Global Information Assurance Certification Paper

Auditing the Cisco Aironet 1200 Wireless Access Point In a Small to Medium Size Business Environment (SMB)

An Auditor's Perspective
GSNA Practical Assignment v2.1 (Option 1)

Ryan Lowdermilk
October 10, 2003

ABSTRACT / SUMMARY

The purpose of this paper is to meet one of two requirements needed to achieve the GSNA certification. The device being audited is the Cisco Aironet 1200 Wireless Access Point. The device is being audited for the ACME Company in regards to wireless security. The ACME Company would like to assess the risk the device poses upon their company network; mainly their company data. This audit will assess the Cisco Aironet 1200 Wireless Access Point in the areas of industry "best practices" for wireless security, factory-default settings, and company policy/procedures.

TABLE OF CONTENTS

Section 1- Research in Audit, Measurement Practice, and Control

Section 1.1 - Audited Device

The device being audited is a Cisco Aironet 1200 Wireless Access Point (CISCO1200AP) as shown in Figure 1.1-1 and Figure 1.1-2. The CISCO1200AP provides Wireless Local Area Network (WLAN) connectivity and coverage to wireless devices compliant with IEEE 802.11a and 802.11b standards. The model being audited is an AIR-AP1230B-x-K9 running Cisco IOS Software version 12.2(8)JA.

Figure 1.1-1 – Cisco Aironet 1200 Wireless Access Point

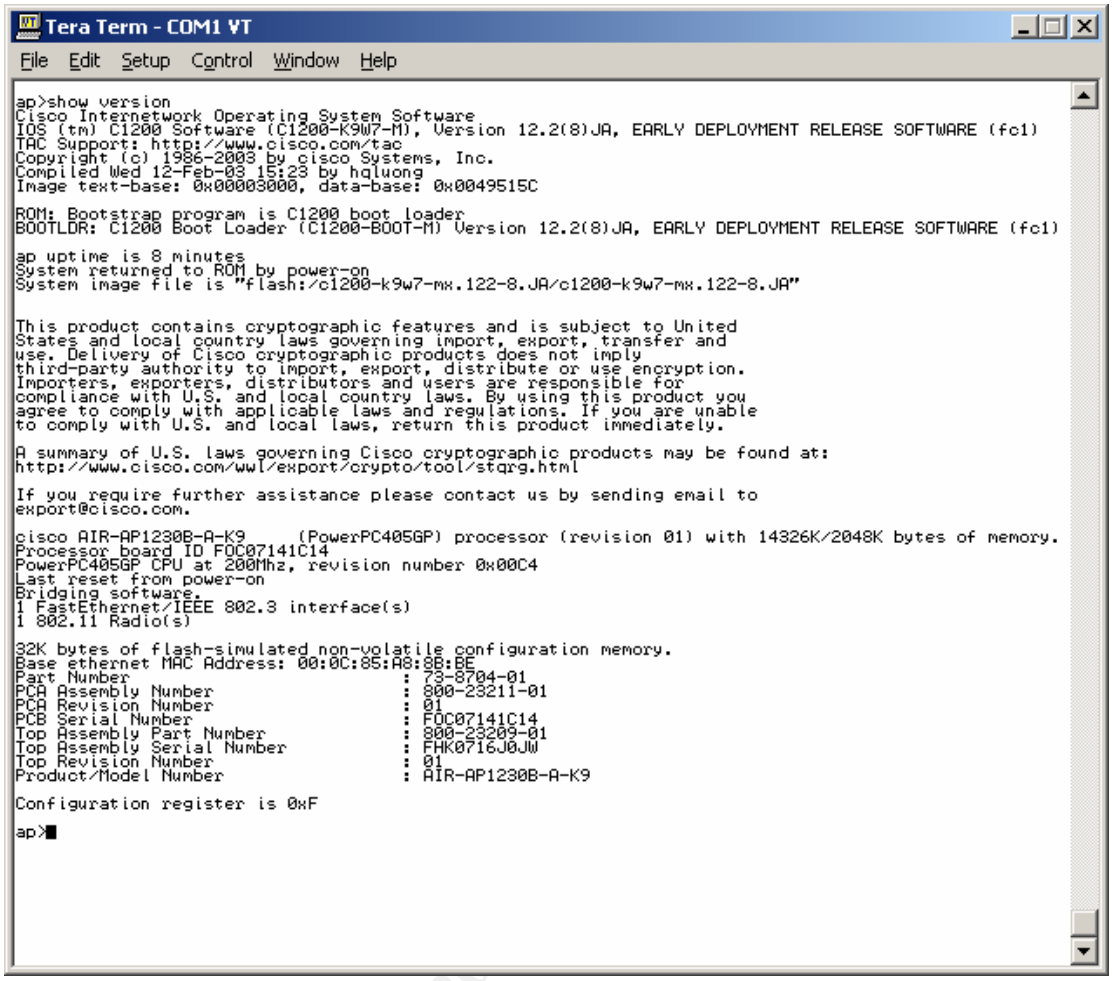

Figure 1.1-2 – '*show version*' command from CISCO1200AP

The CISCO1200AP provides wireless communication by way of exchangeable radio modules. The CISCO1200AP design is unique in that it can support two radio modules in "dual mode." Dual mode allows the CISCO1200AP to provide connectivity for two radio types concurrently. As of the date of this document, the CISCO1200AP can accept two radio module types, 802.11a and 802.11b. However, Cisco has announced that the CISCO1200AP will support newer standards as they are finalized; such as 802.11g and 802.11i. This paper will be limited to the 802.11b spectrum and radio module.

The ACME Company is a small business with 30-40 employees. The ACME Company develops custom applications for casinos and smaller gaming venues. Their location is on the 6th floor of a 12 story building located in the business district of downtown Atlanta.

The role of this device, within the ACME Company, is to provide the programming department with "wire free" access to the company network and Internet. This will allow the programmers to work and collaborate from anywhere

on the 6th floor e.g. lunch room, conference room, etc. ACME management feels this will help with productivity.

Section 1.2- Evaluated Risk of Audited Device

The CISCO1200AP is being audited because of the recent rise in attacks, exploits, awareness and security breaches concerning wireless technologies. If the CISCO1200AP is compromised the possibility of an attacker accessing the company network and obtaining, modifying, or destroy company data is highly possible. For this reason ACME Company has placed specific concern as to the level risk of the CISCO1200AP poses.

Several variables are defined when measuring risk; vulnerability, threat, risk, confidentiality, integrity and availability. Vulnerability can be considered an area of weakness in a system or device. As a system or device contains vulnerabilities it becomes susceptible to threats. Threats are considered to be leveraged activity that preys upon weaknesses or vulnerabilities. Risk is defined as the product of vulnerability and threat. With a high level of vulnerability and threat, the level of risk that exists is high. Risk can be defined as the overall impact of a particular threat leveraging a particular vulnerability.

Confidentiality, Integrity and Availability (CIA) are three areas that security can be broken down into to encompass and overall security posture. Confidentiality is the effort in which information should not be disclosed to unauthorized personal. Integrity is the effort of protect data in its original form. Availability is ability to provide information as needed. As these areas are affected, security as a whole is affected. CIA is extremely effective when measuring various security levels.

Below are the areas addressed in this audit. In each area, information pertaining to each of the above categories: vulnerability, threat, risk and CIA are briefly explained.

- Physical access to the CISCO1200AP
  - Vulnerability
    - Theft, defacement, damage, Denial of Service (DoS), etc.
  - Threat
    - Could lead to downtime, loss of money, etc.
  - Risk
    - With the ability to physically access the CISCO1200AP a wide array of malicious threats become a factor.
  - CIA
    - Confidentiality
      - None
    - Integrity
      - If the CISCO1200AP is stolen, configuration information could be taken from the device e.g.

(internal network configurations, authentication methods, etc.)
        - Availability
            - With damage to the physical or configurationally aspects of the CISCO1200AP, severe downtime could become a factor as replacement parts, re-configuration, etc. are waited upon.
    - Probability
        - Because the ACME Company does not operate in a heavy traffic environment e.g. warehouse, open air marketplace, etc.) the threat is unlikely.

- Discovery of the CISCO1200AP
    - Vulnerability
        - Knowledge of the CISCO1200AP
    - Threat
        - Could possibly become an attack vector
    - Risk
        - With knowledge of the CISCO1200AP existing on the ACME company network an attacker could mark the CISCO1200AP as an attack target
    - CIA
        - Confidentiality
            - Knowledge of a company's information infrastructure
        - Integrity
            - None
        - Availability
            - None
    - Probability
        - Due to the fact that the ACME Company is located in business district of downtown Atlanta, there is a good chance that attackers using wireless scanning software could detect the CISCO1200AP

- Illegal access to the company network via the CISCO1200AP
    - Vulnerability
        - A poorly configured CISCO1200AP with no changes made to the factory defaults, no technical control objectives in regards to wireless security e.g. WEP, MAC filtering, authentication, etc.
    - Threat
        - Illegal access to company network and Internet
    - Risk
        - Malicious intent. Once illegal company network or Internet access is gained e.g. deletion, modification, exportation of company data, attacks on Internet hosts, etc.

- CIA
  - Confidentiality
    - If company data were to be exported, viewed, etc. the confidentiality of that data would be severally effected.
  - Integrity
    - If company data was modified the integrity of company data would be severally effected.
  - Availability
    - With illegal access to the company network and Internet, an attacker could affect availability by causing network congestion, launching network based attacks, such as, ARP spoofing, MAC flooding, etc.
- Probability
  - Because most wireless based attacks are aimed to expose this threat, it is a good possibility that an attack of this nature could happen.

- Compromised client device communications to and from the CISCO1200AP
  - Vulnerability
    - Unprotected data transferring to and from client devices to and from the CISCO1200AP.
  - Threat
    - Compromised client device data transmissions, such as usernames, passwords, etc
  - Risk
    - Compromised company information such as usernames, passwords, email, etc. Leveraging access to company data with captured usernames and password, etc.
  - CIA
    - Confidentiality
      - If an attacker captured a valid username and password, company data could be modified, deleted, exported, viewed, etc.
    - Integrity
      - It is possible for an attacker to modify the data in transit to cause unexpected results
    - Availability
      - None
  - Probability
    - Because the physical nature of wireless communication is susceptible to attack, in that it transfers over open air, the probability of this is great if control objectives have not been put in place.

Below is a risk matrix providing a summary in the areas of threat, vulnerability, risk, and confidentiality, integrity and availability (CIA) as it relates to the level of risk the CISCO1200AP poses on the ACME Company.

Vulnerability	Threat	CIA	Risk	Probability
Physical access gained to the CISCO1200AP	Damage, configuration changes, DoS, etc	Confidentiality: None Integrity: Low Availability: High	LOW	LOW
Knowledge that the CISCO1200AP exists	Becomes a possible attack vector	Confidentiality: Low Integrity: None Availability: None	LOW	MEDIUM
Poorly configured CISCO1200AP with no changes made from the factory defaults. Industry best practices not implemented.	Illegal access to the company network or Internet via the CISCO1200AP	Confidentiality: High Integrity: High Availability: Medium	HIGH	HIGH
Unprotected data transferring to and from client devices to and from the CISCO1200AP.	Compromised client device data transmissions, such as usernames, passwords, etc	Confidentiality: High Integrity: High Availability: None	HIGH	HIGH

At the time of this audit there were no “special” risks of particular concern in regards to the CISCO1200AP.

The scope of this audit is to verify that the CISCO1200AP factory defaults have changed as it relates to wireless security. Also, that the configuration of CISCO1200AP has followed industry “best practices” as it relates to wireless security.

Note: This paper will not cover security control objectives such as Guest hotspots, VLANS, TKIP, LEAP, EAP and/or multiple SSIDs, as they are beyond the scope of this paper.

Section 1.3- Current Practice for Audited Device

Section 1.3.1- Securing the CISCO1200AP
The recent rise of consumer and company interest in wireless technology has resulted in various whitepapers, how-to's, and do's and dont's in regards to wireless security. Most articles, whitepapers, etc. deal with consumer products such as Linksys, D-Link, etc. Because most consumer products boast security features, the guidelines are of some use in regards to the CISCO1200AP. As this is the case, the current state of practice in securing the CISCO1200AP is to use wireless security "best practices" and recommendations from vendor documentation.

Section 1.3.2- Auditing the CISCO1200AP
In regards to auditing the CISCO1200AP two audit guides exist. Ryan Stall's paper outlines the steps to take when auditing a CISCO1200AP in a corporate environment. Oliver Viitamaki's paper provides steps to be taken when auditing a CISCO1200AP in a demonstration network. Both papers are great resources for building sound audit strategy.

Section 1.3.3- Processes and Procedural Checks for the CISCO1200AP
In regards to processes and/or procedural checks for the CISCO1200AP, practices used for devices such as routers, switches, etc. can be. Procedures such as configuration maintenance and backup, upgrade paths, hot fix and patch management can be put in place to ensure that the CISCO1200AP continues to operate in a secure fashion.

Section 1.3.4- Research and References
In researching for this audit, resources such as Google (www.google.com), reading vendor documentation, third-party articles, and experience was used.

Below is a list of keywords used on Google (www.google.com) to search out documentation for the CISCO1200AP as it relates to wireless security.

cisco.aironet 1200
cisco 1200 banner
aironet site:sans.org
best.practices wireless
cisco.aironet site:cisco.com
wep wireless
aironet best.practices
aironet audit
cisco wireless security

Google was found to be extremely helpful in narrowing down Internet content in regards to wireless security.

Below are references used during the audit. Following each listed reference is a brief description

Stall, Ryan. “Auditing a Cisco Aironet Wireless Network from an Auditors Perspective”
January 2003
URL: http://www.giac.org/practical/GSNA/Ryan_Stall_GSNA.pdf

Viitamaki, Oliver. “An Audit of a Wireless Demonstration Network Implementing Cisco Aironet 1200”
December 2002
URL: http://www.giac.org/practical/GSNA/Oliver_Viitamaki_GSNA.pdf

These two papers were very helpful in understanding what has been done thus far to audit the CISCO1200AP.

Lubow, Eric. “Six Basic Tips to Securing Wireless Network”
December 2002
URL: http://www.linuxsecurity.com/articles/documentation_article-6346.html

This article was found to be helpful in listing some of the common security procedures used in securing wireless access points and other wireless devices.

Ellison, Craig. “Exploiting and Protecting 802.11b Wireless Networks”
September 2001
URL: http://www.extremetech.com/article2/0,3973,11388,00.asp

This article was found to be helpful in breaking down not only the most well documented steps, but also some unique steps to secure wireless devices.

Borisov, Nikita and Goldberg, Ian and Wagner, David. “Berkeley papers concerning WEP vulnerabilities”
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Geier, Jim. “802.11 WEP: Concepts and Vulnerability”
June 2002
URL: http://www.80211-planet.com/tutorials/article.php/1368661

The above articles were helpful in understanding WEP concepts.

The following Cisco Systems documentation was found to be extremely helpful in understanding security as it pertains to the CISCO1200AP. Note: A great amount of Cisco Systems documentation is only offered to registered customers. Because of this, URL's to customer only documentation has not been included.

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

Cisco Systems. "Cisco Aironet 1200 Series Access Point Software Configuration Guide"
URL:http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/ap120scg/apbkscg.pdf

Cisco Systems. "Cisco Aironet 1200 Series Administering the Access Point"
URL:
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_chapter09186a0080148694.html#1037319

Section 2 – Audit Evidence

Section 2.1– Audit Preparation

The Audit Preparation section is meant to provide and gather important information pertaining to the audit, mainly the Audit Checklist. This section is broken down into simplified questions with space to write the appropriate answers. Before beginning the Audit Checklist gather the following information as it is possible.

IP ADDRESS:	10.0.0.1
MAC ADDRESS:	00.0C.85.DB.BE.8A
SSID:	ACME
ENABLE PASSWORD:	NOT SURE
USERNAMES AND/OR PASSWORDS FOR THE CISCO1200AP:	CISCO CISCO
CURRENT WEP KEY:	NOT SURE
INITIAL STATE OF WEB MANAGEMENT ON THE CISCO1200AP:	ENABLED
IP ADDRESS OF AUDIT LAPTOP:	10.0.0.2
MAC ADDRESS OF AUDIT LAPTOP:	00.20.A6.4C.60.17

Note: The MAC address of the AP's Dot11Radio card can be found on the HOME page of the CISCO1200AP Web Management Front End.

Section 2.2– Audit Checklist

AUDIT ITEM: AC_001

CONTROL OBJECTIVE:
To mitigate physical theft and/or loss of the CISCO1200AP and radio modules. To physically secure the CISCO1200AP investment.

RISK:
Physical theft and/or defacement of the CISCO1200AP and/or associated radio modules.

THREAT:	*Loss of money and/or downtime due to physical theft/defacement of the device.*
PROBABILITY:	*ACME Company is located in a low traffic area. The risk of the device being defaced, stolen, etc. is unlikely.*
CONSEQUENCE:	*Loss in productivity and/or CISCO1200AP. Staff time needed to purchase and replace. If the device is stolen, configuration information could be taken from the device. This could give an attacker additional information e.g. internal network configurations, authentication methods, etc.) With this information an attacker increases the chances of a successful break-in.*

COMPLIANCE:
The CISCO1200AP has (2) locking mechanism. One is located on the actual unit and the other is located on the radio modules. Ensure that each locking mechanism has been secured with a computer locking cable and padlock. The locking cable should be attached/looped around to a solid state object e.g. steel column, cement column, desk, etc. If a solid state object is not available adhesive plates or hasp mounts can be used.

TESTING:
Observe the CISCO1200AP. (a) Check to ensure a computer locking cable has been run through the locking mechanism CISCO1200AP and is attached securely to a solid state object, adhesive plate, or hasp mount. (b) Check to ensure a computer locking cable has been run through the locking mechanism on the radio modules and is attached securely to a solid state object, adhesive plate, or hasp mount. (c) Check to ensure that the CISCO1200AP is in a protected area e.g. locked room, mounted out of reach of traffic, etc.

OBJECTIVE / SUBJECTIVE:
Subjective

KEYWORDS:
theft cisco aironet 1200 (Google); installing security cables (Google)

REFERENCES:

Cisco System. "Cisco Aironet 1200 Series Installation Guide"
January 2002
URL:http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_chapter09186a0080147d6f.html#1036179

Smith, Del. "Cisco Aironet 1200 APs support multiple WLAN protocols"
August 2002
URL:http://techrepublic.com.com/5100-6265-1051061.html

Flexguard Security System. "Installation Instructions"
2003
URL:http://www.flexguard.com/install_cable.html#attach

AUDIT ITEM: AC_002

CONTROL OBJECTIVE:

To decrease the amount of wireless coverage provided outside of authorized areas in order to mitigate possible discovery of the CISCO1200AP. Unauthorized areas are defined as areas where ACME Company programmers would not work e.g. outside the building, in the lobby, across the street, etc. The authorized wireless coverage has been marked as the entire ACME Company 6th floor production area.

RISK:

With knowledge of the CISCO1200AP an attacker could mark the CISCO1200AP as an attack target.

THREAT:	*Could possibly become an attack vector leading to attacks and unneeded wireless traffic.*
PROBABILITY:	*Medium. Due to the fact that ACME Company is located in the downtown business district of a metropolitan city it is likely that the CISCO1200AP could be discovered.*
CONSEQUENCE:	*Increased wireless attacks. Possible listing on the Internet under "wireless hotspot" databases leading to more attacks. Wireless "hot spot" databases are listings of wireless access points, their location, and configuration information.*

COMPLIANCE:

Coverage in unauthorized areas should be minimal to none e.g. very low to non-existent readings with wireless strength testing software). Unauthorized areas are defined as areas where ACME Company programmers would not work e.g. outside the building, in the building lobby, outside of authorized wireless areas.

