Global Information Assurance Certification Paper

Auditing 802.11 wireless networks focusing on the Linksys BEFW11S4 Access Point

An Auditor's Perspective

Raúl Siles Peláez

February 17, 2004

GIAC Auditing Networks, Perimeters, and Systems (GSNA)
(Version 2.1) - Option 1

Abstract

This paper is the practical assignment required to obtain the GIAC Auditing Networks, Perimeters, and Systems (GSNA) certification (version 2.1), option 1, ”Perform an Audit”.

It describes how to audit a 802.11 wireless network focusing on the Linksys BEFW11S4 wireless access point (AP) router and consists of four sections all related between them:

- First one focuses on researching the best practices for auditing the selected system, the Linksys BEFW11S4 AP and the 802.11 wireless networks. It defines control objectives and methods for achieving the objectives with technology.
- A checklist will be created compiling the best practices: for each checked item it will be shown the what, why and how. This checklist will be grouped based on the concept or layer the item is auditing.
- Third part provides a detailed real audit report of some items selected from the previously created checklist over the AP running in the company analyzed.
- Finally, in the last section I will act as an independent auditor, so a management report summarizing the findings will be included, detailing risks, recommendations and costs.

The information included references the best-practices for securing wireless networks and its application to the access point analyzed.

Acknowledgments

Mónica. . . , just for you !!. Don’t change !!

Contents

ASSIGNMENT 1 - RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL

This section evaluates the state of the art of auditing 802.11 wireless networks and specifically the shades associated to the Linksys BEFW11S4 Access Point.

1.1 Identify the system to be audited

The Linksys BEFW11S4 Wireless Access Point Router, with 4-Port Switch, is a small networking device designed to share the broadband high-speed connection with wired and wireless computers. It provides both, a built-in 4-port FastEthernet switch and an 802.11b wireless access point. It is a WiFi Alliance (WECA) certified product [WIFI1] and also a verified Intel Centrino Mobile Technology product [CENT1], facts that confirm its interoperability with other wireless devices.

Figure 1.1: Linksys BEFW11S4 Wireless Access Point

The analyzed access point model (see figure 1.1) provides compatibility with the 802.3 and 802.3u wired standards, one WAN port for DSL connection, four 10/100 Ethernet switched wired ports plus one shared uplink port and the wireless coverage based on the 802.11b protocol.

It is also capable of up to 128-bit WEP encryption and supports VPN technologies, like IPSec and PPTP Pass-Through. Besides it must be configured as a DHCP server and not only as a switching/bridging device but as a routing device and, additionally, it provides advanced security management functions for port filtering, MAC address filtering and DMZ hosting that would be covered all along the auditing process.

The role of this device is providing wireless access to employees to the company network infrastructure, in order to offer a flexible and easy to use access to the company IT resources and Internet from any place inside the organization facilities.

This type of device is being widely used in both, SOHO, Small Office Home Office, and SMB, small and medium business environments. In the former it is typically used as the core of the wireless infrastructure due to its low price (under $100) and high interoperability. In the later, the same reasoning cause to plug it into the wired network for two purposes:

- First one is a legitimate usage where the IT department use it to offer networking access to telecommuters and visitors.

- Second one is an unauthorized usage based on setting up a new rogue (unofficial) access point by any employee to provide Internet and Intranet access for meetings and conferences.

Although there are several industrial-quality devices in the wireless market oriented to massive deployments in big corporations, such as the Cisco Aironet AP family analyzed in other people practicals (see the end section of this first assignment), the analysis of a low cost and portable access point like the one presented in this paper has been considered a valuable task because it would be useful to measure the security state of small and medium wireless networks environments. The usage of such a portable, inexpensive and easy-to-install device could compromise the whole company infrastructure.

The Linksys Group [1] is a broadband and wireless networking company founded in 1988 and the market leader of wireless technology for the SOHO environments. It was acquired by Cisco Systems during year 2003. Its position as the market leader was also the reason to analyze one of its most famous products for small/medium wireless networks.

The BEFW11S4 model will be analyzed when providing wireless access to both, the internal company network and the Internet access, in a infrastructure similar to the topology of figure 1.2.

[1] http://www.linksys.com

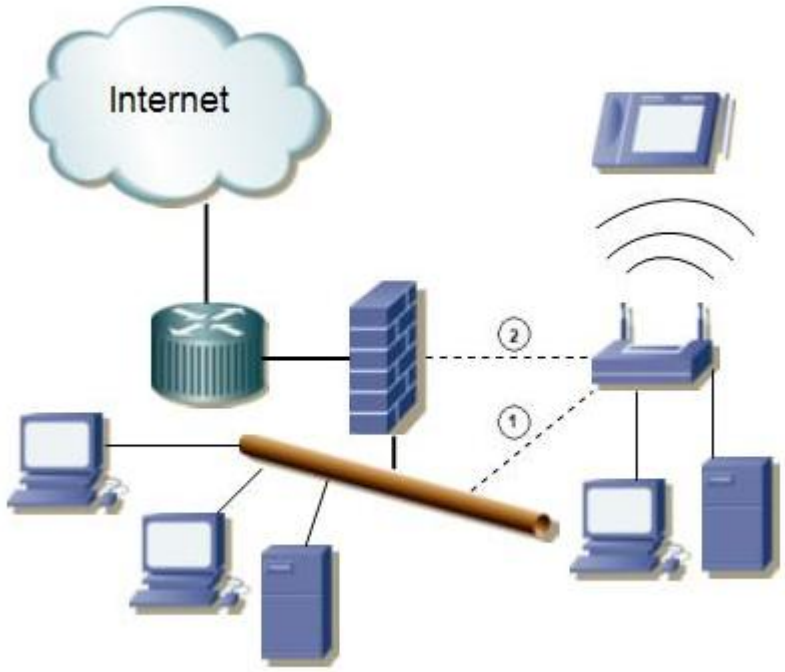

Figure 1.2: Network topology for the access point audited

The topology analyzed could present a significant variation from the security point of view: the AP can be configured in a “plain topology” (option 1), located inside the internal local network without any filtering device separating the wireless users from the wired ones, or it can be placed in a “restricted topology” (option 2), where the wireless subnet is considered a dangerous area and becomes an independent DMZ segment connected to a filtering device, such as a firewall.

From a security perspective, the later is the recommended configuration taking into account the inherent vulnerabilities associated to the wireless standards. It must be explicitly noted that the device analyzed doesn’t take part of what is known as an “open” wireless network or hotspot; a public place providing “free” (or low-cost) Internet access.

The auditing process will cover the wireless capabilities and functionality around the 802.11 technology, but will be mostly focused on the BEFW11S4 model itself. When auditing a wireless network there are other additional aspects that should be covered in order to verify the security status of the network, such as the end wireless devices and the gateways [POTT1]. In this paper these additional elements won’t be covered because they are not part of the device analyzed.

The main wireless clients associated with the Linksys 802.11 functionality are laptops, PDAs and Table PCs. Due to the fact that this device also support wired systems, some aspects related with these clients and its switching capabilities would be included in the auditing process.

From a detailed technical point of view, the BEFW11S4 analyzed is the hardware version 3 of the product and is running the `1.44.2, Dec 13 2002` firmware version (see figure 1.3). Besides, it runs the `1.2.1` wireless firmware version (check the administration web page `http://192.168.1.1/Wireless.htm`).

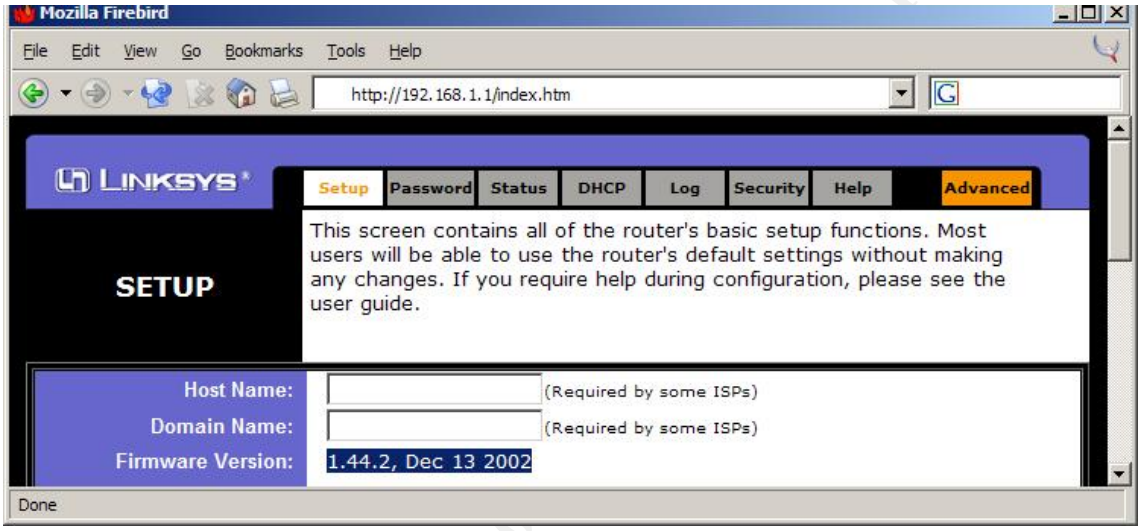

Figure 1.3: Linksys firmware version through Web interface

The hardware version must be obtained looking at the bottom surface of the device. There are two labels indicating the version number (see figure 1.4).

To sum up, the scope of this paper will be focused on auditing the wireless capabilities of a commodity access point, the Linksys BEFW11S4, although some wired functionality will also be covered, mainly from a very technical perspective associated to the nowadays and near-future 802.11 wireless standards plus some policy and recommended procedures extracted from the industry best-practices. This device will be audited in a small business environment described on `assignment 3`.

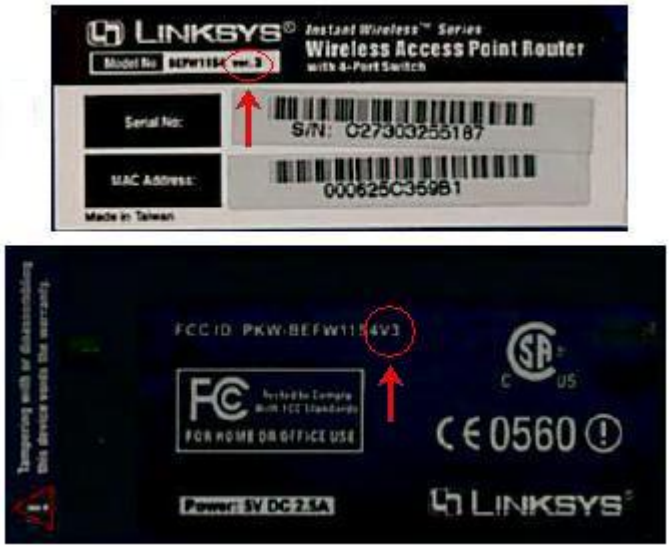

Figure 1.4: Linksys hardware model version: BEFW11S4V3

1.2 Evaluate the risk to the system

The product analyzed conforms with the 802.11b protocol, a wireless IEEE networking standard [IEEE1] that operates at a frequency of 2.4 Ghz, with a maximum physical data rate on 11 Mbps. As almost all 802.11b implementations it is settled on three channels, 1, 6 and 11, to avoid interferences produced by overlapping frequencies.

Although the term "wireless security" is considered an oxymoron, because there is no physical security associated with it, using a careful configuration it can become almost as secure as the wired alternative. To be able to implement the available security mechanisms, the 802.11 protocol risks and threads must be understood.

For every generic security risk associated to the wireless 802.11 technology different aspects will be covered, such as the specific thread, how likely is to suffer it and the consequences of suffering a successful exploitation. The probability will be evaluated from the company point of view where the access point to be analyzed resides.

Besides, some of the specific public free wireless tools that can be used to exploit the vulnerability associated to a given risk will be referenced and slightly

described. Various of the referenced tools can be found at [2] or [3].

The way of being protected against any of the risk identified will be covered in the next section, when developing the auditing checklist.

Although the end stations are not covered by this research paper it must be mentioned that the configuration of a client device using ad-hoc networking, that is, a P2P wireless connection, opens up the device, typically a laptop, for being attacked and used as a bridge into the wired network.

All the auditing considerations covered along this paper apply to any of the nowadays 802.11 wireless networking standards: 802.11a, 802.11b and 802.11g. The main difference between them is the physical radio frequency they operate and the bandwith they provide [4] (see table 1.1):

Technology	Frequency	Max. data rate
802.11b	2.4 Ghz	11 Mbps (*)
802.11g	2.4 Ghz	54 Mbps
802.11a	5 Ghz	54 Mbps

(*): A wireless network set to an 11 Mbps data rate provides approximately 5 Mbps of aggregate throughput.

Table 1.1: Different 802.11 wireless technologies

From a security point of view, the main difference between all them is the interoperability range covered by a single access point. This fact would be analyzed in depth when studying the physical security risks.

1.2.1 Taxonomy of the 802.11 wireless threats and vulnerabilities

Analyzing the security threats and vulnerabilities in the wireless network analyzed (see figure 1.2) it is possible to have different attack types, therefore the following taxonomy has been created (based on both, personal experience and information from [GRIP1],[LOWD1], [STAL1] and [1]):

- **Attacker type**: internal or external based on where he is physically located.
- **Types of resource targeted**: internal (associated to the wired infrastructure inside the firewall or the Internet uplink), wired (directly connected to the cable

[2] http://www.wirelessanarchy.com
[3] http://www.networkintrusion.co.uk/wireless.htm
[4] http://www.linksys.com/products/wirelessstandars.asp

ports in the switch inside the AP) or wireless (those connected to the wireless network).

- **Unauthorized action**: data capture, data injection/modification, wireless identification and association, rogue access point usage, compromising the access point device, illicit use, disruption of service, physical security, misconfiguration, ...
- **Security feature exploited**: confidentiality, integrity or availability.

All the different variables presented can be combined to identify a specific risk. The following sections will explain in detail all these elements and the theory behind them.

1.2.2 Eavesdropping: data capture

Probability: high	**Security**: confidentiality

In conventional wired networks in order to access or modify the data transfered physical access to the medium is required. This fact has been used during long time to mitigate network security threats through physical security inside the company facilities, reducing Man-In-The-Middle attacks (MITM).

In wireless networks based on radio frequency (RF) communications this protection is lost. The RF waves travel through the air and cannot be easily contained, therefore an attacker in the range of the frequencies used can record an analyze the traffic. By default the wireless communications take place in an unencrypted format, facilitating this type of attack.

Some examples showed that data could be intercepted from a distance of 20 miles [5] in the San Francisco area.

These physical constraints of the wireless medium should drive the security countermeasures to be protected against all the risks described. In order to avoid them encryption must be used: SSH, SSL or IPSec are the common used protocols.

The capability of sniffing information from the network in MITM attacks is not only restricted to the use of an evil station. A rogue access point can be placed between an authorized station and an official access point in order to redirect all the traffic through the rogue access point.

[5] http://www.dis.org/wl/maps

This is a very common attack and there are lots of free tools to carry it on, like `kismet` (see table 1.2) or `ethereal` [6]. If successful, the company assets and confidential information could be compromised, exploiting the privacy of the information traveling through the wireless network.

Tool:	*kismet*	http://www.kismetwireless.net
Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.		

Table 1.2: Kismet: wireless sniffer

1.2.3 Injection: data manipulation

Probability: medium	**Security**: integrity

Using the eavesdropping methods already discussed, it is possible for an attacker to inject data in new or pre-existent connections, for example through ARP spoofing attacks [ARPS1]. This attack is based on redirecting the traffic from or to a specific host poisoning its ARP cache table through forged ARP packets. The evil packet will be send to the target system and will associate the attacker MAC address to the IP address of a trusted host, therefore the target host will send the traffic addressed to the trusted host to the attacker station.

This attack is more easily develop in wireless networks than in its wired counterpart. From a higher protocol perspective even more dangerous attacks, such as session hijacking, could be performed. To be able to be protected against it several methods can be used, such as setting static MAC entries, encryption, MAC filtering, monitoring solutions or even more advance protocols, like 802.1X.

There is a paper focused on analyzing the implication of the ARP spoofing attacks in wireless networks [7].

Besides, if an attacker is able to get the SSID and MAC address of a legitimate user (using eavesdropping methods), he can steal its identity and perform the same actions the trusted user is authorized to do.

Different tools can be used to perform ARP spoofing and other traffic manipulation, such as `ettercap` [8], `arpplet` [ARPS1] or `nemesis` [9]. If successful, the company assets and confidential information could be compromised, exploiting the privacy of the information traveling through the wireless network.

