. Any signal that is detected in a public area must provide an additional layer of physical security or visibility so that anonymous wireless access cannot occur. This can be mitigated with awareness of the environment coupled with physical barriers to public access such as locked areas.

Testing	With the access card utility provided with Cisco cards, measure and record signal strength in various places in the building. Pay special attention to areas where the public has full access. Document signal strength, and verify that employees can monitor these public areas for unauthorized laptop users. It would be very unlikely that a customer would be using their laptop in the environment, so verify through interviews with employees that they should understand the potential meaning of a customer seated in a waiting area for a length of time using a personal laptop. Verify the signal strength is low or non-existent outside the building.
Objective/Subjective	Objective-signal strength Subjective-employee awareness

Step 7 - AP powered down when not in use

Reference	General Security knowledge, NIST standards
Control Objective	Make the wireless AP unavailable during periods of no use. This one is pretty straightforward—turn off the AP when no training classes are using it.
Risk	This addresses the risk that over time, the AP security may be cracked. If the wireless AP is powered off, then no opportunity exists for unauthorized access attempts or cracking.
Compliance	Verify that policy and procedure outline that the access point be powered off and locked up when not in use.
Testing	Verify by spot-checking that the AP is locked up and powered off when no training is taking place.
Objective/Subjective	Objective

Step 8 - Default settings changed

Reference	General Security knowledge, NIST standards
Control Objective	This step addresses the fact that systems should be put into place after all default settings for the system have been changed.
Risk	A system with default settings “in the wild” is much easier to crack than a system that does not use default settings. Compromise of the AP would lead to compromise of corporate and customer data.
Compliance	Compliance with this item is straightforward-either the settings are default or they have been changed.
Testing	Make a list of the factory default settings. After the system has been configured, verify these settings have new values.
Objective/Subjective	Objective

Step 9 - Obsolescence of technology

Reference	NIST standards, FDIC guidance
Control Objective	Ensure that technology purchases are made with the "long term" in mind. Ensure hardware or firmware can be upgraded in order to address any newly discovered vulnerabilities. Ensure long-term usage of the technology.
Risk	The risk here is that the technology could become outdated quickly. If purchases are made with the "long term" in mind, then the obsolescence of the technology would not come quickly, ensuring prudent investment for the company.
Compliance	Verify that the system can be upgraded—that the "upgrade-ability" of a system was considered in the purchase process.
Testing	Interview system manager and people responsible for signing off on the purchase. Verify on the manufacturer's website that the system can be upgraded.
Objective/Subjective	Subjective

Step 10 - SNMP management

Reference	NIST standards
Control Objective	If SNMP management is enabled for the AP, SNMP must be configured as securely as possible in the network environment.
Risk	SNMP compromise, which could lead to the compromise of corporate and customer data.
Compliance	(From NIST checklist) Make sure robust community strings are used for SNMP management on the AP. Disable SNMP if not in use.
Testing	First, verify if the network manager uses SNMP. If they don't, then verify that SNMP has been disabled on the AP. If they are using SNMP, look to see if it is SNMPv3 that provides cryptographic protection. Look for strong community strings if SNMP is in use.
Objective/Subjective	Objective – if SNMP not used Subjective – if SNMP in use ("strong" community strings)

Cisco Wireless PC Card AIR-PCM350 Checklist

Step 1 - Administrative access to Aironet Client Utility

Reference	Cisco configuration guide, security knowledge
Control Objective	Limit accessibility to the client utility so that no one but administrators can change wireless client configuration (profiles).
Risk	By limiting the access of end users to the configuration components, an administrator will ensure wireless network stability. Unauthorized end users could change the configuration, or profile, and disconnect the client from the wireless LAN. This is a low level risk to the organization, as it is in place mainly to prevent configuration changes from a "known good" state.
Compliance	Verify that only an administrator can change configuration settings on the training laptops using the client utility.
Testing	Log on to each laptop as a training user. Verify you have connectivity with the AP. Then, access the Cisco Client Utility, and change the configuration. Some settings that could be changed are: 1- SSID 2- Radio Channel 3- WEP key parameters Any of these settings, if successfully changed, would cause disassociation with the AP. If you are able to change these settings and cause the wireless link to drop, then the laptop is out of compliance.
Objective/Subjective	Objective

Step 2 - Anti-virus software

Reference	General Security knowledge, NIST checklist
Control Objective	Control the network environment to keep it free from viruses and Trojans.
Risk	Corruption of corporate and customer data could occur if the training center systems were infected and then infected the local network. The risk is medium level.
Compliance	Verify that anti-virus software is installed on the training laptops.
Testing	Verify that the laptops have up-to-date anti-virus software with current DAT files.
Objective/Subjective	Objective

Step 3 - Physical access to laptops and wireless cards

Reference	NIST standards, common security practice.
Control Objective	Ensure only authorized personnel have physical access to the laptops and Cisco cards.
Risk	Theft of laptops and/or cards. Also, unauthorized setup and use by employees. This is a high level risk, and those responsible need to be aware of the chain of responsibility regarding the access point. This could lead to wireless network compromise, and correlated risk to the corporate network, and customer data.
Compliance	Ensure the physical security of the laptops and wireless cards when in use, and not in use. Are there procedures that address the storage of these laptops when they are not in use? Are there specific "sign-out" procedures for use of the systems? Who holds the keys to the locked area where these systems are stored?
Testing	Review IT internal documentation about securing access point. Review IT procedures for use of laptops/cards. Verify who has the keys to remove the laptops/cards from locked storage. Review and verify available secure storage and use areas for laptops/cards. Check laptops/card storage during and after training sessions.
Objective/Subjective	Objective

Step 4 - Obsolescence of technology

Reference	NIST standards, FDIC guidance
Control Objective	Ensure that technology purchases are made with the "long term" in mind. Ensure hardware or firmware can be upgraded in order to address any newly discovered vulnerabilities. Ensure long-term usage of the technology.
Risk	The risk here is that the technology could become outdated quickly. If purchases are made with the "long term" in mind, then the obsolescence of the technology would not come quickly, ensuring prudent investment for the company.
Compliance	Verify that the system can be upgraded—that the "upgrade-ability" of a system was considered in the purchase process.
Testing	Interview system manager and people responsible for signing off on the purchase. Verify on the manufacturer's website that the system can be upgraded.
Objective/Subjective	Subjective

Step 5 - Ad Hoc or Infrastructure mode

Reference	Cisco configuration guide
Control Objective	Ensure the wireless network does not operate in Ad Hoc (peer to peer) mode.
Risk	Ad Hoc connections could be established with unauthorized users—this could lead to compromise of corporate and customer data.
Compliance	Compliance in this area is clear: Ad Hoc connections must not be enabled for either the AP or the Cisco client cards.
Testing	Verify Ad Hoc or Infrastructure setting in all training laptops.
Objective/Subjective	Objective

Segregation of end users in the training environment Checklist

Step 1 - Segregation by IP address

Reference	NIST standards, security knowledge
Control Objective	Training end users should not be able to access network resources from the training wLAN.
Risk	If the wLAN is compromised, then the corporate WAN environment is at risk. As much as possible, traffic from the wLAN should be limited, and controlled so that even if the wLAN is compromised, corporate network compromise does NOT necessarily follow. This would be a high level risk.
Compliance	If a firewall is in place between the wLAN and the WAN, then segregation can be very granular. If no firewall exists between the wLAN and WAN, it is very difficult to segregate traffic from the WAN. The best solution would be to have a firewall between the two environments.

Testing	If a firewall exists between the wLAN and WAN, then the firewall rule base should be examined to verify how wLAN traffic is passed. (Because this is really a separate audit in and of itself, I won't cover this in detail at this time) At the very least, look for firewall rules that allow traffic based on IP addresses. Also, the firewall should have an existing list of wireless client card IP addresses (or even MAC addresses—even better!) that are "allowed." No other addresses should be allowed to pass through the firewall. If no firewall exists, at the very least, the AP should be attached to a Layer 2 switch rather than a hub. Also, if no firewall is available, then the training users' access must be address by USER rather than IP. (Again, this could be an audit in and of itself) The training users access levels should be examined in detail (in our case, by examining the Novell NDS settings for the training users) to verify that their access exists at a very low level.
Objective/Subjective	Subjective

Assignment 3

Conduct the Audit

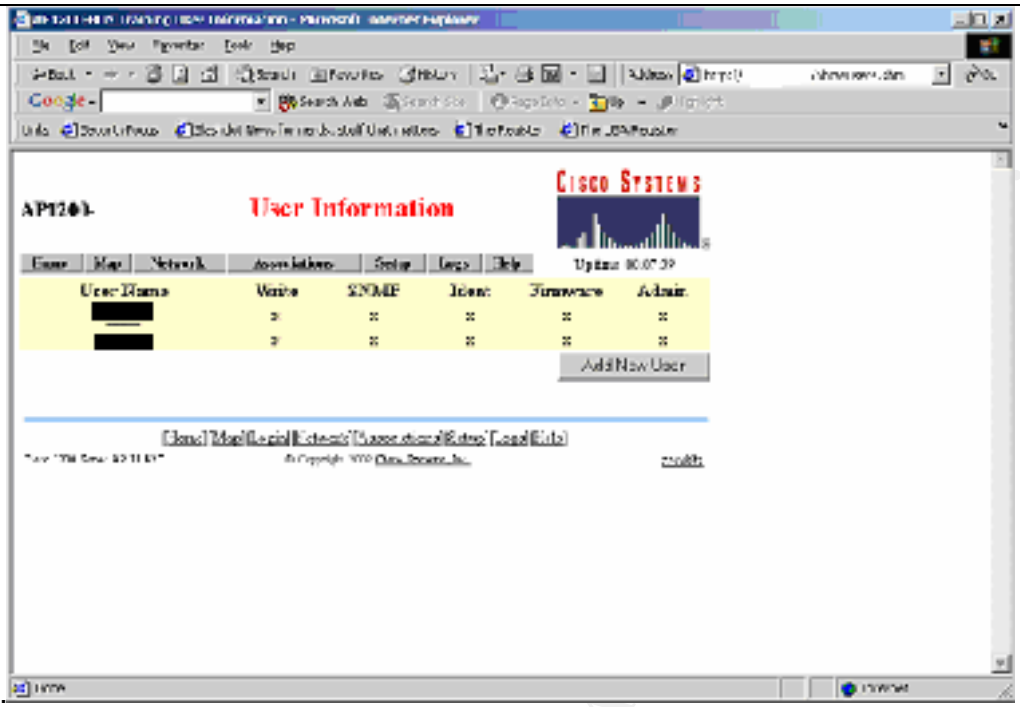
Cisco Aironet 1200 Access Point Checklist

Step 1 - Policy for wireless training LAN

Method
The auditor looked at existing policies that cover most areas of Information Security for the organization. There were three policies that cover systems, end users, and disaster recovery. The auditor searched the text for "wireless" and "802.1*" using the CTRL-F function in Microsoft word. The auditor also spoke with the Administrator about procedures regarding the wireless training LAN.
Results
No currently board approved policies cover 802.11b or any other wireless network connections. The Administrator is developing procedures that will cover setup, storage, and security of the wireless training LAN.
Conclusion-FAIL
No policies currently exist on wireless network access and the corporate WAN.

Step 2 - Administrative access to AP

Method
The auditor discussed the current password parameters and users who are set up for administrative access to the AP with the Administrator. The auditor viewed the page outlining who the users are, and what rights they have to the



AP.

Results

There are two users who have administrative rights to the AP. Both users use alphanumeric passwords of 9 characters in length. Passwords are changed according to IT policy—every 60 days.