TESTING:

On a laptop, use Netstumbler with a Lucent Orinoco Card to measure signal strength of the CISCO1200AP from various unauthorized areas. (a) Execute Netstumbler. (b) Under Netstumbler select the "Device" menu and ensure that the NDIS drivers are being used for the Lucent Orinoco. (c) Next, restart Netstumbler by clicking on the "Green VCR-like Play button" twice. (e) The CISCO1200AP will now appear in the right pane window. (f) On the left pane window, select the CISCO1200AP, by either MAC address or SSID. (g) Ensure that the MAC address in Netstumbler matches that of the MAC address gathered from Audit Preparation. (h) Once the CISCO1200AP is selected on the left pane window, a strength meter should appear on the right pane window. (i) Test for a minimum of 1 minute. Note the measurements. (j) Save the information, By using the "File >> Save" menu command (k) After saving, move to the next unauthorized location and repeat.

OBJECTIVE / SUBJECTIVE:

Subjective

KEYWORDS:

wireless exposure (Google); wireless discovery exposure netstumbler (Google)

REFERENCES:

Hassick, Brian. "Simple Wireless Exposure in Traditional Networks"
First Quarter 2002
URL:http://www.sbq.com/sbq/wireless/sbq_wireless_exposures.pdf

IBM. "Wireless Networks: Avoid security exposure; protect your investment"
N/A
URL http://www-1.ibm.com/services/strategy/e_strategy/security_exposure.html

Piscitello, David M. "Tools and Tactics for Safer WLAN Deployment"
N/A
URL:http://www.corecom.com/external/livesecurity/saferwlan.htm

AUDIT ITEM: AC_003

CONTROL OBJECTIVE:
To inform unauthorized users and/or attackers that illegal activity can and will be prosecuted and is prohibited under the full length of the law. This allows ACME Company to prosecute those individuals who use the CISCO1200AP without authorization.

RISK:
To inform unauthorized users that illegal activity can and will be prosecuted.

THREAT:	*An attacker is found but prosecution is unsuccessful due to the lack of warning or informative caution to the attacker.*
PROBABILITY:	*Low. Because wireless attacks are different in the aspect of the physical nature e.g. an unauthorized user and/or attacker could attack from 30 miles away, finding and prosecuting a wireless attacker and/or unauthorized user could be difficult.*
CONSEQUENCE:	*Possible unsuccessful prosecution.*

COMPLIANCE:
Warning banner exists on the CISCO1200AP. Also, that the banner warns that "unauthorized access will be prosecuted under the full length of the law.

TESTING:
(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-4. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check to ensure that the below lines exist in the running-config (l) If found, ensure that the <sample text> warns that unauthorized access will be prosecuted. (m) Lastly, log out by using the 'exit' command, and ensure the banner displays.

banner motd ^c
<sample text>
^c

OBJECTIVE / SUBJECTIVE:
Subjective

KEYWORDS:
warning banner (Google); warning banner use.of (Google)

REFERENCES:

NASA IT. "Security Warning Banner"
N/A
URL:http://lupus.gsfc.nasa.gov/security_web.html

ITSC. "Logon Warning Banners"
N/A
URL:http://www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/WarnBanner.htm

AUDIT ITEM: AC_004

CONTROL OBJECTIVE:
To ensure timeout periods have been set so that idle administrative connections will be disconnected.

RISK:
If a user with administrative privileges leaves a live session unattended it is possible for an attacker to use that live session, while they are away, and finish before the user comes back.

THREAT:	*Unauthorized administrative access to the CISCO1200AP.*
PROBABILITY:	*Low. Again, the ACME Company is in a low traffic environment. Someone accessing the console port of the CISCO1200AP would be noticed due to the nature of the office and production floor size.*
CONSEQUENCE:	*Configuration changes, removal of software on the CISCO1200AP rendering the CISCO1200AP useless.*

COMPLIANCE:
Timeout periods have been set in the configuration of the access point.

TESTING:
(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-4. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Ensure that the first numerical digit preceding "exec-timeout' is between 1 and 3. These numbers are represented by minutes. (l) Ensure that waiting for the designated idle time, disconnects the session.

line con 0
exec-timeout 1 0

OBJECTIVE / SUBJECTIVE:
Objective

KEYWORDS:
cisco aironet timeout console (Google)

REFERENCES:
Cisco Systems. "List of Supported IOS Commands"
N/A
URL:http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_command_reference_chapter09186a00801494f3.html

AUDIT ITEM: AC_005

CONTROL OBJECTIVE:

To ensure the SSID is not set to factory-default. With the SSID configured with factory-default settings an attacker could gain further knowledge of the device and/or model of the CISCO1200AP whereby increasing the chances of a successful break-in.

RISK:

An attacker could increase the chances of a successful break-in by using the SSID to better identify the CISCO1200AP e.g. vendor, model, etc.)

THREAT:	*With sensitive information such as the vendor and/or model of the CISCO1200AP an attacker could increase the chances of a successful break-in by tailoring the attack methods to a particular vendor and/or model. With information such as model and/or vendor an attacker can drastically minimize the amount of time it would take to successfully break-in.*
PROBABILITY:	*Medium. If the CISCO1200AP is configured with a factory-default SSID, an attacker would need less time to complete a successful break-in.*
CONSEQUENCE:	*With a factory-default SSID configured on the CISCO1200AP an increased chance of a successful break-in is a possibility. If a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. .deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.*

COMPLIANCE:

Configuration line "ssid tsunami" does not exist in the running-config.

TESTING:

(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-2. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to ensure that the string "ssid tsunami" does not exist. (l) Next, Using Netstumbler on the audit laptop with an Orinoco Card, scan for the SSID "tsunami". (m) Execute Netstumbler. (n) Under Netstumbler select the "Device" menu and ensure that the NDIS drivers are being used for the Lucent Orinoco. (o) Next, restart Netstumbler by clicking on the "Green VCR-like Play button" twice. (p) The CISCO1200AP will now appear in the right pane window. (q) On the left pane window, select the CISCO1200AP, by either MAC address or SSID. (r) Ensure that the MAC address in Netstumbler matches that of the MAC address gathered from Audit Preparation.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

factory.default SSID listing (Google); factory default SSID security (Google)

REFERENCES:

PC Magazine. "Wireless LANS at Risk"
N/A
URL:http://www.pcmag.com/article2/0,4149,1175896,00.asp

Mohney, Doug. "WiFi Wardriving"
September 1, 2003
URL http://www.synchrologic.com/2003/09/23/eng-primemedia/eng-primemedia_112118_5773960666571695083.html

Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practice"
N/A
URL:http://www.arstechnica.com/paedia/w/wireless-security-howto/home-802.11b-2.html

AUDIT ITEM: AC_006

CONTROL OBJECTIVE:

To ensure the SSID does not reveal information pertaining to the company, business type and/or physical location. If the SSID is configured for the company name, business type, and/or physical address an attacker could increase the chances of a successful break-in. By utilizing the information gathered from the SSID e.g. A donut store using "DONUTS" as the SSID an attacker could increase the chances of break-in by using password combinations tailored to the company.

RISK:

Leaking sensitive information to the attacker, such as the owning company of the CISCO1200AP, that companies business type and or physical location.

THREAT:	*Loss of sensitive information leading to increase in vulnerability to a successful break-in.*
PROBABILITY:	*Medium. Due to the fact that ACME Company is located in the downtown business district of a metropolitan city it is likely that the CISCO1200AP SSID could be discovered. Depending on the configuration of the SSID sensitive information could be gathered from the CISCO1200AP SSID.*
CONSEQUENCE:	*Increase chance of break-in. If a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.*

COMPLIANCE:

SSID does not match the company name, business type and/or the physical address.

TESTING:

(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-2. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to display the string "ssid xxxxxxxxxx". Ensure that the xxxxxxxxxx does not match the company name, business type, and/or physical location (e.g. address, etc.) (l) Next, Using a laptop with an Orinoco card connect to the xxxxxxxxxx SSID. Upon connection, the CISCO1200AP should report a new association in Tera Term, matching the MAC address of the audit laptop, gathered during the Audit Preparation.

Note: If WEP is needed to associate with the CISCO1200AP use the WEP key gathered during the Audit Preparation.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

factory.default SSID listing (Google); factory default SSID security (Google)

REFERENCES:

PC Magazine. "Wireless LANS at Risk" N/A

Mohney, Doug. "WiFi Wardriving" September 1, 2003

Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practice"

URL:http://www.pcmag.com/article2/0,4149,1175896,00.asp	*URL http://www.synchrologic.com/2003/09/23/eng-primemedia/eng-primemedia_112118_5773960666571695083.html*	*N/A* *URL:http://www.arstechnica.com/paedia/w/wireless-security-howto/home-802.11b-2.html*

AUDIT ITEM: AC_007

CONTROL OBJECTIVE:

To ensure that the CISCO1200AP is not "broadcasting" the SSID. The CISCO1200AP by factory-default will broadcast the SSID for wireless devices looking for a wireless access point. The broadcast is a radio packet, or "beacon packet" that is constantly broadcasted. By broadcasting the SSID an attacker could discover the CISCO1200AP and the SSID. With the knowledge of the CISCO1200AP existence and/or the SSID, an attacker could increase the chances of a successful break-in.

RISK:

Knowledge of the CISCO1200AP could lead to increased attempts to break-in.

THREAT:	*Discovery and/or identification of the CISCO1200AP. Once discovered attack attempts could follow.*
PROBABILITY:	*Medium. Due to the fact that the CISCO1200AP is shipped with "broadcasting" of the SSID enabled, it is likely that the CISCO120AP is broadcasting the SSID.*
CONSEQUENCE:	*Discovery and/or identification of the CISCO1200AP. This could lead to an attempt to break-in and/or attack the CISCO1200AP. If a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.*

COMPLIANCE:

If the running-config does not contain the line "guest-mode". Also, using Netstumbler yields no results for the coordinating SSID.

TESTING:

(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-2. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to ensure that the string "guest-mode" does not exist. (l) Next, Using Netstumbler on the audit laptop with an Orinoco Card, we will scan for the SSID of the CISCO1200AP. (m) Execute Netstumbler. (n) Under Netstumbler select the "Device" menu and ensure that the NDIS drivers are being used for the Lucent Orinoco. (o) Next, restart Netstumbler by clicking on the "Green VCR-like Play button" twice. (p) The CISCO1200AP will now appear in the right pane window. (q) On the left pane window, select the CISCO1200AP, by either MAC address or SSID. (r) Ensure that the MAC address in Netstumbler matches that of the MAC address gathered from Audit Preparation.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

broadcasting SSID security (Google))

REFERENCES:

MobileComputing.com. "Service Set Identifier" N/A

Duke University. "Securing the Personal Computer: Wireless Configuration"

Geier, Jim. "Guarding against WLAN Security Threats"

URL:http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci853455,00.html

URL:http://security.duke.edu/securepc/wireless.html

September 12, 2002
URL: http://www.wi-fiplanet.com/tutorials/article.php/1462031

AUDIT ITEM: AC_008

CONTROL OBJECTIVE:

To ensure a secure access control is being used. There are two authentication methods, Open and Shared. When authenticating with the Open method authentication packets are not encrypted. When authenticating with Shared mode the authentication packets are encrypted. Secure access and authentication to the CISCO1200AP is important to how clients and devices are granted access to the CISCO1200AP.

RISK:

Unauthorized authentication and access to the CISCO1200AP. Also, by using Open authentication it is possible for an attacker to break other security measures in place e.g. WEP. With unauthorized authentication and/or access to the CISCO1200AP an attacker increases the chances of a successful break-in. Also if an attacker broke other security measures, secure communication to the CISCO1200AP could be compromised.

THREAT:	*With the CISCO1200AP authenticating unauthorized devices an increase in a successful break-in or attack is possible.*
PROBABILITY:	*Medium. Due to the fact that the CISCO1200AP is shipped with Open mode enabled it is likely that the CISCO120AP is using Open mode to authenticate clients and devices.*
CONSEQUENCE:	*If an attacker were to "sniff" or capture the unencrypted authentication packets it is possible for an attacker to use that information to gain access to the CISCO1200AP. If an attacker were to gain If a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.*

COMPLIANCE:

If the CISCO1200AP running-config does not contain the line "authentication open".

TESTING:

(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-2. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to ensure that the string "authentication open" does not exist.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

authentication packets wireless shared (Google)

REFERENCES:

IBM. "Wireless Security Auditor"
N/A
URL: http://www.research.ibm.com/gsal/wsa/

ExtremeTech. "Wireless LAN deployment and Security Basics"
URL:http://www.extremetech.com/article2/0,3973,1157726,00.asp

InteropNet. ""Whats wrong with WEP?"
N/A
URL:http://www.ilabs.interop.net/WLAN_Sec/What_is_wrong_with_WEP-lv03.pdf

AUDIT ITEM: AC_009

CONTROL OBJECTIVE:

To ensure that unauthorized administrative access to the Web Management Front End is not gained. The Web Management Front End of the CISCO1200AP is used to make configurationally changes on the CISCO1200AP. If an attacker were to access the Web Management Front End changes could be made e.g. security, configuration, etc.

RISK:

With unauthorized administrative access to the Web Management Front End an attacker could take over the CISCO1200AP, possibly erasing the firmware, reconfiguring to provide access to other attackers, and compromising company data.

THREAT:	*With unauthorized administrative access to the CISCO1200AP an attacker could cause downtime leading to a loss in productivity or access to company data and resources.*
PROBABILITY:	*High. Due to the fact that the CISCO1200AP is shipped with factory-default usernames and passwords it is likely that an attacker could gain access to the Web Management Front End.*
CONSEQUENCE:	*If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.)*

COMPLIANCE:

Using the "factory-default" username and password does not yield an administrative connection to the Web Management Front End.

TESTING:

Using a web browser connect to the CISCO1200AP over HTTP. Connect to the following address where CISCO1200AP is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ When prompted for a username and password attempt to use the "factory-default" username and password. The factory default username and password are below. Check to ensure that administrative access to the Web Management Front End is denied

Username: Cisco
Password: Cisco

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

aironet default cisco username (Google)

REFERENCES:

Cisco Systems. "Password Recovery for the Cisco Aironet Equipment"
N/A
URL:http://www.cisco.com/warp/public/102/wlan/pwrec-2.html

AUDIT ITEM: AC_010

CONTROL OBJECTIVE:

To ensure that the factory-default authentication settings have been changed. By factory-default the CISCO1200AP comes with several accounts enabled to administrate the device from remote e.g. Web Management Front End, telnet, ssh. The factory-default way of authenticating these accounts is with a "Global Password". The "Global Password" is used by all user accounts, including the factory-default user account "Cisco". Because the CISCO1200AP has the ability to create administrative defined users, the default "Cisco" user account should be removed and replaced with another name with identical rights. In addition the "Global Password" feature should be disabled, and at minimum, replaced with the feature "Local User List Only"

RISK:

With the use of factory-default authentication mechanisms and factory-default username and passwords the chances of a successful break-in are high. Once in, an attacker would have full access to the CISCO1200AP. If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.

THREAT:	*By using factory-default authentication settings an attacker could leverage administrative access to the CISCO1200AP. If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.*
PROBABILITY:	*High. Due to the fact that the CISCO1200AP is shipped with these factory-default authentication settings in place, it is very likely that an attacker could gain administrative access to the CISCO1200AP.*
CONSEQUENCE:	*If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.*

COMPLIANCE:

By default there are two settings that need to be made to modify the default authentication settings. Under, "Authentication Settings", at minimum, "Local User List Only" should be selected. In addition, the factory-default "Cisco" user account should be deleted, with a new account in place.

TESTING:

(a) Using a web browser connect to the CISCO1200AP over HTTP. Connect to the following address where CISCO1200AP is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ap_sec_local-admin-access.htm. (b) Once connected, Under "Security: Admin Access" under "Administrator Authenticated by:" Ensure that "Default Authentication (Global Password)" is not checked. (c) Next, under "User List" ensure that the factory-default user account "Cisco" has been deleted, and that a new account has been setup.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

aironet default cisco username (Google) cisco aironet default.authentication (Google)

REFERENCES:

Cisco Systems. "Password Recovery for the Cisco Aironet Equipment"
N/A

Cisco Systems. "Configuring Authentication Types"
N/A

URL:http://www.cisco.com/warp/public/102/wlan/pwrec-2.html

URL:http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_chapter09186a008014868e.html

AUDIT ITEM: AC_011

CONTROL OBJECTIVE:

To ensure unauthorized administrative access is not gained by way of weak username/password combos. Because all administrative Front Ends to the CISCO1200AP are protected with usernames and passwords it is possible for an attacker to attempt a brute force attack against weak username/password combos.

RISK:

If an attacker were to brute force a successful administrative user account and password, an attacker would have full access to the CISCO1200AP. If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.

THREAT:	*A successful brute force attack yielding an active administrative username and password for the CISCO1200AP. If an attacker were to obtain an administrative username and password the attacker would have administrative access to the CISCO1200AP.*
PROBABILITY:	*Medium. If password best practices have been used, in that passwords have been assigned with alpha-numeric, uppercase and lowercase with symbols, it would take an attacker significant time to leverage administrative access. However, if the passwords assigned are dictionary words, the word "password, admin, etc", it is likely that an attacker could leverage administrative access.*
CONSEQUENCE:	*If an attacker were to gain administrative access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.)*

COMPLIANCE:

With an attempt to brute force the username and password combo using a custom dictionary that comes packaged with Brutus. Brutus is a brute force tool used to attempt multiple combinations of command usernames and passwords. Attempt to obtain a successful username and password for the CISCO1200AP using the default dictionary.

TESTING:

Using Brutus configure the following settings: For the "Target" enter the IP Address of the CISCO1200AP gathered from the Audit Preparation. For the "Type" select "HTTP: Basic Auth". Under "Connection Options"; the "Port" setting should be set for "80", "Connections" should be "10", and "Timeout" should be set for "10". Under "HTTP Basic Options" the "Method" should be set for "HEAD" with "KeepAlive" checked. Under "Authentication Options" check "Use Username" and "Browse" for the username file in the Brutus folder. For "Pass Mode" use "Word List" and browse to select the word list in the Brutus folder. To begin the test, click "Start" NOTE: The user list and wordlist should contain the following word "Cisco". Default Brutus dictionary files do not contain "Cisco".

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

brutus (Google)

REFERENCES:

SANS. "SANS 2002 San Diego Seminar"
March 2002
URL: www.sans.org

Hobbie.net. "Brutus - FAQ"
N/A
URL: http://www.hoobie.net/brutus/brutus-faq.html

AUDIT ITEM: AC_012

CONTROL OBJECTIVE:

To ensure that only authorized devices are able to connect to the CISCO1200AP. By listing the "MAC addresses" of authorized devices only, an additional layer of security is created for the CISCO1200AP. By specifying the MAC addresses for authorized devices only, any other device attempting to authenticate or route traffic to/through the CISCO1200AP would be denied.

RISK:

Unauthorized devices authenticating and possibly routing traffic through the CISCO1200AP. If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.)

THREAT:	*Unauthorized associated and/or traffic to the CISCO1200AP. Once access is gained it is possible for an attacker to be malicious in intent e.g. deleted, modify company data, use the Internet to spam or launch attacks to Internet or company computers*
PROBABILITY:	*Medium. Due to the fact that the CISCO1200AP is shipped with MAC address filtering turned off it is likely that an attacker could associate with the CISCO1200AP and route traffic to the CISCO1200AP.*
CONSEQUENCE:	*If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.)*

COMPLIANCE:

The CISCO1200AP supports MAC address filtering. If MAC address filtering has been configured a list of authorized MAC addresses are stated under "Local List:" Check to ensure that authorized MAC addresses are listed in the "Local List" section.