[6] http://www.ethereal.com
[7] http://www.cigitallabs.com/resources/papers/download/arppoison.pdf
[8] http://ettercap.sourceforge.net
[9] http://www.packetfactory.net/projects/nemesis/

Even when using WEP (see bellow) it is possible to execute some replay attacks (injection) knowing the keystream (easy to obtain) and modify the traffic without being discovered. It is based on exploiting the algorithms used in the CRC checksum used [BORI1].

The risk associated to the eavesdropping and injection threats is high, because it reflects an illegal access to the company network, where the attacker is able to delete, modify or read valuable information.

1.2.4 Wardriving: network reconnaissance

Probability: high	**Security**: confidentiality

Attackers tried during the first stages of this new technology (born in 1999) to answer one question: "*How could I identify the existence of a vulnerable wireless network?*" The response generated a new thread based on the way the end-stations and the infrastructure access points must establish an initial relationship, called "association", in order to exchange information.

This new threat allows to acquire information or access to a company network through the usage of a wireless laptop (or PDA), a GPS and a car [10]. Driving along a metropolitan area it is possible to find wireless networks and access points.

Wireless networks are really easy to find because in order to join a wireless network, the wireless station should first listen for "beacon messages" transmitted by the access point, which is continuously "shouting" its name through the air. These messages are sent unencrypted and contain the network's information, such as the network's SSID (Service Set Identifier, or network name, also called ESSID) and the IP address of the access point.

Using specific software, such as NetStumbler (see table 1.3) or AirMagnet (for PDAs and PCs; see table 1.4), while driving it is possible to locate in the globe every wireless network found with its configuration based on its associated latitude and longitude values (recorded with the help of the GPS). Once the device has been identified a new attack vector emerges and the attacker could gain knowledge about the company infrastructure.

If an attacker is able to get enough information he may get free bandwidth and free Internet access through your wireless network, but also access confidential information and resources within the company network.

There are companies like Smart ID [11] that sell portable WiFi detectors and other

[10] http://www.wardriving.com
[11] http://www.smartid.com.sg

Tool:	*netstumbler*	http://www.stumbler.net, http://www.netstumbler.com
Netstumbler is a program used to locate access points including all its associated configuration values, such as SSID, MAC address, transmission channels... It also provides lot of information about the signal strength and quality.		

Table 1.3: Netstumbler: the wireless searcher

Tool:	*airmagnet*	http://www.airmagnet.com
Airmagnet is able of tracking down any wireless device. it also includes tools to ensure the 802.11 policies and check for other anomalies and problems.		

Table 1.4: Airmagnet: the PDA wireless searcher

like AirTouch Networks [12] even provide wardriving kits for about $400.

This and the following “War” terms originated in a phone line scanning method known as “Wardialing” and popularized by the movie “War Games”.

1.2.5 Warchalking

Probability: low | **Security**: confidentiality

When someone has detected an open wireless network using any method, typically Wardriving, he can draw a picture outside the company facilities (in the building walls or in the near street) with the specific details of the network configuration, such as the SSID, the bandwith, and the node type (open, close or WEP-based).

The picture is based on a new language based on symbols and known as Warchalking [13] (see figure1.5).

The goal of the symbols is to notify others about the existence of the network in order to let them use it as easily as possible [14] (see figure1.5).

1.2.6 Warmapping

Probability: low | **Security**: confidentiality

This term has been created for this paper in order to reflect the new way of promoting the information found while wardriving and searching for wireless networks.

[12] http://www.airtouchnetworks.com
[13] http://www.warchalking.org
[14] http://notabug.com/warchalking/card300.png

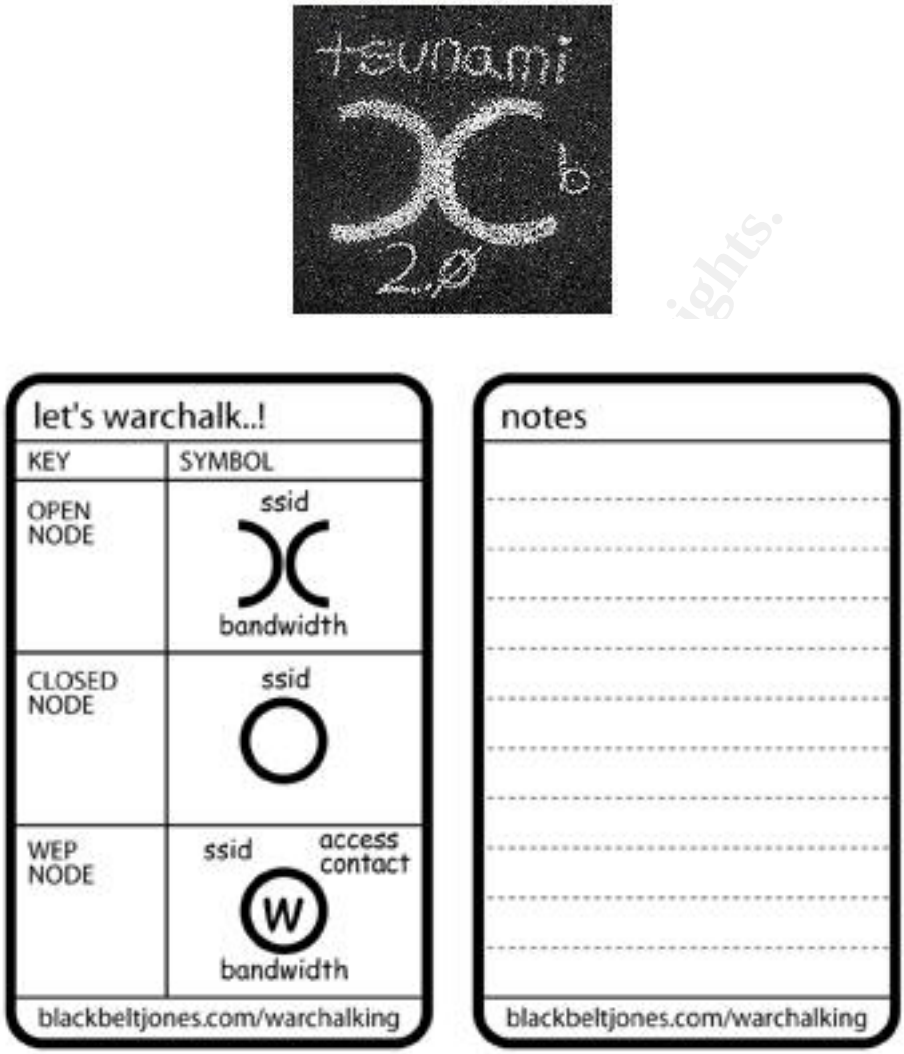

Figure 1.5: Warchalking picture of a 2 Mbps Cisco open-node and symbols

There are lot of publicly available web pages publishing a database of the found networks, its configuration details and the exact location in a global/local map, although the main "problem" is that almost all them reference US locations:

- http://www.wifimaps.com
- http://www.netstumbler.com/nation.php
- http://www.shmoo.com/gawd

- http://www.wigle.net (including Europe)
- http://www.wififreespot.com (including Europe)
- http://www.wi-fihotspotlist.com
- http://www.apdirectory.com
- http://www.cisco.com/pcgi-bin/cimo/Home
- http://nodos.madridwireless.net [15]

Apart from this list there are other public and free-access wireless community groups:

- http://www.wirelessanarchy.com/#Community%20Groups
- http://www.toaster.net/wireless/community.html
- http://www.personaltelco.net/index.cgi/WirelessCommunities

1.2.7 Illicit use: resources consumption

Probability: high | **Security**: availability

Using some of the previously discussed methods, an attacker can discover a wireless network and therefore use it for his own benefit. Although this is probably the less dangerous of the mentioned risks, the attacker will consume network resources (what means money loss) to access Internet, for example, to browse the Web, check his e-mail or even launch attacks to other networks, with the implications this could have from a legal perspective.

1.2.8 Wireless DoS attacks: network availability

Probability: medium | **Security**: availability

From a physical point of view, an attacker can saturate the frequency bands with RF noise, reducing the signal-to-noise ratio to an unusable level, therefore taking offline the wireless users in the affected area. Some cordless phones operating in the 2.4 Ghz band are able to interfere with WiFi as well as other technologies, such as large-scale bluetooth [POTT1] (although some solutions try to avoid this, such as, AFH [16]). This DoS method will collapse the airwaves or will force the end stations to continuously disconnect from the access point.

[15] the Web for the city where the analyzed AP was located, Madrid (Spain)
[16] http://www.ericsson.com/bluetooth/files/whitepaper_on_afh_final.pdf

From a network perspective, if an attacker is able to associate to an access point he can flood the network with traffic, because the 802.11 protocol uses a shared medium, saturating the bandwith.

Another DoS attacks related with the physical access to the device appears if it is stolen or damaged, affecting the availability of the wireless network. This is an unlikely threat and is conditioned by the physical security of the company facilities.

1.2.9 Direct attacks against the access point: compromising the network

Probability: medium	**Security**: confidentiality, integrity, availability

It is possible for an attacker to compromise the access point device as any other networked system, using basic tools to obtain as much information as possible remotely:

- SNMP protocol: it is possible to extract lot of configuration and execution information through the SNMP agent running on the device [17].
- Telnet access: establishing a Telnet connection with the device may allow privileged access to it, using easy to guess passwords or trying dictionary or brute force attacks [18].
- HTTP protocol: due to the fact that the device provides a Web configuration utility, it can be used to get control over the access point, exploiting password vulnerabilities (such as the Telnet ones) or HTTP weakness (vulnerable CGI scripts, or any other dynamic content tools).
- Open ports: it is possible to search for other services running in the device.
- Banner information: all the services offered may potentially provide more information through banners and login messages. This information could help an attacker to identify the device model and OS version.
- Service implementation: as any other piece of software, any of the service implemented in the access point may potentially suffer from programming vulnerabilities, such as buffer overflows, format strings or input validation.

[17] Not available in the BEFW11S4 model
[18] Not available in the BEFW11S4 model

1.2.10 Policy violations

Probability: medium	**Security**: confidentiality, integrity, availability

It is very easy for authorized users to violate the network security policies plugging rogue access points to the corporate network, allowing anyone within a long distance to access the network.

All the other aspects included in the security company policy must be assured for the access point device, such as robust passwords, allowed services, protection levels...

SANS Institute provides several security policies [19] and one of them is directly related with the wireless networks: http://www.sans.org/resources/policies/Wireless_Communication_Policy.pdf. This basic policy specifies standards for wireless systems used to connect to the organization's networks.

The company security policies should also reference the need of having a detailed logging environment that will provide evidence and events if the attacker prosecution is required after a security incident.

1.2.11 Trying to mitigate the risk: WEP

Interception of the radio signals is a real threat, so when the 802.11 protocols were designed, a built-in encryption mechanism was defined. WEP, Wired Equivalent Privacy. It provides two security features to the networking protocol, authentication and confidentiality, through a symmetric cypher called RC4, based on a shared key.

The keys are shared between the access point and the client stations wireless cards and can have a length of 40 or 104 bits. Although the Linksys AP analyzed claims to manage 128 bits WEP keys in reality it is using a 104 bits key plus the 24 bits associated to the Initialization Vector (IV), a value that is transmitted in the clear with the packet.

The 40-bits RC4 algorithm has been broken using brute-force attacks using a modern PC based on the main study around the RC4 mathematics [FLUH1]. Based on the way WEP uses the RC4 algorithm, if enough traffic is captured the keys can be cracked (see tables 1.5 and 1.6). This fact is even worse due to the way the vendors have implemented the usage of the IV values, where they are never rotated, helping in the cryptanalysis attack.

There are several papers analyzing the pros and cons of the WEP design and implementations: [WALK1], [GOLD1], [NEWS1]

[19] http://www.sans.org/resources/policies/

Tool:	*airsnort*	http://airsnort.shmoo.com
AirSnort is a wireless LAN tool which recovers WEP encryption keys. It passively monitors transmissions, and computes the encryption key when enough packets (approximately 5-10 million encrypted packets, over 1GB of data) have been gathered.		

Table 1.5: Airsnort: wireless WEP-cracker

Tool:	*wepcrack*	http://wepcrack.sourceforge.net
WEPCrack is an open source tool for breaking 802.11 WEP secret keys and it is an implementation of the attack described in [FLUH1]. It was created before AirSnort.		

Table 1.6: WEPCrack: wireless WEP-cracker

WEP Key Management

The WEP standard doesn't define the issue of how to manage the keys shared between all the users. The problem is associated to the trust chain inherent to all end entities that know the same pre-shared keys. In order to maintain the correct end user trust set (those that are aware of the key) the keys must be rotated in a daily/weekly/monthly basis.

The solution that it is being implemented by vendors is the usage of per-user individual keys, protecting the user from other users in the wireless network.

Authentication: with and without WEP

As previously described in the "Wardriving" section, the default authentication method between the end stations an the access point during the association process has no security at all: anyone could connect to the access point if the SSID value is known.

When using WEP the access point and the end station can authenticate each other using the shared key during the association process, a secure wireless method of identifying new end systems and join the network. This authentication method is known as "Shared Key Authentication".

1.3 What is the current state of practice?

1.3.1 802.11 wireless security

There are several papers focused on mitigating the risks of wireless devices and hardening wireless networks:

- "802.11 Security Vulnerabilities": http://www.cs.umd.edu/~waa/wireless.html
- "An Initial Security Analysis of the IEEE 802.1X Protocol": [ARBA1] http://www.cs.umd.edu/~waa/1x.pdf
- "The Unofficial 802.11 Security Web Page" (a technical Bible): http://www.drizzle.com/~aboba/IEEE/
- "Wireless LAN Security FAQ". Christopher W. Klaus (ISS): [1] http://www.iss.net/wireless/WLAN_FAQ.php
- "Wireless Security articles": http://www.ebcvg.com/wireless.php
- "Wireless Security: Thoughts on Risks and Solutions": http://www.ebcvg.com/download.php?id=1371
- "Your 802.11 wireless network has no clothes": http://www.cs.umd.edu/~waa/wireless.pdf
- "Securing Wi-Fi Wireless Networks with Today Technologies": [WIFI2] http://www.80211info.com/publications/page289-655794.asp
- "Night of the Living Wi-Fi's (A Security Parable for Our Times)": [20]
- "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards": http://www.sans.org/rr/papers/68/1109.pdf

Due to the fact that there are lots of papers and documentation related with the security aspects of the 802.11 wireless technology, this paper will be mainly focused on the specific aspects of the Linksys model analyzed.

[20] http://www.informit.com/isapi/product_id~%7BE790142B-5F3E-4CBD-8F66-4789DB29BC78%7D/content/index.asp

1.3.2 Auditing 802.11 wireless networks

Some GSNA practicals have been published about the auditing of wireless devices, although most them are focused on the Cisco Aironet 1200 product family:

- ”An Audit of a Wireless Demonstration network Implementing Cisco Aironet 1200”. Oliver Viitamaki. GSNA Practical v2.1. [VIIT1]
- ”Auditing the Cisco Aironet 1200 Wireless AP In a Small to Medium Business Environment (SMB)”. Ryan Lowdermilk. GSNA Practical v2.1. [LOWD1]
- ”Auditing a Cisco Aironet Wireless Network”. Ryan Stall. GSNA Practical v2.1. [STAL1]
- ”Auditing the Cisco Aironet 340 Wireless Access Point”. Mark Griparis. GSNA Practical v2.0. [GRIP1]
- ”Auditing the Wireless environment: A mobile wireless LAN used for training in multiple sites on a corporate WAN”. Angela Loonis. GSNA Practical v2.0. [LOON1]. She also used a Cisco Aironet 1200.

Other practicals are more generic [CORA1] or based on a not very widely deployed device, such as the Orinoco Outdoor Router 1000 [MARC1]. Almost all practicals referenced some NIST documents related with wireless security.

Although the set of resources (outside SANS/GIAC) for auditing wireless environments is a small set of the overall bibliography the following ones are the most relevant:

- “Initial Wireless Networking Audit for Higher Educational Institutions”. A non-technical checklist provided by John Dillon: [DILL1]
  http://www.auditnet.org/docs/wireless.doc
- “Introduction to Wireless Auditing”. Sean Whalen:
  http://www.node99.org/projects/waudit/waudit.pdf
- “Make a robust wireless audit of your network with Kismet”:
  http://techupdate.zdnet.com/techupdate/stories/main/robust_wireless_audit_Kismet.html
- There is a really good repository for auditors called Audinet:
  http://www.auditnet.org/asapind.htm

  This repository contains some documents related with the wireless networks:

  - "Wireless LAN Audit Briefings": http://www.auditnet.org/docs/WLAN%20Audit%20Briefing.doc
  - "Basic audit WLAN review": http://www.auditnet.org/docs/Wireless%20Local%20Area%20Network%20_WLAN_.pdf

- With the goal of being able to audit a wireless network from the wardriving perspective, a new Linux bootable distribution has been created, called War-Linux [21]:
  "*A new Linux distribution for Wardrivers. It is available on disk and bootable CD. It's main intended use is for systems administrators that want to audit and evaluate their wireless network installations. Should be handy for wardriving also.*"

- IBM has also released a very similar new auditing software tool running on Linux over an HP iPAQ PDA called WSA, Wireless Security Auditor [22] [23] to combat the wardriving and rogue access points existence.