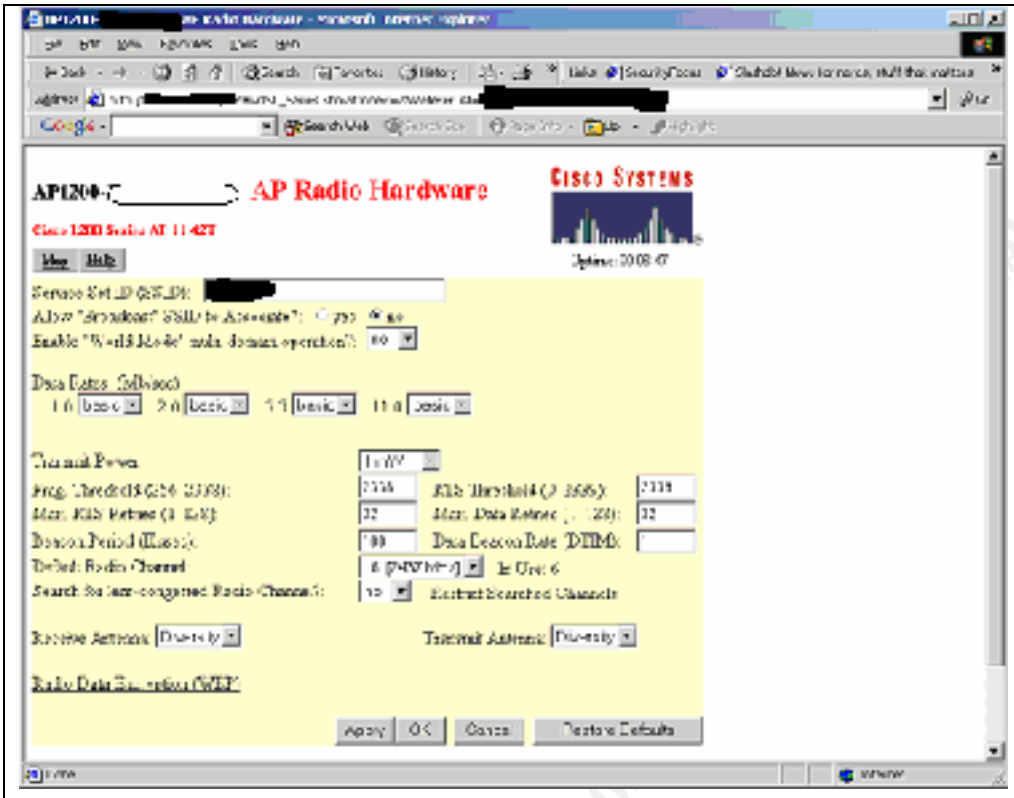
Conclusion-PASS

Passwords adhere to company standards. Having two administrative users provides checks and balances for correct configuration.

Step 3 - AP Security settings

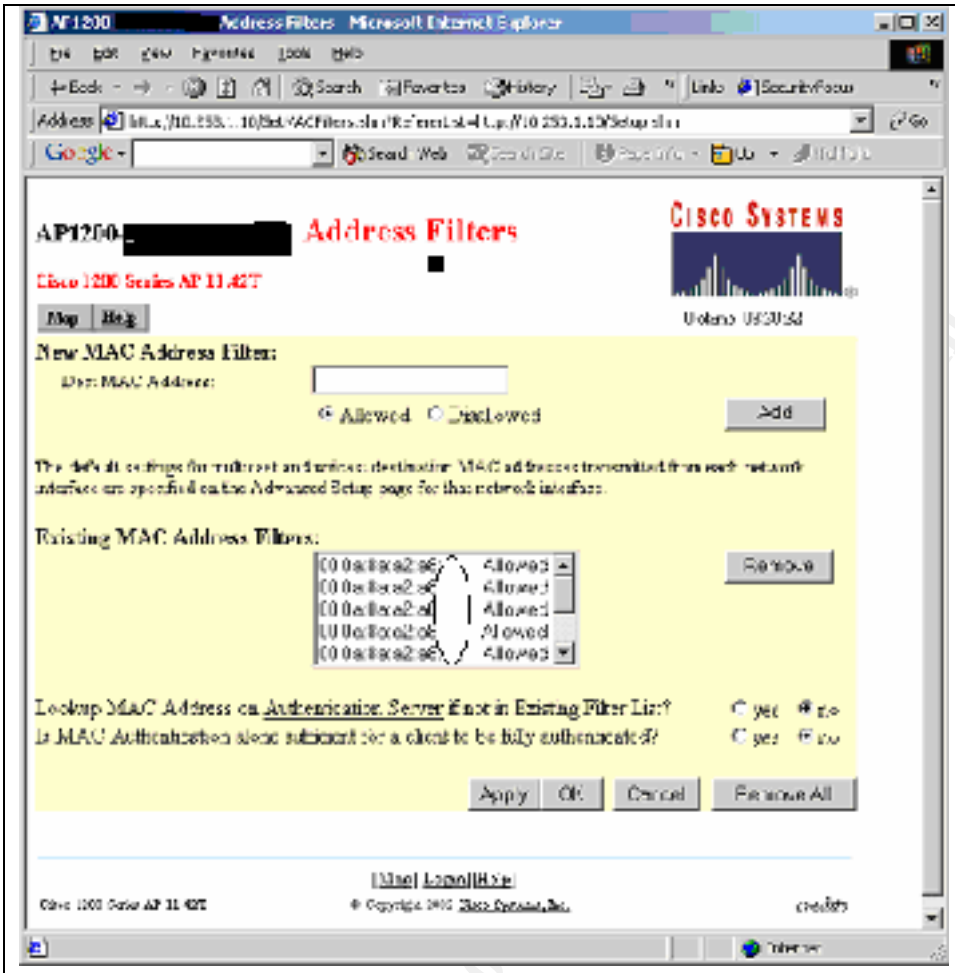
Method

To verify that the broadcast SSID was disabled, the Auditor screen shot the http configuration page which had a radio button for “Allow Broadcast SSID to Associate” to verify that “NO” had been chosen.



According to Cisco configuration guidelines, by checking “NO” you only allow devices that specify the SSID to associate with the AP. To test this, the auditor removed the SSID from a client that had associated to the AP. Upon removal, the client was no longer associated.

Now, the auditor needs to verify that MAC address filtering in addition to non-broadcast SSID prevents non-identified (rogue) MAC addresses from associating with the AP. This step was interesting to prove. After configuring the Cisco ACU so that it would associate with the AP by configuring WEP and the SSID, the Administrator entered all MAC addresses of the wireless cards into the Address Filters section of the AP configuration. After verifying which MAC address was on the auditor’s laptop, the Administrator removed the auditor’s MAC address from the AP filter. But the auditor’s laptop was still associated, and could still pass traffic through the AP!



The auditor, after referencing the Cisco configuration guide, had the Administrator look to see if an Advanced Radio setting had been changed which would correctly (and fully) enable MAC address filtering by the AP.
Once this setting was in place, MAC address filtering worked as documented by Cisco.

Results

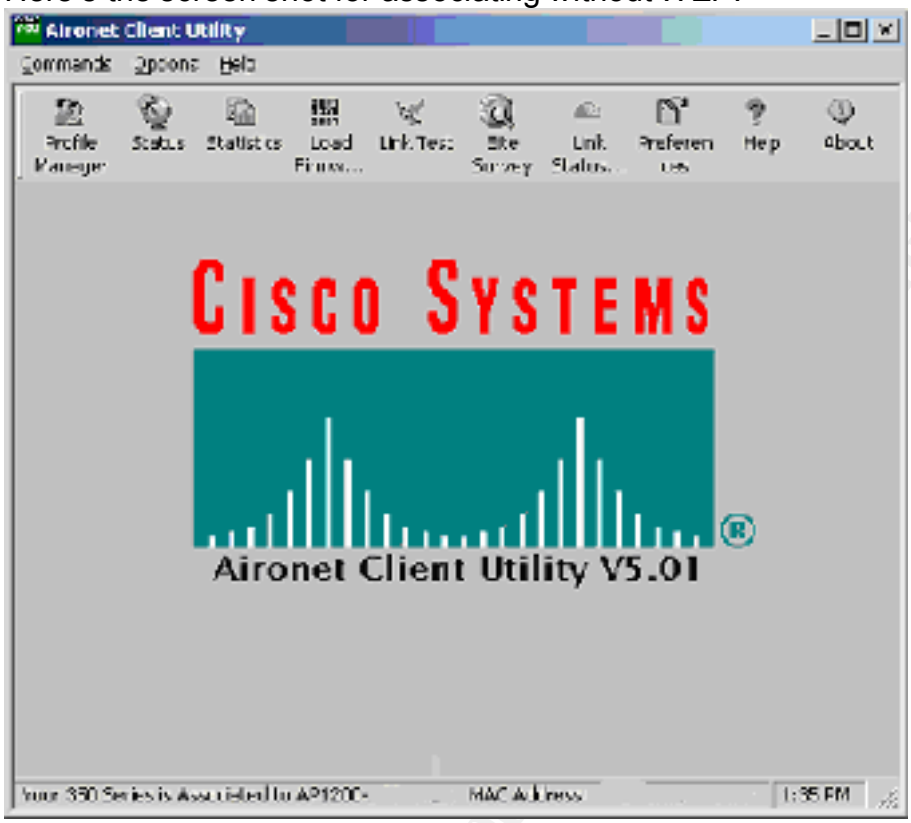
The auditor created a matrix that gives the possible combinations to try associating with the AP.

SSID	X			X	X		X
WEP		X		X		X	X
MAC			X		X	X	X
Can associate	NO	NO	NO	NO	YES	NO	YES
Can pass traffic	NO	NO	NO	NO	NO	NO	YES

If an item is checked, that means it was set up to match the correct settings in the AP. Interestingly, sometimes the card/laptop could associate but couldn't

pass traffic.

Here's the screen shot for associating without WEP:



Notice that MAC, not IP, defines the AP.
Once WEP is correctly configured for the wireless card, the card associates to the AP, and identifies it by IP address because WEP enables decryption.

Only wireless cards configured with the SSID, WEP, and "allowed" MAC addresses should be able to associate with the AP. Testing proved that all three needed to be in place in order to associate and pass traffic through the AP.

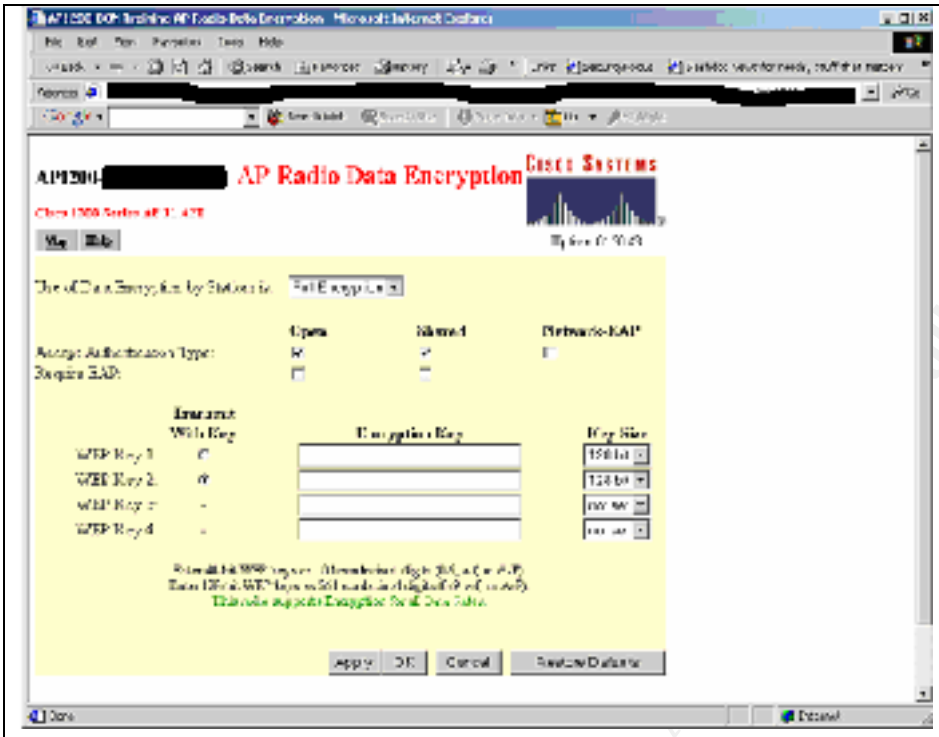
Conclusion-PASS

After initially misconfiguring the MAC filter, the Administrator correctly implemented changing the SSID, disabling Broadcast SSID, enabling WEP, and enabling MAC filters so that only users with all three elements correctly configured would be able to associate and pass traffic through the AP.