TESTING:

(a) Using a web browser connect to the CISCO1200AP over HTTP. Connect using the following address, where "CISCO1200AP" is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ap_sec_ap-client-security-adv_a.htm . (b) Verify that authorized MAC addresses are specified under "Local MAC Address". (c) Next, using a wireless network card that is authorized attempt to authenticate to the CISCO1200AP. (d) Once authenticated, which is indicated by an active connection to the CISCO1200AP's SSID, attempt to ping the IP address of the CISCO1200AP. (e) Lastly, repeat steps with an unauthorized wireless card. (f) When using the unauthorized wireless card a failure in an attempt to connect indicates that MAC authentication is functioning properly.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

wireless mac address filtering (Google); wireless mac.address security (Google)

REFERENCES:

Dismukes, Trey. "Wireless Security Blackpaper" July 2002 URL:http://www.arstechnica.com/paedia/w/wireless/security-3.html

Hobbie.net. "Brutus - FAQ" N/A URL: http://www.hoobie.net/brutus/brutus-faq.html

Wright, Joshua. "Detecting Wireless LAN Mac Address Spoofing" January 21, 2003 URL: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

AUDIT ITEM: AC_013

CONTROL OBJECTIVE:

To ensure data communications destined to the CISCO1200AP are not compromised or intercepted. Because communication is performed over wireless an attacker could attempt to "sniff" or capture the RF transmissions in route to the CISCO1200AP. In order to mitigate this, WEP was created. WEP encrypts the packets or RF transmissions to and from the CISCO1200AP.

RISK:

The capture and/or modification of RF transmissions and/or packets to and from the CISCO1200AP.

THREAT:	*Because the information being transferred to and from the CISCO1200AP is sensitive to the ACME Company, if an attacker were to intercept or modify the data the integrity could be significantly affected.*
PROBABILITY:	*High. Due to the fact that the CISCO1200AP is shipped with WEP turned off it is likely that an attacker could capture and/or modify the data transmitted to and from the CISCO1200AP.*
CONSEQUENCE:	*If an attacker were to capture and/or modify data transferred to and from the CISCO1200AP, it is possible for that data to contain usernames, passwords, company data, etc. With this an attacker could possibly gain access to ACME Company. If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.)*

COMPLIANCE:

The CISCO1200AP has the ability to support 128-bit WEP encryption. Check to ensure that WEP is enabled. The use of WEP should be mandatory. Also the encryption level should be set for 128-bit.

TESTING:

(a) Using a web browser connect to the CISCO1200AP over HTTP. Use the following address, where "CISCO1200AP" is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ap_sec_ap-key-security.htm . (b) Under "Encryption Modes" ensure that "WEP Encryption" is set to mandatory. (c) Next, under "WEP Keys" ensure that 128bit encryption is being used. If the above is tests fail, DO NOT move onto the next testing steps, as it is unnecessary. (d) Next, test that WEP is functioning by connecting with a Lucent Orinoco Card. Enter the WEP key and WEP level given during the Audit Preparation into the Lucent Orinoco Card wireless utility. (e) Attempt to associate. (f) If associated, ensure the WEP is 128-bit, by attempting to ping the CISCO1200AP. (g) Ensure that the connected AP's MAC address matches that of the audited CISCO1200AP.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

wep (Google); wep auditing (Google)

REFERENCES:

Geier, Jim. "802.11 WEP: Concepts and Vulnerabilities" June, 2002 URL:http://www.wifiplanet.com/tutorials/article.php/1368661

Borisov, Nikita. Goldberg, Ian. Wagner, David. "Intercepting Mobile Communications: The Insecurity of 802.11" N/A URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

AUDIT ITEM: AC_014

CONTROL OBJECTIVE:

To ensure that the WEP key is not compromised. In 2001, individuals from California State University Berkeley found several flaws in WEP. These flaws allow an attacker to compromise the WEP key, the key used to encrypt wireless transmissions and/or packets. However, in order to leverage the attack, the attacker must gather a significant amount of sample transmissions and/or packets. In order to mitigate this attack the WEP key should be changed in scheduled intervals.

RISK:

The capture and/or modification of RF transmissions and/or packets to and from the CISCO1200AP.

THREAT:	*Because the information being transferred to and from the CISCO1200AP is sensitive, if an attacker were to crack the WEP key then attacker could possibly intercept or modify transmissions and/or packets transferred to and from the CISCO1200AP.*
PROBABILITY:	*Medium. Due to the fact that the attacker needs to obtain a large amount of sample transmissions, the likelihood is medium. It can take 1 hour or 3 months to break a WEP key.*
CONSEQUENCE:	*If an attacker were to capture and/or modify data transferred to and from the CISCO1200AP, it is possible for that data to contain usernames, passwords, company data, etc. With this an attacker could possibly gain access to ACME Company. If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.*

COMPLIANCE:

To mitigate the WEP key being compromised. The current polices and procedures should include verbiage speaking to "WEP key management" in regards to the CISCO1200AP. It is recommended that the WEP key be changed once every 2-4 weeks.

TESTING:

(a) Using a web browser connect to the CISCO1200AP over HTTP. Connect to the following address where CISCO1200AP is substituted for the IP Address gathered from the Audit Preparation: http://10.0.0.1/ap_sec_ap-key-security.htm . (b) Under the category "Encryption Modes" ensure that "WEP Encryption" is set to mandatory. (c) Next, under "WEP Keys" ensure that 128bit encryption is being used. (d) Next, interview those responsible for administrating the CISCO1200AP. Verify that the WEP key is changed on the CISCO1200AP, at minimum, once every 2-4 weeks, record the findings. (e) Next, search all current policy and procedure documentation for the words "WEP".

OBJECTIVE / SUBJECTIVE:

Subjective

KEYWORDS:

wep (Google); wep Berkeley (Google)

REFERENCES:

Geier, Jim. "802.11 WEP: Concepts and Vulnerabilities" June, 2002 URL:http://www.wifiplanet.com/tutorials/article.php/1368661

Borisov, Nikita. Goldberg, Ian. Wagner, David. "Intercepting Mobile Communications: The Insecurity of 802.11" N/A URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

AUDIT ITEM: AC_015

CONTROL OBJECTIVE:

To allow only secure remote connections when administrating the device. Because the CISCO1200AP offers a wide array of remote vehicles and protocols to administrate e.g. SSH, TELNET, and HTTP is vital that the communication is secure. Because it is possible for an attacker to possibly hijack/intercept/modify/etc. the transmissions to and from the CISCO1200AP during an administrative session, it is important that communications are secure.

RISK:

Access with less secure protocols such as TELNET and HTTP send the username and password in clear text. It is possible for an attacker to grab the username and password in transit for later use.

THREAT:	*An attacker hijacking/intercepting/modifying/etc. an administrative session to gain administrative privileges to the CISCO1200AP.*
PROBABILITY:	*Medium. Due to the fact that the CISCO1200AP is shipped with TELNET and HTTP enabled for administration access, is likely that an attacker could hijack/intercept/modify/etc. administrative data being transmitted to and from the CISCO1200AP.*
CONSEQUENCE:	*If an attacker were to capture and/or modify data transferred to and from the CISCO1200AP, it is possible for that data to contain usernames, passwords, company data, etc. With this an attacker could possibly gain access to ACME Company. If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.*

COMPLIANCE:

Because HTTP and TELNET both send the username and password information in clear test, check to ensure that TELNET and HTTP have been disabled. NOTE: Check the Audit Preparation report to indicate whether Web Management was initially disabled or enabled. If Web Management was initially disabled, then compliance has been met for the HTTP portion of this test.

TESTING:

(a) Using a web browser connect to the CISCO1200AP over HTTP. If you are prompted for a username and password note that HTTP was enabled. (b) Use the following address where "CISCO1200AP" is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ap_services_console-telnet.htm . (c) Ensure that "Telnet" is disabled. (d) Next, attempt to telnet to the IP address of the CISCO1200AP gathered during the Audit Preparation.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

telnet http clear.text username password (Google)

REFERENCES:

Phenoelit. "Insecure Protocols"
N/A
URL: http://www.phenoelit.de/fr/protos.html

AUDIT ITEM: AC_016

CONTROL OBJECTIVE:

To allow only secure remote connections when administrating the device. Because the CISCO1200AP offers a wide array of remote vehicles and protocols to administrate with e.g. SSH, TELNET, and HTTP, is vital that the communication is secure. Because it is possible for an attacker to possibly hijack/intercept/modify/etc. the transmissions to and from the CISCO1200AP during an administrative session, it is important that SSH be enabled.

RISK:

Without SSH enabled only clear text communication protocols remain. Access with less secure protocols such as TELNET and HTTP send the username and password in clear text. It is possible for an attacker to grab the username and password in transit for later use.

THREAT:	*An attacker hijacking/intercepting/modifying/etc. an administrative session to gain administrative privileges to the CISCO1200AP.*
PROBABILITY:	*Medium. Due to the fact that the CISCO1200AP is shipped with SSH disabled it is likely that the CISCO1200AP is not configured for SSH.*
CONSEQUENCE:	*If an attacker were to capture and/or modify data transferred to and from the CISCO1200AP, it is possible for that data to contain usernames, passwords, company data, etc. With this an attacker could possibly gain access to ACME Company. If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.)*

COMPLIANCE:

If a remote administrative session is needed only SSH should be used. Because HTTP and TELNET both send the username and password information in clear test. Check to ensure that SSH is enabled and functioning.

TESTING:

(a) Using a web browser connect to the CISCO1200AP over HTTP. Use the following address, where "CISCO1200AP" is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ap_services_console-telnet.htm . (b) Ensure that "SSH" is enabled. (c) Next, attempt to SSH to the IP address of the CISCO1200AP using Putty. Putty is a SSH client that is extremely simple to use and can be found at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html (d) Type in the IP address of the CISCO1200AP and select "SSH" and click "Open".

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

ssh clear.text (Google)

REFERENCES:

Phenoelit. "Insecure Protocols"
N/A
URL: http://www.phenoelit.de/fr/protos.html

Maricopa Community College. "Replacing Clear Text Protocols"
N/A
URL: http://www.guardian.maricopa.edu/policy/ssh/

AUDIT ITEM: AC_017

CONTROL OBJECTIVE:

Because connectivity to the CISCO1200AP is vital to the productivity of the programming department, the uptime of the CISCO1200AP is critical. Before configuration changes take place a backup of the current running config should be made prior to make any configurationally changes. If changes are made without a configuration backup productivity could be drastically affected in addition to unnecessary downtime. In addition, if the CISCO1200AP were to fail, a configuration backup would be needed to replace the unit in a timely fashion.

RISK:

Unnecessary downtime and lost of productivity due to the absence of a backup of the current configuration.

THREAT:	*Unnecessary downtime, loss of CISCO1200AP configuration and productivity.*
PROBABILITY:	*Medium. Because Cisco product has a good reputation for reliability and uptime the CISCO1200AP has a low expectancy for loosing its configuration or going down. However, configurationally changes should be backed up as good practice.*
CONSEQUENCE:	*Loss of CISCO1200AP configuration, downtime and loss of productivity.*

COMPLIANCE:

Before making authorized changes, policy and procedures should be in place for the steps taken to perform a configuration backup.

TESTING:

Check current policies and procedures that a procedure is outlined for backing up the CISCO1200AP configurations. Check to ensure that current backups exist for the CISCO1200AP.

OBJECTIVE / SUBJECTIVE:

Objective

KEYWORDS:

N/A

REFERENCES:

Knowledge

AUDIT ITEM: AC_018

CONTROL OBJECTIVE:
To ensure changes are done and are authorized against current policy and procedures. Because connectivity to the CISCO1200AP is vital to the productivity of the programming department, the uptime of the CISCO1200AP is critical. If configuration changes e.g. WEP key changes, security changes, etc. need to be done they should first be authorized and scheduled. If changes are made without authorization and scheduling, productivity could be drastically affected.

RISK:
Unnecessary downtime and lost of productivity due to the absence of policies and procedures authorizing configuration changes to the CISCO1200AP

THREAT:	*Unnecessary downtime and loss of productivity due to unauthorized modifications made to the CISCO1200AP configuration.*
PROBABILITY:	*Low. Because the CISCO1200AP does not require a great deal of administrative overhead, changes can be rare.*
CONSEQUENCE:	*Downtime and loss of productivity.*

COMPLIANCE:
Check to ensure current policies and procedures outline the steps taken to submit a configuration change for the CISCO1200AP. Changes should be authorized by management or supervisors responsible for the CISCO1200AP.

TESTING:
Check current policies and procedures to check for steps taken to submit configuration changes for the CISCO1200AP. Interview those responsible

OBJECTIVE / SUBJECTIVE:
Objective

KEYWORDS:
N/A

REFERENCES:
Knowledge

AUDIT ITEM: AC_019

CONTROL OBJECTIVE:
Because the CISCO1200AP is vital to the productivity of the programming department, a development environment/stage for major configurationally changes should be used.

RISK:
Bringing a major configuration change into production may cause the CISCO1200AP to fail causing unnecessary downtime and loss of productivity.

THREAT:	*Unnecessary downtime and loss of productivity due to major modifications made to the CISCO1200AP configuration without testing in a development environment/stage.*
PROBABILITY:	*Low. Because the CISCO1200AP does not require a great deal of administrative overhead, changes can be rare.*
CONSEQUENCE:	*Downtime and loss of productivity.*

COMPLIANCE:
Policy and procedures are in place that outline steps taken for major configurationally changes to the CISCO1200AP.

TESTING:
Check to ensure policy and procedures are in place that outline steps taken for major configurationally changes to the CISCO1200AP. Interview those responsible.

OBJECTIVE / SUBJECTIVE:
Subjective

KEYWORDS:
N/A

REFERENCES:
Knowledge

AUDIT ITEM: AC_020

CONTROL OBJECTIVE:

To ensure the CISCO1200AP is up to date with patches, upgrades and security bulletins released by the vendor. In the ever increasing security field, new patches/hot fixes, etc. are released constantly. Keeping the CISCO1200AP up-to-date with patches, hot fixes, etc. is a must. Because most attackers use known vulnerabilities that have been addressed by vendors with patches, patching the CISCO1200AP is extremely important.

RISK:

An unpatched system could be compromised or perform poorly. If the CISCO1200AP is compromised an attacker could gain access to the company network.

THREAT:	*Compromised unpatched CISC1200AP.*
PROBABILITY:	*High. Most attackers use known vulnerabilities that have been addressed or patched with a fix released from the vendor.*
CONSEQUENCE:	*If an attacker were to gain access and/or a break-in were to occur company resources such as company data, Internet resources, etc. could be maliciously attacked or used e.g. deleting of data, modifying of data, launching attacks to the Internet from ACME Company, etc.)*

COMPLIANCE:

A policy or procedure should be in place that outlines update procedures, patch updating routines and notification of security bulletins. A person involved in updating the CISCO1200AP should periodically check http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletins_list.html for bulletins related to the CISCO1200AP.

TESTING:

Check to ensure that a policy or procedure outlines the updating, patching and notification of updates for the CISC1200AP. Interview those responsible

OBJECTIVE / SUBJECTIVE:

Subjective

REFERENCES:

Cisco Systems. "Cisco Aironet 1200 – Bulletins"
N/A
URL:http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletins_list.html

Section 3– Audit Checklist

Audit Checklist Item - (ACI_01)
Ref: AI_002

Explanation:
The following test will take RF samples from unauthorized areas to report on signal strength and coverage outside of authorized WLAN areas. This Audit Checklist Item references AI_002.

Test:
On a laptop, use Netstumbler with a Lucent Orinoco Card to measure the signal strength of the CISCO1200AP from various unauthorized areas. (a) Execute Netstumbler. (b) Under Netstumbler select the "Device" menu and ensure that the NDIS drivers are being used for the Lucent Orinoco. (c) Next, restart Netstumbler by clicking on the "Green VCR-like Play button" twice. (e) The CISCO1200AP will now appear in the right pane window. (f) On the left pane window, select the CISCO1200AP, by either MAC address or SSID. (g) Ensure that the MAC address in Netstumbler matches that of the MAC address gathered from Audit Preparation. (h) Once the CISCO1200AP is selected on the left pane window, a strength meter should appear on the right pane window. (i) Test for a minimum of 1 minute. Note the measurements. (j) Save the information, by using the "File >> Save" menu command. (k) After saving, move to the next unauthorized location and repeat.

Command Line and/or Switches:
Netstumbler will be used with a default configuration. Ensure that the NDIS drivers for the Lucent Orinoco Card are being used under Netstumbler.

Evidence:
Below is a rough sketch of the floor plan of the ACME building. In yellow is authorized WLAN area. It is basically the entire production floor. Also, the current placement of the CISCO1200AP is indicted by a red square. Following the floor plan, are RF samples taken from the ACME Company building lobby and across the street from the ACME Company building.