There is a lack of information about the security recommendations for hardening and auditing checklist on Linksys devices, reason why this paper will cover their peculiarities. Their purpose is offering a method to be able to audit and secure a low-cost device in order to provide a basic and secure initial configuration.

1.3.3 Audit and security aspects of Linksys wireless devices

Some information has been provided by the vendor [24]. The recommended security actions suggested are:

- Change the default SSID.
- Disable SSID Broadcasts.
- Change the default password for the Administrator account.
- Enable MAC Address Filtering.
- Change the SSID periodically.
- Enable WEP 128-bit Encryption. Please note that this will reduce your network performance.

[21] http://sourceforge.net/projects/warlinux
[22] http://www.research.ibm.com/gsal/wsa/
[23] http://www.internetnews.com/bus-news/article.php/800221
[24] http://www.linksys.com/splash/wirelessnotes.asp

- Change the WEP encryption keys periodically.

There is a really good article about some internals aspects of the Linksys BEFW11S4 device [25]. It contains configuration guides and other firmware features and options not only related with security.

Other generic reviews about this product, its weakness and strengths have been published [26].

The BEFW11S4 support page provides information about this product [27]. Linksys has created the address *security@linksys.com* to receive information on vulnerabilities within any of their products.

Additionally, there is a document called "Follow these steps to tighten security on Linksys wireless networks" that provides some basic recommendations to secure the device [28].

The following is a known list of specific vulnerabilities [29] [30] associated to the Linksys BEFW11S4 model. These will be checked during the auditing process described on the `assignment 2` section:

- The "iDEFENSE Security Advisory 11.19.02" shows a well-known DoS vulnerability: http://www.idefense.com/application/poi/display?id=36&type=vulnerabilities

- "Linksys BEFW11S4 Wireless Router Buffer Overflows and Parsing Bugs Let Remote Users Take Full Control of the Router": http://www.securitytracker.com/alerts/2002/Dec/1005744.html

- "Linksys WRT54G Denial of Service Vulnerability": http://lists.seifried.org/pipermail/security/2003-December/000069.html
  It is not directly related with the product analyzed but it is well worth to check it due to its simplicity. There are other vulnerabilities associated to other Linksys products that won't be tested.

[25] http://www.allaboutjake.com/network/linksys/befw11s4/
[26] http://www.ibookzone.com/linksys.shtml
[27] http://www.linksys.com/support/support.asp?spid=68
[28] http://techrepublic.com.com/5102-6329-1058551.html
[29] http://www.securitytracker.com/archives/target/1579.html
[30] Search by "linksys" at http://www.securiteam.com

ASSIGNMENT 2 - CREATE AND AUDIT CHECKLIST

This section provides the recommended Auditing Checklist (called "AC-xx-yy") steps that allow performing the auditing of the Linksys BEFW11S4 access point.

To generate this list, apart from the information and references provided in the previous assignment section, the personal experience auditing wireless and wired networks has been used.

Although it is explicitly required by the GSNA assignment to include the references used for each checklist item included, most of the ones presented here have not been obtained from an individual source but from a set of the sources previously mentioned in the `assignment 1` section so, if no `Reference` section is included, the following description applies:

"*Item checklist obtained from several references described in the previous `assignment1` section and personal experience.*"

The main set of references used are the ones included under the "1.3" section.

For other specific cases where a valuable source has been used it will be referenced in the specific audit check.

The auditing checklist presented tries to check several security elements and their countermeasures with the goal of protecting a wireless network, focused on the access point, as much as possible. Some individual measures are useless but the combination of all them tries to provide a very secure and controlled environment, raising the bar that an attacker must trespass.

The scope of this checklist is mainly focused on the technical aspects of the device because it is commonly used in SOHO or SMB environments, where the security policies, procedures, administrative and organizational aspects are not as complex as in large corporations with dozens of access points. However, some basic procedural aspects will be covered.

First step is identifying the device to be audited. All the details involved in this

process have been included in `assignment 1`.

Finally, special attention will be taken in order to provide information about the factory default settings for each of the values analyzed and the aspects associated to locking down (hardening) the access point.

2.1 Physical considerations

2.1.1 Interoperability range (AC-1-1)

Control objective:
Although the device analyzed conforms with the 802.11b technology, it is possible to find other wireless access points compatible with the 802.11a or 802.11g standards. It must be taken into account the difference distances these devices operate because they influence the range an attacker could be placed in order to interfere with the access point signal:

- **802.11b**: 100-150 m
- **802.11g**: 100-150 m
- **802.11a**: 25-75 m

In an infrastructure environment, the distance from the access point and the placement and orientation of the wireless devices antennas, determine the speed and signal quality. As you get farther away, the transmission speed will decrease. The shape and structure of the building (type and building materials) also influences these variables.

These factors increase/decrease the attacker capabilities when exploiting the network. It is possible to configure some access points to not allow the lower speed station, mainly those trying to connect from a far distance, such as the external places surrounding the company buildings, like a parking lot or another floor (above or bellow).

The process of checking the company facilities searching for access points, their signals strength and bandwith is usually called a “site survey”.

Risk:
If the wireless signals are not blocked from leaking through the walls, ceilings and floors of the company facilities a potential attacker may be able to interact with the wireless network. As a consequence he could discover it, for example through wardriving methods, obtain configuration values and even being able to connect to it to develop more specific and advanced attacks.

This risk is usually associated to the reconnaissance attack phase.

The Linksys device provides two small antennas that can be slightly oriented based on the area that should be covered. See [GAST1, page318] for the different types of possible antennas.

Compliance:
To analyze this variable two different approaches must be used:

- First one is based on just going to the location where a potential attacker could be placed and check the signal strength and features.
- Second, and more advanced one, is based on walking through all the relevant places into and around the company facilities and evaluate the wireless signal and network connection capabilities (recommended). This one requires to have a building map or diagram to be able to draw the results all along the company. For companies with several building even a GPS would be helpful.

The signal features can be controlled using the `Advanced` configuration menu, and selecting the `Wireless` tab.

Testing:
To be able to obtain all the parameters related with the signal the `netstumbler` application will be used. The tracking process must be carried on taking into account different dimensions, that is, locations on the same floor level and on different floors.

This check focuses only on the signal generated by the official access points.

To perform this check run the `netstumbler` application and select the SSID associated to the wireless network audited in the left tree. A graphic will be drawn indicating the "Signal/Noise" ratio (dBm) along the time.

These values will indicate the signal strength and quality in the area captured. It is even possible to complement the analysis with the usage of a GPS although it is not useful for small buildings. Additionally, if it is possible to connect to the wireless network, the bandwith should be evaluated, to confirm the datarate available from every specific location (2, 5 or 11 Mbps).

In order to develop a deepest analysis about the signal values and its relationship with other variables the following paper may be very useful "Converting Signal Strength Percentage to dBm Values" [1].

[1] http://www.wildpackets.com/elements/whitepapers/Converting_Signal_Strength.pdf

Objective/Subjective:
This is an objective test based on measuring the wireless signal and network connection bandwith on different locations.

2.1.2 Interferences (AC-1-2)

Reference:
It is based on the AC-1-1 audit check and performs a more specific test.

Control objective:
Any device operating in the 2.4 GHz spectrum may cause network interference with a 802.11b wireless device. Therefore, if an attacker has the capability of placing a 2.4 GHz cordless phones, microwave oven or another AP, such as a hotspot, it may interfere and even provoke a DoS over the trusted users.

Risk:
Possibility of a DoS attack, affecting the availability of the wireless service.

Compliance:
It is recommended to periodically test the wireless signal searching for an anomalous amount of noise in the waves. It is difficult to confirm the reason for the noise unless the originating source device is found.

The interferences could be confirmed if there is a great change in the signal properties in a reduced area.

Testing:
Again, using the `netstumbler` tool check for the signal to noise ratio (see “AC-1-1”).

Objective/Subjective:
The signal to noise ratio is a mathematical number value that could be compared against a baseline associated to the wireless signal in several places inside the company facilities during normal conditions (without interferences), thus an objective value.

2.1.3 Searching for rogue (unofficial) access points (AC-1-3)

Reference:
It is based on the AC-1-1 audit check and performs a more specific test.

Control objective:
The goal of this item is discovering rogue access points circumventing the network security policies and investments [2].

It is recommended to search periodically for rogue access points in order to shutdown them and enforce the company security policies.

Risk:
There are several risks associated to the existence of rogue access points (see the `assignment 1` section). These devices typically present a notorious lack of security and represent a backdoor for entering into the company wired network.

Compliance:
The existence of unofficial access points may be confirmed when receiving unexpected signals in specific areas or wireless signals with non-official SSID values.

As a result a report indicating the number of new access points detected and their main features, such as SSID value, waves ranges and channels, WEP-enabled..., must be obtained. This would confirm their existence and could be used as a management probe.

Testing:
There are two different tests to check the existence of unauthorized devices:

1. Walking the facility area using an scanner (as in AC-1-1):

   The network administrator should walk through the physical facilities using a laptop or PDA running a 802.11 scanner, such as `netstumbler` or `kismet`, in the same way attackers locate wireless networks. This task could be called `Warwalking`.

   The results obtained from this test only apply to the moment it was performed, so it is recommended to use it in a periodic basis.

2. Monitoring the wireless network remotely using sensors:

   A more advanced protection is based on monitoring the network using sensors as the ones provided by AirDefense RogueWatch [3]. If a new rogue AP is connected into the network, it will be directly detected and notified.

   A similar solution is the one provided by Wavelink [4] a wireless network management solution based on the SNMP protocol. It can detect au-

[2] http://aptools.sourceforge.net/wireless.ppt
[3] http://www.airdefense.net
[4] http://www.wavelink.com

tomatically the installation of new AP in the network an manage them, sending a predefined configuration.

Objective/Subjective:
This is an objective measure based on finding new SSID values or wireless signals in non-documented areas.

2.1.4 Physical access to the device (AC-1-4)

Reference:
Personal experience in physical security for IT environments associated to other devices, such as hosts, storage and wired devices.

Control objective:
The previous auditing checks have been focused on the wireless signal range. This check tries to focus on the device itself. To be able to ensure all the logical security countermeasures it is a must to have a tightly physical control over the device.

It must be stored securely in a locked cabin and room, and access should be allowed only to authorized people. Due to the fact that access points provide a physical service, the waves operation range where the wireless network is offered, they must be located all over the building and not in a very specific controlled IT room.

Risk:
If the device is physically available to unauthorized individuals several security aspects could be affected, such as, the availability due to powering off the access point, it may be stolen (the hardest DoS attack ;-)), new MITM attacks could be carried on using the wired connectors in the switch...

For example, the SSID is stored unencrypted in the access point, therefore an attacker with physical access to the access point could obtain it dumping out the device memory (this is a complex attack).

Additionally, some access point reset to the factory defaults (without security countermeasures, such as encryption, authentication, ACLs...) when they suffer a long power failure. The Linksys device doesn't present this behavior.

But for sure, the most dangerous and simple attack is pressing the reset button at the back of the BEFW11S4 during some seconds. This will leave the access point with the factory default settings, thus in an insecure state, without WEP, ACLs, DHCP enabled, broadcasting the SSID...

Compliance:
It is recommended to conclude this item with a summary report of all the physical vulnerabilities found related with the possibility of having an unauthorized access to the device. This is a relative measure based on the policies involved in the security of the IT facilities.

It would be recommended to obtain a estimation (in the form of a percentage value) of how the facilities conform with this requirement compared with the perfect situation: the device is not available to anyone without authorization.

Testing:
Check the access point location and evaluate the security controls in place. Check both, blocking controls, such as locks, and monitoring devices, such as surveillance cameras.

Compare the results with the status of other IT resources, such as networking equipment or Unix/Windows hosts.

Objective/Subjective:
Although an experienced consultant can objectively determine if the place where the access point is located is secure enough, this is a subjective value depending of several factors, being the main one the company policy.

2.2 Network design

2.2.1 Evaluate the network topology (AC-2-1)

Control objective:
It is recommended to consider the wireless network as any insecure network, such as a firewall DMZ. The connection between the wireless and the wired segments should be separated by a filtering device and authentication mechanisms be in place.

Wireless access points shouldn't be directly connected to the classic wired internal network. If these devices are connected without authorization are known as "rogue" access points.

Risk:
Due to other insecurities associated to the wireless technology, if the access points are directly connected to the corporate wired network, without other security controls in place, a vulnerable access point could compromise the whole network infrastructure.

Compliance:
The recommendations obtained are based on the security consultant experience and the information obtained about the network topology, elements and security controls applied.

Testing:
To be able to analyze the network design it is recommended to get as much information as possible about the company requirements, the network topology map, the subnetworks involved and theirs specific purpose as well as all the security controls used: filtering devices, ACL configuration at the host and network devices, monitoring equipment, such as IDSes...

As a general example, a network architecture as the option 2 presented in figure 1.2 is recommended while option 1 in the same figure is not.

Objective/Subjective:
This is a subjective control that must be checked in order to have a general idea about the best network topology for any given specific environment.

2.2.2 Wired and wireless built-in networks (AC-2-2)

Reference:
Extracted from personal experience working with SOHO/SMB devices combining multiple functionalities, such as hub/switch, router, VPN or firewall capabilities.

Control objective:
Due to the fact that the access point model analyzed belongs to the SOHO/SMB markets it combines several features in the same device: it has three differentiated capabilities, wireless access point, wired switch and router.

It is necessary to be able to evaluate the real relationship between these built-in features, mainly the association between the wired switch and the wireless network.

The main point to be evaluated resides in the type of networking domain set up, that is: Do the wired and wireless networks live in the same collision domain? Are the wired and wireless domains connected through a hub or switch built-in bus? Do the wired and wireless networks live in the same broadcast domain, therefore in the same IP subnet?

The answers to these questions will determine the traffic that is visible from one network belonging to the other and the type of attacks possible, such as sniffing, ARP spoofing...

Risk:
Based on the internal network topology defined in the design of this device, an attacker could be able to sniff and modify specific network traffic using basic methods (if the connection between the wired and wireless networks is similar to a hub) or he will require more advanced hacking techniques (if it is similar to a switch), such as ARP spoofing.

Compliance:
To be able to determine the internal design the traffic visible from one segment must be analyzed when generating traffic from the other segment. Taking network traces (sniffing the traffic) is required.

In the same collision domain, all the traffic is visible, such as a hub. In the same broadcast domain, only the multicast or broadcast traffic is available, but not the unicast packets, like in a switch.

Not having WEP enabled or knowing the WEP key to be able to inspect the traffic will help into determining the traffic type and performing this test.

Testing:
It is recommended to have three systems: two must be placed in the wireless segment while the other should be plugged into one of the four wired jacks available in the device built-in switch.

All systems should be configured to extract all the traffic from the network interface, so it is recommended to run `ethereal` (see table 2.1) and set up the network interface in promiscuous mode.

Then at least two types of traffic should be generated from one of the wireless systems:

- **Unicast** traffic: if an Internet connection is available, for example, send an ICMP echo request to an external pingable address, such as `www.google.com` or `www.cisco.com`:

  ```
  ping www.google.com
  ```

- **Broadcast** traffic: send an ICMP echo request packet addressed to the subnet broadcast address, such as `192.168.1.255`. Although the Windows devices doesn't respond to this traffic they can generate it; in Linux, the `-b` option must be used.

  ```
  ping [-b] 192.168.1.255
  ```

The other wireless system will evaluate the wireless network behavior while the wired system will analyzed the wired segment and its relationship with the wireless portion.

Due to the fact that the built-in network is based on a switched environment it is not necessary to evaluate the relationship between two wired ports.

Tool:	*ethereal*	http://www.ethereal.com
Ethereal is one of the most famous and powerful network sniffers with a really useful GUI interface.		

Table 2.1: Ethereal: wired/wireless sniffer

Objective/Subjective:
Based on the type of traffic observed when sniffing the communications generated from the other network segment it is possible to objectively determine the internal topology.

2.3 The SSID

There are several things to keep in mind about the SSID:

- Disable broadcast.
- Make it unique (change the default value).
- Change it often.

2.3.1 Broadcasting the SSID (AC-3-1)

Control objective:
The wireless networking device, AP, announce itself by beaconing or broadcasting the SSID, in order to indicate its presence to the wireless clients, over 100 times per second. While this option facilitates the easy of use of this technology, it allows anyone to locate the WLAN and log into your wireless network, including attackers. Therefore it is totally recommended not to broadcast the SSID, requiring authorized wireless stations to know it before being able to connect.