Step 4 - Key length and use

Method

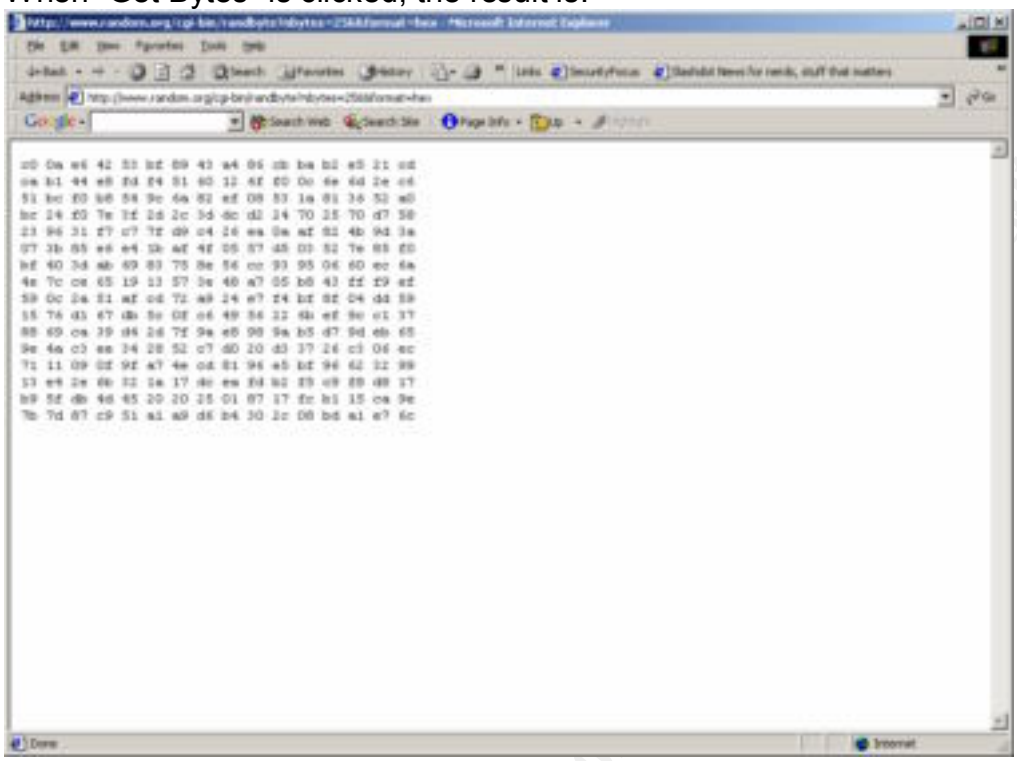
The auditor asked the Administrator to demonstrate how keys are chosen for WEP. Also, the auditor asked the Administrator to explain how often keys will change, how long the keys are, and if there is written documentation explaining this process.
The auditor also looked at the configuration settings in the AP to verify that 128-bit WEP keys are used.



Results

The Administrator outlined that WEP keys will change for each class. For example, if a class lasts one day, the key will be in place for one day. If a class lasts four days, the key for that class will be in effect for four days.
The Administrator demonstrated for the auditor how the keys are developed:
The Administrator goes to the Random.org website and chooses “Hexadecimal.”

When “Get Bytes” is clicked, the result is:



Keys are pulled from this hex block by designating a starting place by row. Each hex key is 26 characters in length, and is manually keyed into the AP and each laptop’s ACU by the Administrator. The hex block generated by random.org is used only one time for one class.

Conclusion-PASS

WEP key length is 128-bit.
Keys are random in nature.
Keys are used for one class only.
No written procedures exist for WEP key implementation.

Step 5 - Physical access to AP

Method

The auditor looked at existing policies that cover most areas of Information Security for the organization. There were three policies that cover systems, end users, and disaster recovery. The auditor searched the text for “wireless” and “802.1*” using the CTRL-F function in Microsoft word. The auditor also spoke with the Administrator about procedures regarding physical security of the wireless training LAN.

Results

No currently board approved policies cover 802.11b or any other wireless network connections. The Administrator is developing procedures that will cover setup, storage, and security of the wireless training LAN.

Conclusion-FAIL

No Policy or written procedure exists at this time regarding the Cisco AP. Policy and procedure need to be written to address the physical security of the AP.

Two employees have access to the locked storage area where the AP is kept—there are no current sign out procedures for use of the AP (and training environment.) While the Administrator is very "hands on" with the AP, and accepts full responsibility for the physical access to the AP, he also understands and agrees that policies and procedures need to be developed in this area.

Step 6 - Wireless "perimeter" site survey-signal strength and security

Method

The auditor utilized Cisco's Aironet Client Utility (ACU) to measure signal strength both inside and outside the building where the training LAN was set up. The auditor started by standing near the AP, and fully associating. The ACU provides a graphic depiction of signal strength and quality, as well as specifically outlining, "not associated" when out of range.

The training LAN is in a physically restricted area in the basement of a one-story brick building. Upstairs, both public and restricted areas are accessed. One restricted area is only accessed by employees who have keys to the area. This area is partially walled off so that the public has interaction with the employees over a counter. Other employees have cubicles and offices where customers can interact in a more private setting with the employees. Fully public areas include a lobby area with an L-shaped seating area in front of a fireplace, a corridor that leads to an exit, and a glass double door entry.

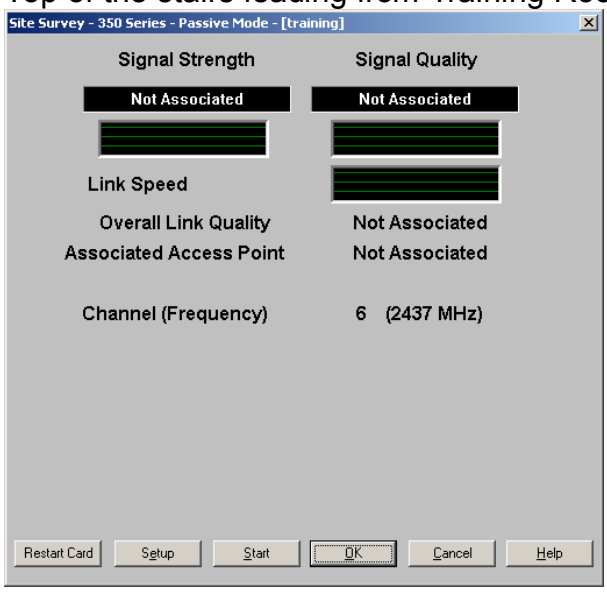
The auditor walked various areas of the building, documenting location and screenshotting signal strength to determine radio coverage.

Results

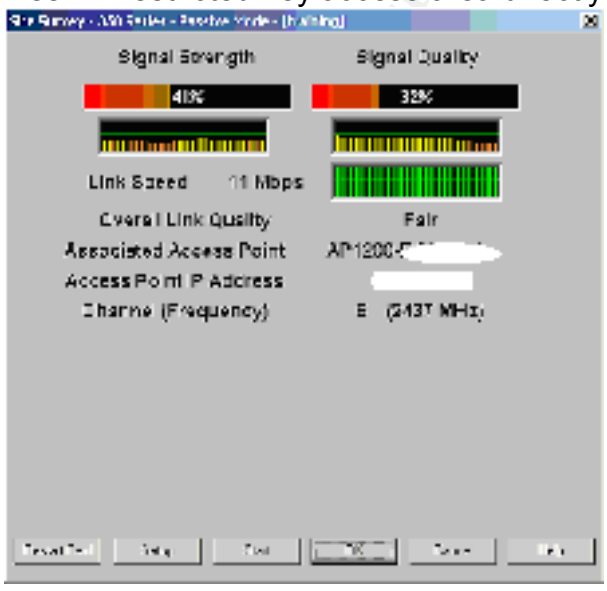
Here are the screen shots with description of locations:

Site survey in training room next to AP

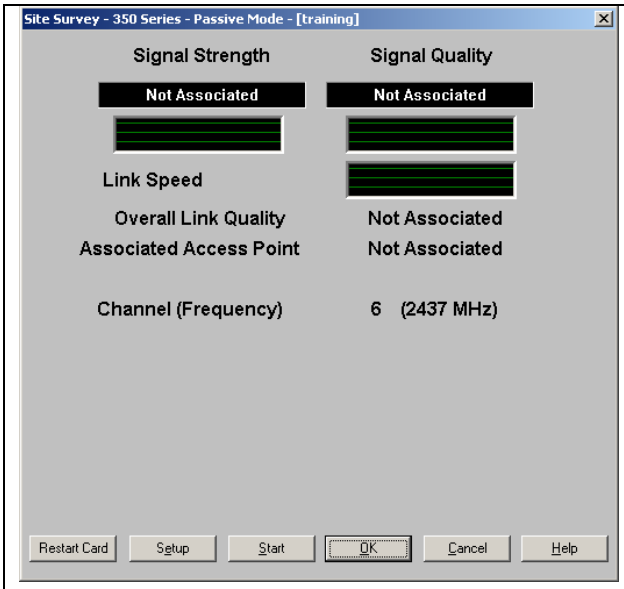
Top of the stairs leading from Training Room to Restricted key access area



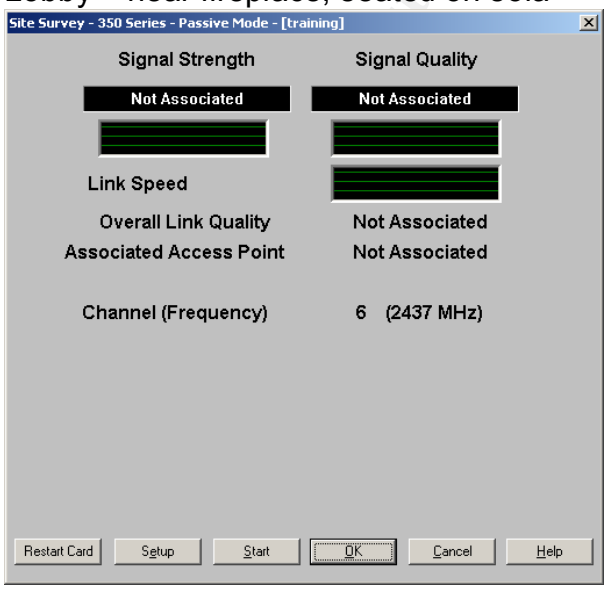
Desk in restricted key access area directly above training room