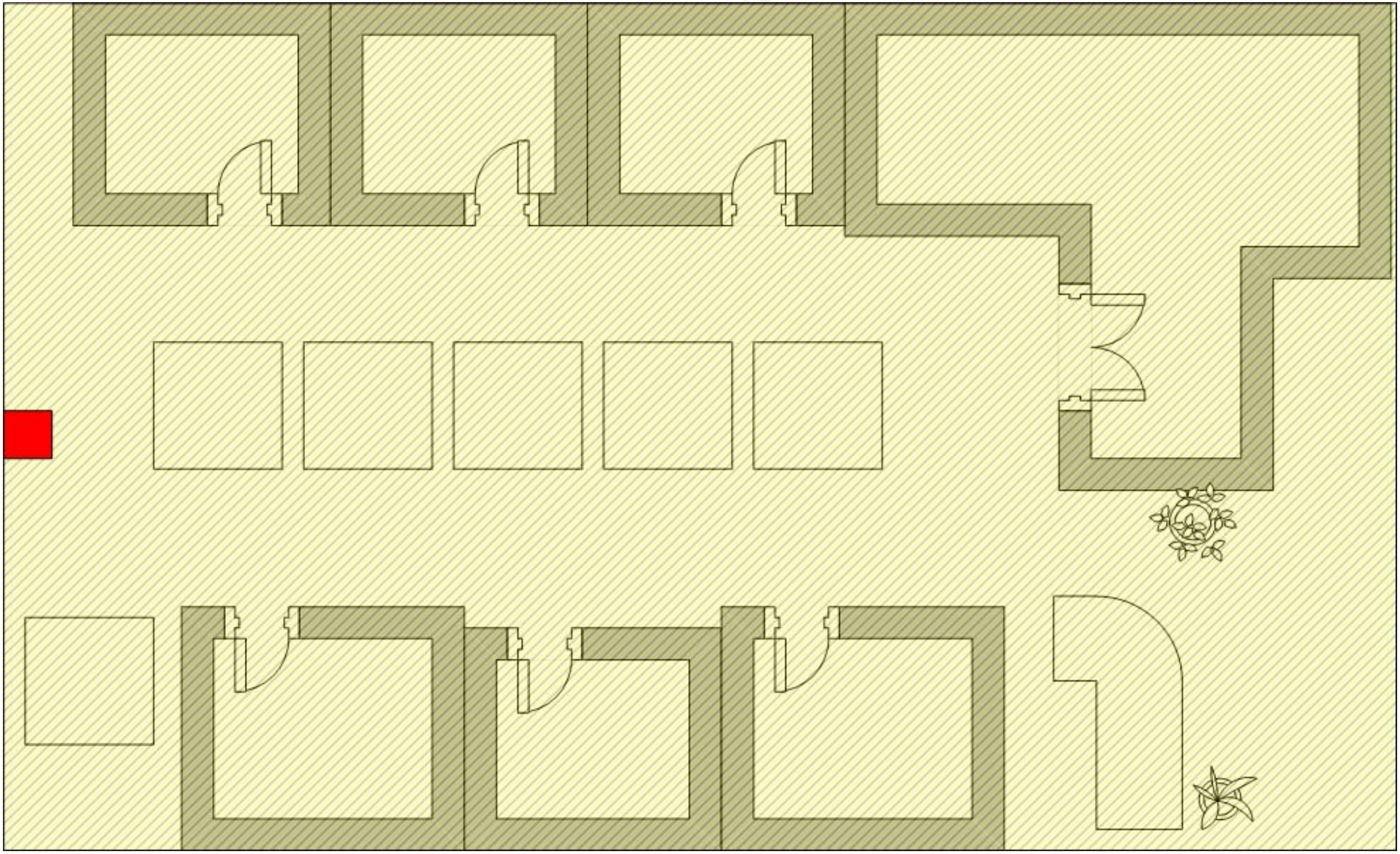

Figure 3-1 - ACME Floor Plan

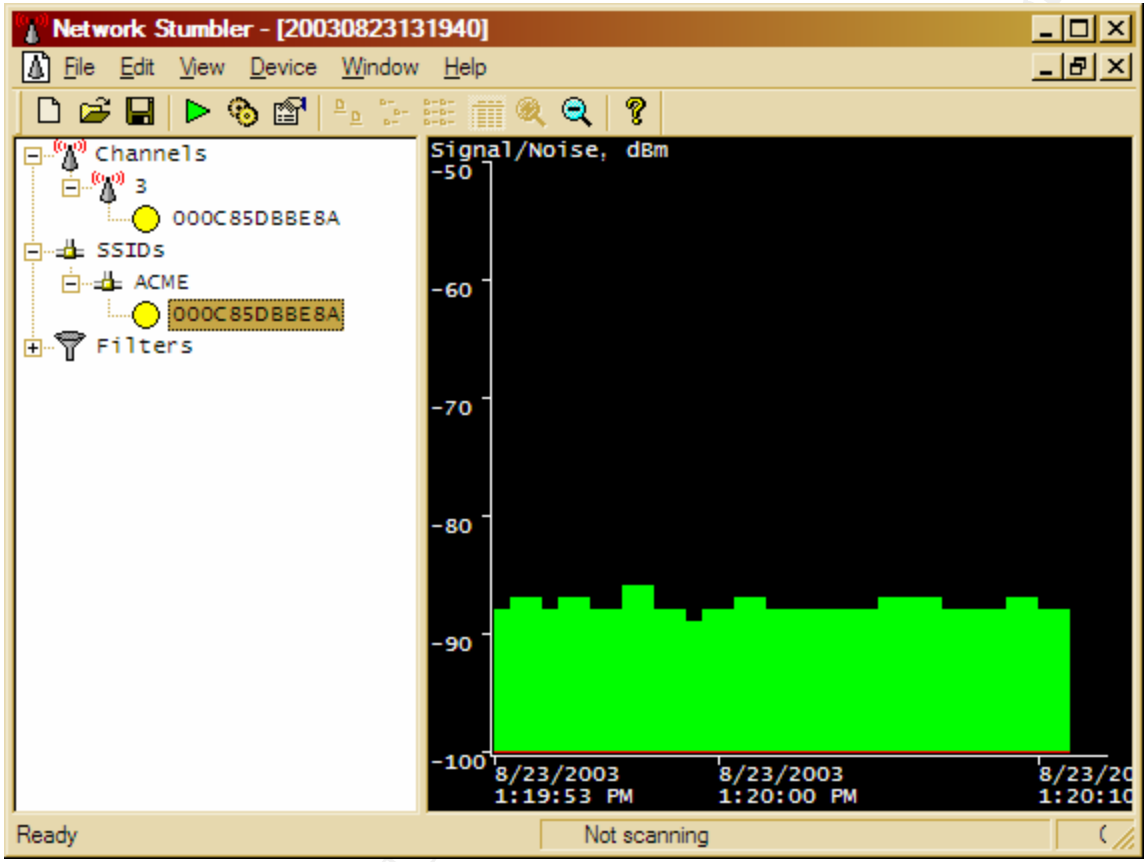

Figure 3-2 - RF Sample from ACME building lobby

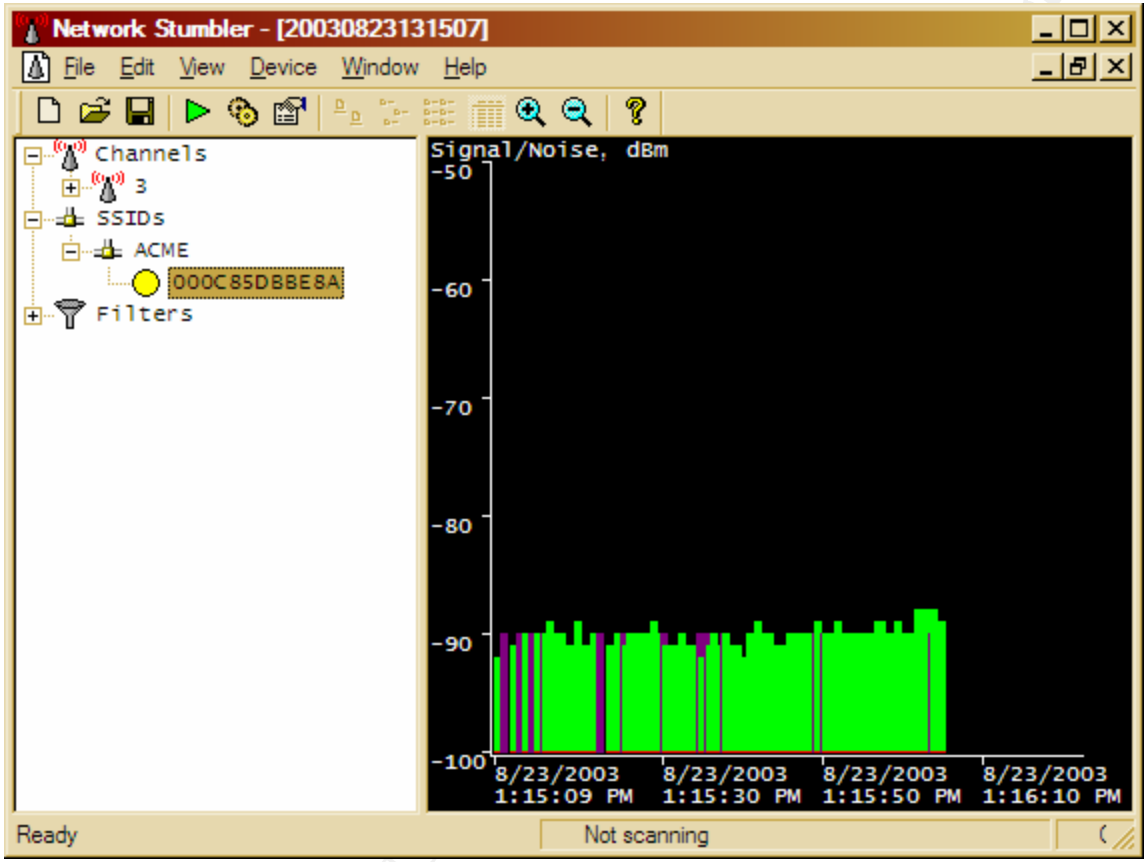

Figure 3-3 - RF Sample from 6th floor building across the street

Results:

Failed. The amount of coverage in unauthorized areas is too strong. RF samples were taken and measured from the ACME Company building lobby, shown in Figure 3-2, and across the street, shown in Figure 3-3. In both locations the "Signal / Noise, dbm" measured an average of "-90". This should be measured at "-100" to "no signal".

Audit Checklist Item - (ACI_02)
Ref: AI_003

Explanation:
The following test will check for warning banners on a successful administrative management connection to the console port of the CISCO1200AP. In addition, ensure that the warning banner informs that unauthorized access will be prosecuted. This Audit Checklist Item references AI_003.

Test:
(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK". Note: The COM1 settings can be found in Figure 3-4. (g) Next, strike the "ENTER/RETURN" key (h) the screen should display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check to ensure that the below lines exist in the running-config (l) If found, ensure that the <sample text> warns that unauthorized access will be prosecuted. (m) Lastly, log out by using the 'exit' command and ensure the banner displays.

…
banner motd ^c
<sample text>
^c
…

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Command Line and/or Switches:

SERIAL, COM1, 9600, 8 BIT, NONE (Figure 3-4)

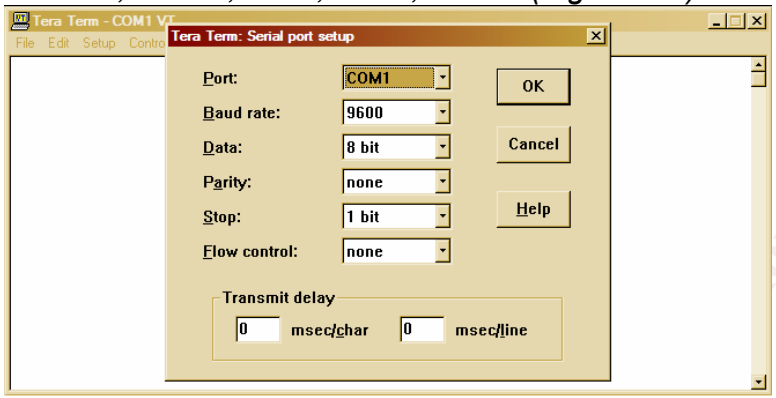

Figure 3-4 – Switches used

***Evidence*:**

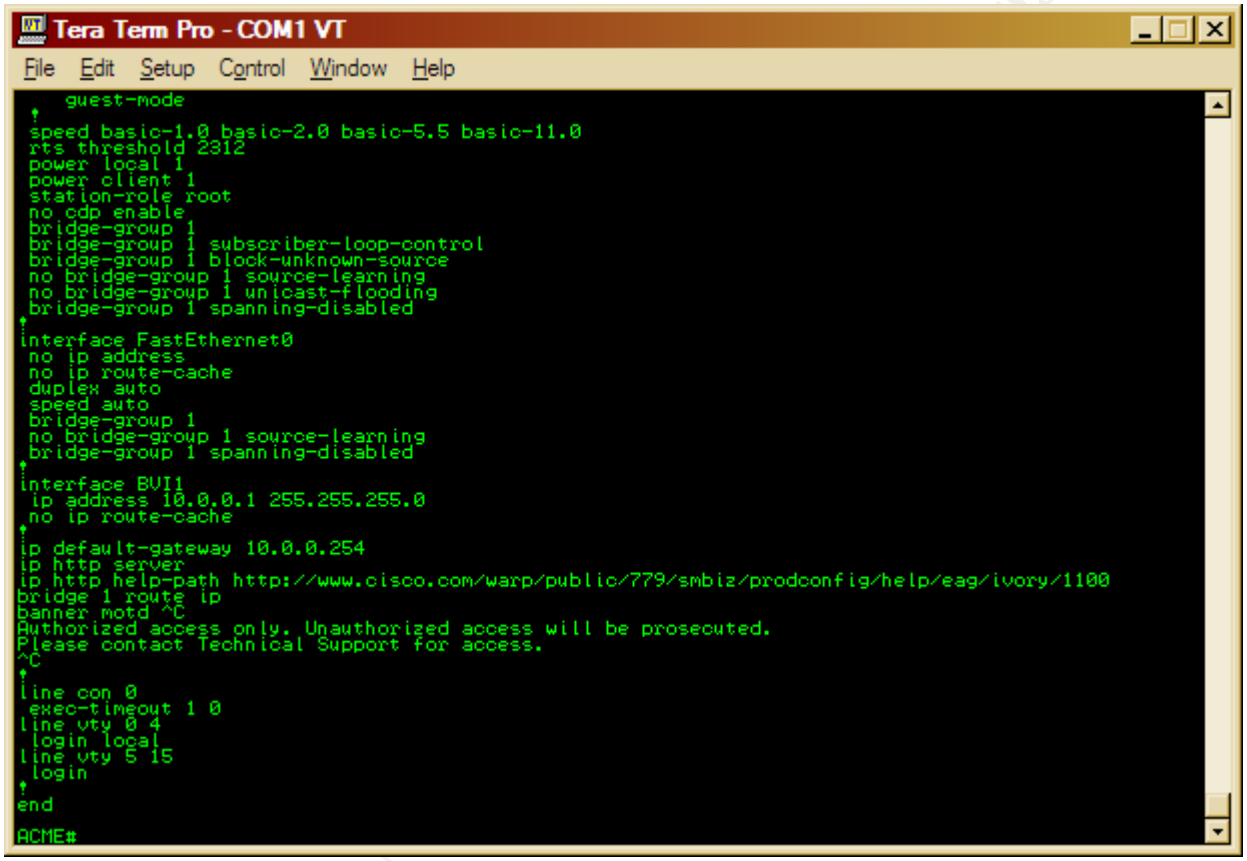

Figure 3-5 – Warning banner in place

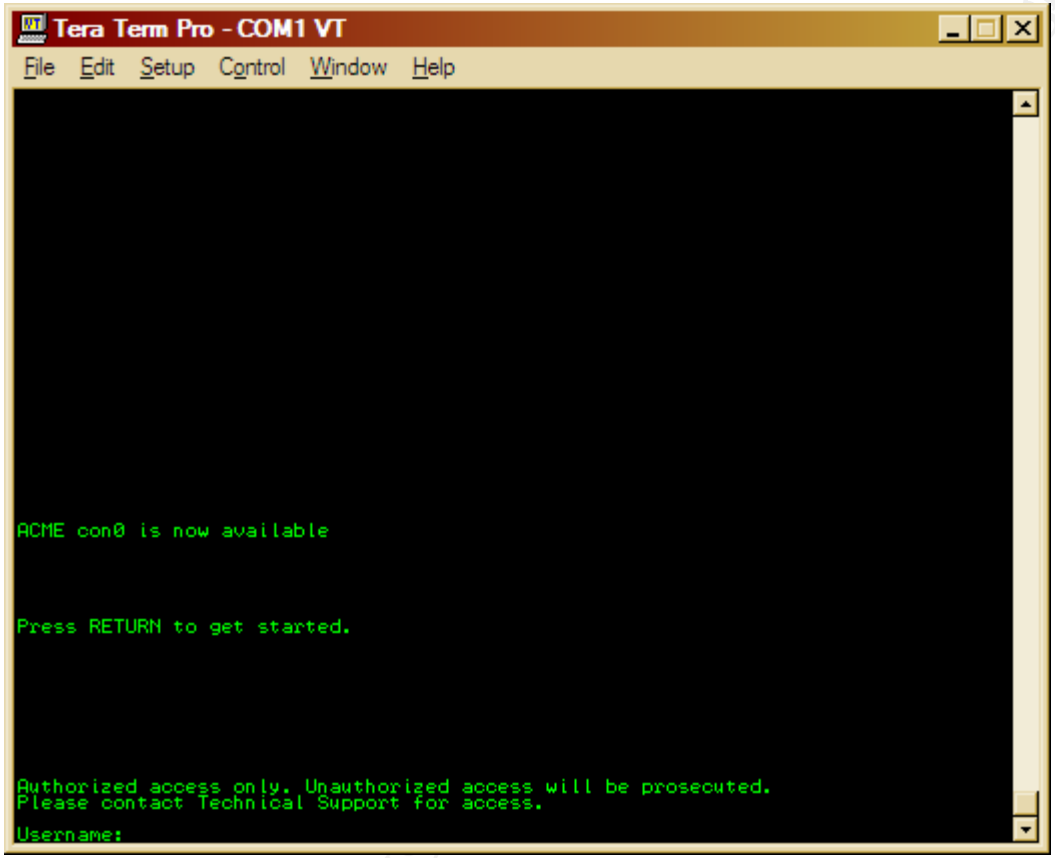

Figure 3-6 - Warning banner being displayed on login

***Results*:**
Passed. Warning banners were found to be configured under the running-config, as shown in Figure 3-5. The warning banner informed that unauthorized access will be prosecuted, as shown in Figure 3-6.

Audit Checklist Item - (ACI_03)
Ref: AI_004

Explanation:
The following test will ensure that timeouts are in place for administrative management connections to the CISCO1200AP. This Audit Checklist Item references AI_004.

Test:
(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-7. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to ensure that the timeout string settings are found. (l) Next, allow for timeout period to occur to test the timeout settings are working. (m) If the timeouts are working then the session within the console will be reset.

Command Line and/or Switches:
show running-config
SERIAL, COM1, 9600, 8 BIT, NONE (Figure 3-7)