A network without SSID broadcast is called CNAC, Closed Network Access Control. Although the AP is not broadcasting the SSID, if WEP is not enabled, the end station will send it in the clear over the network, so it is not hard for an attacker to obtain it.

Risk:
The access point should have the broadcast mode disable not to constantly

broadcast the SSID as a beacon announcing stations its location and the possibility of connecting to the network. If turned off an end station must know the SSID to be able to connect to the access point.

If the device provide its SSID the wireless network will be available for anyone searching for it, therefore having the possibility on establish a future association if WEP is not enabled or the WEP key is known.

Compliance:
If the network is found (see the "Testing" section) then the SSID is being broadcasted. The SSID value should be obtained plus the signal intensity in order to know the wireless quality.

Not having WEP enabled or knowing the WEP key to be able to inspect the traffic will help into determining the SSID value and performing this test using the stimulus/response variant.

Testing:
Use `netstumbler` to check the available networks.

If the network broadcast the SSID, it would appear in the left hand column of the application. Besides, several configuration setting will be showed: one of them is the number of times per second the beacon frames are sent. Check it !!

Netstumbler uses probes, not beacons, to determine the existence of APs. To be sure that the access point is not accepting broadcast SSIDs, Netstumbler must be used either with a profile that has a blank SSID or with "auto reconfigure" switched on [5].

Besides, some client OS detect the broadcasted SSID, such as Windows XP, and allow to specify the SSID to be used. Check the found networks in the wireless icon on the taskbar or/and test the `ANY` SSID, which means in the station dialect to connect to any open wireless network available, independently of the SSID value.

It is also possible to check the configuration of the access point to confirm the status of this setting.

Default value:
By default, the Linksys BEFW11S4 access point enables the broadcast of the SSID value (see figure 2.1).

Objective/Subjective:
This is an objective test based on finding the SSID in `netstumbler`. Apart

[5] http://lists.bawug.org/pipermail/wireless/2001-September/002671.html

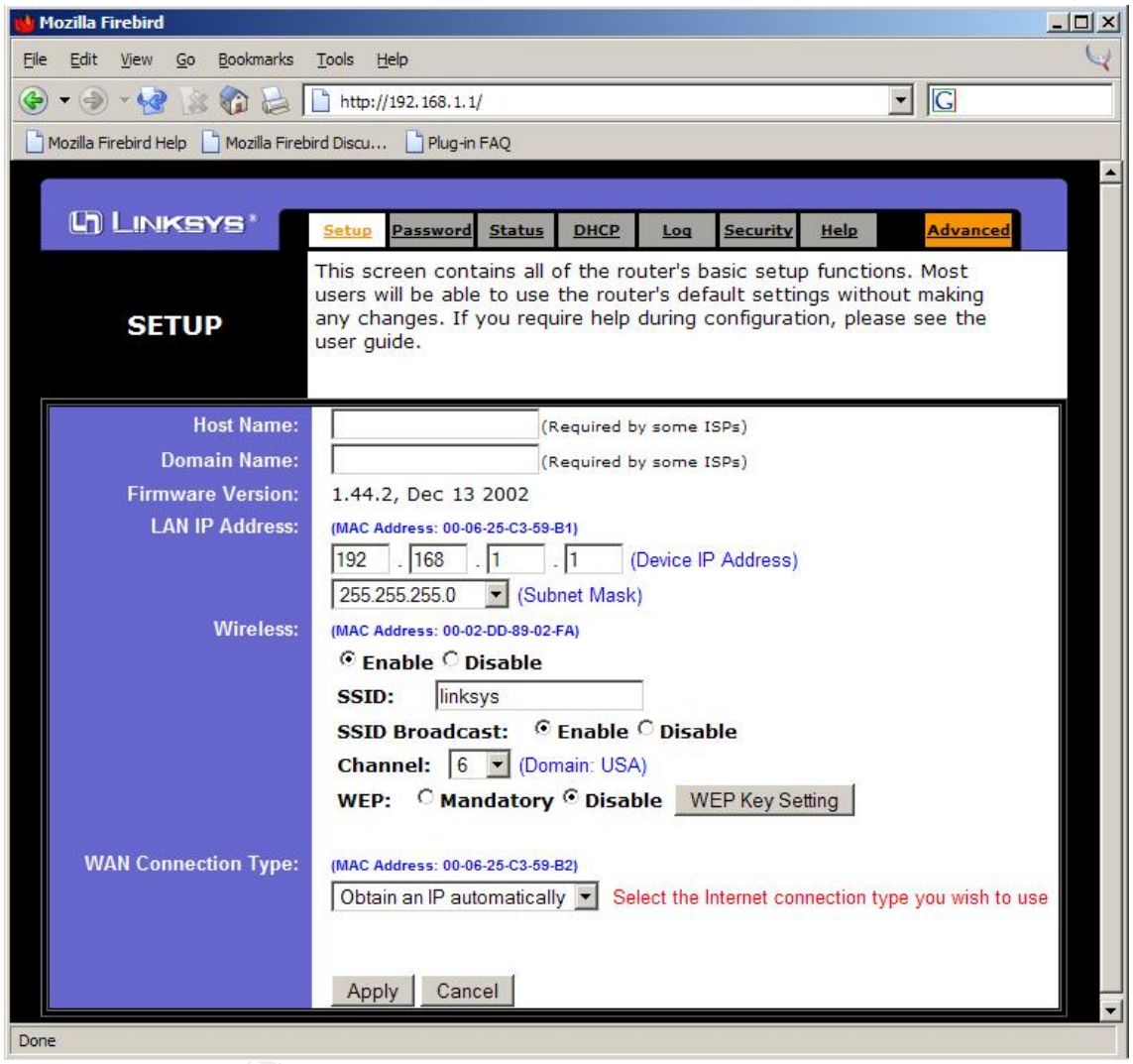

Figure 2.1: Default Linksys BEFW11S4 SETUP options

from that, network traces could be captured in order to confirm that beacon packets are frequently sent.

In order to accomplish this a special version of `ethereal` should be used [GAST1].

Apart from that, the device configuration could be checked.

2.3.2 Default SSID (AC-3-2)

Control objective:
Wireless networking products come with a default SSID set up by the factory, for example, the Linksys default SSID is "`linksys`". Attackers know these default values and will check them against your network. There are even Web pages containing all the default setting (SSID, channels, WEP keys...) classified by vendor [6] [7].

Change your SSID to something unique and meaningless to outsiders. The SSID is case sensitive and must not exceed 32 characters.

Risk:
If not changed it would allow an attacker to find and connect to the network even when the SSID is not broadcasted.

Apart from that it will reveal information about the vendor and type of device used, what can be used for more advanced attacks exploiting specific vulnerabilities associated to this type of equipment.

Compliance:
If the vendor SSID match with the one configured, this audit item matches. Additionally, it could be checked against other vendors values and with non auto-descriptive or significant values.

To be able to use the testing method based on a stimulus/response procedure the AP should broadcast its SSID.

Not having WEP enabled or knowing the WEP key to be able to inspect the traffic will help into determining the SSID value and performing this test using the stimulus/response variant.

Testing:
Get the device SSID and check if it is the default value through the access point Web management interface, checking the configuration available. To do so, connect to the default administration page (`http://192.168.1.1`) and check the SSID value in the `Setup` tab.

The SSID value could also be obtained using `netstumbler` if the network is broadcasting the SSID (see the previous check).

Besides, don't use a value which is the default used by other vendor or that could be meaningful for an attacker, such as, "Sales network".

[6] http://www.doc-x.de/cgi-bin/wiki.pl?DefaultSSID
[7] http://www.wi2600.org/mediawhore/nf0/wireless/ssid_deaults/

Default value:
By default, the Linksys BEFW11S4 access point uses the “linksys” SSID value.

Objective/Subjective:
This is an objective value once the default SSID vendor value is known (look at the vendor’s manuals).

2.3.3 Change the SSID frequently (AC-3-3)

Control objective:
It is also recommended to change your SSID regularly in order to force an attacker that have gained access to the network to start from the beginning in breaking in.

This process should be done manually based on the company procedures.

Risk:
If the SSID is maintained during long time periods then if for some reason it is obtained by an attacker (such as an information leakage), the time window to use it increase, decreasing the overall security status.

Compliance:
The company policies and IT staff must be queried and asked about the procedures for changing the SSID value. A solid conclusion should be obtained to affirm it is periodically changed.

Testing:
Check if there is a manual procedure involved and the frequency used to change it. Check also if there is some kind of historic registry when the last “N” SSIDs values used are saved.

Objective/Subjective:
This is a subjective measure based on asking about the policies related with the SSID values: people responses may be contradictory or not very clear.

2.4 Filters and Access Control Lists (ACLs)

2.4.1 MAC address based ACLs (AC-4-1)

Control objective:
Enable MAC address filtering through the usage of Access Control Lists

(ACLs).

Access points must contain a list of trusted end stations so they will only provide access to those wireless nodes with certain previously-known MAC addresses. This makes harder for an attacker to access your network with their own, or a random, MAC address.

When using large scale 802.11 networks other authentication methods, such as RADIUS servers, are recommended due to the associated overhead of managing hundreds or thousands potential clients.

Risk:
Although this is not an advanced protection method it would avoid the usage of the network by anyone using basic wardriving techniques. Lots of wireless cards allow a user to change the MAC address value by software, so an attacker could set it up to a value permitted in the filters.

Compliance:
The answer to this audit item should be “yes” or “no”, although it is possible to have some outdated filters, not covering the nowadays available clients.

Testing:
The BEFW11S4 model has two different MAC ACLs list: one is associated to the Internet access (WAN link) while the other refers to the device access.

- Internet access (WAN link): Check the configuration tab related with the `Filters` information. It is available inside the `Advanced` tab.

  Once there, the `Edit MAC Filter Setting` button allows to obtain a new window with the MAC ACLs.
- Device functions access: Go to the `Advanced` tab and enter into the `Wireless` tab, where the physical AP features are configured. At the end of this windows there is a section called `Station MAC filter`.

  It is possible to see the current ARP MAC table and to set specific MAC filters.

Default value:
By default, the Linksys BEFW11S4 access point doesn’t have any MAC ACL configured (Internet or device based).

Objective/Subjective:
It must be objectively checked if MAC address filters are being used verifying if the configuration have at least one MAC address in the correct field.

2.4.2 IP Filters and other filtering options (AC-4-2)

Reference:
Personal experience working with more advanced filtering devices, such as packet filtering and stateful firelwalls: Cisco PIX, Checkpoint FW-1, Linux iptables...

Control objective:
All nowadays networking devices provide some features to act as a packet filter system, blocking or allowing traffic based on the configured settings. Typically, networking devices, like routers, use ACLs while more advanced elements, such as firewalls, use a filtering policy.

The Linksys access point provides a `Filter` tab to configure layer-3 filters, at the IP level and TCP/UDP levels, layer-4, based on destination ports.

A very important point about filters is that the Linksys device filters from the wireless or wired network to Internet, that is, the WAN Link: it filters at the routing function level, but not between the wired or wireless networks.

Additionally, this Linksys model provides some specific configuration elements to allow or deny certain types of IP traffic, such as Multicast, IPSec, PPTP... These elements must also be checked.

Risk:
If the traffic allowed and denied is not filtered, any potential wireless attacker could generate any kind of traffic being capable of exploiting different remote vulnerabilities over the systems connected at the other side of the access point.

Compliance:
It is possible to verify the device filter configuration in order to figure out the traffic allowed into the “internal” wired network.

Testing:
Check the configuration tab related with the `Filters` information. It is available inside the `Advanced` tab. The first section references the IP range filters while the second section references the port ranges.

The additional configuration elements related with the IP filtering state are available in the same `Filters` tab but in the last portion of the Web page (after the previous filters).

Default value:
By default, the Linksys BEFW11S4 access point doesn’t have any IP or port filter configured.

By default the additional options are the ones showed in figure 2.2.

Objective/Subjective:
Getting the list of IP addresses and ports denied, and as a consequence allowed, is based on querying the device settings.

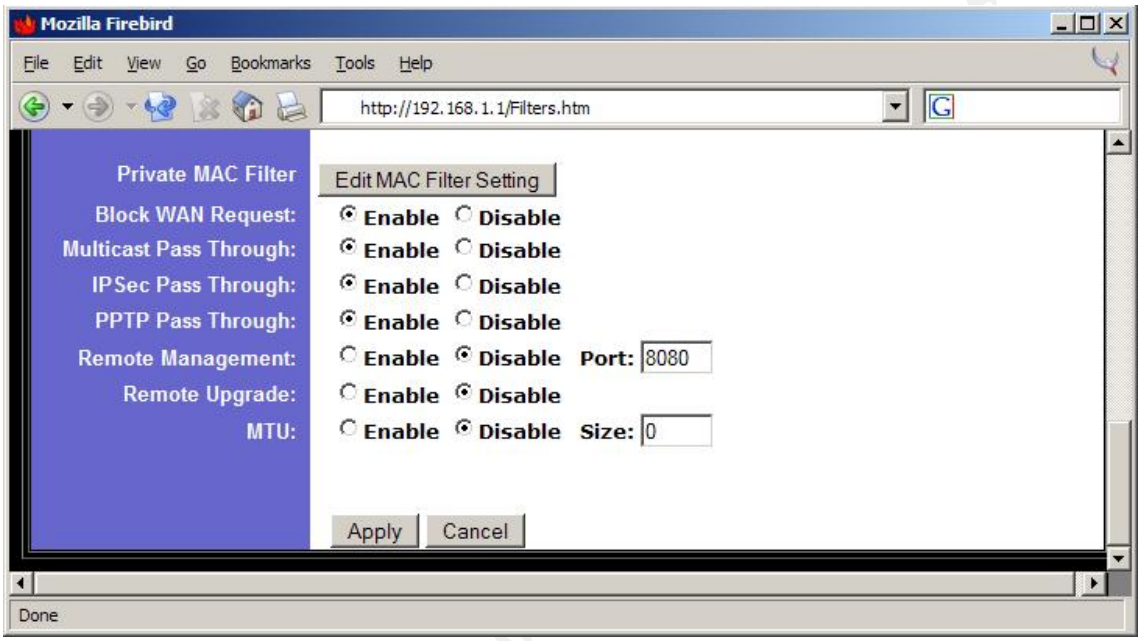

Figure 2.2: Default Linksys BEFW11S4 Advanced - Filters options

2.5 WEP Encryption

2.5.1 Highest WEP encryption level (AC-5-1)

Control objective:
It is recommended to use the highest level of encryption available, typically 128 bits. Enabling WEP 128-bit encryption will reduce the network performance.

Although it has been probed that WEP is vulnerable, it must be configured as a barrier between a trivial and an advanced attack. Some legal aspects are also involved in the usage of the WEP protection [POTT1, page 92], as a sign denoting that unauthorized access is not allowed.

Risk:
If the highest encryption level is not used it may be trivial (if WEP is not used) or very easy (if 40-bits WEP is used), for an attacker to crack WEP and obtain both, the WEP keys and all the traffic traveling through the wireless network.

Compliance:
The vendor documentation and device configuration must be compared to ensure the highest encryption level available. For the Linksys device analyzed 128 bits is the maximum level.

WEP must be enabled to be able to check this item through the configuration Web interface.

Testing:
Through the default `Setup` configuration tab it is possible to check the status of WEP: Mandatory or Disabled. To be able to confirm the encryption level used, the `WEP Key Setting` button must be used.

A new window will appear where the keys and their bit length is specified.

It is also possible to check the real WEP status capturing network traces and analyzing the packets payload in order to confirm if the traffic travels encrypted or not.

Default value:
By default the WEP feature is in the disabled state (see figure 2.1).

Objective/Subjective:
The highest level is a documented value that can be checked in the device configuration, therefore it is an objective value.

2.5.2 Multiple WEP keys (AC-5-2)

Control objective:
Multiple WEP keys must be used in order to enable a key rotation process to reduce the risk associated to an attackers that has obtained the WEP key in a very specific moment.

Almost all products allow the setting of 4 different keys. The Linksys device analyzed only allow 4 keys for 40-bits WEP. For 128-bits WEP only one key can be set.

Besides, it is recommended to follow an established procedure to change the 4 keys regularly (see it in a later check, AC-5-4).

Risk:
If only one WEP key is used, if an attacker is able to crack it, the wireless traffic will be compromised.

Compliance:
Check the number of keys in the configuration interface in order to determine if multiple keys are used. Only valid if WEP has been enabled and also if 128 bits keys are not used.

Testing:
Through the default `Setup` configuration tab it is possible to check the status of WEP. To be able to see the WEP keys and its number, the `WEP Key Setting` button must be used. A new window will appear where the keys values are displayed.

Objective/Subjective:
This is an objective item based on checking how many keys have been configured (at least four is recommended). Some device constraints could apply to the maximum number of keys.