Lobby – public area fully open to the public

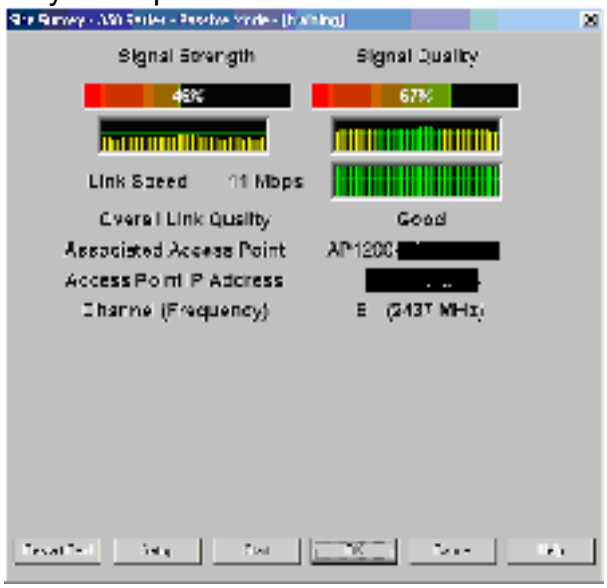


Lobby – near fireplace, seated on sofa

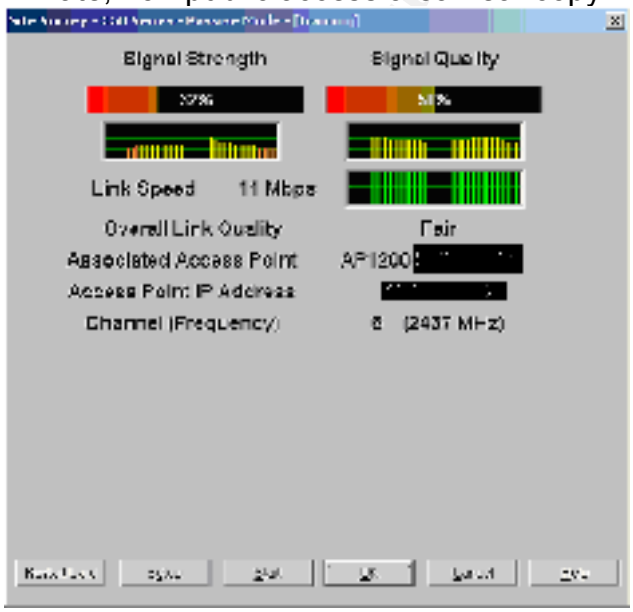


Private office area – publicly accessible, but accompanied by employee access

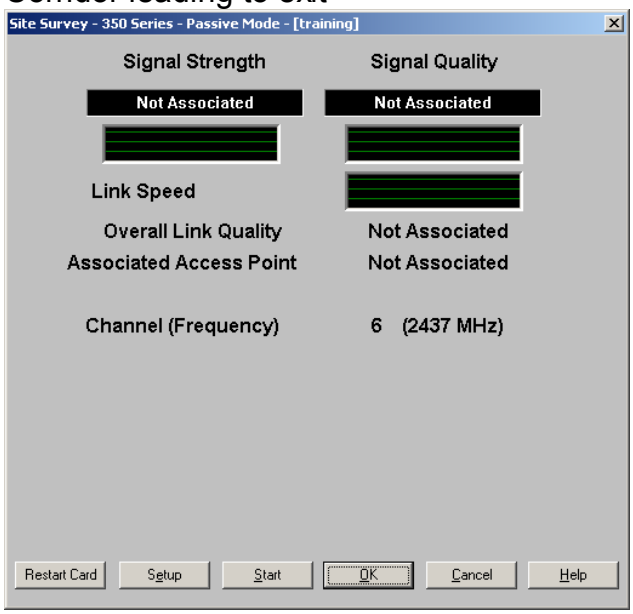
only. The public can't be alone here without drawing attention to themselves.



Private, non-public access area near copy machines

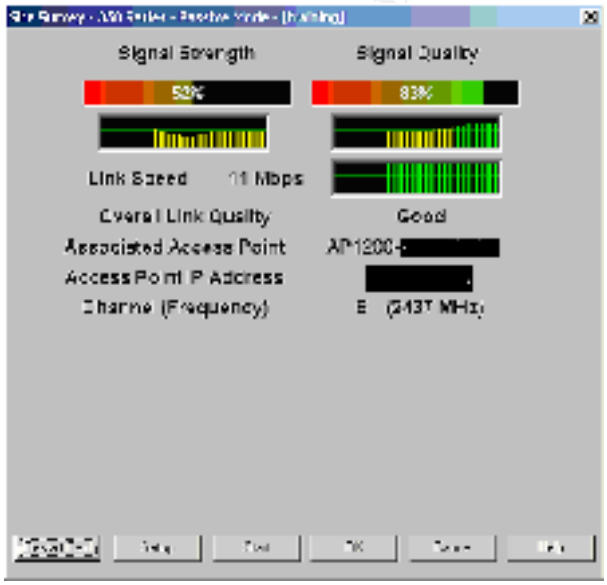


Corridor leading to exit



The entire outside perimeter of the building registered as Not Associated
The area near the front double glass door entrance also registered as Not Associated

Back downstairs about 20 feet from the AP (near the restroom)



Approximately 8 feet further away, the 350 again becomes unassociated.
Conclusion-PASS
Signal strength in the AP was configured to the lowest transmission level of 1 megawatt. In addition, the Administrator detached one antenna, leaving the AP with only one antenna. This limited the radio range of the AP. A site survey using Cisco's ACU during a thorough walkabout the building both indoors and outdoors showed that access is limited. While signal strength and quality are sometimes fair to good in publicly accessible areas, the existence of security cameras recording activity in the public areas provides a control. An additional control in those areas is provided by employee observation that limits the amount of time someone could spend in an area before arousing employees' suspicion.

Step 7 - AP powered down when not in use

Conclusion-PASS
No Policy or written procedure exists at this time regarding the Cisco AP. Policy and procedure need to be written to address the physical security of the AP. While the Administrator is very "hands on" with the AP, and accepts full responsibility for the physical access to the AP, he also understands and agrees that policies and procedures need to be developed in this area. Two different spot checks of the AP verified that it was powered off when not in use. Currently, the Administrator is the one primarily responsible for the training LAN. If another IT person is involved in setup and breakdown of the area, the Administrator emphasizes the importance of powering off the AP.

Step 8 - Default settings changed

Method

The auditor saved the configuration file currently in use by the AP. Then, with the Administrator's OK, she also saved the default configuration, preserving the IP information. (This brought the AP back to the default config, but it's easy enough to flash the saved config back to the AP) Flashing the AP back to the default while preserving the IP information ALSO preserved user information. Both admin users still existed with the same usernames and passwords that existed before flashing back to default.

Then, the auditor used Windows file compare (fc.exe) and output the differences to a text file (diff.txt), shown here:

```
Comparing files config.ini and DEFAULT.INI
***** config.ini
#===Beginning of AP1200-ABCD (Cisco 1200 Series AP 11.42T) Configuration
File===
dot11AuthenticationResponseTimeOut.2=2000
***** DEFAULT.INI
#===Beginning of AP1200-a45fff (Cisco 1200 Series AP 11.42T) Configuration
File===
dot11AuthenticationResponseTimeOut.2=2000
*****

***** config.ini
dot11PowerManagementMode.2=active
dot11DesiredSSID.2=.<edited out by auditor>
dot11OperationalRateSet.2=\x82\x84\x8b\x96
***** DEFAULT.INI
dot11PowerManagementMode.2=active
dot11DesiredSSID.2=tsunami
dot11OperationalRateSet.2=\x82\x84\x8b\x96
*****

***** config.ini
dot11AuthenticationAlgorithmsEnable.2.1=true
dot11AuthenticationAlgorithmsEnable.2.2=true
dot11AuthenticationAlgorithmsEnable.2.3=false
***** DEFAULT.INI
dot11AuthenticationAlgorithmsEnable.2.1=true
dot11AuthenticationAlgorithmsEnable.2.2=false
dot11AuthenticationAlgorithmsEnable.2.3=false
*****

***** config.ini
dot11WEPKeyMappingLength.2=0
dot11ExcludeUnencrypted.2=true
dot11RTSThreshold.2=2339
***** DEFAULT.INI
dot11WEPKeyMappingLength.2=0
dot11ExcludeUnencrypted.2=false
dot11RTSThreshold.2=2339
```

Default SSID changed

Only allow WEP encrypted traffic

```
*****

***** config.ini
dot11CurrentRxAntenna.2=diversity
dot11CurrentTxPowerLevel.2=1
dot11CurrentDwellTime.2=19
***** DEFAULT.INI
dot11CurrentRxAntenna.2=diversity
dot11CurrentTxPowerLevel.2=6
dot11CurrentDwellTime.2=19
*****

***** config.ini
sysContact=Aironet Wireless Communications, Inc.
sysName=AP1200-ABCD
sysLocation=
***** DEFAULT.INI
sysContact=Aironet Wireless Communications, Inc.
sysName=AP1200-a45fff
sysLocation=
*****

***** config.ini
dot1dTpAgingTime.0=300
dot1dStaticAllowedToGoTo.<edited out by auditor>=ffffffff
dot1dStaticAllowedToGoTo.<edited out by auditor>=ffffffff
dot1dStaticAllowedToGoTo.<edited out by auditor>=ffffffff
dot1dStaticAllowedToGoTo.<edited out by auditor>=ffffffff
dot1dStaticAllowedToGoTo.<edited out by auditor>=ffffffff
dot1dStaticAllowedToGoTo.<edited out by audi
dot1dStaticAllowedToGoTo.<edited out by aud
dot1dStaticAllowedToGoTo.<edited out by audi
dot1dStaticStatus.<edited out by auditor>=pe
dot1dStaticStatus.<edited out by auditor>=pe
dot1dStaticStatus.<edited out by auditor>=permanent
dot1dStaticStatus.<edited out by auditor>=permanent
dot1dStaticStatus.<edited out by auditor>=permanent
dot1dStaticStatus.<edited out by auditor>=permanent
dot1dStaticStatus.<edited out by auditor>=permanent
dot1dStaticStatus.<edited out by auditor>=permanent
cdpGlobalRun=T
***** DEFAULT.INI
dot1dTpAgingTime.0=300
cdpGlobalRun=T
*****

***** config.ini
enableTelnet=T
enableSNMP=T
enableDnsResolver=T
***** DEFAULT.INI
enableTelnet=T
enableSNMP=F
```

Transmit power level changed to 1 mW from default 6 mW

Only specified MAC addresses are allowed

SNMP disabled

```
enableDnsResolver=T
*****

***** config.ini
awcDot11UseAWCExtensions.2=T
awcDot11AllowAssocBroadcastSSID.2=F
awcDot11EnetEncapsulationDefault.2=encapRfc1042
***** DEFAULT.INI
awcDot11UseAWCExtensions.2=T
awcDot11AllowAssocBroadcastSSID.2=T
awcDot11EnetEncapsulationDefault.2=encapRfc1042
*****

***** config.ini
awcDot11AuthenticationRequireEAP.2.3=true
awcDot11AuthenticationDefaultUcastAllowedToGoTo.2.1=00000000
awcDot11AuthenticationDefaultUcastAllowedToGoTo.2.2=00000000
awcDot11AuthenticationDefaultUcastAllowedToGoTo.2.3=ffffffff
***** DEFAULT.INI
awcDot11AuthenticationRequireEAP.2.3=true
awcDot11AuthenticationDefaultUcastAllowedToGoTo.2.1=ffffffff
awcDot11AuthenticationDefaultUcastAllowedToGoTo.2.2=ffffffff
awcDot11AuthenticationDefaultUcastAllowedToGoTo.2.3=ffffffff
*****

***** config.ini
awcDot11AuthenticationDefaultVlanId.2.3=0
awcDot11AllowEncrypted.2=true
awcDot11LEAPUserName.2=
***** DEFAULT.INI
awcDot11AuthenticationDefaultVlanId.2.3=0
awcDot11AllowEncrypted.2=false
awcDot11LEAPUserName.2=
*****

***** config.ini
awcDot11ChanSelectEnable.2.14=T
allowBrowseWithoutLogin=F
protectLegalPage=F
***** DEFAULT.INI
awcDot11ChanSelectEnable.2.14=T
allowBrowseWithoutLogin=T
protectLegalPage=F
*****

***** config.ini
awcConsoleAutoApply=T
resolverDomainSuffix=.nothing.com
defaultResolverDomain=nothing.com
defaultResolverDomainServer.1=255.255.255.255
defaultResolverDomainServer.2=255.255.255.255
defaultResolverDomainServer.3=
***** DEFAULT.INI
```

Broadcast SSID disabled

Access to Management of AP required username/pw login

```
awcConsoleAutoApply=T
resolverDomainSuffix=
defaultResolverDomain=
defaultResolverDomainServer.1=
defaultResolverDomainServer.2=
defaultResolverDomainServer.3=
*****

***** config.ini
awcPublicVlanId=0
#===End of AP1200-ABCD Configuration File===
***** DEFAULT.INI
awcPublicVlanId=0
#===End of AP1200-a45fff Configuration File===
*****
```

Results

The output in diff.txt simplifies looking for changes from the default configuration.