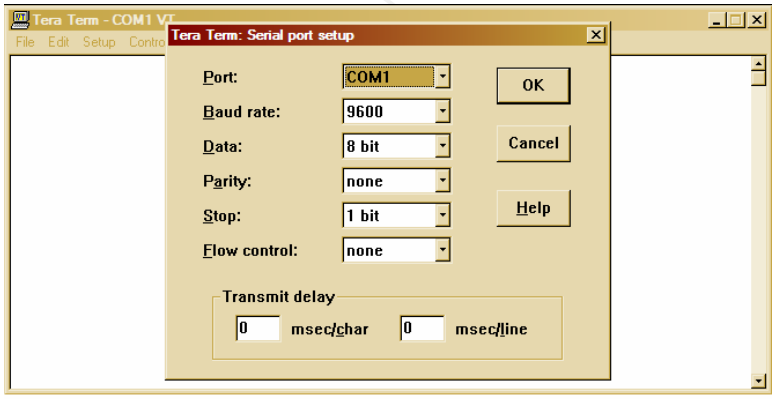

Figure 3-7 – Switches used

***Evidence*:**

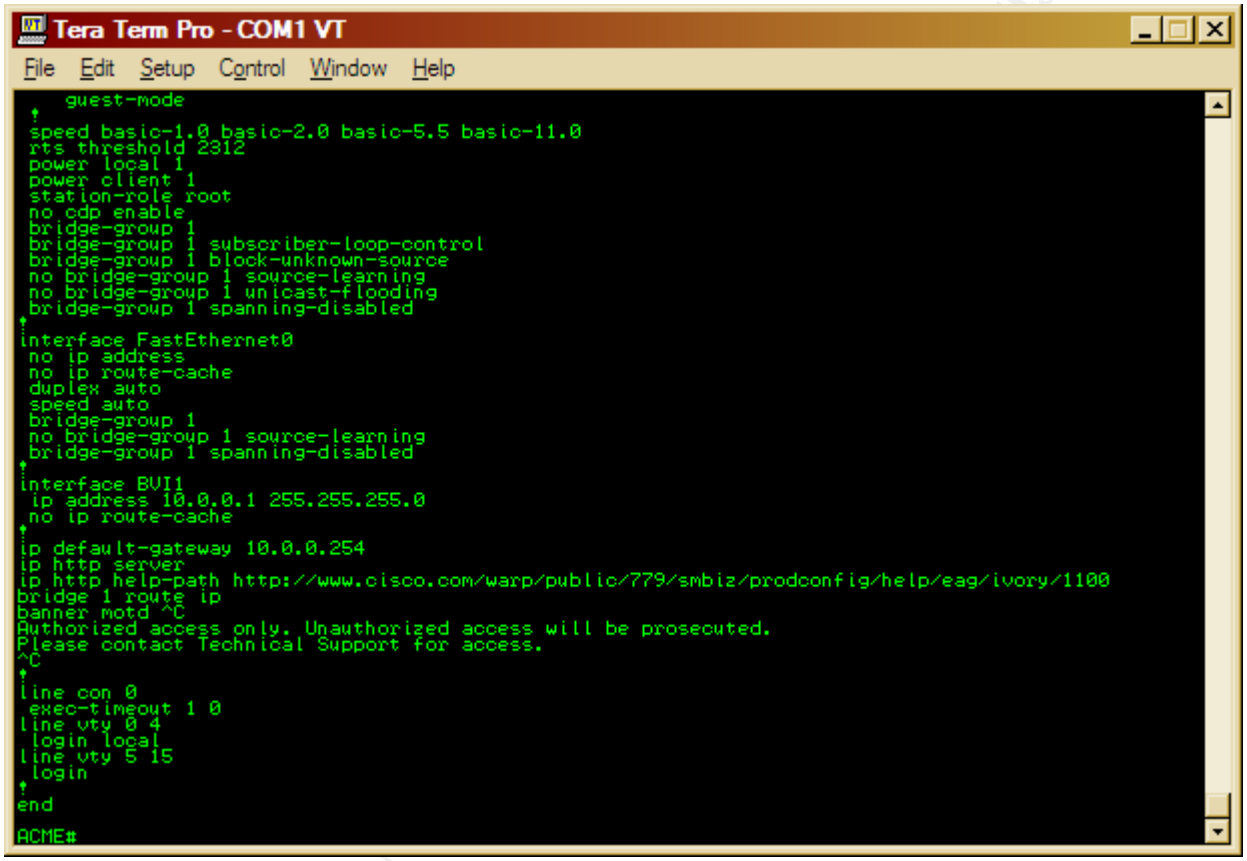

Figure 3-8 - Time out configuration

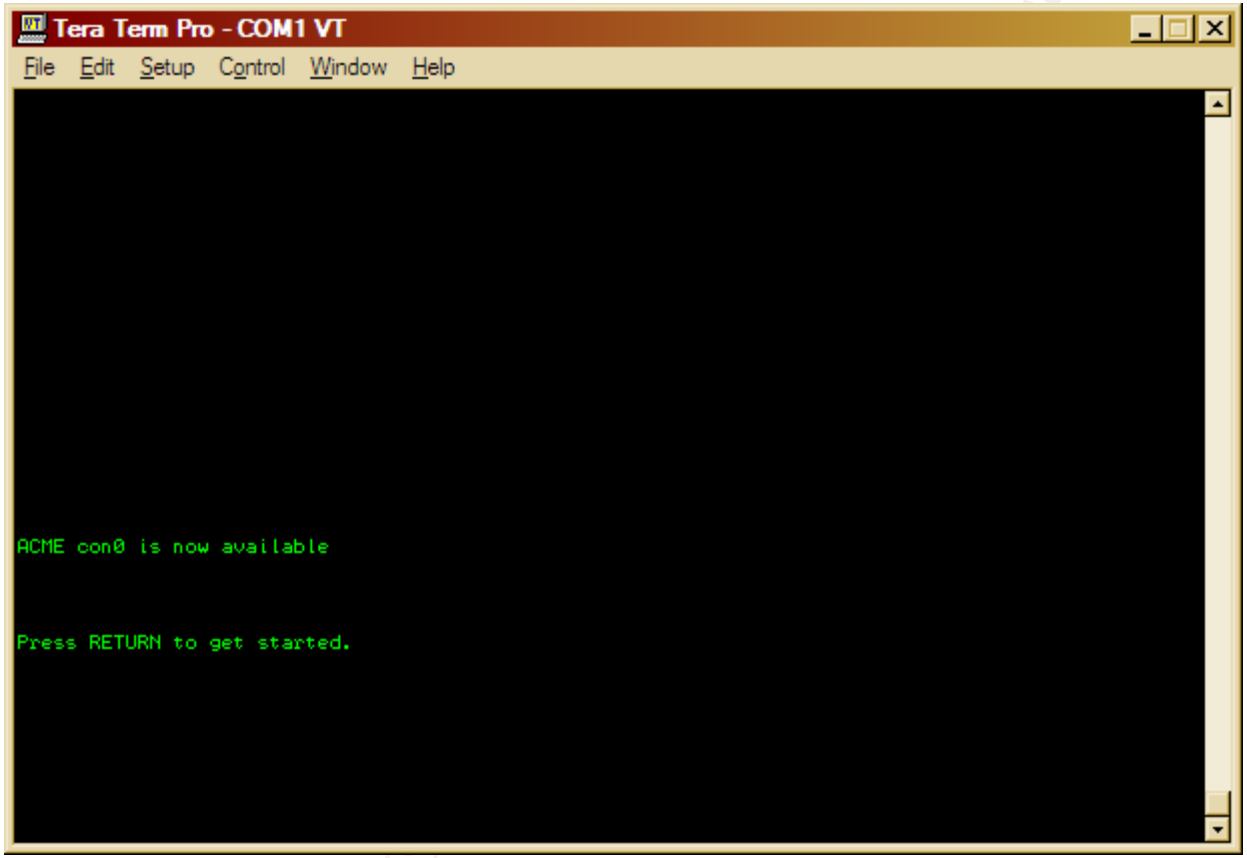

Figure 3-9 - Timed out Administrative Session

***Results*:**
Passed. The timeout strings were found in the running-config as shown in Figure 3-8. Also, shown in Figure 3-9, are the results when testing the timeout configurations; the console session was reset.

Audit Checklist Item - (ACI_04)
Ref: AI_005

Explanation:
The following test will ensure that the factory-default SSID is not being used by the CISCO1200AP. This Audit Checklist Item references AI_005.

Test:
(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-2. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to ensure that the string "ssid tsunami" does not exist. (l) Next, Using Netstumbler on the audit laptop with an Orinoco Card, scan for the SSID "tsunami". (m) Execute Netstumbler. (n) Under Netstumbler select the "Device" menu and ensure that the NDIS drivers are being used for the Lucent Orinoco. (o) Next, restart Netstumbler by clicking on the "Green VCR-like Play button" twice. (p) The CISCO1200AP will now appear in the right pane window. (q) On the left pane window, select the CISCO1200AP by either MAC address or SSID. (r) Ensure that the MAC address in Netstumbler matches that of the MAC address gathered from Audit Preparation.

Command Line and/or Switches:
show running-config
Netstumbler will be used with a default configuration. Ensure that the NDIS drivers for the Lucent Orinoco Card are being used under Netstumbler.

***Evidence*:**

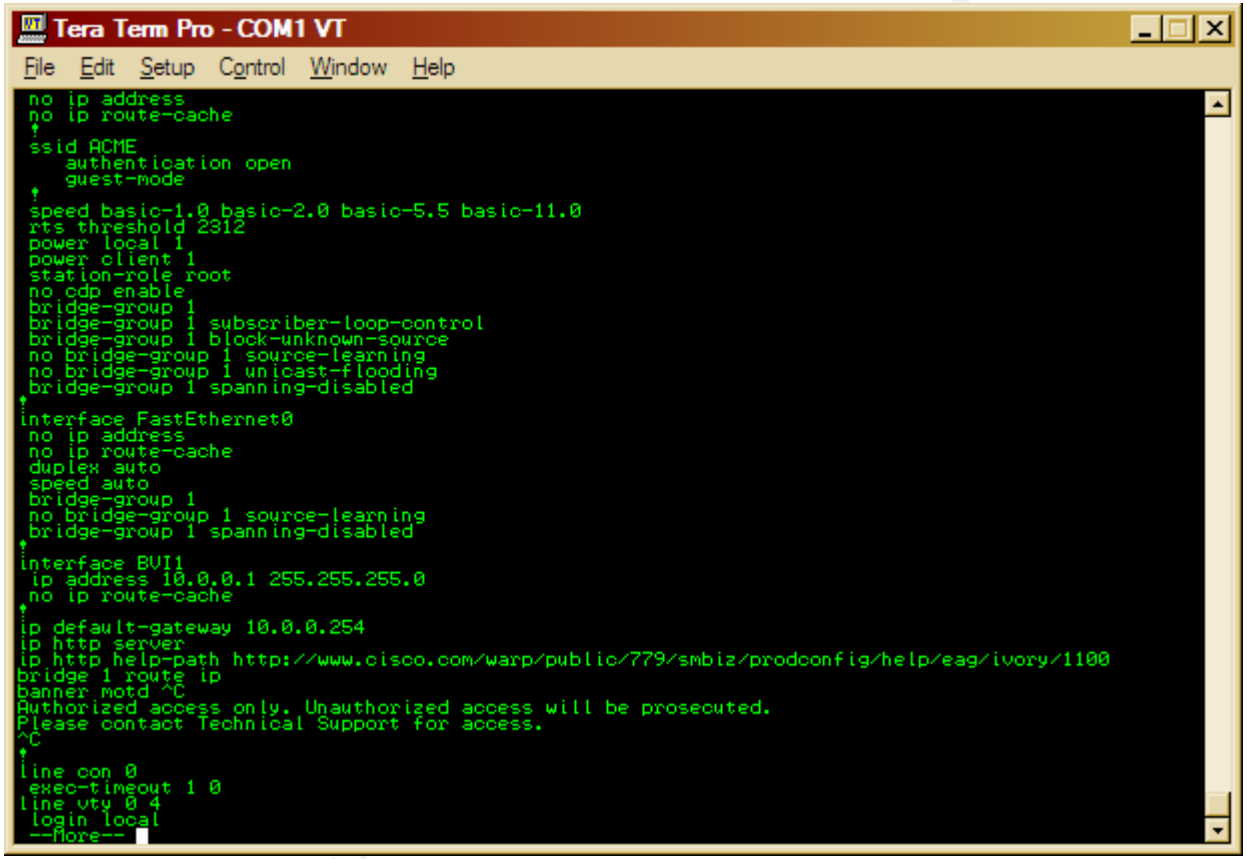

Figure 3-10 - Factory-default SSID is not found

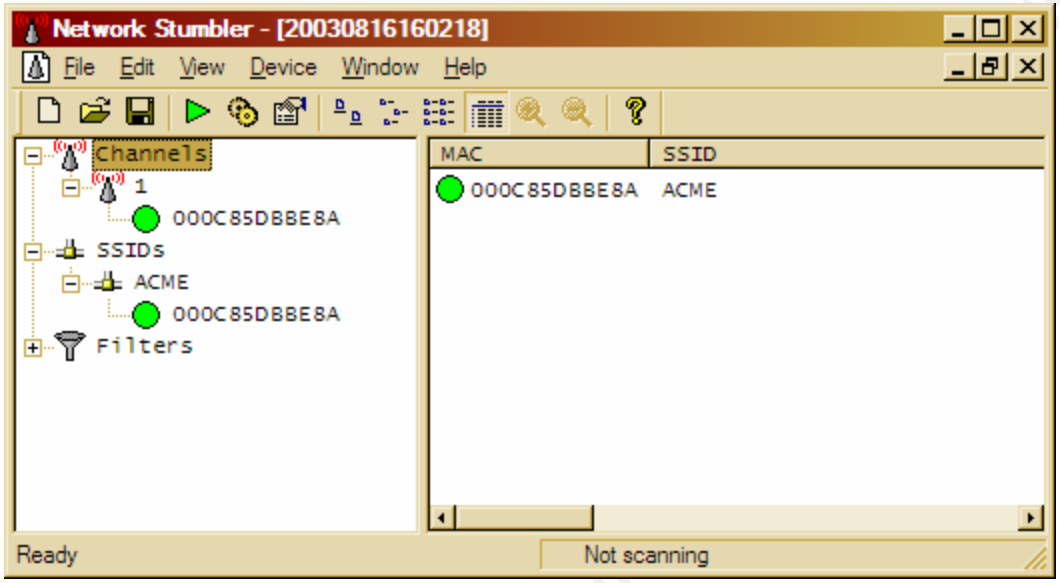

Figure 3-11 - Netstumbler displaying the current SSID of the CISCO1200AP in addition to the MAC address

***Results*:**
Passed. The CISCO1200AP is not configured with the SSID "tsunami". As shown in Figure 3-10, the running-config was found not to contain a line configuring the SSID for "tsunami". In Figure 3-11, Netstumbler was used to verify the SSID was "ACME" not "tsunami".

Audit Checklist Item - (ACI_05)
Ref: AI_006

Explanation:
The following test will ensure that the SSID does not reveal information pertaining to the company, business type and/or physical location. This Audit Checklist Item references AI_006.

Test:
(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-2. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to display the string "ssid xxxxxxxxxx". Ensure that the xxxxxxxxxx does not match the company name, business type, and/or physical location (e.g. address, etc.) (l) Next, Using a laptop with an Orinoco card connect to the xxxxxxxxxx SSID. Upon connection, the CISCO1200AP should report a new association in Tera Term, matching the MAC address of the audit laptop, gathered during the Audit Preparation.

Note: If WEP is needed to associate with the CISCO1200AP use the WEP key gathered during the Audit Preparation.

Command Line and/or Switches:
show config
show running-config
SERIAL, COM1, 9600, 8 BIT, NONE (Figure 3-12)

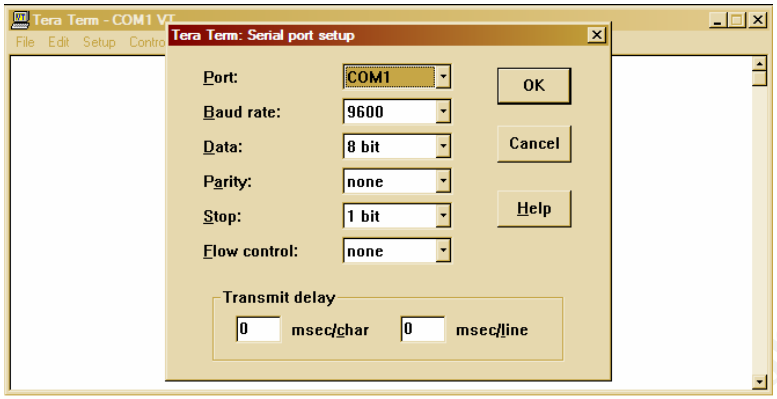

Figure 3-12 – Switches used for Tera Term

***Evidence*:**

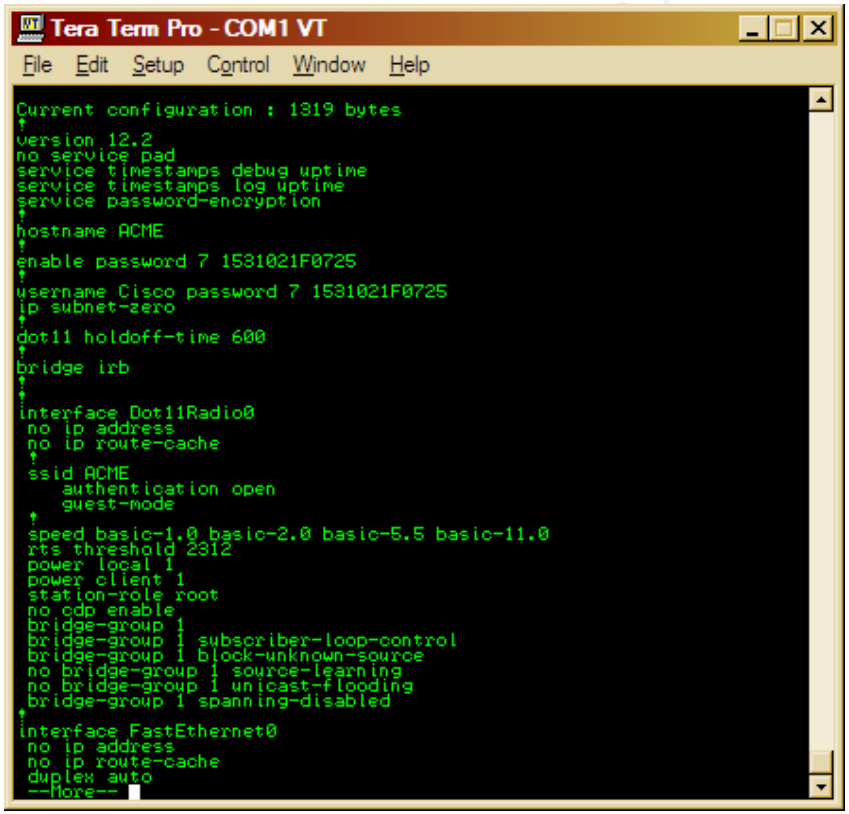

Figure 3-13 - SSID contains the company name, business type or physical location e.g. physical address

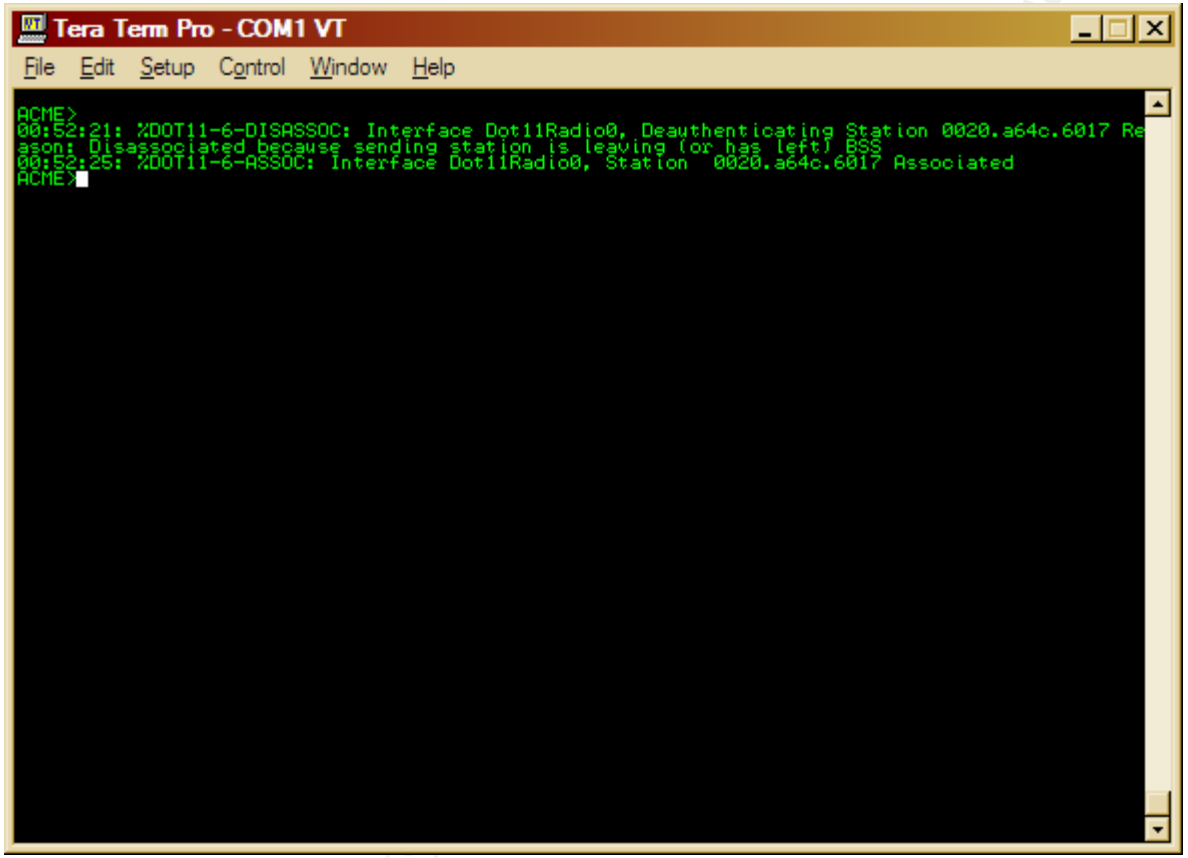

Figure 3-14- Audit laptop connecting to the CISCO1200AP

***Results*:**
Failed. The SSID was "ACME", which matches the company name. As shown in Figure 3-13, the CISCO1200AP running-config contained the line ssid "ACME". To verify the correct CISCO1200AP was being tested, the audit laptop associated, as seen in Figure 3-14, in which the MAC address matches that of the audit laptop. The MAC addressed for the audit laptop was gathered during Audit Preparation.

Audit Checklist Item - (ACI_06)
Ref: AI_007

Explanation:
The following test will ensure that the CISCO1200AP is not "broadcasting" the SSID. This Audit Checklist Item references AI_007.

Test:
(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-2. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to ensure that the string "guest-mode" does not exist. (l) Next, Using Netstumbler on the audit laptop with an Orinoco Card, we will scan for the SSID of the CISCO1200AP. (m) Execute Netstumbler. (n) Under Netstumbler select the "Device" menu and ensure that the NDIS drivers are being used for the Lucent Orinoco. (o) Next, restart Netstumbler by clicking on the "Green VCR-like Play button" twice. (p) The CISCO1200AP will now appear in the right pane window. (q) On the left pane window, select the CISCO1200AP, by either MAC address or SSID. (r) Ensure that the MAC address in Netstumbler matches that of the MAC address gathered from Audit Preparation.