2.5.3 WEP authentication (AC-5-3)

Control objective:
It is a must to check not only if the device allows to configure WEP for data encryption but for authenticating end stations. It is recommended to set up a pure WEP authentication environment, where non-WEP clients are not allowed to associate with the AP.

Risk:
If authentication is not secure, for example using the WEP keys configured for encryption, any client station will be able to connect to the network and establish an association. Once the attacker is "inside" more advanced attacks could be performed.

Compliance:
To be able to authenticate using WEP, WEP encryption must be active. The device documentation and configuration must be analyzed.

Testing:
To definitely confirm that the authentication between the end station and the access point is based on the WEP keys two tests are required:

- First one is based on configuring a client with the correct WEP parameters and test if it can connect to the network. For this test having the DHCP server enabled will facilitate to see if the communication is correct; if so, the DHCP configuration parameters will be received.
- Second one is based on performing the same actions with a non-WEP client.

Taking network traces during the association/authentication process will help to determine the traffic exchanged and if the association takes place or not.

Objective/Subjective:
This is an objective check based on the manual documentation about the product and the traffic interchanged when creating an association and WEP has been enabled.

2.5.4 Change the WEP keys frequently (AC-5-4)

Control objective:
It is also recommended to change the WEP keys regularly in order to force an attacker that have gained access to their values to start from the beginning in breaking in.

This process can be done manually based on the company procedures or automatically using advanced features such as WPA.

There are also some proprietary solutions, such as “Enhanced WEP” for key management in the end systems [8].

Risk:
If the WEP keys are maintained during long time periods then, if for some reason, they are obtained by an attacker (such as cracking them), the time window to use them increase, decreasing the overall security status.

Compliance:
To determine if the keys are frequently changed or not, the company policies must be checked when there is no use of an automatic solution such as WPA.

If WPA is used then its specific configuration should be checked.

Testing:
Check if there is a manual procedure involved and the frequency used to

[8] http://www.wi-fiplanet.com/news/article.php/955641

change it asking the wireless network administrators and reading the wireless company policies.

Additionally, check if there is an automatic mechanism to change it, such as WPA (see the audit checklist AC-9-3).

Objective/Subjective:
The manual procedure is subjective because is based on company policies and its application. However, the automatic procedure is safely determined by the usage of the technology, like WPA.

2.6 Administration

2.6.1 Change the (default) administrator's password regularly (AC-6-1)

Control objective:
The network settings associated to the wireless device (SSID, WEP keys...) are stored in its firmware. The network administrator is the only person who can change these settings, so if an attacker gets the password, he will acquire the highest privileges in the device and will take its control.

This item try to check two elements: that the default administrator password has been substituted and that the nowadays password is frequently changed based on a clearly established company policy.

For the BEFW11S4 model the administrator password must be less than 64 characters.

Risk:
If the administrator password is obtained then the system could be totally compromised.

Compliance:
It is trivial to confirm if the default password has been changed. A more efficient step would be to analyze if the password if robust enough against dictionary attacks.

Testing:
The easiest method of verifying the device password is accessing the Web management interface and trying to authenticate using it. It is not possible to obtain the nowadays running value because the configuration displays it using the "*" character (see figure 2.3).

This Linksys AP model doesn't provide the concept of users, thus to authenticate the `username` field must be left blank.

Default value:
The Linksys default password is `admin`.

Objective/Subjective:
The initial change is an objective test knowing the default value, but the change frequency is subjective based on the policies used.

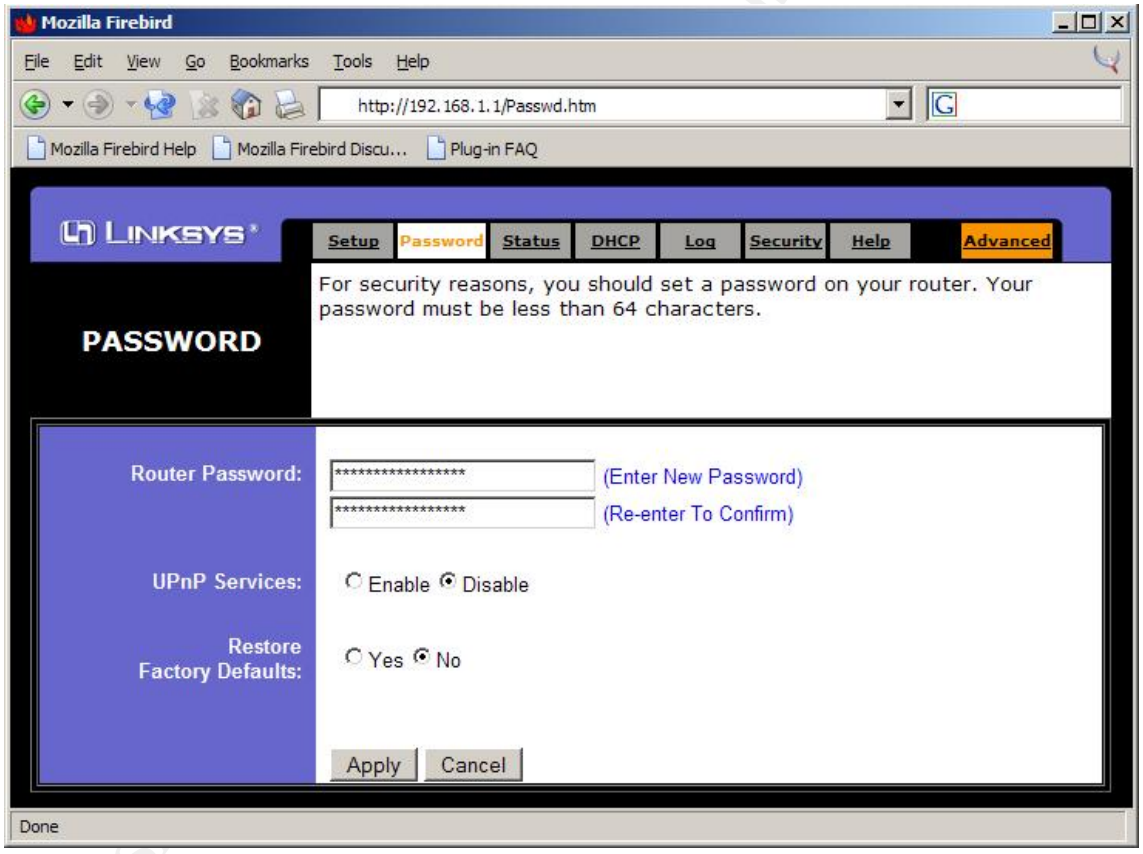

Figure 2.3: Linksys BEFW11S4 password configuration

2.6.2 Management interfaces (AC-6-2)

Control objective:
The access point devices typically provide different methods for administer-

ing the system, such as Telnet, HTTP, serial console..., called management or administration interfaces. Let's analyze some basic concepts about the security involved in all them:

- TELNET: This method should be avoided due to the lack of encryption. The administrator password will travel in clear over the network so any local attacker can intercept it. The Linksys model doesn't provide this method.
- HTTP: This is the unique method available in the Linksys device analyzed, and the problem is that it doesn't use a encrypted channel, such as HTTPS (based on SSL).
- Serial connection: the Linksys model doesn't provide a direct connection, which typically represent the most secure way of managing a networking device.

Additionally it is possible to manage the device remotely, that is, from Internet instead of only from the internal (wireless + wired) network. The Linksys BEFW11S4 has a configuration menu for this purpose.

On firmwares newer than 1.43.3 the "Remote Management" port can be changed. This will not make the attack impossible at all, but will somehow make it a little tougher for an attacker, probably giving you some more time to detect him.

If possible limit the management access only to the internal wired side.

Risk:
If an attacker is capable of interacting with the device management interface there is a possibility of getting the password, for example because it is using the default value, or because it is a weak password that can be guessed through dictionary or brute force attacks, and get overall control of the access point.

This situation is even worse if it is possible to access the system from Internet.

Compliance:
The management methods should be evaluated in two steps:

- First one is based on identifying all the possible access methods and the security involved in all them, mainly from a encryption perspective.
- Second one is based on analyzing from where the access to any of the previously identified management doors is allowed: Is it allowed only from the internal network or is accessible through Internet?

Testing:
The Linksys BEFW11S4 only provides Web access for administering the box.

The model analyzed has a menu to enable the remote access of the Web management interface. It is the same one previously analyzed for establishing IP filters (see figure 2.2). The remote management port can be changed.

It is possible to evaluate the robustness of the management access taking network traces to confirm how the data travel through the network. This is a recommended step in order to confirm if encryption is used.

Default value:
By default, the Linksys model only provides the Web administration interface and the remote management port is listening on the TCP 8080 port.

Objective/Subjective:
This is an objective measurement once all the available management methods have been identified: the decision factor is based on a solution using encryption or traveling in the clear over the network.

2.6.3 Configuration backup (AC-6-3)

Reference:
SANS assignment description for the GSNA certification, the one is trying to accomplish this paper.

Control objective:
It is recommended to have an easy and fast method to backup and recover the device configuration, containing all the operational and security settings.

This feature is available for the BEFW11S4 in firmware version 1.45: "*5. Added backup & restore configuration function.*"

Risk:
Not having a fast procedure to restore the device configuration in case of a failure could force to large periods without service, increasing the consequences of a DoS/failure event.

Compliance:
Check the firmware version of the access point and check the associated menu.

Testing:
To check if the backup function is available the device firmware version must be checked, should being equal or greater than 1.45 (see figure 1.3).

Objective/Subjective:
Once it has been confirmed that the appropriate firmware version is running, the required functionality is implicitly available.

2.7 TCP/IP stack and services

2.7.1 DHCP server (AC-7-1)

Control objective:
The access point provides a built-in DHCP server with the idea of increasing the flexibility and easy of use of the network. If a client, wired or wireless, requests an IP address and all the associated network configuration through the DHCP protocol, the Linksys AP will provide all the data required.

It is recommended not to have the DHCP service enabled, increasing the security although decrementing the flexibility.

The device is also capable of providing a “DHCP Active IP Table” showing the current DHCP leases.

Risk:
If a potential attacker is able to find the wireless network and create an association, it has obtained access at the physical and link level (layer 2). To be able to use the networking resources, both internal and external (Internet) he needs an IP address and other settings, such as the default gateway, DNS servers... Once he obtain this information it is possible to have complete network access. The DHCP server provides this information.

If the DHCP settings are not published, the attacker would need to sniff the network traffic trying to get this data from the packets sent and received by other users.

Compliance:
To be able to check if the DHCP server is enabled, the access point configuration must be queried or network traces analysis is required.

Testing:
The DHCP server is configured under the `DHCP` tab. A new window appears containing all the DHCP configuration: IP address range, number of clients, lease time, and DNS and WINS information.

Another way of testing it is taking network traces and checking if the access point is responding to DHCP queries. It is very easy to send a query, for example, in Windows through the `ipconfig /renew` command.

Default value:
By default, the DHCP server in the Linksys model is enabled.

Objective/Subjective:
This is a deterministic item, based on the access point running configuration.

2.7.2 TCP portscan (AC-7-2)

Reference:
Item obtained from the personal experience scanning other network devices and systems while performing penetration testing and auditing services.

Control objective:
The access point device would have different active TCP/IP services based on the configuration settings associated to the running state. For example, it may have the Web admin interface, the remote management facilities enabled, the remote firmware update feature enabled...

Additionally the Linksys AP could define some filters, but those only apply to the Internet (external) traffic, therefore they don't protect the device itself.

Risk:
Any open TCP service not required is a new potential vulnerable door for accessing and taking control of the device or to be able to launch a DoS attack.

Compliance:
The purpose of this check item is having as less services as possible, that is, activate only the required services.

To be able to confirm if the actual status match with the expected results it must be explicitly known the necessary services that must be running to provide the required functionality.

Testing:
In order to test the TCP opened ports and services the whole possible range will be analyzed, from port 1 to 65535, using the `nmap` utility (see table 2.2).

```
nmap -sT -p 1-65535 AP_IP_address
```

Objective/Subjective:
This is an objective verification once the required services are known, because they can be compared against the results obtained from the testing

Tool:	*nmap*	http://www.insecure.org/nmap/
Nmap is a security portscanner (TCP and UDP), an OS fingerprinting tool and network exploration tool. It is recommended to use the latest `nmap` version, 3.50, mainly for tests such as the AC-7-5.		

Table 2.2: Nmap: network "security" mapper

phase. However, typically it is very difficult to have a deep knowledge about all the required services.

It is recommended to analyze all those opened ports not associated to the services identified.

2.7.3 UDP portscan (AC-7-3)

Reference:
Item obtained from the personal experience scanning other network devices and systems while performing penetration testing and auditing services.

Control objective:
The access point device would have different active TCP/IP services based on the configuration settings associated to the running state. For example, it may have dynamic routing capabilities, such as RIP, the DHCP service enabled...

Additionally the Linksys AP could define some filters, but those only apply to the Internet (external) traffic, therefore they don't protect the device itself.

Risk:
Any open UDP service not required is a new potential vulnerable door for accessing and taking control of the device.

Compliance:
The purpose of this check item is having as less services as possible, that is, activate only the required services. To be able to confirm if the actual status match with the expected results it must be explicitly known the necessary services that must be running to provide the required functionality.

Testing:
In order to test the UDP opened ports and services the whole possible range will be analyzed, from port 1 to 65535, using the `nmap` utility (see table 2.2).

```
nmap -sU -p 1-65535 AP_IP_address
```

Objective/Subjective:
This is an objective verification once the required services are known, because they can be compared against the results obtained from the testing phase. However, typically it is very difficult to have a deep knowledge about all the required services.

It is recommended to analyze all those opened ports not associated to the services identified.

2.7.4 ICMP typescan (AC-7-4)

Reference:
Item obtained from the personal experience scanning other network devices and systems while performing penetration testing and auditing services.

Control objective:
Based on the TCP/IP stack implementation of a specific device, it is possible that it replies to specific ICMP queries that could provide internal information.

The ICMP protocol has different query types, such as ECHO, TIMESTAMP, MASK...[9]

The Linksys BEFW11S4 TCP/IP stack cannot be configured by the administrator so it is interesting to evaluate how it behaves in order to know if an additional filtering device should be placed in front of the access point not to provide too much information.

Risk:
A potential attacker could obtain information about the existence of the device, its network mask (specified in its configuration), the timestamp value... This type of information could be helpful for more advanced attacks and use to be acquired during the initial attack reconnaissance phase.

Compliance:
Check the device responses to verify the type of ICMP queries it is able to respond.

Testing:
Using the `hping2` (see table 2.3) utility it is possible to generate all types of ICMP queries, besides, it provides information about the responses received in a similar way the `ping` command does.

[9] http://www.iana.org/assignments/icmp-parameters

- **Echo request**: hping2 192.168.1.1 -1 -C 8 -c 5
- **Timestamp request**: hping2 192.168.1.1 -1 -C 13 -c 5
- **Mask request**: hping2 192.168.1.1 -1 -C 17 -c 5

Objective/Subjective:
This is an objective check based on the deterministic device responses to the different ICMP protocol stimulus.

Tool:	*hping*	http://www.hping.org
Hping is a packet crafting tool, and supports TCP, UDP, ICMP and RAW-IP protocols.		

Table 2.3: Hping: TCP/IP packet assembler/analyzer

2.7.5 Operating System fingerprinting (AC-7-5)

Reference:
Item obtained from the personal experience scanning other network devices and systems while performing penetration testing and auditing services.

Control objective:
The TCP/IP stack implementation of every network device has different features and behaviors based on the crafted packets that can be sent. The `nmap` utility uses this type of special packets to determine and differentiate between various device types or operating systems and versions.

This audit item tries to evaluate how `nmap` is able to fingerprint the operating system of the Linksys access point.

Risk:
An attacker could be able to identify the BEFW11S4 using the mentioned tool in order to exploit specific vulnerabilities over the device, such as the ones that will be analyzed later.

Compliance:
This test would generate 3 different outputs:

1. It is possible that `nmap` will accurately identify the Linksys model.
2. Perhaps the tool will confuse the model with another one, associated to a distinct system.

3. Finally, the tool can display the fingerprint but it doesn't have any associated OS or system to it, so it is a new device from the `nmap` perspective.

Testing:
To obtain the OS identified by the utility just run it with the following options:

```
nmap -O 192.168.1.1
```

Objective/Subjective:
The result obtained when using the same `nmap` version, and it is recommended to use the last one, 3.50, will be always the same because it is based on the detection database associated to the tool.

2.8 Logging: syslog messages (AC-8-1)

Control objective:
The purpose of the syslog server is being able to record all the different messages and warnings generated by networked devices alerting about errors or anomalous conditions. Through this service it is possible to trust another system (the syslog server) in order to verify a device status. Besides, having the capability of being able to select the logged events would allow focusing only on the information required by the security policies.