The changes outlined in diff.txt include:

1-Default SSID changed
2-Allow WEP encrypted traffic
3-Transmit power level at lowest level
4-MAC filtering enabled
5-SNMP disabled
6-Broadcast SSID disabled
7-Access to http management of AP requires login

So, with a quick review, the auditor can verify these default settings have changed.

Conclusion-PASS

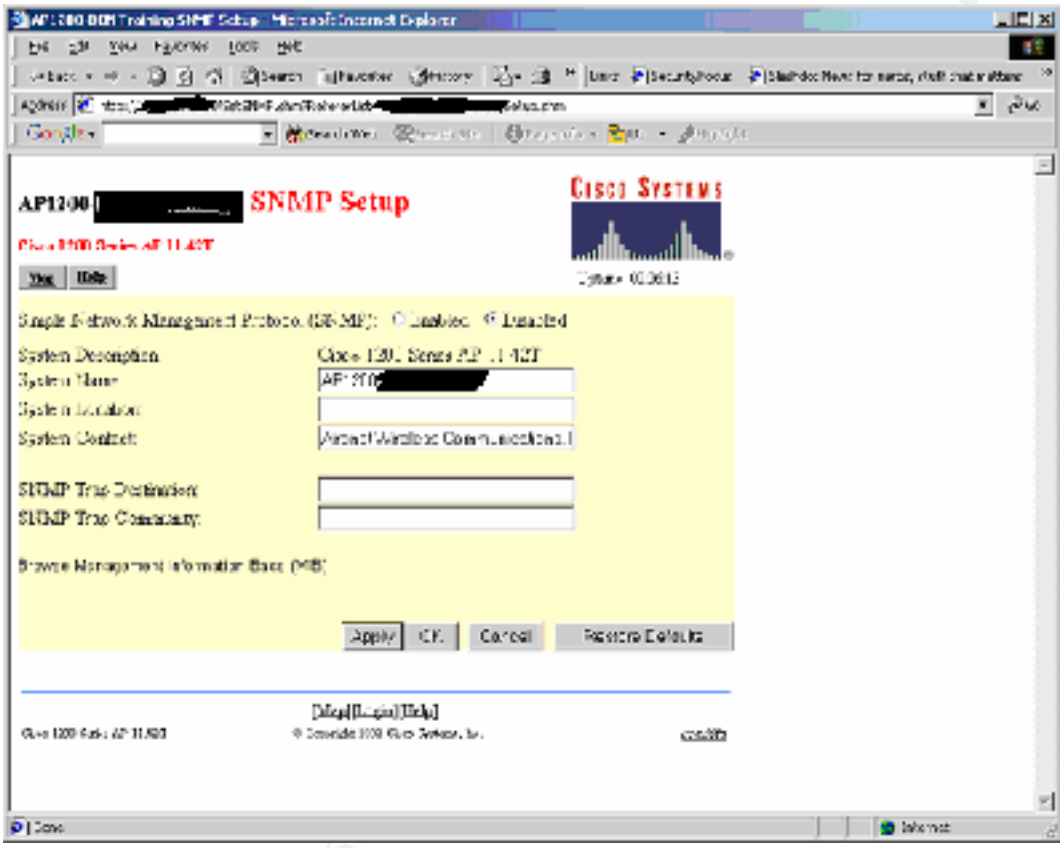
The most important default settings have changed, securing the AP according to NIST recommendations.

Step 9 - Obsolescence of technology

Conclusion-PASS

(www.informationweek.com/shared/printableArticle?doc_id=IWK20020417S0008) The Information Week article coupled with discussions between the Administrator and a CCIE who recommended the Cisco 1200 AP supports the opinion of the auditor that the purchase of this technology was made with consideration for long-term use. The AP is not consumer-grade, and can be upgraded over time.

Step 10 - SNMP management

Method
Determine whether SNMP is enabled or disabled by viewing the configuration page. If SNMP is enabled, continue with further testing.
Results
The auditor viewed the SNMP setup page in the configuration and discussed SNMP with the Administrator.    SNMP is disabled. Also, recall from Step 8 that the default settings changed, one of which was SNMP.
Conclusion-PASS
Even though much of the network is monitored via SNMP, the Administrator determined that the AP does not need SNMP monitoring because of its limited use. SNMP is disabled for the AP.

Cisco Wireless PC Card AIR-PCM350 Checklist
Step 1 - Administrative access to Aironet Client Utility

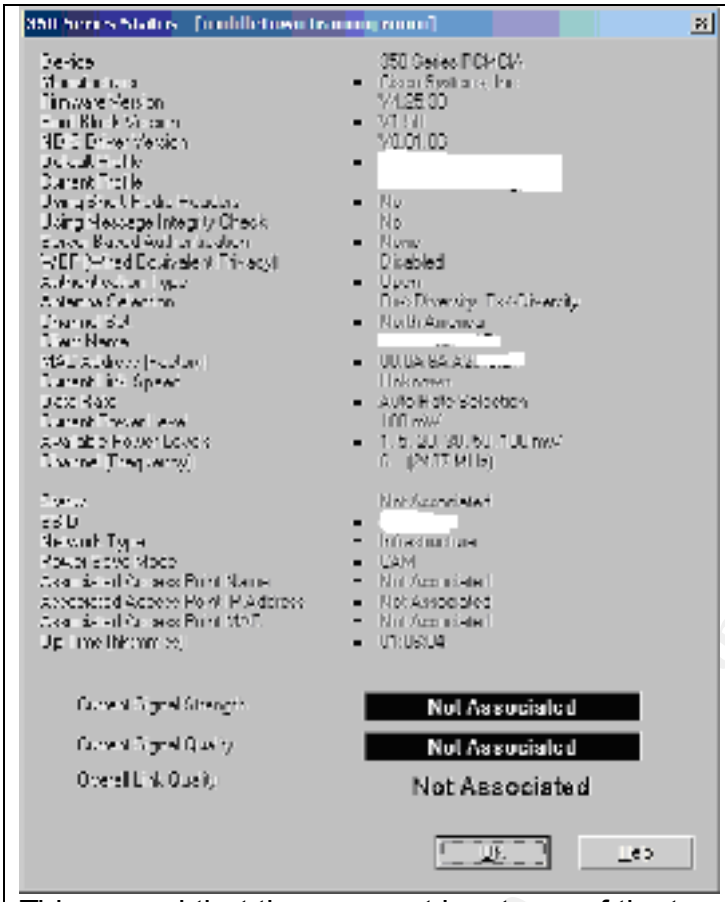
Method

In order for policy creation/modification to be disabled for a training user, the user must not have administrative or power user status on the laptop. Additionally, the Cisco Aironet Client Utility must be enabled during installation in order for rights to be restricted to administrators only. Thirdly, a box must be unchecked so that regular users cannot modify the ACU.

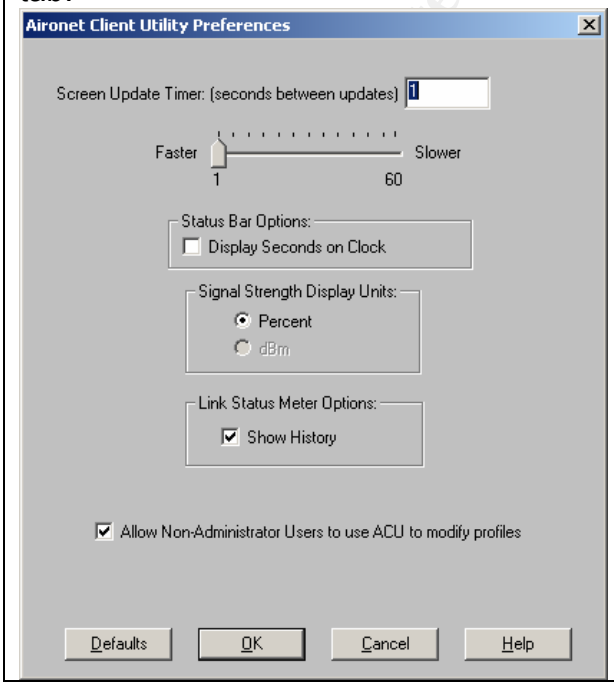
In order to verify that these three conditions are met with each of the ten training laptops, the auditor created a matrix like the one shown here:

Laptop number ID	Admin ACU access	User member of group	Aironet Client Utility Installed correctly
608	Yes	User	No
609	Yes	Power user Administrator	Yes
610	Yes	Power user	No
611	Yes	Power user	No
612	Yes	Administrator Power user	Yes
613	Yes	Administrator Power user	Yes
614	Yes	Administrator Power user	Yes
615	Yes	Power user	No
616	Yes	Power user	No
617	No	User	Yes

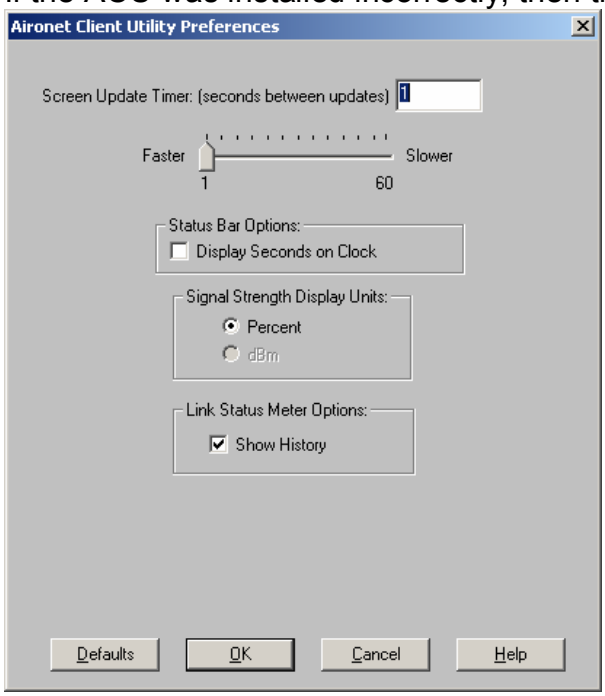
In order to prove these conditions, the auditor logged in to each laptop as the training user for that laptop. The ACU showed that the laptop was associated with the AP, then the auditor disabled WEP, and the laptop was no longer associated with the AP.