Command Line and/or Switches:
show running-config
Netstumbler will be used with a default configuration. Ensure that the NDIS drivers for the Lucent Orinoco Card are being used under Netstumbler.
SERIAL, COM1, 9600, 8 BIT, NONE (Figure 3-15)

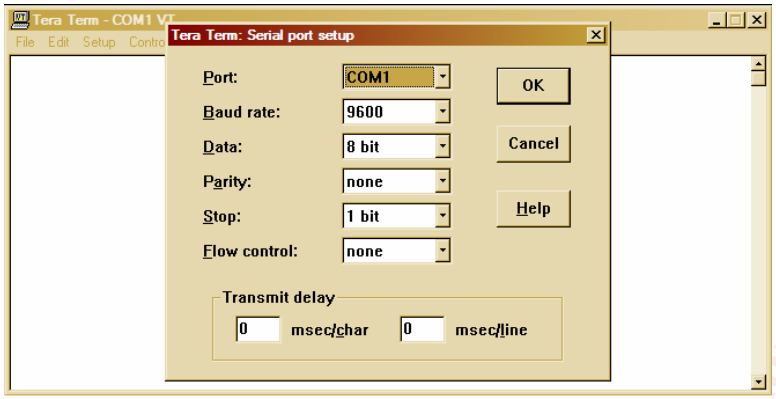

Figure 3-15 - Switches used for Tera Term

***Evidence*:**

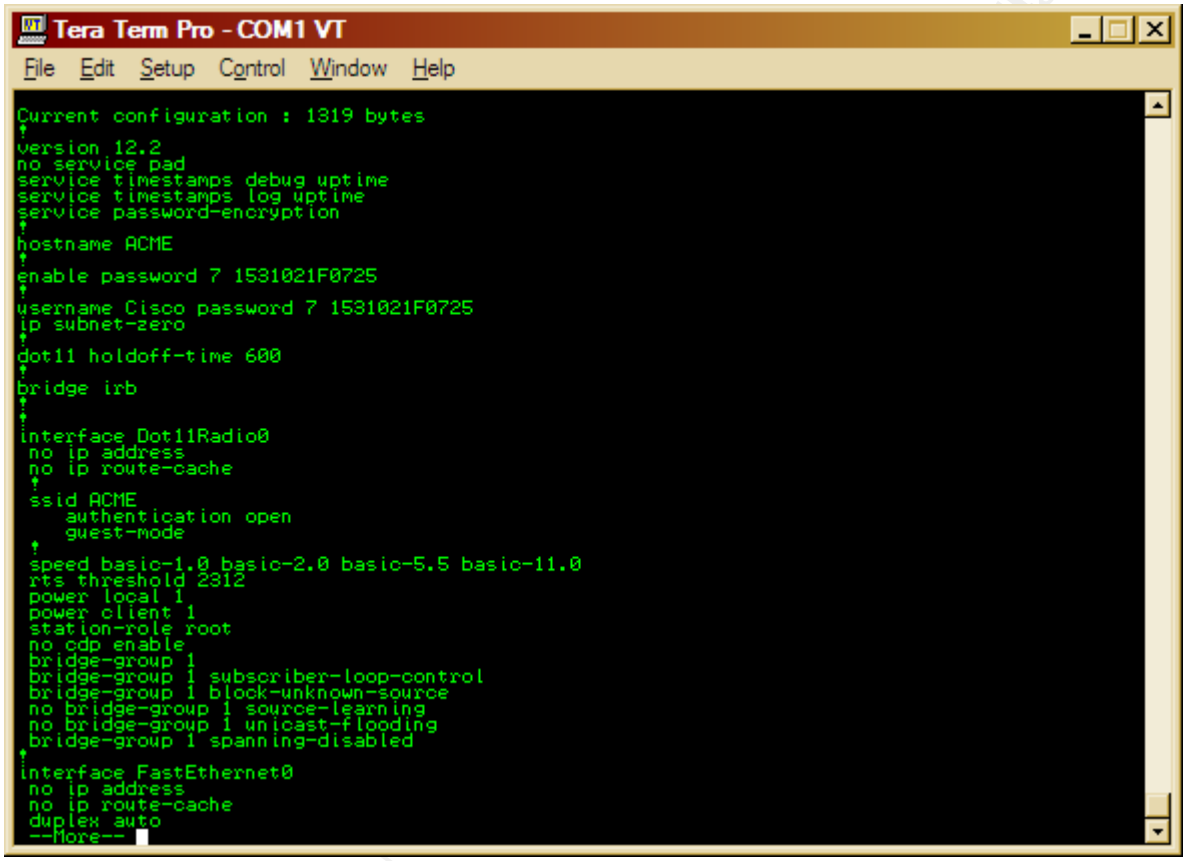

Figure 3-16 - Guest-mode was found enabled

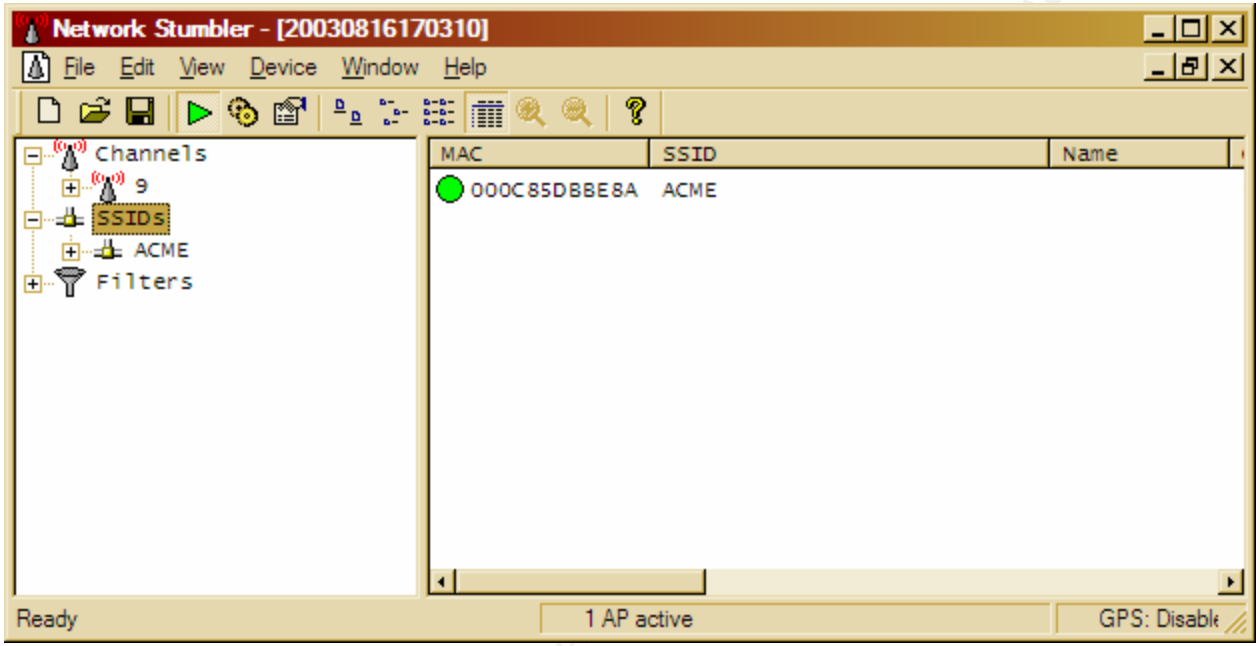

Figure 3-17 - Netstumbler shows that the CISCO1200AP is "broadcasting" the SSID

***Results*:**
Failed. The CISCO1200AP was found "broadcasting" the SSID. As shown in Figure 3-16, the CISCO1200AP running config contained the line "guest-mode" which enables "broadcasting" of the SSID. In Figure 3-17, a test was ran using Netstumbler to ensure that the CISCO1200AP being audited was indeed "broadcasting" the SSID. Shown in Figure 3-17 the CISCO1200AP was "broadcasting" the SSID "ACME".

Audit Checklist Item - (ACI_07)
Ref: AI_008

Explanation:
The following test will ensure the access point authentication method recommended by Cisco is being used. This Audit Checklist Item references AI_008.

Test:
(a) Using a Cisco certified console cable, connect the serial end to the audit laptop's COM1 port (b) Plug the opposite end of the console cable into the console port of the CISCO1200AP, designated by a "light blue" label entitled "console". (c) Execute Tera Term. (d) Under the "File" menu select "New Connection" (f) Select "Serial" and "COM1" and click "OK", Note: The COM1 settings can be found in Figure 3-2. (g) Next, strike the "ENTER/RETURN" key (h) the screen should now display a command line for the CISCO1200AP. (h) If prompted for a username and password, type in the username and password gathered during the Audit Preparation. (i) Next, the command line prompt should end in a "#" symbol, if it does not, type "enable" and hit ENTER. When prompted for the enable password type in the enable password gathered during the Audit Preparation. (j) With the command line ending in a "#" type "show running-config" and hit ENTER" (k) Check the running-config to ensure that the string "authentication open" does not exist.

Command Line and/or Switches:
show config
show running-config
SERIAL, COM1, 9600, 8 BIT, NONE (Figure 3-68)

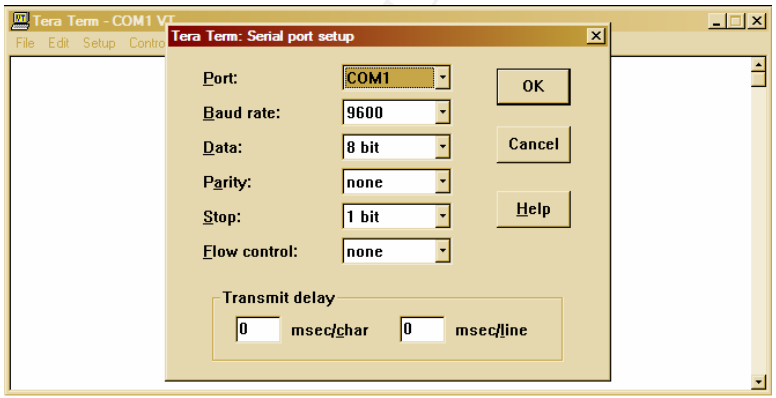

Figure 3-18 - Switches used for Tera Term

***Evidence*:**

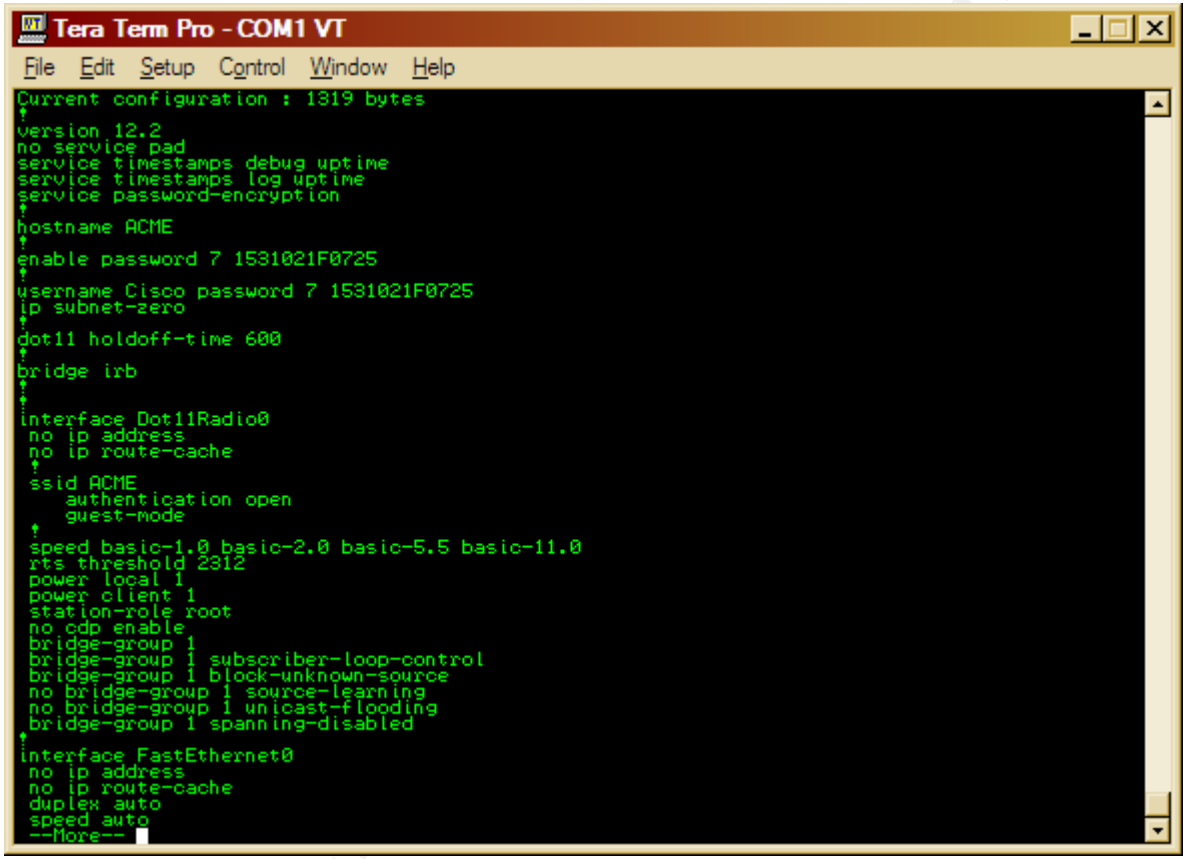

Figure 3-19 - The line "authentication open" does exist

***Results*:**

Passed. As shown in Figure 3-19, the line "authentication open" was found.

Audit Checklist Item - (ACI_08)
Ref: AI_009

Explanation:
The following test ensures that "factory-default" username and password for the administrative Web Management Front End is not being used. This Audit Checklist Item references AI_009.

Test:
Using a web browser connect to the CISCO1200AP over HTTP. Connect to the following address where CISCO1200AP is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ . When prompted for a username and password attempt to use the "factory-default" username and password. The factory default username and password are below. Check to ensure that administrative access to the Web Management Front End is denied

Username: Cisco
Password: Cisco

Command Line and/or Switches:
username: Cisco
password: Cisco

Evidence:

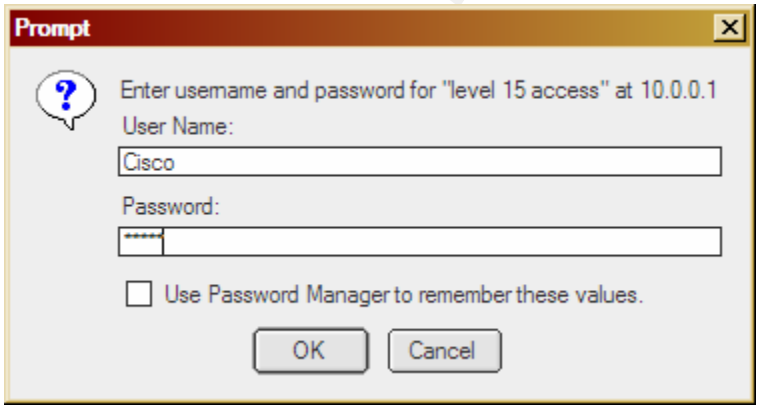

Figure 3-20 - Using the factory-default username and password

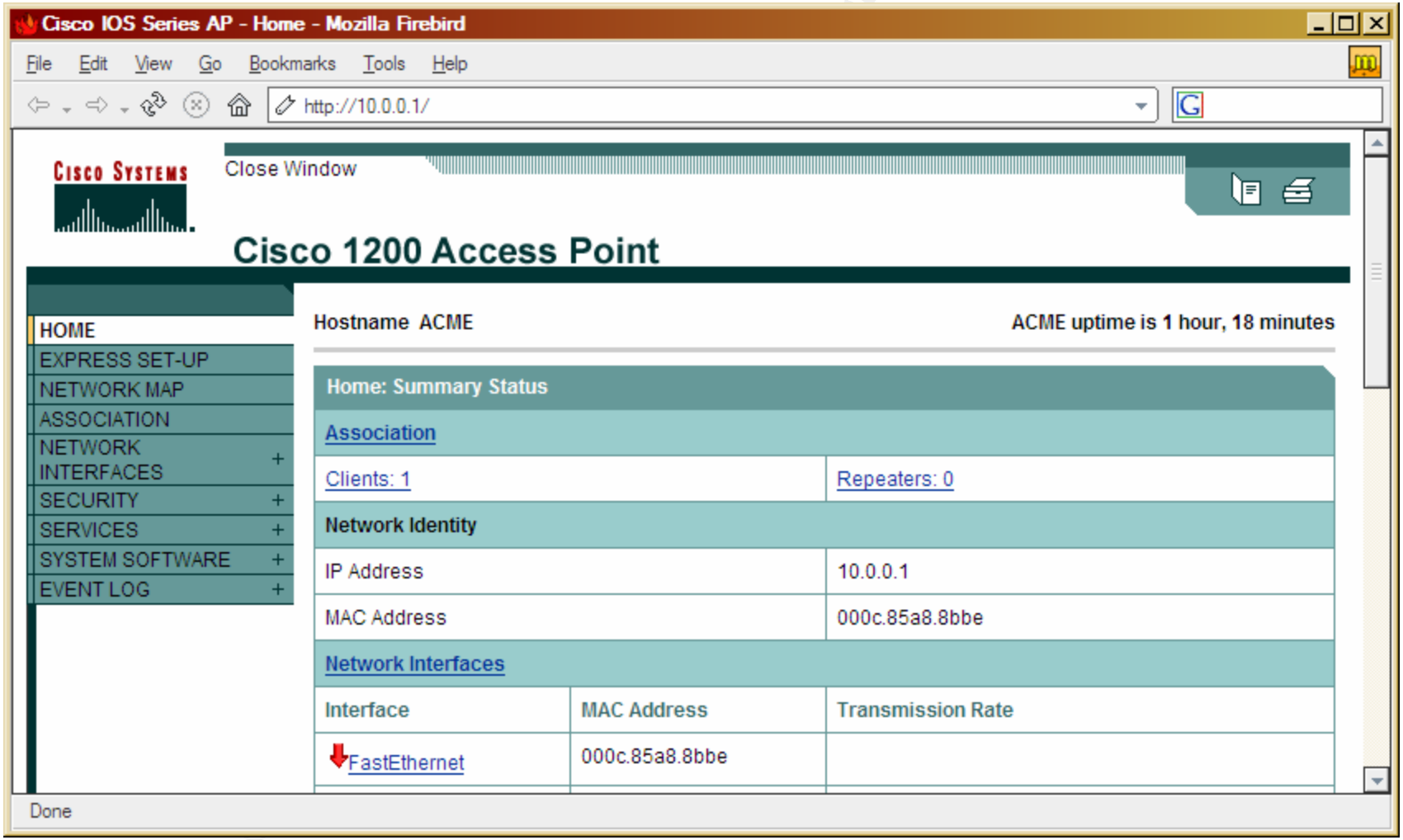

Figure 3-21 - Successful login with the factory-default username and password

***Results*:**
Failed. The "factory-default" username and password granted access to the administrative web front-end. As shown in Figure 3-20, when prompted for the username and password, entering Cisco for the username and Cisco for the password yielded a successful administrative session as shown in Figure 3-21.

Audit Checklist Item - (ACI_09)
Ref: AI_010

Explanation:
The following test will ensure that the default authentication used for the administrative management front-ends has been disabled. This Audit Checklist Item references AI_010.

Test:
(a) Using a web browser connect to the CISCO1200AP over HTTP. Connect to the following address where CISCO1200AP is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ap_sec_local-admin-access.htm. (b) Once connected, under "Security: Admin Access" under "Administrator Authenticated by:" Ensure that "Default Authentication (Global Password)" is not checked. (c) Next, under "User List" ensure that the factory-default user account "Cisco" has been deleted and that a new account has been setup.