This type of messages are also very helpful during incident investigation in order to correlate events from different sources.

Risk:
Not having a remote capability for capturing system events provides a situation in which the network and system administrators are partially blind about the activities that are taking place in the network.

Additionally, if an attacker takes the control of a system and the logging events are only stored on the system compromised, the attacker will be able to delete all them; that is the reason why a remote logging capability is desired.

Compliance:
To be able to confirm if a syslog server has been configured the Web management interface must be accessed and the `Log` menu reviewed.

Apart from that, it will be recommended to analyze the system that is referenced as the logging server, mainly to confirm that the log server is up and running and working as expected.

Testing:
Access the Web management interface and review the `Log` menu checking if it is `Enabled` and the IP address of the log server.

In order to review the remote server, it is recommended by Linksys to run the `logviewer` [10] utility to capture and process the log messages generated by the access point.

Is is also possible to check the logging messages locally through the `Incoming Access Log` and the `Outgoing Access Log` buttons.

Default value:
By default, the logging capability of the Linksys BEFW11S4 access point is disabled.

Objective/Subjective:
This is a deterministic item, based on the access point running configuration.

2.9 Advanced security features

2.9.1 VPNs usage (AC-9-1)

Control objective:
In an inherent insecure environment, such as the 802.11 networks, it is recommended to make use of other encryption and authentication protocols, like the ones around the VPN solutions: SSH, HTTPS and IPSec.

As have been analyzed in other sections of this paper, the WEP protocol has been broken, therefore the wireless built-in encryption methods are not enough to protect sensitive information. Thus, it is recommended to include another encryption level based on a robust and secure technology like the ones mentioned above.

Risk:
Not having a nowadays “unbreakable” encryption technology could lead to information leakage, thus giving a potential attacker the opportunity of getting the network traffic and all the company confidential information.

Compliance:
It is recommended to take a significant amount of network traces through

[10] ftp://ftp.linksys.com/pub/befsr41/logviewer.exe

sniffing methods to be able to confirm the usage or not of encryption protocols. To be able to test it the WEP feature should be disabled or the WEP key known.

Typically, the nowadays environments could be considered “mixed” solutions, where both, non-encrypted protocols, such as telnet or ftp, share the network with encrypted protocols, such as ssh, ssl... so it is recommended to evaluate the criticality of the information carried by each of them.

Testing:
Take network traces from the wireless and wired environments. It is recommended to inspect the wireless environment because it acts as a physical hub, instead of the switch used inside the wired segment of the device analyzed.

Again, use `ethereal` during a significant time period, between 1 and 3 hours, and analyze the traffic and protocols used. To do so, use the option `Protocol Hierarchy Statistics` under the `Tools` menu.

Objective/Subjective:
Determining if at least one unencrypted protocol is used is an objective decision, but it would be appreciated a deepest evaluation about the contents of all the unencrypted protocols and also the number, features and purpose of the encrypted ones.

Therefore it is a subjective measure determining the risk associated to the unencrypted protocols used when there is a mixture of encrypted and unencrypted traffic.

2.9.2 802.1X (AC-9-2)

Control objective:
This authentication standard is based in the EAP protocol, Extensible Authentication Protocol [GAST1]. This standard adds a new “dynamic key” distribution procedure in order to increase the frequency the encryption keys are generated and interchanged [POTT1] and also provides more robust authentication methods based on external RADIUS servers, as for example, digital certificates.

Risk:
The most extended authentication method used nowadays, WEP authentication, has probed to be weak enough to allow an attacker to get the WEP key, thus being able to authenticate and access the network. Once this first step has been performed, more advanced attacks could be launched.

However, 802.1X has been also broken as showed in [ARBA1].

Compliance:
It is required to check if the specific firmware version supports the 802.1X protocol. It could be checked through the vendor documentation and then, compared with the running configuration version.

Testing:
Linksys devices don't support the 802.1X protocol individually. Only the firmwares supporting WPA are able to provide 802.1X controls (see "AC-11-1").

Objective/Subjective:
It is a configuration item that can be directly checked looking at the device settings.

2.9.3 WPA (WiFi Protected Access) and 802.1i support (AC-9-3)

Control objective:
As has been already analyzed, WEP is not as secure as expected when it was designed. Therefore, the IEEE has released an intermediate security solution until the final 802.11i security standard is finally published [WPA1], [LOEB1].

WPA introduces a new cipher suite called TKIP, Temporal Key Integrity Protocol. It is based on:

- Using longer keys: 256 bits.
- Generates individual keys based on the preshared key for each station. Each data packet sent has its own unique encryption key generated from a temporal key, also unique per station.
- Changing the encryption keys: these are changed after a certain number of frames have been sent. It is used for the unicast traffic.
- Message Integrity Checking (MIChael method): it avoids injection of forged packets checking the data integrity.

Additionally WPA provides a rekeying feature where the AP is able to advertise the global key (used for multicast and broadcast traffic) to all the connected stations.

It also forces the usage of strong authentication. The authentication is based on the usage of the 802.1X protocol supported by a preshared key or RADIUS servers. In small environments it uses the preshared key method because there are no authentication servers available.

This standard has been already widely deployed in the WiFi market, for example in the Windows OS: "Overview of the WPA Wireless Security Update in Windows XP" (MKB: 815485): http://support.microsoft.com/?kbid=815485.

WPA recommends the use of the AES encryption algorithm instead of the RC4, but is an optional feature. This algorithm will be required in the 802.11i standard (sometimes called WAP2) due to being more robust and secure. The AES variant is called CCMP, Counter mode with CBC-MAC, compared with the RC4 variant called TKIP.

802.11i is an inter-operable protocol but requires a hardware update in both, access points and end stations, to being able to perform the AES computation using built-in chipsets. It also manages keys in an dynamic way using an automatic distribution method (TKIP) and the authentication process uses the 802.1X and EAP protocols. Let say that WPA is a subset of 802.11i.

Risk:
Not having an advanced standard like the ones proposed, WPA or 802.11i, could lead to several authentication and encryption breaches discussed all along this paper and associated with the standards used today: WEP, WEP authentication, preshared keys...

An attacker could be able to connect, consume the network resources, eavesdrop and modify the network traffic, having control over very sensitive pieces of information.

Compliance:
Based on the firmware version it must be checked if the device supports this modern security solutions. If so, they should be enabled. This information can be confirmed getting the vendor documentation and checking the access point configuration.

Testing:
It is recommended to read and analyzed the Linksys documentation and Web pages, particularly the new firmware versions release notes (see "AC-11-1").

Objective/Subjective:
This item is only trying to evaluate the usage of these new security features, not their details or vulnerabilities, so it is an objective check to know if WAP or 802.11i are used or not.

2.10 Wireless LAN policies (AC-10-1)

The company should have a wireless policy specifying its correct use and the security aspects of this environment, with the goal of reducing security breaches.

The policy should forbid unauthorized access points and official access points with incorrect, not validated, settings (WEP configuration, broadcast mode, SSID value...).

Other technology constraints that should be enforced through the company policy is the usage of:

- specific connection speeds, such as 5 Mbps and 11 Mbps, limiting attackers coming from longer distances and connecting to 2 Mbps rates.
- specific 802.11 channels. All the traffic out of these official channels could be considered suspicious.
- specific hours for the wireless traffic, in order to avoid attacks during the night, when the company activity and surveillance is less than during working hours.

The policy should also consider other general networking aspects, such as the correct use of the bandwith. In wireless networks this is a limited resource, and the usage of high bandwith consuming application, such as multimedia downloading, will affect the network performance and could even generate a DoS situation.

Finally, the policy should include other general IT aspects, such as the recommended password guidelines, or the change frequency, as well as specific hardening tips, for both, the physical location and the logical elements (services, banner messages...).

Due to the fact that this checklist is mostly focused on the technical aspects of the model analyzed, detailed policy checklist will be slightly covered but the references mentioned in the previous section could be used.

2.11 Device Firmware (AC-11-1)

Control objective:
The purpose of this item is the verification of the firmware version running in the device compared with the most actual version released by the vendor. Newer versions provide bug resolution, what increases the security of the system, plus additional features, of which some of them could be security related.

Risk:
Non having the latest available firmware could lead to a vulnerable system. It is also possible that a newer firmware version solves some publicly know vulnerabilities for which proof-of-concept exploits have been released.

Compliance:
As a rule of thumb it could be strictly checked if the device is running the latest firmware revision, available through the Web management interface.

Testing:
Check the vendor web page for information about the latest firmware versions and its new features.

The Linksys firmware page is http://www.linksys.com/download/. The specific access point model and version should be selected.

Once known, check the version running in the device (see figure 1.3).

Objective/Subjective:
It is an objective fact to confirm if the latest firmware version have being installed but it doesn't ensure to solve all vulnerabilities or problems in the device.

As a subjective test based on all the different aspects involved, an in-depth evaluation of every new feature included for each new revision should be made in order to evaluate if a new firmware is well worth for the environment where the AP is running.

2.12 Specific Linksys vulnerabilities

2.12.1 Linksys long password field vulnerability (AC-12-1)

Reference:
"iDEFENSE Security Advisory 11.19.02": [11]

Control objective:
It checks a well-known vulnerability associated to the built-in web server running into the device.

The BEFW11S4 version 2 can be crashed when several thousand characters are passed in the password field of the device's Web management interface.

[11] http://www.idefense.com/application/poi/display?id=36&type=vulnerabilities

Exploitation simply requires the use of a web browser that can send long "Basic Authentication" fields to the affected router's interface.

Risk:
This may allow an attacker to force the administrator to reboot the router, therefore provoking a DoS attack. Besides, it may allow the attacker to gain sensitive information during router authentication.

Compliance:
It directly affects the BEFW11S4 model with firmware earlier than version 1.43.3.

Checking is based on analyzing the response of the access point to the request, verifying if it gets hanged (doesn't respond to other HTTP requests) or not.

Testing:
Remote exploitation is only possible if the remote Web management interface is enabled (this is disabled by default). An attacker on the internal network can access the Web management interface by using a web browser and accessing the device URL `http://IP_address` (192.168.1.1 is the default IP address).

For example, the Mozilla Web browser version 1.5 accepts long authentication fields.

Objective/Subjective:
It is an objective test based on the results obtained after sending the malicious HTTP request.

2.12.2 Linksys multiple vulnerabilities advisory (AC-12-2)

Reference:
"Linksys BEFW11S4 Wireless Router Buffer Overflows and Parsing Bugs Let Remote Users Take Full Control of the Router":
http://www.securitytracker.com/alerts/2002/Dec/1005744.html
http://www1.corest.com/common/showdoc.php?idx=276&idxseccion=10
http://www.securiteam.com/securitynews/6H004156AO.html

Control objective:
Several vulnerabilities were reported in the Linksys BEFW11S4 Wireless router:

- It is reported that there is an error in parsing requests for '.xml' pages. A remote user can access any page of the remote administration interface without having to authenticate to the device.
- It is also reported that several stack-based buffer overflows can be triggered by a remote user (before authentication is required).
- It is also reported that there are some heap-based overflows that can be triggered by a remote authenticated user.

Risk:
A remote user can bypass authentication to gain administrative control of the router or can execute arbitrary code on the router.

Compliance:
It directly affects the BEFW11S4 model with firmware earlier than version 1.44. For each of the vulnerabilities it could be confirmed if access has been obtained to the device.

Testing:
This is a summary of some of the test that allow an initial verification of the mentioned vulnerabilities. It is recommended to access the references above to obtain the working exploit codes:

```
- Changing the remote management application:
Send the following URL contents to the device Web management interface.

http://192.168.1.1/Gozila.cgi?setPasswd=hola&RemoteManagement=1&.xml=1

- Try the UPnP URL to confirm it is running:
http://IP_address:5678/rootDesc.xml

- Buffer-overflows and SNMP traps:
Use the Python scripts "linksys_exploit.py" and "snmp-traps.py" from
"http://www1.corest.com/common/showdoc.php?idx=276&idxseccion=10".
```

Figure 2.4: Testing the AC-12-2

Objective/Subjective:
It is an objective test based on the results obtained after sending the malicious Web request or using the referenced exploits.

2.12.3 Linksys SNMP vulnerability (AC-12-3)

Reference:
"Linksys Routers Found to be Vulnerable to SNMP Issues":
http://www.securiteam.com/securitynews/5AP0G0A61Y.html

Control objective:
Querying the Linksys device with the default SNMP community of "public" causes it to set the IP address that queried as its snmptrap host, therefore the messages and alarm information will be dump to it.

Although the device analyzed doesn't have a configurable SNMP agent, it provides some SNMP embedded functionality because when it boots an SNMP trap is generated (more details at the end of the `assignment 3` section), so it was considered well worth to check this specific vulnerability.

Risk:
Serious information leakage problems, as well as a potential opening to be used as a DDoS initiator.

Compliance:
It affects the BEFN and BEFS router plus switch product families. Once the SNMP query packet has been sent it is possible to check if the SNMP trap information is received.

Testing:
Send an SNMP get packet and check if other SNMP information, traps, are received later. To select a specific SNMP variable it is recommended to consult the 802.11 MIB tree [GAST1].

```
- Sending the SNMP query:
$ snmpget -c public IP_address SNMP_variable

- Check if SNMP traps are received setting up an SNMP server or, more easily,
taking network traces, for example through "ethereal".
```

Figure 2.5: Testing the AC-12-3

Objective/Subjective:
It is an objective test based on the results obtained after sending the malicious SNMP request: check network traces or verify the device configuration.

2.12.4 Linksys DoS vulnerability (AC-12-4)

Reference:
"Linksys WRT54G Denial of Service Vulnerability":
http://lists.seifried.org/pipermail/security/2003-December/000069.html

Control objective:
It checks a well-known vulnerability associated to the built-in web server running into the device.

Risk:
This may allow an attacker to force the administrator to reboot the router, therefore provoking a DoS attack. Besides, it may allow the attacker to gain sensitive information during router authentication.

Compliance:
It doesn't directly apply over the model analyzed, but it affects other Linksys routing devices such as the Linksys WRT54G v1.0 (firmware v 1.42.3), so it is well worth to check it.

Checking is based on analyzing the response of the access point to the request, verifying if it gets hanged (doesn't respond to other HTTP requests) or not.

Testing:
Send a blank GET request to the router on port 80 (or 8080) to check if it halts the embedded webserver. The `netcat` [NETC1] utility will be used for both, sending the evil packet and checking the HTTP server availability:

```
$ nc <<IP_address>> 80
GET
$
$ nc <<IP_address>> 80
... Checking response ...
```

Figure 2.6: Testing the AC-12-4

Objective/Subjective:
It is an objective test based on the results obtained after sending the malicious HTTP request.

ASSIGNMENT 3 - AUDIT EVIDENCE

The following paragraphs introduce a brief description of the auditing environment.

The access point analyzed is installed inside the network of a small business company (SMB), using an environment similar to the one presented in figure 1.2, reference 1, where the wireless device is not isolated in the DMZ of a firewall.

The company goal for using this type of device is based on providing flexible and easy access to some sales and engineering staff when temporarily visit the company facilities for accessing the internal resources as well as Internet.

In order to perform the audit the access point must be up and running using the company established configuration. To be able to test the default values, another similar model access point was used from scratch. All the initial configuration steps were taken out of the vendor "User Guide" manual [LINK1].

All the direct checks have been developed accessing the Linksys interfaces, HTTP web server and network features, through a laptop using two methods based on the audit item to be checked: a wireless access through the wireless network audited or a wired connection plugged in into one of the device switched ports. The laptop used run Windows XP and Linux Red Hat 9.0 depending on the test executed.

Before performing the audit it is recommended to obtain a written authorization from the company management. Additionally, and given the fact that this is an audit and not a penetration test, some information was required to check some audit items:

- In order to verify the device settings through the Web management interface, the administration password was needed. It was provided by the network administrator.
- Some items should be checked with WEP disabled or knowing the WEP key to be able to analyze the wireless traffic. Initially, the WEP key was provided by the administrator, although an extra exercise was performed to check if it could be obtained (see the end of this section, "Is the system auditable?").

3.1 Conduct the audit

The most relevant audit items, and most directly associated with the Linksys BEFW11S4 model analyzed, developed when running the auditing are showed bellow.

3.1.1 Interoperability range (AC-1-1)

In order to evaluate the signal status around the company building, and given the fact that the AP device is physically running on the top floor (3rd) of the building (the building has 3 floors and an underground garage), the following places were checked:

- Garage
- 1st floor
- 2nd floor
- Street signal out of the building fences (about 100 meters from the building walls)

The figure 3.1 screen capture shows the signal strength and features for one of the different locations analyzed, 2nd floor. The table 3.1 reflects all the average values obtained without using a special unidirectional antenna.