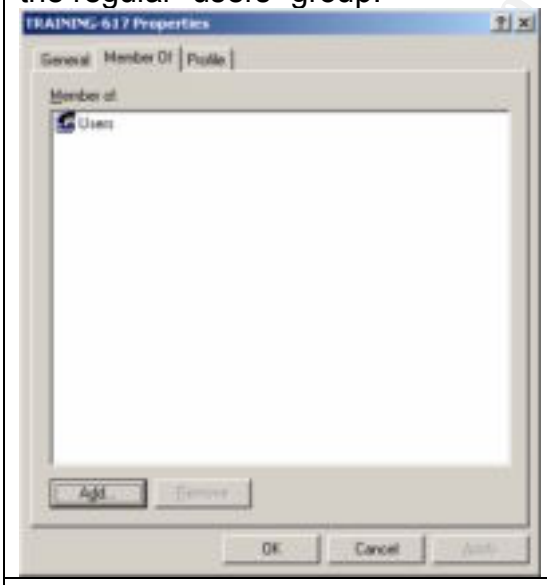
This proved that there was at least one of the two instances when regular users could modify the ACU profile. In order to verify that the software was installed correctly, the auditor looked for the checkbox to appear on the ACU preferences tab:



If the ACU was installed incorrectly, then the checkbox was not present:



Then, the auditor also confirmed which groups the training user was a member of on each laptop.
Only one was set up correctly where the training user was ONLY a member of the regular "users" group:



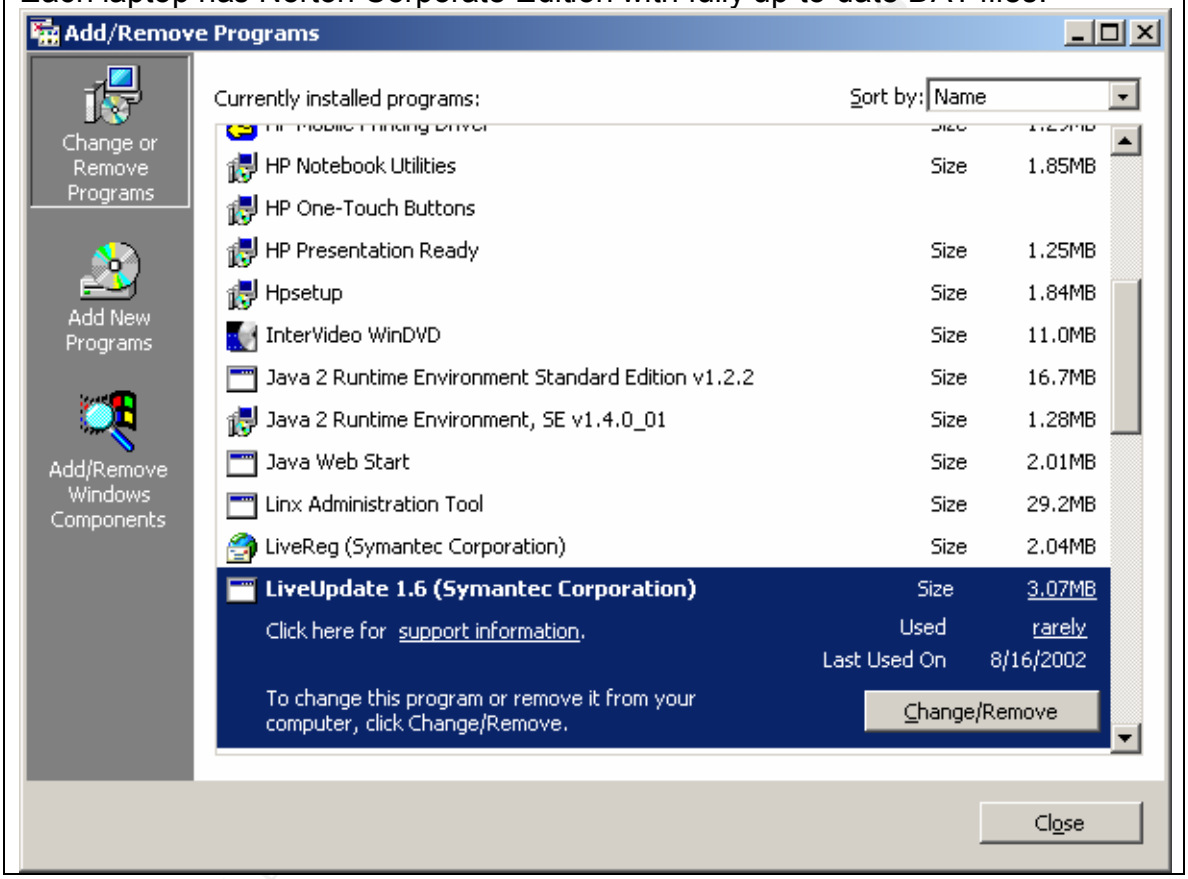
Results

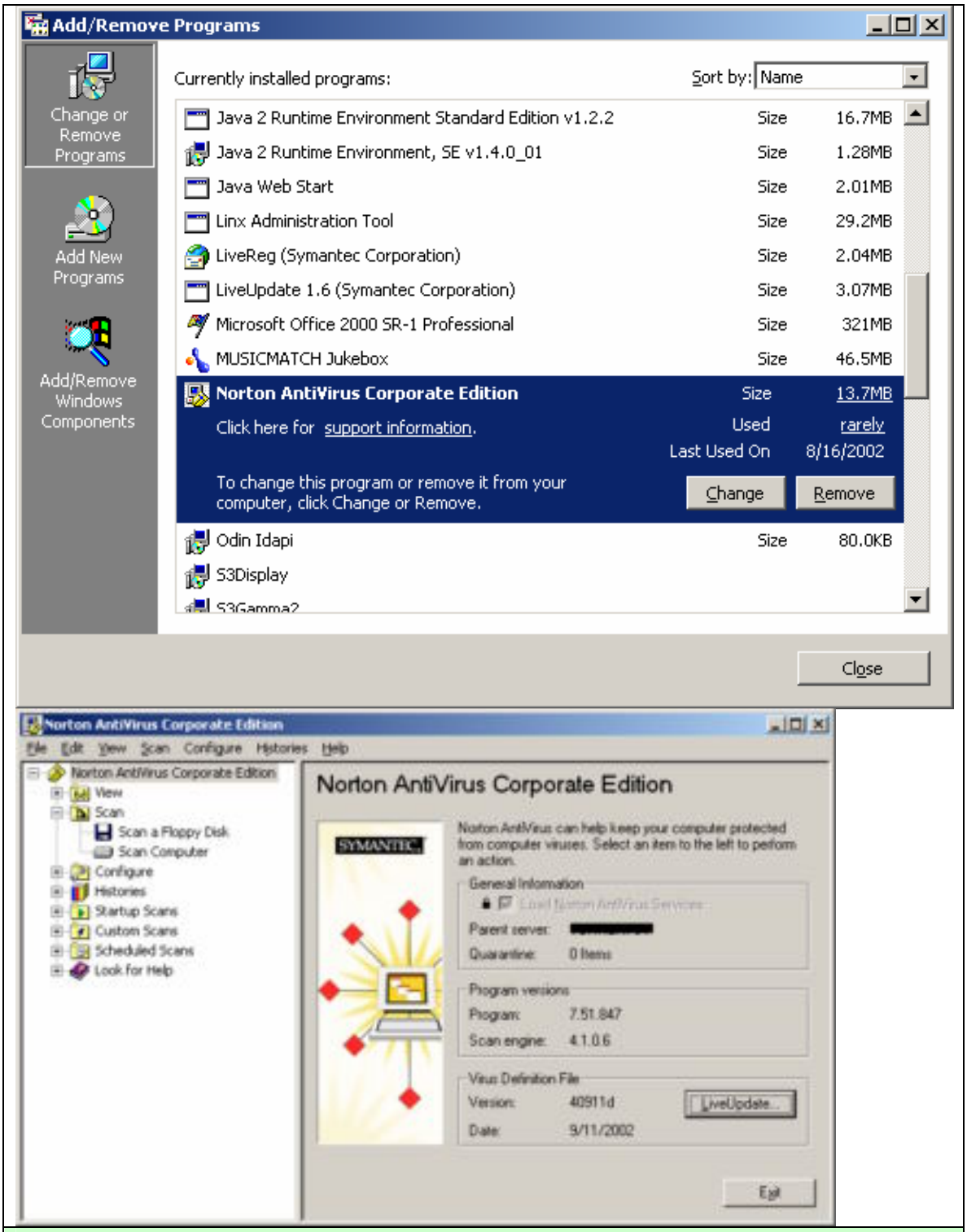
Half of the laptops' installation of the Aironet Client Utility was incorrect—the choice to make the ACU configurable by a regular user was unavailable. Most of the Training users were set up incorrectly on the laptops. All laptops except for one allowed the training users to modify the ACU profiles.

Conclusion-FAIL
The laptop setup and configuration allows the training center user to modify the Aironet Client Utility.

Step 2 - Anti-virus software

Method
Verify that anti-virus software is installed and correctly configured so that DAT files are up-to-date.
Results
Each laptop has Norton Corporate Edition with fully up-to-date DAT files.





Conclusion-PASS

A visual inspection of all the laptops verified that they have anti-virus installed correctly. All DAT files were up to date as of the date of the inspection.

Step 3 - Physical access to laptops and wireless cards

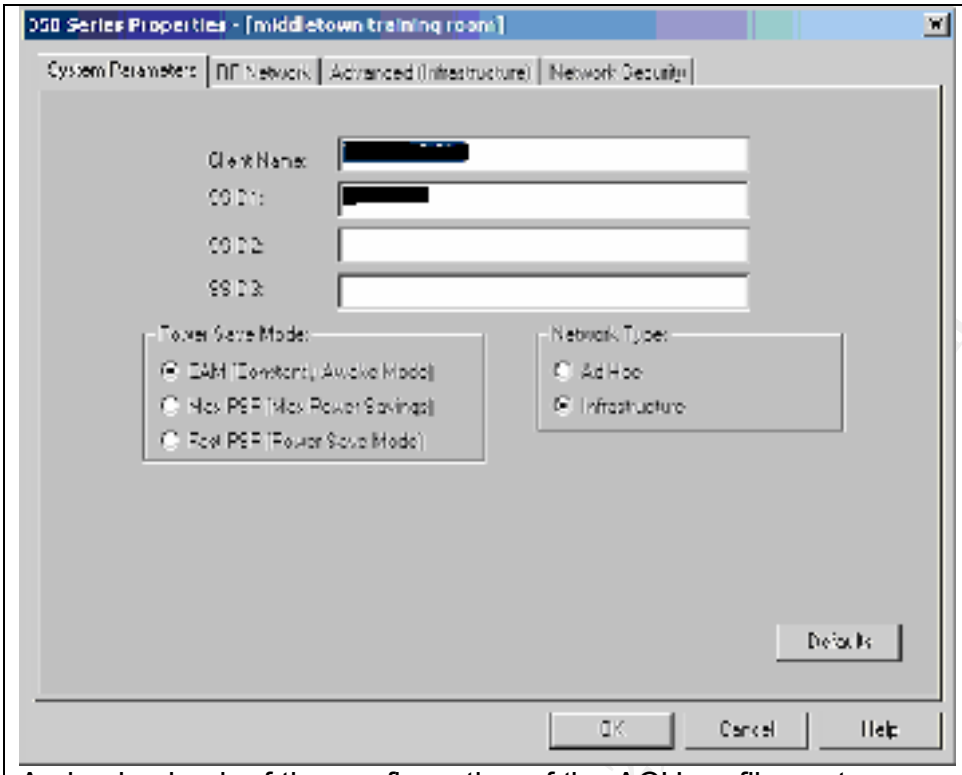
Method
The auditor looked at existing policies that cover most areas of Information Security for the organization. There were three policies that cover systems, end users, and disaster recovery. The auditor searched the text for "wireless" and "802.1*" using the CTRL-F function in Microsoft word. The auditor also spoke with the Administrator about procedures regarding the wireless training LAN.
Results
No currently board approved policies cover 802.11b or any other wireless network connections. The Administrator is developing procedures that will cover setup, storage, and security of the wireless training LAN.
Conclusion-FAIL
No Policy or written procedure exists at this time regarding the laptops and Aironet cards. Policy and procedure need to be written to address their physical security. Two IT department employees have access to the locked storage area where the laptops are kept. There are sign out procedures for use of the laptops, but not specifically in conjunction with the wireless environment. At this time, the wireless cards are not marked as "property of Company A" but the laptops are identified with company specific identity labels.