Command Line and/or Switches:
None

Evidence:

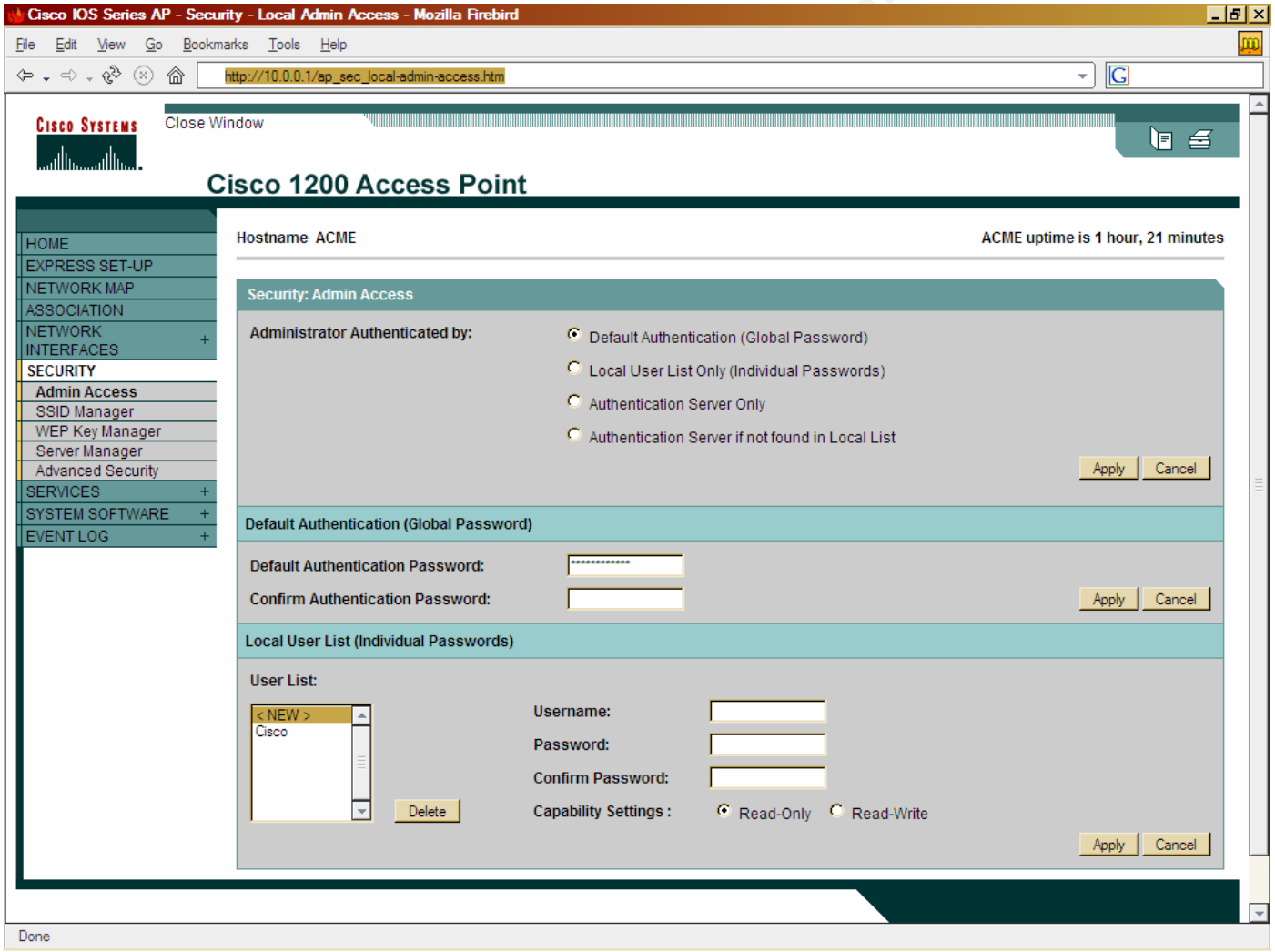

Figure 3-22 - Global Authentication is enabled, with the factory-default user account "Cisco"

***Results*:**

Failed. "Default Authentication" was found enabled with the factory-default user account "Cisco" still in tact. As shown in Figure 3-22, the radio button for "Default Authentication (Global Password)" is filled, enabling the "Default Authentication". Also shown in Figure 3-22, is the default administrative account "Cisco" under the "User List".

Audit Checklist Item - (ACI_10)
Ref: AI_011

Explanation:
The following test will ensure that "best practices for passwords" have been used for the administrative username and password for administrative Web Management Front End. This Audit Checklist Item references AI_011.

Test:
Using Brutus, with a customized dictionary file, attempt to brute force the administrative account through the web front-end. (a) Execute Brutus. (b) Once executed modify the settings of Brutus to match Figure 3-23. (c) Run the test.

Command Line and/or Switches:

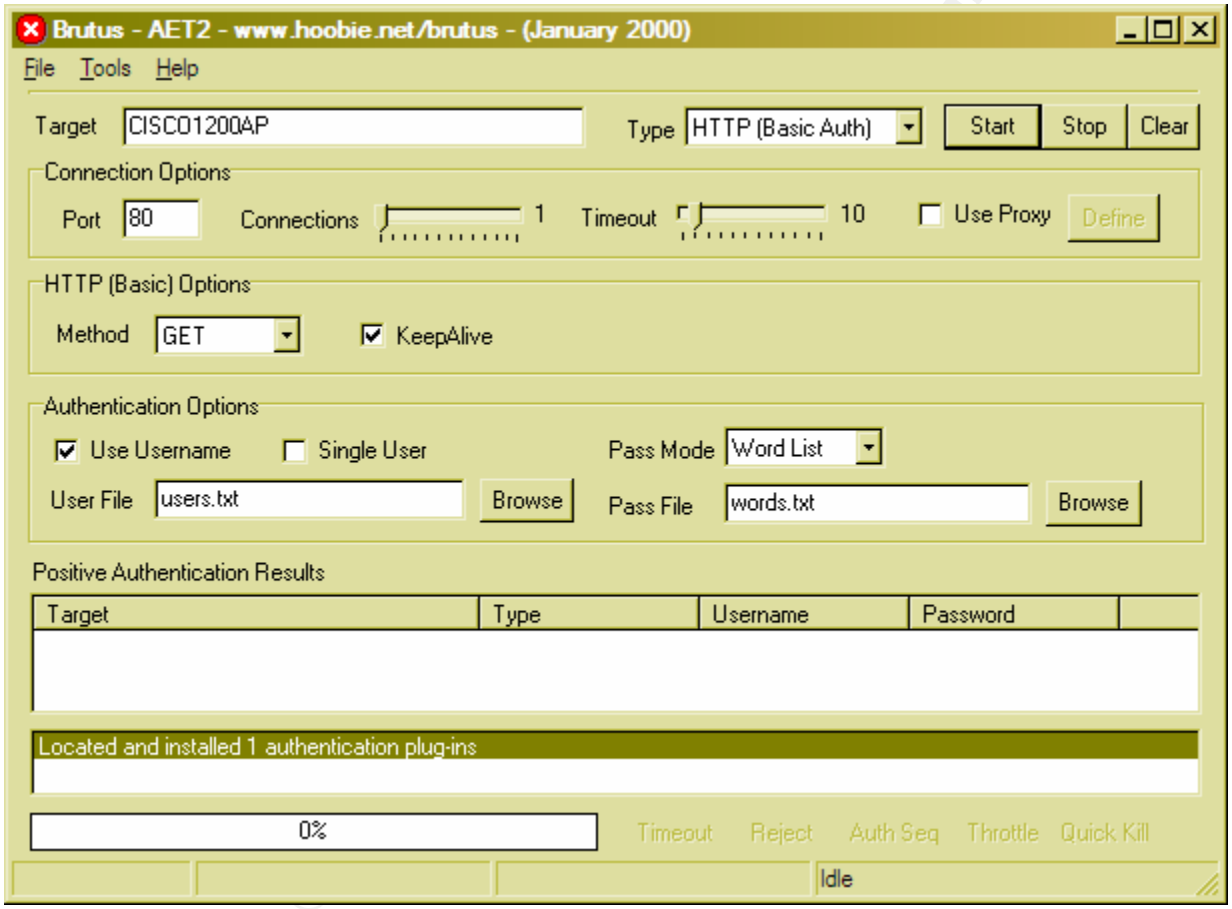

Figure 3-23 - Switches used for Brutus

***Evidence*:**

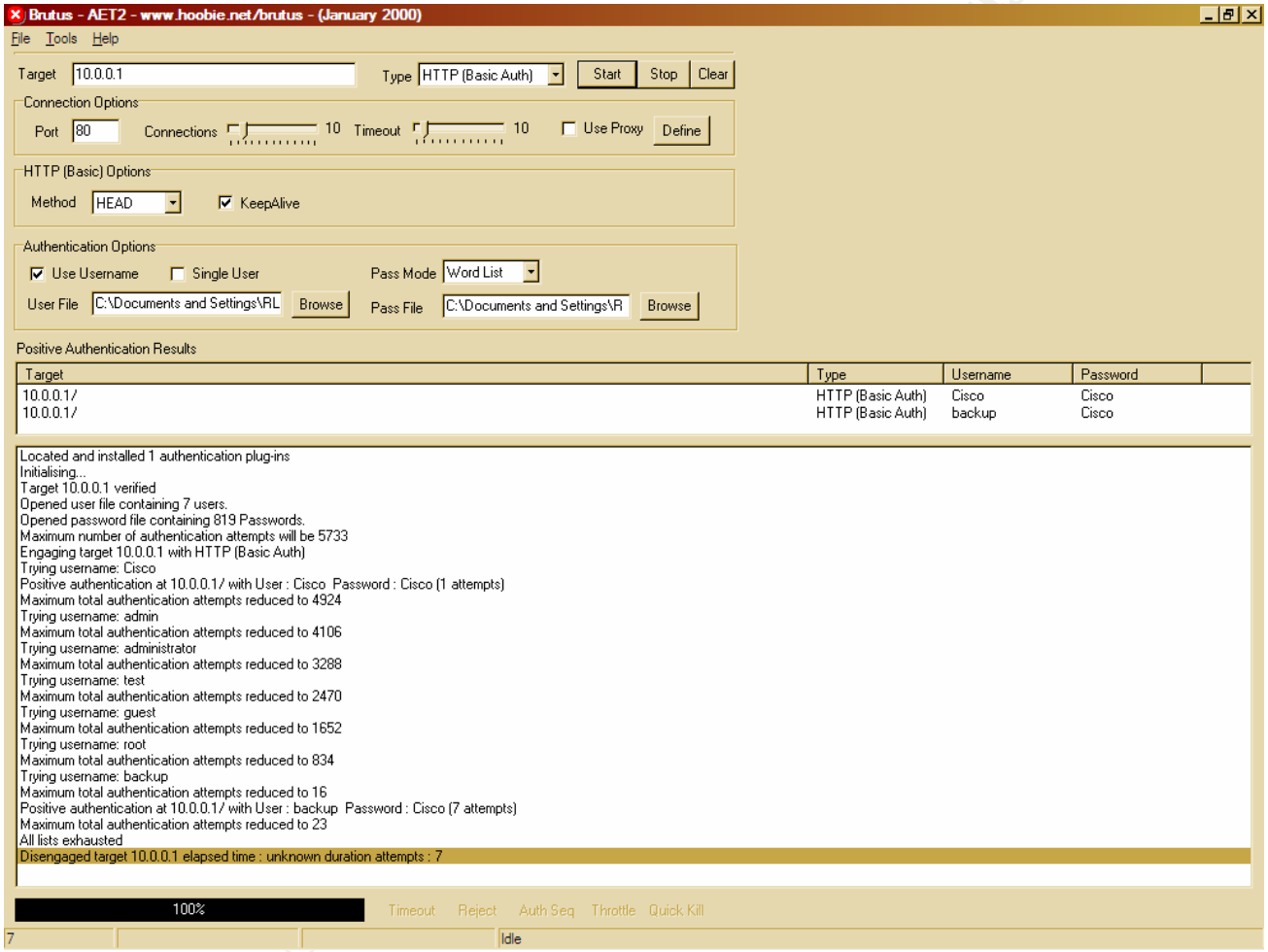

Figure 3-24 - Showing those usernames and passwords that Brutus successfully cracked

***Results*:**

Failed. Username and passwords were successfully brute forced by Brutus. As shown in Figure 3-23, Brutus was configured with the following settings and a custom dictionary file, which contained the user, "Cisco" and a word list that contained the word "Cisco". As shown in Figure 3-24, Brutus was successfully able to brute force the username and password "Cisco:Cisco" and "backup:Cisco".

Audit Checklist Item - (ACI_11)
Ref: AI_012

Explanation:
The following test will ensure that MAC authentication is enabled and working properly. This Audit Checklist Item references AI_012.

Test:
(a) Using a web browser connect to the CISCO1200AP over HTTP. Connect using the following address, where "CISCO1200AP" is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ap_sec_ap-client-security-adv_a.htm . (b) Verify that authorized MAC addresses are specified under "Local MAC Address". (c) Next, using a wireless network card that is authorized attempt to authenticate to the CISCO1200AP. (d) Once authenticated, which is indicated by an active connection to the CISCO1200AP's SSID, attempt to ping the IP address of the CISCO1200AP. (e) Lastly, repeat steps with an unauthorized wireless card. (f) When using the unauthorized wireless card a failure in an attempt to connect indicates that MAC authentication is functioning properly.

Command Line and/or Switches:
ping CISCO1200AP

Evidence:

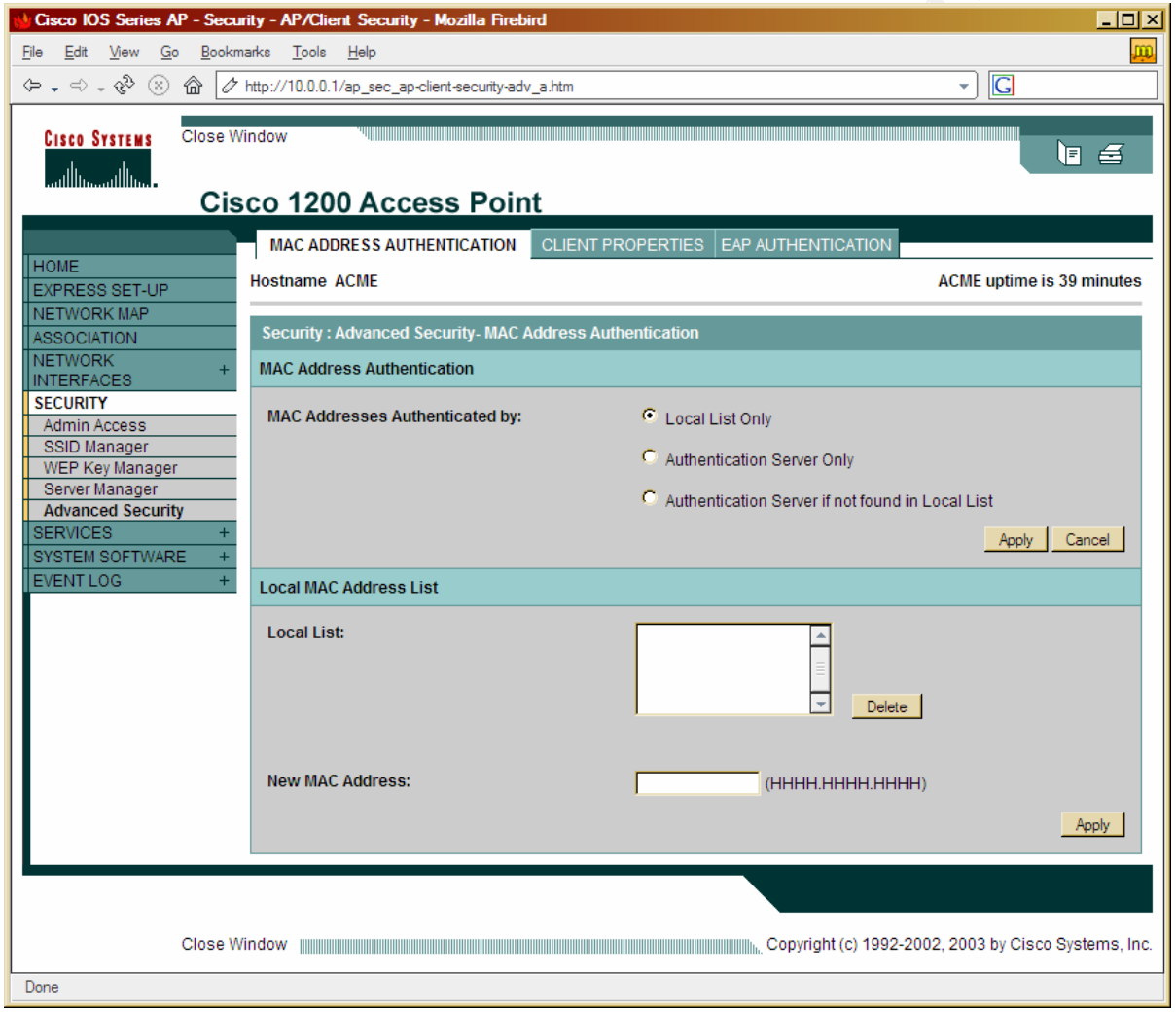

Figure 3-25 - The Local List does not include any MAC addresses

Results:

Failed. The "Local List" did not include any MAC addresses. Due to the fact that there are no MAC addresses in the "Local List"; the testing of authorized and unauthorized MAC addresses could not be done.

Audit Checklist Item - (ACI_12)
Ref: AI_013

Explanation:
The following test will ensure that WEP is enabled, that its use is mandatory and that WEP is set for 128-bit. This Audit Checklist Item references AI_013.

Test:
(a) Using a web browser connect to the CISCO1200AP over HTTP. Use the following address, where "CISCO1200AP" is substituted for the IP Address gathered from the Audit Preparation: http://CISCO1200AP/ap_sec_ap-key-security.htm . (b) Under "Encryption Modes" ensure that "WEP Encryption" is set to mandatory. (c) Next, under "WEP Keys" ensure that 128bit encryption is being used. If the above test fails, DO NOT move onto the next testing steps, as it is unnecessary. Reason being is the rest of the audit tests the WEP configuration. Because WEP is not enabled, the remaining items cannot be tested.(d) Next, test that WEP is functioning by connecting with a Lucent Orinoco Card. Enter the WEP key and WEP level given during the Audit Preparation into the Lucent Orinoco Card wireless utility. (e) Attempt to associate. (f) If associated, ensure the WEP is 128-bit, by attempting to ping the CISCO1200AP. (g) Ensure that the connected AP's MAC address matches that of the audited CISCO1200AP.

Command Line and/or Switches:
ping CISCO1200AP

Evidence:

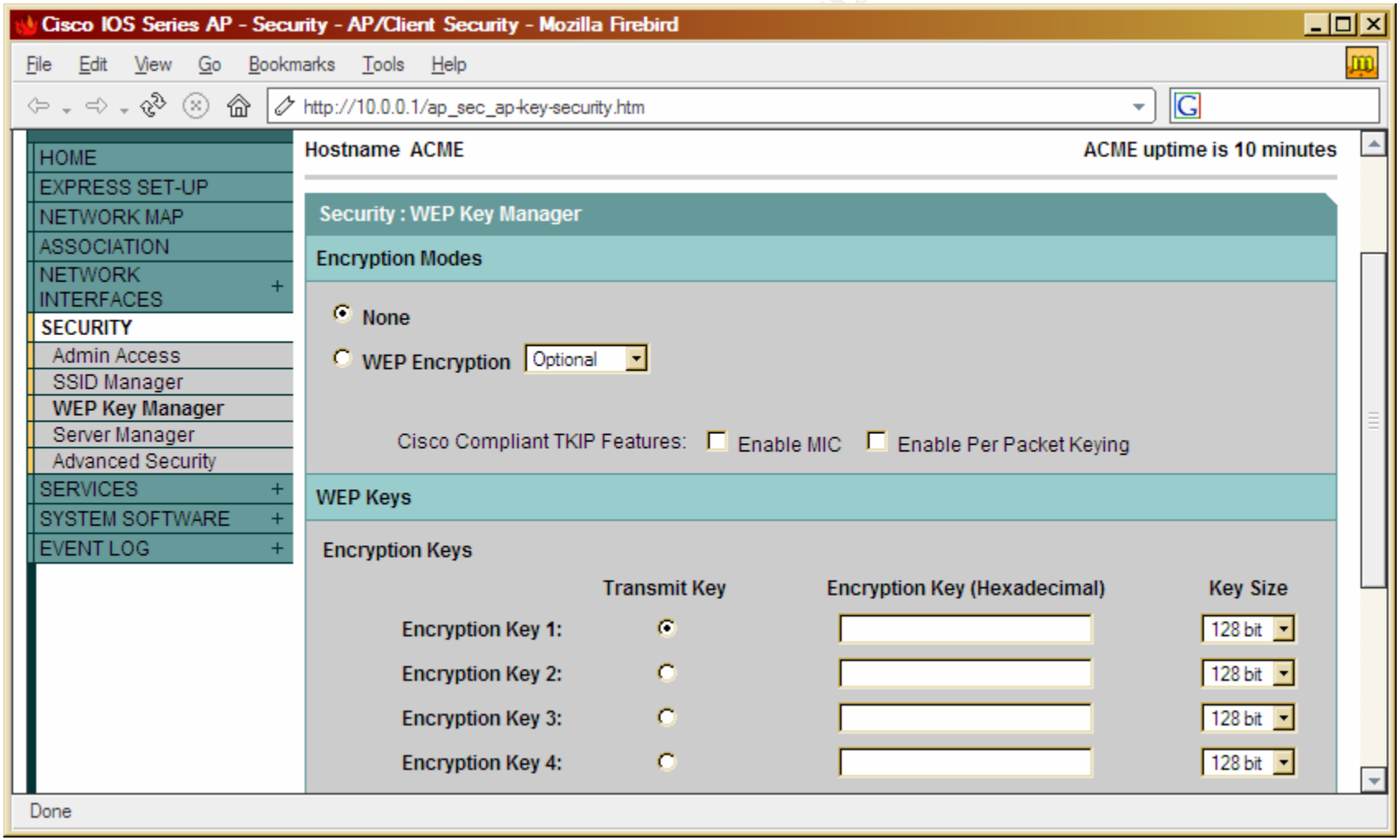

Figure 3-26 - WEP settings for the CISCO1200AP

***Results*:**

Failed. WEP was disabled. As shown in Figure 3-26, the CISCO1200AP was found to have WEB disabled and unconfigured.