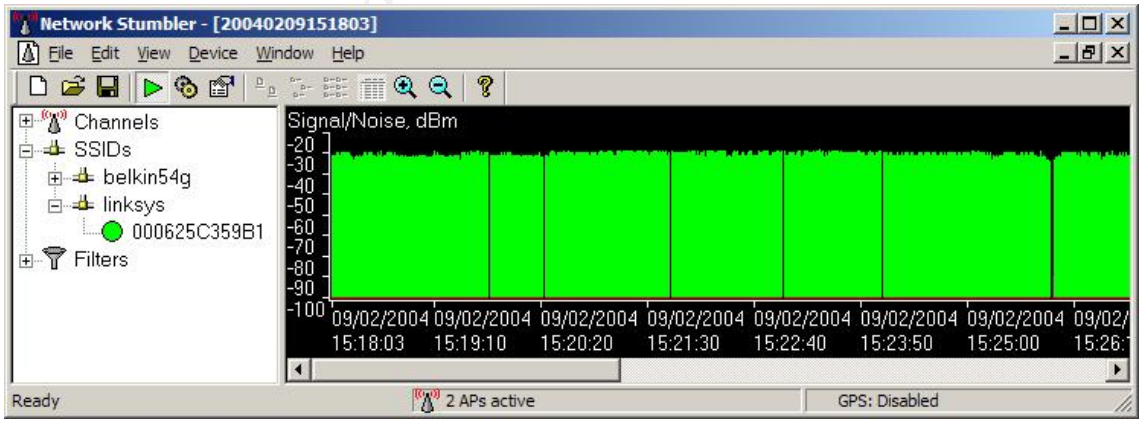

Figure 3.1: Linksys BEFW11S4 signal strength (2nd floor)

This information was captured using `netstumbler`. It could be not possible, based on the access point configuration, to get the signal range with this tool, for example if the SSID is not broadcasted. Therefore, other utilities can be used

such as the Windows XP network card status screen (see figure 3.2) or a particular wireless client application, based on the network card vendor and model used (see figure 3.3 for a Compaq WL200). Both them were captured in the 2nd floor.

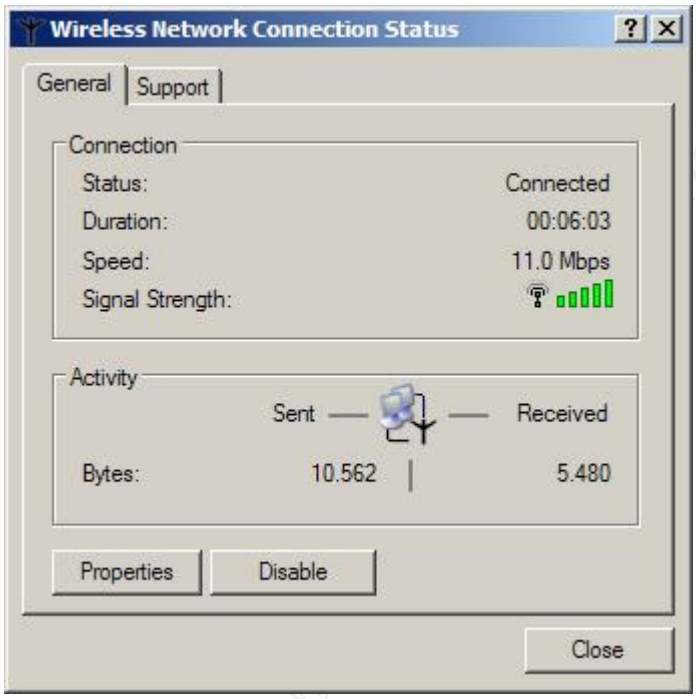

Figure 3.2: Signal quality from a Windows XP client

Location	SNR (dBm)	Data rate
Garage	-40	11 Mbps
1st floor	-35	11 Mbps
2nd floor	-30	11 Mbps
Street	-55	Between 5.5 and 11 Mbps

Table 3.1: 802.11 wireless signal and data rate in different locations

The signal analyzed was generated using the default configurable values: see the `Advanced` configuration tab, and select the `Wireless` tab (figure 3.4). This parameters make the signal available from outside the company facilities and building walls.

Figure 3.3: Signal quality from a Compaq WL200 client

3.1.2 Wired and wireless built-in networks (AC-2-2)

With the goal of analyzing the internal network structure of the device the proposed tests described in this item in the checklist section were run, plus the confirmation of the topology of the internal built-in switch.

Traffic was generated using the `ping` utility, from the wireless and the wired network to both, unicast and broadcast addresses:

- **Unicast** traffic:
  - Traffic generated from the Wireless segment: this traffic is seen on the wireless network, so it acts like a hub, but it is not seen in the wired network.
  - Traffic generated from the Wired segment: it is not seen in any of the networks. It is a pure switch environment.
- **Broadcast** traffic:
  - Traffic generated from the Wireless segment: again, this traffic is seen on the wireless network, but also on the wired segment.
  - Traffic generated from the Wired segment: as the previous test, it is seen in all segments.

Based on the results obtained it could be concluded that:

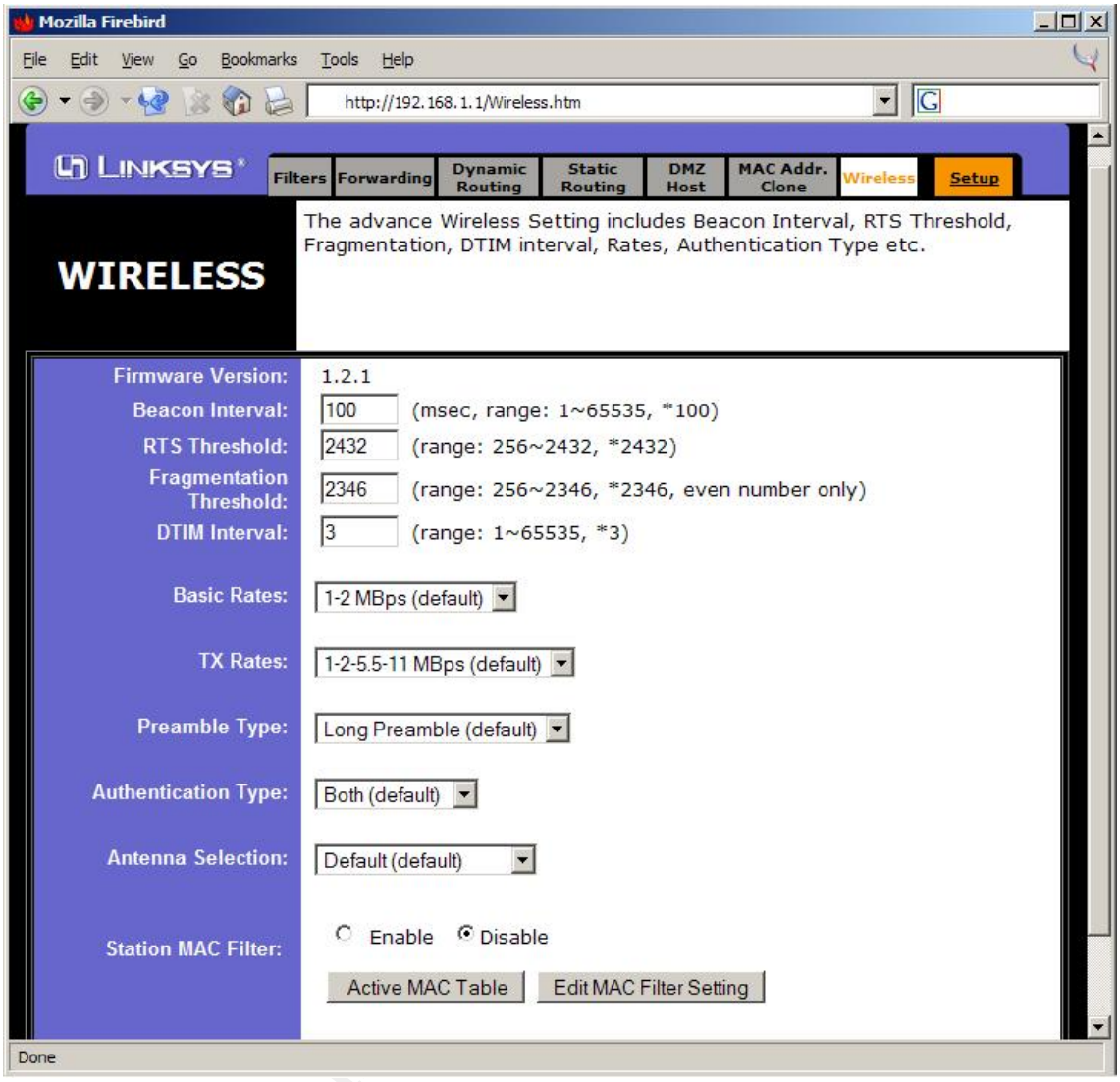

Figure 3.4: Linksys BEFW11S4 physical signal features

- The wired and wireless networks belong to the same broadcast domain, therefore the same IP subnet.
- The wireless network acts like a hub in a wired environment, where the broadcast and collision domains are the same for all the end stations.
- There are different collision domains between the wired and the wireless segments, and between all the switched ports of the built-in switch (as expected).

3.1.3 Broadcasting the SSID (AC-3-1)

Running the recommended testing action using `netstumbler` and the built-in network interface features of Windows XP it was confirmed that the default SSID broadcast feature was disabled.

The wireless network didn't appear in the Windows XP connection adapter properties nor in the `netstumbler` scanning screen.

The default Linksys configuration is to broadcast the SSID so this parameter had been changed (see figure3.5).

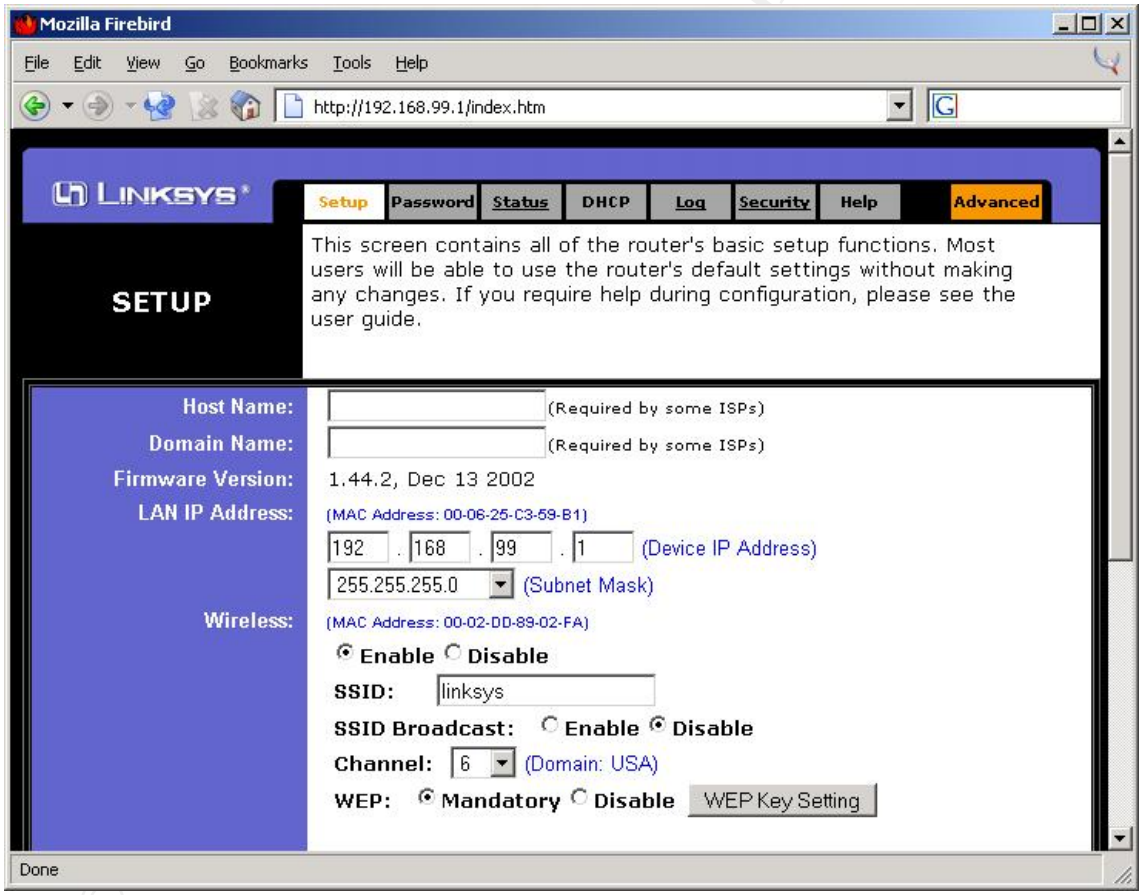

Figure 3.5: Linksys BEFW11S4 SETUP options

The recommended test based on the Windows XP wireless network interface capabilities were also checked. As can be seen in figure 3.6 the wireless network is not detected, instead a rogue access point appeared ("belkin54g") in the left windows, so it is necessary to configure manually the SSID ("linksys") in the right

hand window. This status can be compared when the SSID is broadcasted (see figure 3.7).

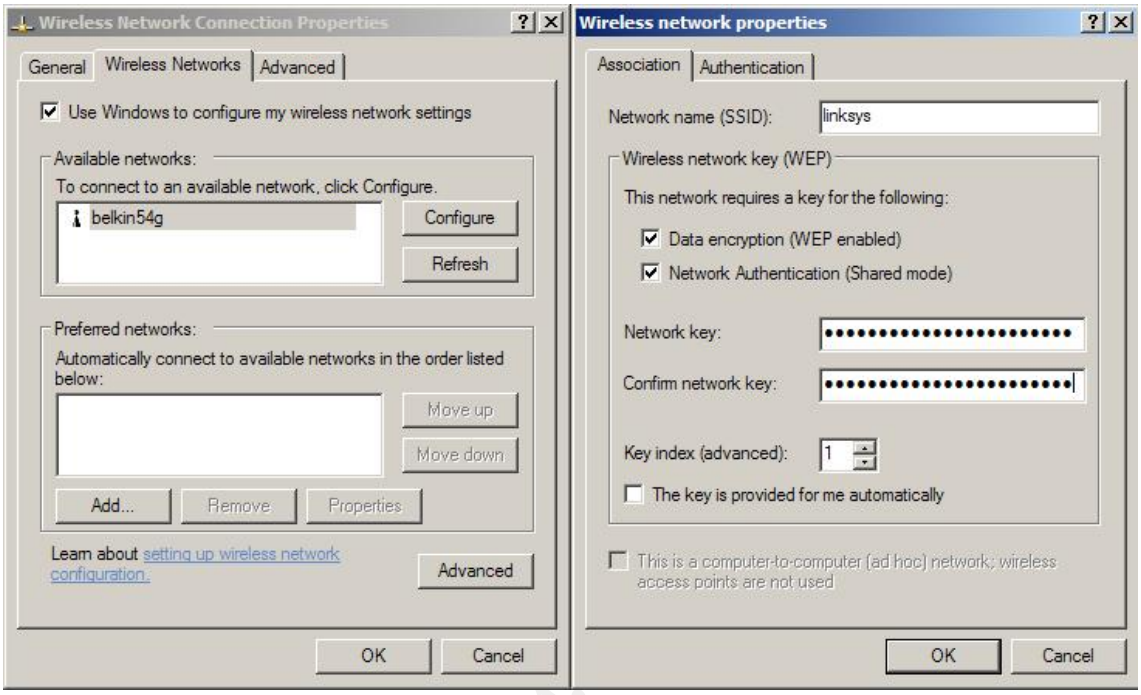

Figure 3.6: Windows XP didn't detect the no broadcasted SSID

When using the default configuration the SSID is broadcasted and it can be detected by `netstumbler` (see figure 3.8), including all its configuration and operational parameters (see figure 3.9).

3.1.4 Default SSID (AC-3-2)

Due to the fact that the device was not broadcasting its SSID, the access point configuration was checked to obtain its value (see figure 3.5): the SSID set was "linksys", thus the default string was not changed.