Step 4 - Obsolescence of technology

Conclusion-PASS
(www.informationweek.com/shared/printableArticle?doc_id=IWK20020417S0008) The Information Week article coupled with discussions between the Administrator and a CCIE who recommended the Cisco wireless environment including the PCM350 cards supports the opinion of the auditor that the purchase of this technology was made with consideration for long-term use. The AP is not consumer-grade, and can be upgraded over time.

Step 5 - Ad Hoc or Infrastructure mode

Method
Using Cisco's Aironet Client Utility, verify that the laptop is set up in Infrastructure mode.



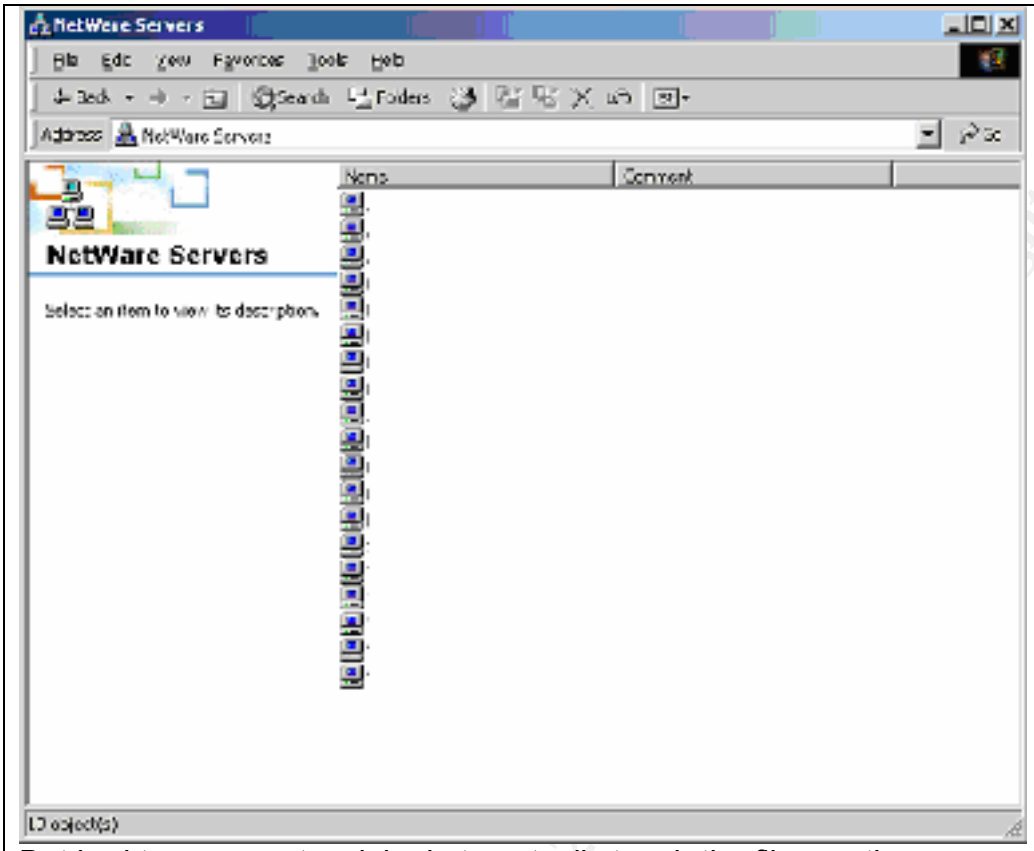
A simple check of the configuration of the ACU profile system parameters shows that a laptop is running in Infrastructure mode.

Results
All 10 laptops are configured for Infrastructure mode.
Conclusion-PASS
The laptops are running in Infrastructure mode.

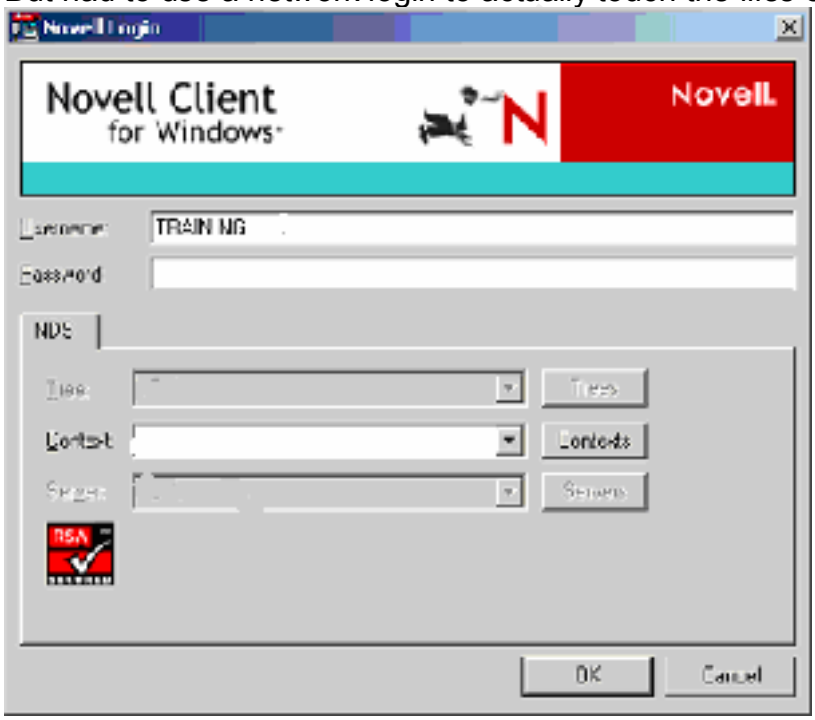
Segregation of end users in the training environment Checklist

Step 1 - Segregation by IP address

Method
A firewall between the AP and the trusted network would provide a means to segregate traffic from the WAN. Is a firewall part of the Training LAN setup? If no firewall is in place, is the AP plugged directly into a switch rather than a hub? The auditor observed that the AP is plugged directly into a switch, and even pulls power from the switch. Do the training end users have limited accounts on the network? See how training users login-is it locally or on the network. The auditor logged in as a training user and attempted to access files on the WAN. Access was denied for all resources—the auditor could see all the servers in a browse session



But had to use a network login to actually touch the files on the servers.



The auditor COULD share data between the training laptops as a “workgroup” LAN.

Results

No firewall is in place at this time. The AP is directly connected to a switch. End users log on locally rather than authenticating to the Novell network. Training users do not exist in the Novell network at all, and consequently have absolutely no rights on the network as a Training user.
Conclusion-PASS
While no firewall is in place, the other criteria for this step were met. Additionally, training users are not able to access corporate or customer data by network browsing from the training LAN as a training user.

Summary table
This table provides an overview of audit findings

Audit section	Audit step	Audit outcome
Cisco Aironet 1200 Access Point	Step 1 - Policy for wireless training LAN	FAIL
	Step 2 - Administrative access to AP	PASS
	Step 3 - AP Security settings	PASS
	Step 4 - Key length and use	PASS
	Step 5 - Physical access to AP	FAIL
	Step 6 - Wireless "perimeter" site survey- signal strength and security	PASS
	Step 7 - AP powered down when not in use	PASS
	Step 8 - Default settings changed	PASS
	Step 9 - Obsolescence of technology	PASS
	Step 10 - SNMP management	PASS
Cisco Wireless PC Card AIR-PCM350	Step 1 - Administrative access to Aironet Client Utility	FAIL
	Step 2 - Anti-virus software	PASS
	Step 3 - Physical access to laptops and wireless cards	FAIL
	Step 4 - Obsolescence of	PASS

	technology	
	Step 5 - Ad Hoc or Infrastructure mode	PASS
Segregation of end users in the training environment	Step 1 - Segregation by IP address	PASS

Is the system securable?

Because this wireless LAN environment is not used continuously, it presents an easier environment to secure. While consideration must be given to opportunities available for unauthorized individuals to crack WEP, the SSID, and ultimately compromise the corporate WAN; actually, these high level risks are abated significantly because the wireless LAN will only be operating sporadically. The Administrator's and the Auditor's biggest concerns were the risks associated with cracking the network wirelessly.

After evaluating the wireless training environment, it is the auditor's opinion that this environment can be secured, but some improvement will have to be made. The checklist brought to light the fact that specifically outlined policies and procedures have not been created for this wireless LAN. Because the Administrator will delegate setup and breakdown of the LAN, the Administrator needs to develop specific procedures so that the wireless LAN operates correctly. Specific sign out procedures and storage procedures will also mitigate physical risk to the systems.

Policy and procedure development coupled with training for the IT department in those policies and procedures will cost only in hours. The Auditor estimates a week for the development of the policies and procedures, with a training session of less than an hour for the IT department.

A significant finding during the audit was the misconfiguration of the laptops. Not only was the Aironet Client Utility installed incorrectly on many of the laptops, but also the training users were given Administrative and Power User rights. Even if the ACU had been installed correctly, many users would have had rights to change the profiles.

Again, this will cost only time to clear up. It shouldn't take much longer than 2 hours for all 10 laptops to be set up correctly. That's an estimate including changing the groups for the training users, uninstalling and reinstalling the ACU, and configuring the ACU profiles.

Finally, the NIST standards and common security practice suggest the use of a firewall between the AP and the local network. In the training LAN, a firewall would deny anything except http and https traffic through to the Internet across the corporate WAN. While the security of "Location A" was sufficiently proven in regards to cracking the wireless link, the objective of segregating the training traffic wasn't fully met.

The Administrator places a high priority on preserving the portability of the training environment. This would preclude the implementation of a "desktop box" firewall. However, a small, portable firewall like the Netscreen-5 would certainly meet both the firewall and portability needs for the training LAN. The Netscreen-

5 is generally between $500-$700. If the Administrator takes into account that the training LAN itself (laptops, AP, and wireless cards) cost around $16,000, then the cost of the firewall is only 3% or 4% of the cost of the training center.

Is the system auditable?

Each component of the wireless training LAN is auditable. Taken together as a whole, the training LAN environment is auditable. The checklists addressed specific system and configuration issues as thoroughly as possible to mitigate the risk of unauthorized wireless access.

The specific hardware within the environment is most definitely auditable. The NIST checklist defined specific objectives with a wireless network. By auditing more than just the Cisco Access Point, the auditor provided a more thorough audit of the entire wireless LAN. An audit of the AP alone would not have uncovered the issues with the training laptops. But does the audit of just the systems themselves really "certify" a classroom for use as a wireless training area?