Section 3.1.1– Residual Risk and System Auditable Details

Residual Risk
During the audit several audit checks were done to test integrity, confidentiality and availability as it relates to the CISCO1200AP. Over the course of the audit a majority of the audit checks reported a status of 'failed'. The majority of the audit checks that reported failure were due to misconfiguration or unmodified factory-default settings. Factory-default settings are the configuration a device has when leaving the factory. Factory-default settings are the first thing an attacker will try in an attempt to break-in. Because factory-default settings are such an easy target the risk is HIGH that a break-in could occur. All vulnerabilities found could be fixed by reconfiguring the CICSCO1200AP with wireless security best practices in mind.

It is highly recommended that WEP be enabled and that the key be changed once a month. Because WEP was found disabled and unconfigured, it is possible that data being transmitted to and from the CISCO1200AP to client devices could be compromised. It is recommended that factory-default settings such as user authentication, usernames and passwords, be changed from their factory-default settings.

The amount of residual risk that exists from the audit checks that were done is minimal. The audit aims to exercise industry best practices as it relates to wireless security. Although this audit briefly addressed the cracking of WEP it should be noted that residual risk exists in this area. For example, it is possible for an attacker to crack WEP by grabbing sample RF transmissions destine to and from the CISCO1200AP and using them to decipher and decrypt the active WEP key. The mitigating control for this would be the use of TKIP. Although, TKIP is out of the scope of this paper, it is highly recommended that research go into how TKIP could be used in the ACME Company environment. More advanced wireless attacks such a de-auth floods, RF jamming, AP spoofing, etc. were not addressed in this audit. However, because some of the advanced attacks prey on the physical nature of wireless it becomes rather difficult to mitigate. Because advanced wireless attacks exist there still remains a measure of residual risk.

The cost to mitigate vulnerabilities found in the audit checklist would be minimal. Initially no additional hardware/software is needed. The majority of the fixes needed could be done in-house.

System Auditable Details
A majority of the CISCO1200AP is auditable. In many respects the methods used to audit routers and firewalls, can be carried over similarly to the CISCO1200AP. However, because of the physical medium aspect of the CISCO1200AP, in that it is wireless, it is difficult to pin down or secure the RF signals. An attack with high gain antennas and special wireless equipment could continue to connect to the

RF stream of the CISCO1200AP. In addition, the decrypting of wireless communication is susceptible to known attacks, but unknown attacks could exist or a flaw in the implementation by the manufacturer. Also, if the CISCO1200AP is made secure there is not guaranty that configuration policies and procedures are or will be followed.

Section 4– Audit Report

Section 4.1 - Executive Summary

The scope of this audit was to measure risk; in particular the device being used to provide the programming department wireless access to the company network and Internet. The device being audited was a Cisco Aironet 1200 Wireless Access Point (CISCO1200AP). With regards to risk, ACME Company management expressed concern that the CISCO1200AP, if compromised, could cause company resources to be susceptible to attack (deleting, modifying, stealing, etc.)

The main concern is that any unauthorized individual with a wireless card and little to no knowledge could easily connect to the ACME Company network and Internet service from anywhere e.g. parking lot, building lobby, across the street, several miles away. With access to the company network and/or Internet an attacker could begin to attempt deletion, modification, theft, etc. to any or all company resources. The CISCO1200AP comes packaged with several security features to mitigate such attacks and can be configured in a minimal amount time to do so.

The CISCO1200AP was found to have a HIGH risk. The following areas are where the majority efforts should be pointed.

- **Increasing security supported by the CISCO1200AP** – Because the CISCO1200AP supports several security features to mitigate a majority of the issues, the CISCO1200AP should be taken offline until security features such as WEP, MAC authentication, RF transmission strength, SSID naming convention, and the modification of factory-default usernames and passwords are configured. The estimated cost of this would be 1-2 days. No additional hardware is needed.
- **CISCO1200AP placement** – Because the CISCO1200AP is near an outside wall and window the radio coverage leaks outside the ACME Company 6th floor. The radio coverage provided outside and to unauthorized areas is to strong. The CISCO1200AP should be placed in the center of the 6th floor as it is possible. The estimated cost would be 1-2 days with $300-$1,000 invested in wiring cable. However, the cabling could be down in house if staff is able.
- **Staff training and/or lab equipment** – Because the CISCO1200AP needs to be configured for security and stay secure, staff should be sent to training and/or provided lab equipment to test on. The estimated cost of

this would be 3-4 days in addition to training costs estimated at $300-$2000.

The summarized results of the audit can be found in the below matrix, shown in Figure 4-1. All audit objectives were complete and thoroughly tested. Below, a matrix makes reference to the Audit Checklist Items (ACI) and the Audit Items (AI) used in this report.

(ACI_01) – Unauthorized wireless coverage	*FAILED*
(ACI_02) – Warning banners	*PASSED*
(ACI_03) – Timeouts for administrative connections	*PASSED*
(ACI_04) – Factory default SSID	*PASSED*
(ACI_05) – SSID name convention	*FAILED*
(ACI_06) – SSID broadcasting	*FAILED*
(ACI_07) – Access point authentication type	*PASSED*
(ACI_08) – Factory default username and password	*FAILED*
(ACI_09) – Factory default Web Front authentication	*FAILED*
(ACI_10) – Best practices for usernames and passwords	*FAILED*
(ACI_11) – MAC address filtering	*FAILED*
(ACI_12) – WEP enabled, mandatory and 128-bit	*FAILED*

Figure 4-1 – Matrix summarizing Audit Checklist results

Section 4.1.1– Audit Findings

An audit was taken to assess the level of risk posed to ACME Company by the use of the Cisco Aironet 1200 Wireless Access Point (CISCO1200AP). A checklist was written encompassing industry "best practices" for wireless security and vendor recommendations. Each checklist item was checked for compliancy. Below is a summary of the results.

The CISCO1200AP was found with many "factory-default" configurations in place. Factory-default are those settings that are set by the factory before delivery. Factory-default settings are the usual cause of most break-ins. The CISCO1200AP was found to have failed all audit checks that address factory-defaults. Those failed were ACI_04, ACI_08, ACI_09.

The CISCO1200AP has not been configured with wireless "best practices" in mind. The CISCO1200AP was found to have failed five out of six audit checks that address wireless "best practices". Those failed were ACI_01, ACI_06, ACI_08, ACI_11, ACI_12.

Section 4.1.2– Background / Risk

The CISCO1200AP was found with many "factory-default" configurations in place. Factory-default are those settings that are set by the factory before delivery. Factory-default settings are the usual cause of most break-ins. The

CISCO1200AP was found to have failed all audit checks that address factory-defaults. Those failed were ACI_04, ACI_08, ACI_09.

The CISCO1200AP has not been configured with wireless “best practices” in mind. The CISCO1200AP was found to have failed five out of six audit checks that address wireless “best practices”. Those failed were ACI_01, ACI_06, ACI_08, ACI_11, ACI_12.

The following is a summary of the findings of each audit item. The failing items contain a brief explanation as to why the status was reported as FAILED. Each item references its parent Audit Checklist Item (ACI) and Audit Item (AI).

- (ACI_01) – Unauthorized wireless coverage - FAILED
  - The amount of coverage in unauthorized areas is too great.
- (ACI_02) – Warning banners - PASSED
- (ACI_03) – Timeouts for administrative connections - PASSED
- (ACI_04) – Factory default SSID - PASSED
- (ACI_05) – SSID name convention – FAILED
  - The SSID was found to be “ACME” which reveals the owning company of the CISCO1200AP. This could lead to possible attacks.
- (ACI_06) – SSID broadcasting - FAILED
  - The SSID was found broadcasting. SSID broadcasting gives an attacker the ability to discover the CISCO1200AP. If discovered the CISCO1200AP could become an attack vector.
- (ACI_07) – Access point authentication type – PASSED
- (ACI_08) – Factory default username and password - FAILED
  - With the factory default username and password set, an attacker could gain administrative access to the CISCO1200AP.
- (ACI_09) – Web Management Front end – FAILED
  - The web management was found to be enabled on the CISCO1200AP. Because the web management passes the administrative username and password in clear text it should be disabled.
- (ACI_10) – Best practices username and passwords – FAILED
  - An attempt to brute force the username and password was successful. An attack could launch the same brute force attack on the CISCO1200AP to gain administrative access to the CISCO1200AP.
- (ACI_11) – MAC address filtering – FAILED
  - MAC address filtering was found to be disabled.
- (ACI_12) – WEP enabled, mandatory and 128-bit – FAILED
  - WEP was found to be disabled and not configured.

Section 4.1.3– Audit Recommendations

To mitigate the level of risk posed by the CISCO1200AP it is recommended that all wireless security “best practices” outlined in the full audit report be put in

place. In addition, the below information is a brief outline into industry “best practices” as it relates to wireless security.

Access point placement
Placing the access point near a window or adjoining door is not recommended. It is recommended that the access point be placed as close to the center of the infrastructure as it is possible. Checking the coverage the wireless implementation provides is key to security. Using site survey tools is a great way to test coverage.

Enable WEP
Although Berkeley was able to prove that the key exchange used by WEP is flawed, it is still highly recommended that WEP be enabled. One recommendation to mitigate this risk is to change your WEP key often. The frequency in which one should change the WEP key depends on the amount of data transmitted; as it takes anywhere from 5 million to 10 million packets of sample data to successfully crack WEP. However, newer methods to speed the process of cracking WEP are being used; such as packet injection to gather sample data. Also using the highest level of WEP offered (128-bit or more) is highly recommended.

Disable broadcasting SSID or an SSID of “ANY”
By disabling the broadcasting of the SSID you are able to raise the level of security by minimizing the successful detection of the CISCO1200AP. Tools like “Netstumbler” rely on beacon packets; packets sent out by an access point to broadcast the SSID. However, tools like “Kismet” can use raw RF monitoring to detect access points, regardless if broadcasting is turned off.

Securing the SSID
Changing the SSID from its factory default setting is recommended. With the knowledge that an access point is a specific vendor an attacker could attempt default usernames and passwords and other known vulnerabilities pertaining to the access point to further increase the success of a break in. Also, it is not recommended that the SSID be the name of the company, physical address or something in relation to the companies business type; e.g. donuts for a Donut Store WLAN.

Filtering
Most access points now ship with the ability to filter by MAC address (Layer 2) and IP (Layer 3). It is recommended that you enter the MAC addresses of those clients authorized to access the WLAN. It is also recommended that ACL’s be put in place where appropriate. Although, it is quite possible to spoof an authorized MAC address, this allows for one more layer of security the attacker would have to overcome to be successful.

Disabling unneeded services
It is recommended that unneeded services be disabled such as telnet, should be disabled.

In addition, a firewall should be purchased to raise the level of security and add an additional layer of security to the ACME Company. The firewall can be put in place so that it would be between the ACME Company network and the CISCO1200AP.

It is also recommended that better authentication for access to the CISCO1200AP be put in place, Authentication, such as RADIUS, can be put in place with no additional equipment.

It is also recommended that a wireless policy be put in place in regards to management of the CISCO1200AP e.g. how often the WEP key should be changed, logging of configuration changes to the CISCO1200AP, upgrades, patches, etc. preventative controls in place, such as policies, allow the CISCO1200AP to stay current with the latest security updates and upgrades

It is recommended that training be offered to MIS or those in charge of managing the CISCO1200AP. The CISCO1200AP boasts an array of enterprise class controls such as; VLANS, filtering, LEAP, RADIUS support, etc. that ACME Company could take advantage of immediately for a very minimal cost. At the time of this document the cost of CISCO1200AP training is unknown.

Section 4.1.4– Cost
The following is a cost summary for the recommendations giving.

- **Increasing security supported by the CISCO1200AP**
  - Time Needed: 1-2 days
  - Hardware/Software Cost: None
  - Total Cost: 1-2 days
- **CISCO1200AP placement**
  - Time Needed: 1-2 days
  - Hardware/Software:
  - Other: $300-$1,000, depending on wiring crew.
  - Total Cost: 1-2 days and wiring
- **Staff training and/or lab**
  - Time Needed: 3-4 days
  - Hardware/Software: None
  - Other: Training est. $300-$2000.
  - Total Cost: 3-4 days and training

References

Note: A great amount of Cisco Systems documentation is only offered to registered customers. Because of this, URL's to customer only documentation has not been included.

Geirer, Jim. "802.11 WEP: Concepts and Vulnerability"
June 2002
URL: http://www.80211-planet.com/tutorials/article.php/1368661

Lubow, Eric. "Six Basic Tips to Securing Wireless Network"
December 2002
URL: http://www.linuxsecurity.com/articles/documentation_article-6346.html

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

Convery, Sean and Miller, Darring and Sundaralingam, Sri. "Cisco SAFE: Wireless LAN Security in Depth (version 2)"
URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

Borisov, Nikita and Goldberg, Ian and Wagner, David. "Berkeley papers concerning WEP vulnerabilities"
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Cisco Systems. "Cisco Aironet 1200 Series Access Point Software Configuration Guide"
URL:http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/ap120scg/apbkscg.pdf

Cisco Systems. "Cisco Aironet 1200 Access Point – Security Setup"
URL: http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/ap120scg/bkscgc8.htm

Wikipedia Encyclopedia. "Explanation of the RC4 cipher"
August 2003
URL: http://www.wikipedia.org/wiki/RC4_cipher

Cisco System. "Cisco Aironet 1200 Series Installation Guide"
January 2002
URL:http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_chapter09186a0080147d6f.html#1036179

Smith, Del. "Cisco Aironet 1200 APs support multiple WLAN protocols"
August 2002
URL:http://techrepublic.com.com/5100-6265-1051061.html

Flexguard Security System. "Installation Instructions"
2003
URL:http://www.flexguard.com/install_cable.html#attach

Hassick, Brian. "Simple Wireless Exposure in Traditional Networks"
First Quarter 2002
URL:http://www.sbq.com/sbq/wireless/sbq_wireless_exposures.pdf

IBM. "Wireless Networks: Avoid security exposure; protect your investment"
N/A
URL http://www-1.ibm.com/services/strategy/e_strategy/security_exposure.html

Piscitello, David M. "Tools and Tactics for Safer WLAN Deployment"
N/A
URL:http://www.corecom.com/external/livesecurity/saferwlan.htm

NASA IT. "Security Warning Banner"
N/A
URL:http://lupus.gsfc.nasa.gov/security_web.html

ITSC. "Logon Warning Banners"
N/A
URL:http://www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/WarnBanner.htm

Cisco Systems. "List of Supported IOS Commands"
N/A
URL:http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_command_reference_chapter09186a00801494f3.html

PC Magazine. "Wireless LANS at Risk"
N/A
URL:http://www.pcmag.com/article2/0,4149,1175896,00.asp

Mohney, Doug. "WiFi Wardriving"
September 1, 2003
URL http://www.synchrologic.com/2003/09/23/eng-primemedia/eng-primemedia_112118_5773960666571695083.html

Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practice"
N/A
URL:http://www.arstechnica.com/paedia/w/wireless-security-howto/home-802.11b-2.html

PC Magazine. "Wireless LANS at Risk"
N/A

URL:http://www.pcmag.com/article2/0,4149,1175896,00.asp

Mohney, Doug. "WiFi Wardriving"
September 1, 2003
URL http://www.synchrologic.com/2003/09/23/eng-primemedia/eng-primemedia_112118_5773960666571695083.html

Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practice"
N/A
URL:http://www.arstechnica.com/paedia/w/wireless-security-howto/home-802.11b-2.html

MobileComputing.com. "Service Set Identifier"
N/A
URL:http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci855455,00.html

Geier, Jim. "Guarding against WLAN Security Threats"
September 12, 2002
URL: http://www.wi-fiplanet.com/tutorials/article.php/1462031

IBM. "Wireless Security Auditor"
N/A
URL: http://www.research.ibm.com/gsal/wsa/

ExtremeTech. "Wireless LAN deployment and Security Basics"
URL:http://www.extremetech.com/article2/0,3973,1157726,00.asp

InteropNet. "'Whats wrong with WEP?"
N/A
URL:http://www.ilabs.interop.net/WLAN_Sec/What_is_wrong_with_WEP-lv03.pdf

Cisco Systems. "Password Recovery for the Cisco Aironet Equipment"
N/A
URL:http://www.cisco.com/warp/public/102/wlan/pwrec-2.html

Cisco Systems. "Password Recovery for the Cisco Aironet Equipment"
N/A
URL:http://www.cisco.com/warp/public/102/wlan/pwrec-2.html

Cisco Systems. "Configuring Authentication Types"
N/A
URL:http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_chapter09186a008014868e.html

SANS. "SANS 2002 San Diego Seminar"

March 2002
URL: http://www.sans.org

Hobbie.net. "Brutus - FAQ"
N/A
URL: http://www.hoobie.net/brutus/brutus-faq.html

Dismukes, Trey. "Wireless Security Blackpaper"
July 2002
URL:http://www.arstechnica.com/paedia/w/wireless/security-3.html

Hobbie.net. "Brutus - FAQ"
N/A
URL: http://www.hoobie.net/brutus/brutus-faq.html

Wright, Joshua. "Detecting Wireless LAN Mac Address Spoofing"
January 21, 2003
URL: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

Geier, Jim. "802.11 WEP: Concepts and Vulnerabilities"
June, 2002
URL:http://www.wifiplanet.com/tutorials/article.php/1368661

Borisov, Nikita. Goldberg, Ian. Wagner, David. "Intercepting Mobile Communications: The Insecurity of 802.11"
N/A
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Geier, Jim. "802.11 WEP: Concepts and Vulnerabilities"
June, 2002
URL:http://www.wifiplanet.com/tutorials/article.php/1368661

Borisov, Nikita. Goldberg, Ian. Wagner, David. "Intercepting Mobile Communications: The Insecurity of 802.11" N/A
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Phenoelit. "Insecure Protocols"
N/A
URL: http://www.phenoelit.de/fr/protos.html

Maricopa Community College. "Replacing Clear Text Protocols"
N/A
URL: http://www.guardian.maricopa.edu/policy/ssh/

Cisco Systems. "Cisco Aironet 1200 - Bulletins"
N/A

URL:http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletins_list.html

Tools:

Netstumbler
URL: www.netstumbler.com

Kismet
URL: www.kismetwireless.net

Airtraf
URL: http://airtraf.sourceforge.net/

Last Updated: July 26th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**