While the auditor's objective was to "certify" a setting for training, so much more is involved other than just making sure that the wireless radio waves won't be available outside the physical building.

What became clear during the audit was that a deeper examination of the training users must occur. Over time, how will the systems be used? The assumption made by the auditor throughout this audit was that only corporate employees would be trained on these laptops in this environment. What if that is not the case?

Not only must the IT department, who is responsible for setup and breakdown of the classroom, adhere to policies and procedures to mitigate risk, but also consideration must be given to the people sitting at the laptops for the training classes. Shouldn't they also be briefly instructed on wireless security at the start of their training session? And how would that be audited?

One area within the audit that lacked more technical substantiation was in the very last section, **Segregation of users in the training environment.** The checklist developed for this area was vague, even though the objective was clearly stated. The auditor discovered during the audit that the training users would log on locally to the laptops. Also, since no firewall is in place between the corporate WAN and the wireless training LAN, extensive testing would be required to sufficiently prove that the training users did not have access to corporate servers. In addition, it is the opinion of the Administrator that training users should be able to access their email while in training, which would be

opposed to the opinion of the auditor that the traffic remains fully segregated from the corporate network.
The tools available with the Cisco ACU were sufficient to discover the wireless AP's range. Signal strength and signal quality were easily seen, and the site survey function kept communication open until the auditor was out of range. The auditor was originally intending to use Netstumbler, but after reading more specifics, found that Netstumbler does not support the Cisco card. Down the road, the auditor is budgeting for hardware that will be supported, so that while training sessions are meeting the auditor can again verify the range of wireless for that specific training location.

After the audit of the Cisco Aironet AP was completed, the auditor was curious about the difference between "open" or "shared" authentication with WEP. At first glance, it appears "shared" would be more secure than "open" – the auditor based her interpretation on the common definition of the two words. So the auditor consulted the configuration guide. Because of this further reading, the auditor determined that ONLY "open" authentication should be enabled. "Shared" authentication should not be enabled because it is actually LESS secure than open authentication.

From the configuration guide:

> "Cisco recommends Open authentication as preferable to Shared Key authentication. The challenge queries and responses used in Shared Key leave the access point particularly vulnerable to intruders."

This additional check should be included in Audit Step 4- Key length and use to verify that only OPEN AUTHENTICATION should be used.

Assignment 4

Executive Summary

The wireless training center recently approved by XYZ Company's Technology Risk Committee was audited by XYZ Company's Internal Audit Department in late August 2002 This pre-implementation audit examined the wireless environment, the risks inherent in wireless networks, and the risks specific to XYZ Company in installing and operating the wireless training center.

We found the overall security of the wireless training center to be satisfactory.

Risks that can arise for a wireless network include the possibility of unauthorized persons connecting via the wireless access point. The most significant risks to XYZ Company revolve around the insecurity of wireless—and the auditor concludes that these risks have been significantly mitigated by proper configuration and deployment of the Cisco 1200 Access Point.

The weaknesses discovered in the audit are mostly related to the absence of current written policies and procedures regarding the wireless training network. Another important audit finding was specific to the training center laptops' configuration.

The audit process used to evaluate the wireless network and specifically the XYZ Company Training Room A can also be used to certify the security of other potential training locations. As such, the site certification process should be implemented as policy so that new training sites can be identified and certified before their use as training rooms.

Audit Findings

The audit of the training environment consisted of a thorough examination of the Cisco wireless access point that provides a bridge to XYZ's wired network. It also included a close examination of the laptops that will be used for the training. Additionally, the audit examined how the training users would be segregated from XYZ's corporate network to prevent unauthorized access to corporate and customer data.

The auditor discussed the configuration of the access point with XYZ's Administrator, and examined the configuration in detail. The auditor verified from viewing the configuration that the access point's SSID had been changed from the manufacturer's default, and that the "broadcast SSID" had been disabled. The auditor also verified that the encryption level for access through the AP had been set to 128-bit encryption, and the key selection was random and changed periodically. (Please reference Access Point Audit steps 3 and 4)

The auditor used the Cisco Site Survey tool to complete a thorough survey of signal strength and quality for training location A. Signal strength was set so that the auditor was not able to detect a signal outside the perimeter of the building. In some public areas of location A, signal strength and quality is enough to permit use of wireless connections. (Please review Access Point Step 6 in the full report to reference signal strength and quality in building A) A mitigating factor for those areas includes the installed security cameras coupled with the presence of XYZ employees. It is unlikely that a successful attempt to access the wireless network would go undetected in those areas.

Policies and procedures regarding the wireless network are still in development. There are no written policies and procedures outlining the set up and use of the wireless training environment. (Reference Access Point Audit steps 1, 5, 8, and Wireless Card step 3)

The laptops for use in the training center and the configuration of those laptops are key to the security of the wireless training environment. Administrators should be the only people who can modify the Aironet Client Utility—in this case the auditor discovered that most of the regular training users could modify the profile settings. Training users could create a network vulnerability if they modified the client utility. Also, by modifying the client utility, a training user could break the connection with the access point, which could impact them negatively during a training session. (Reference Wireless Card Step 1)

All laptops have correctly configured Anti-virus software installed. Other settings within the Client Utility have been correctly configured which also mitigates risk. (Please refer to Wireless Card Steps 2 and 5)

Finally, the auditor examined how the training users access the training network. The training users do not have any rights to the corporate network. However, if someone in a class logged in as themselves rather than the training user, then they have their normal network rights on XYZ's Novell network. (Please refer to Segregation of Users Step 1)

Background/Risk

The technology of wireless is still evolving. Much has been written about the insecurities of wireless—there are many tools that could be used to break into a wireless connection. In this case, the wireless access will not be used every day. The training network will be locked in a cabinet when not in use. The fact that the wireless access point will generally be used for short periods rather than left on at all times significantly mitigates the risk of unauthorized access.

Because the wireless signal can be detected in public areas at the building where the training room is located, other compensating controls on unauthorized wireless access will deter that access at training room A. Again, the presence of security cameras coupled with employee awareness will deter an unauthorized person from sitting for long periods of time attempting to crack XYZ Company's wireless setup. Because the training will take place in a basement training room, the wireless signal is not even detectable outside the building. Only people with prior knowledge of the wireless environment would even know to attempt access during a training session.

Because the Aironet Client Utility is installed incorrectly on many of the laptops, and because the training users are members of Power Users and Administrators in some cases, the risk is that a regular training user could modify the profile. This could result in the laptop losing communication with the Access Point. The risk evident here is that training would be interrupted or even halted until the ACU was configured correctly. This could take a great deal of time – a training user may not even be aware of what they changed.

Also, if the training user changed the mode from Infrastructure mode to Ad Hoc mode, the laptop will try to associate directly with other wireless connections rather that through the Access Point. By associating directly with other wireless laptop connections, there is a chance that the training user could associate with an unauthorized user. Then, the unauthorized user may be able to glean information that could lead to the compromise of confidential information.

The training users' access itself poses some risk. Training users should not log on to the training laptops using their regular network logon. When at a class session, they should not access any confidential information—information could possibly be "left" on the training laptop. People could open a document, and save a copy locally without realizing they had done so. The next training user to log in could very well have access to that information. Because there is no firewall between the training environment and the corporate network, there is no means to clearly define and limit the type of access through the corporate network. A firewall could be set to specifically outline what type of network traffic is allowed. Additionally, VPN connections (Virtual Private Network-encrypted connections from the laptops to the firewall using software on each laptop) from the laptops to the firewall would add another layer of security by adding additional encryption over the wireless connections.

Because no policies and corresponding procedures have been clearly written yet, the organization is at some risk. Policies and procedures lay the groundwork for securing not only the technology, but also the users' behavior. People who have received training in the policy and procedures regarding the wireless training network would be more apt to recognize configuration issue. They would also know the risks involved in implementing wireless, so they would be more likely to

safely operate and store the training room equipment. This, in turn, would certainly help to deter unauthorized access.

The hardware that was purchased for the wireless training environment is a good investment that can be upgraded in the future. It is a business class system that should prove useful over many years. (See Access Point Audit step 10, and Wireless Card step 4)

Audit Recommendations

First, a clearly written policy that addresses wireless needs to be developed. From that policy, procedures that outline specifics such as secure operation and storage of the wireless training network should be written. Accordingly, anyone who will be authorized to set up the training network should receive training in these newly developed policies and procedures.

For the laptops, the Aironet Client Utility should be installed so that only an administrator can modify the profiles. Training users should be associated to groups that do not allow them to modify the profiles.

Finally, Company XYZ should consider implementing a firewall between the wireless network and their corporate network. The firewall would serve to clearly define the traffic allowed from the training network over the corporate network. Company XYZ could also consider implementing VPN technology to further secure the wireless environment.

Costs

The firewall would be the only direct costs associated with our audit recommendations. For less than $800, a Netscreen-5 firewall would be portable and easily configurable for securing the wireless training network.

Other recommendations require time alone; an estimate for reconfiguring the laptop users and the Aironet Client Utility on those laptops is less than 3 hours.

Consider approximately 1 week for writing policies and procedures.

Compensating Controls

If Company XYZ decides to forego purchasing a small firewall, the risk of unauthorized access via wireless is mitigated somewhat by the correct configuration of the Access Point. As described in Access Point Audit step 3, three factors must be correct in order to associate with the Access Point. The SSID must be correct, the WEP key must match, and the client's MAC address

must also be entered into the "Allowed" field in the Access Point's configuration settings. Testing during step 3 proved this to be true.

Clear and effective communication between the members of the IT department and to any training users may compensate for the absence of policy and procedure. However, Internal Audit does not recognize any clearly defined compensating controls for this area.

References

Karygiannis, Tom & Les Owens. "DRAFT- Wireless Network Security- 802.11, Bluetooth™ and Handheld Devices." Special Publication 800-48, National Institute of Standards and Technology, July 2002. (August 2002)
URL:http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf

"Cisco Aironet 1200 Series Access Point Software Configuration Guide." Software Release 11.41T. April 2002.

"Cisco Release Notes for Cisco Aironet Client Utilities, Version 5.01.001 for Windows" c. 2001

"Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows" OL-1394-03. c.2001

"Cisco Aironet Wireless LAN Security Overview" undated white paper 8/2002.
URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

Convery, Sean and Darrin Miller. "SAFE: Wireless LAN Security in Depth" undated Cisco white paper. 8/2002
URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

Gonsalves, Antone. "Cisco's Vision of a Wireless Future" InformationWeek. April 17, 2002.
URL: http://www.informationweek.com/story/IWK20020417S0008

Arbaugh, William A. & Narendar Shankar, Y.C. Justin Wan. "Your 802.11 Wireless Network has No Clothes" Department of Computer Science, University of Maryland. March 30, 2001. (8/2002)
URL: http://www.cs.umd.edu/~waa/wireless.pdf

Snyder, Joel. “Securing the wireless LAN.” Network World/ Computerworld. August 12, 2002.
URL: http://computerworld.com/mobiletopics/mobile/technology/story/0,10801,73421,00.html

Brewin, Bob. “Tools for detecting rogue wireless LAN users.” Computerworld. July 15, 2002.
URL: http://www.computerworld.com/securitytopics/security/story/0,10801,72601,00.html

Sutton, Michael. “Hackers user Wi-Fi invisibility cloak.” Tech Update, ZDNet UK. July 25, 2002.
URL: http://techupdate.zdnet.co.uk/story/0,,t481-s2119788-p2,00.html

Trudeau, Garry. “Doonesbury.” July 21, 2002
http://www.doonesbury.com/strip/dailydose/index.cfm?uc_full_date=20020721&uc_comic=db&uc_daction=X