3.1.5 MAC address based ACLs (AC-4-1)

Additionally, the MAC filter setting were not used due to the limitation this functionality have in the Linksys implementation: instead of denying by default all the

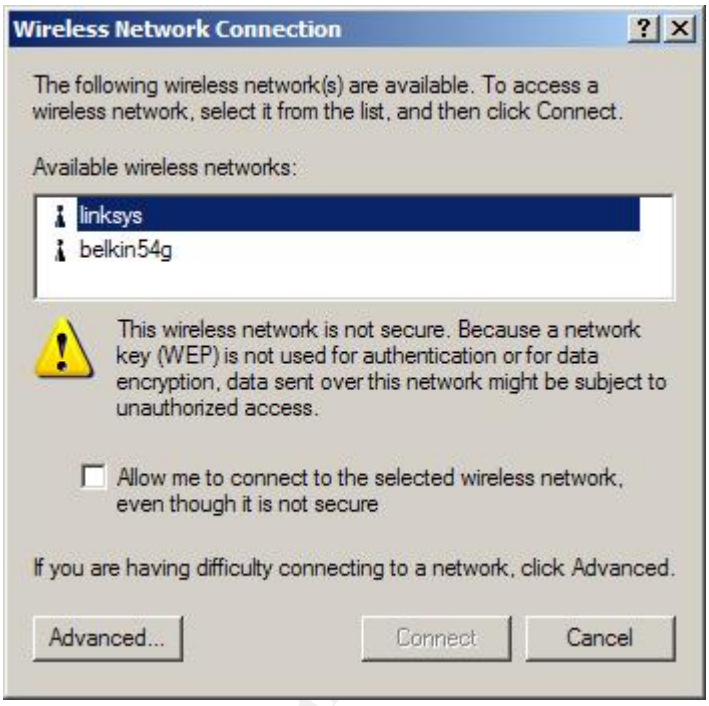

Figure 3.7: Windows XP detecting the broadcasted SSID

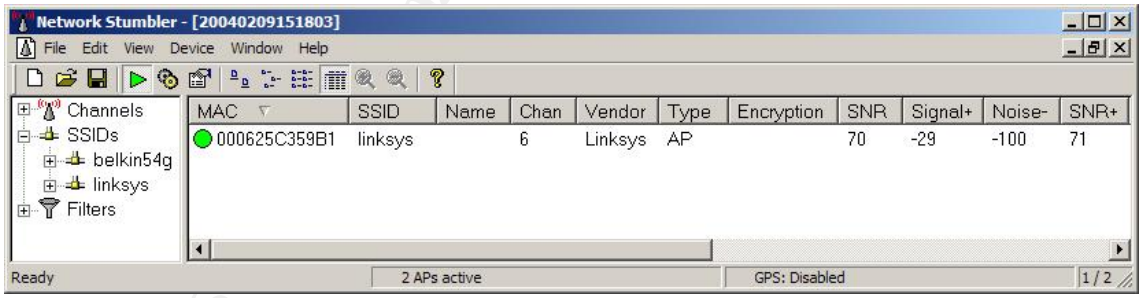

Figure 3.8: Netstumbler SSID broadcast (default)

MAC addresses not specified in this list it allows all addresses except the ones registered here (see figure 3.10).

This is not very useful from the security point of view because it is not possible to know the potential attacker MAC address.

Additionally, this model provides another MAC filtering table associated not to the Internet access (WAN link) but to manage the access to the device itself.

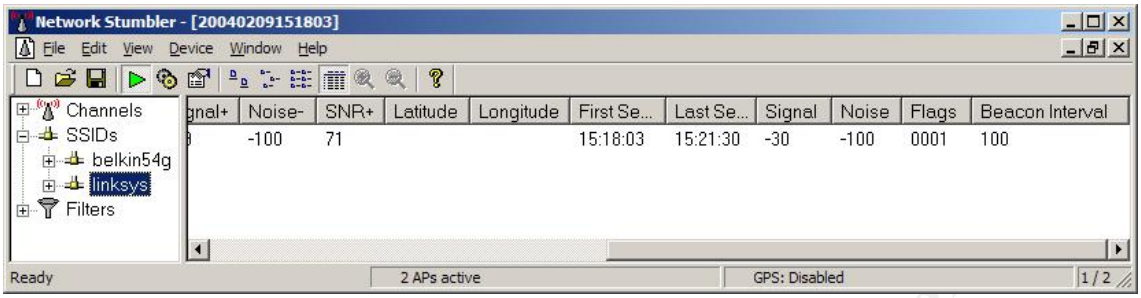

Figure 3.9: Netstumbler SSID broadcast parameters

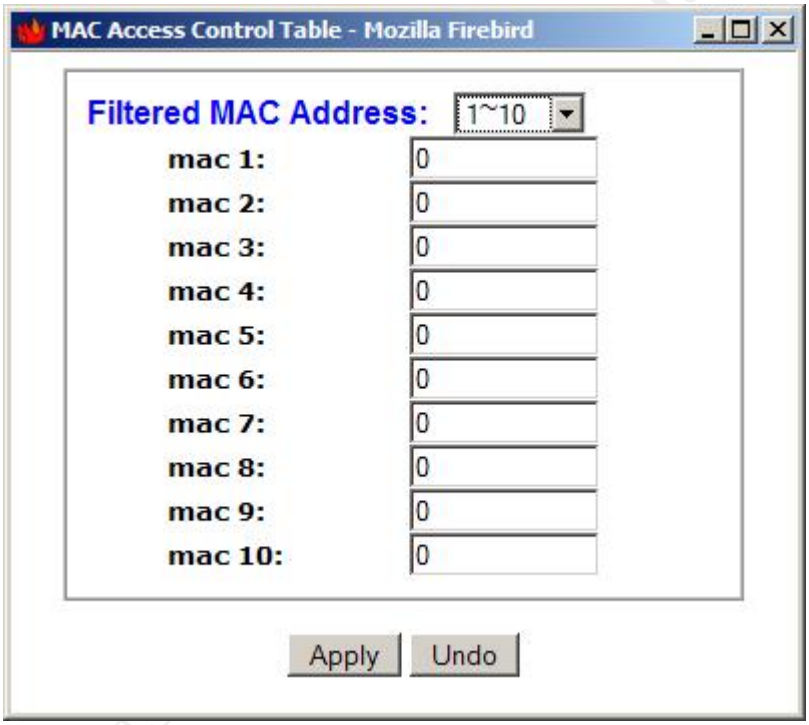

Figure 3.10: Linksys BEFW11S4 Internet MAC filter table

In this case, this table, filtering the access to the device functions, allows to specify that the access will only be permitted for the MAC addresses configured, leaving unchecked the `Filter` checkboxes (see figure 3.11). Again, in this case, no MAC addresses had been configured.

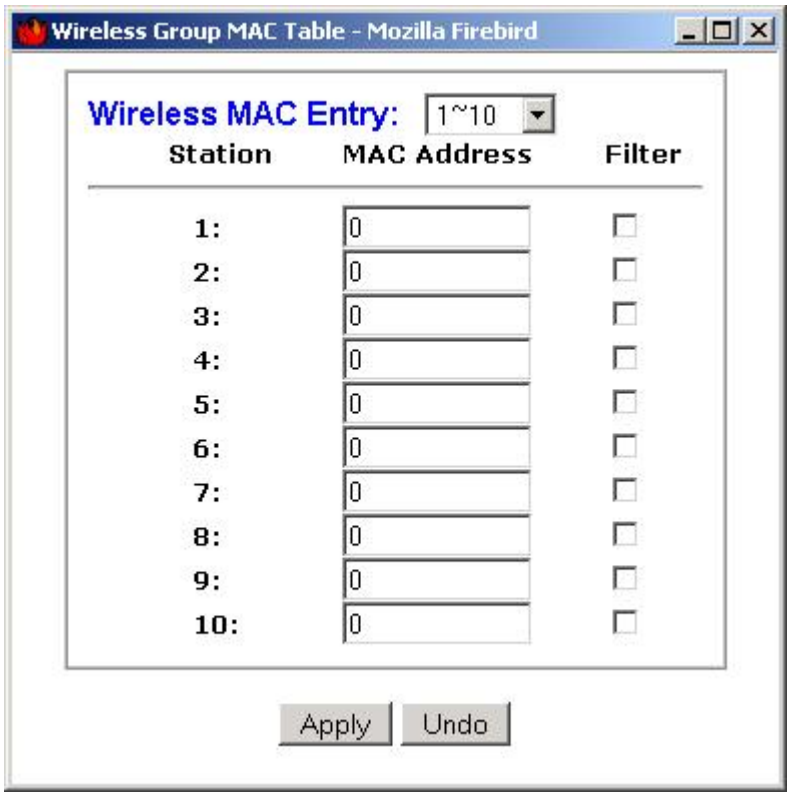

Figure 3.11: Linksys BEFW11S4 direct MAC filter table

3.1.6 IP Filters and other filtering options (AC-4-2)

The Linksys BEFW11S4 allows setting some TCP/IP filters by IP address or port. In this case there were no filters associated to specific ports or IP addresses (see figure 3.12).

When analyzing the Linksys filtering implementation, setting up a denied IP address, a "vulnerability" was discovered: when a filter has been applied the direct traffic is not allowed but other "indirect traffic" can bypass the restriction.

For example, the Linksys device provides a DNS proxy server, so if it has the DNS addresses configured properly for the WAN link and the wireless clients reference the access point as the DNS server, it is possible for the clients to resolve public names and addresses although they had been included in the IP filter. The reason is they are not contacting Internet directly but the access point address (the one acting as a DNS proxy).

This situation applies to all filters, IP, port and MAC.

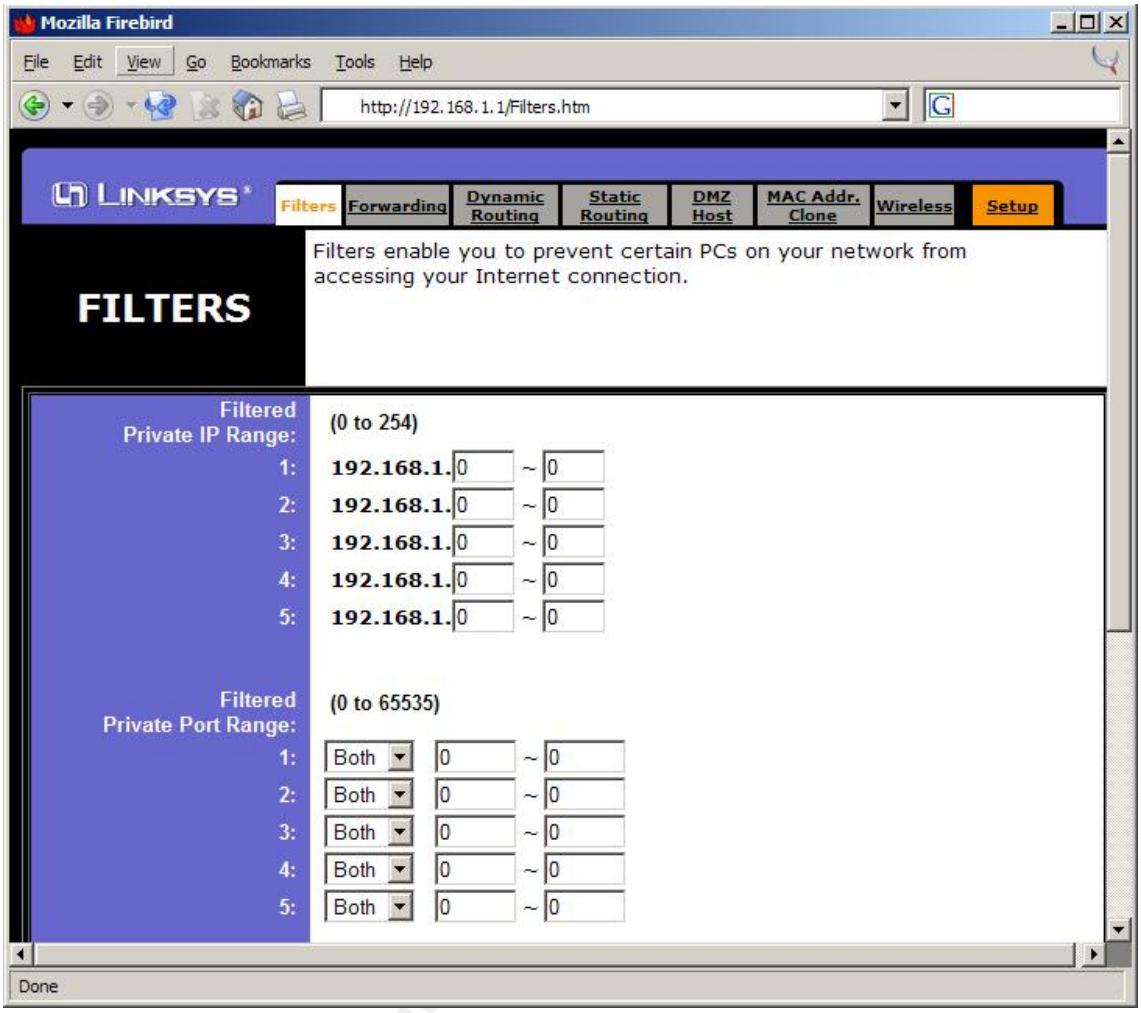

Figure 3.12: Linksys BEFW11S4 Advanced - IP Filters

Besides, the WAN interface of the access point is not protected by the filters, only the traffic going out of this interface is protected. So a filtered wireless attacker could be able to contact the LAN and WAN access point interfaces and also any other system connected to the wireless or wired network. To sum up, this feature only protects the Internet uplink connection.

For the additional filtering options, the default values were used and they are enough secure for almost all users while keeping various useful functionalities running. As can be seen in figure 2.2 the `Block WAN Request` avoids the network from been accessed from Internet (WAN link) using `ping` or other methods. This

situation will be validated when running the TCP and UDP portscans.

All the other enabled features allow desired functionalities, such as multicast traffic and VPN traffic, for both, IPSec and PPTP.

The remote management and upgrade functions, which could open a dangerous door to outsiders, are closed by default. The default MTU when disabled is 1500, as the Ethernet one.

3.1.7 Highest WEP encryption level (AC-5-1)

The WEP configuration tab was accessed to confirm that WEP was enabled. Additionally the key length used was not the maximum supported by the device (128 bits): only 40-bits keys were active (see figure 3.5 and figure 3.13).

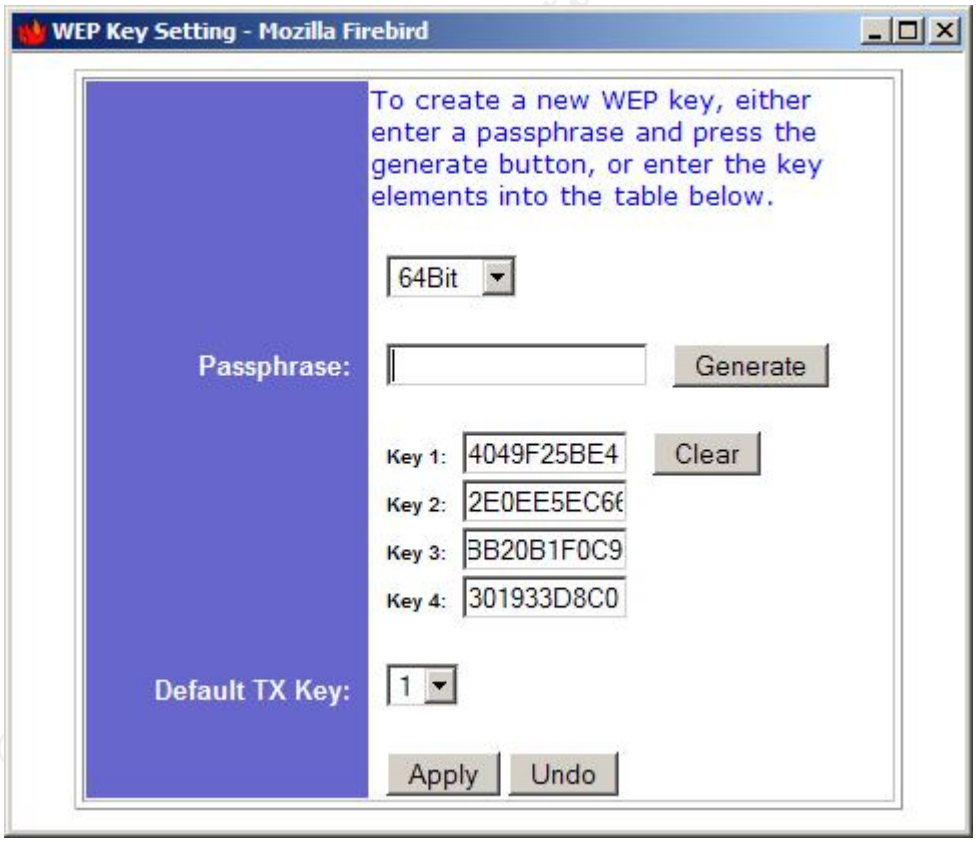

Figure 3.13: Linksys BEFW11S4 WEP keys

3.1.8 Multiple WEP keys (AC-5-2)

In relationship with the previous check, the device had multiples WEP keys configured; the maximum number allowed by the current firmware version is 4 keys (see figure 3.13).

3.1.9 Change the (default) administrator's password regularly (AC-6-1)

When accessing the BEFW11S4 Web management interface the default password was used but it was not possible to authenticate to access the device configuration. The default password had been changed (see figure 3.14).

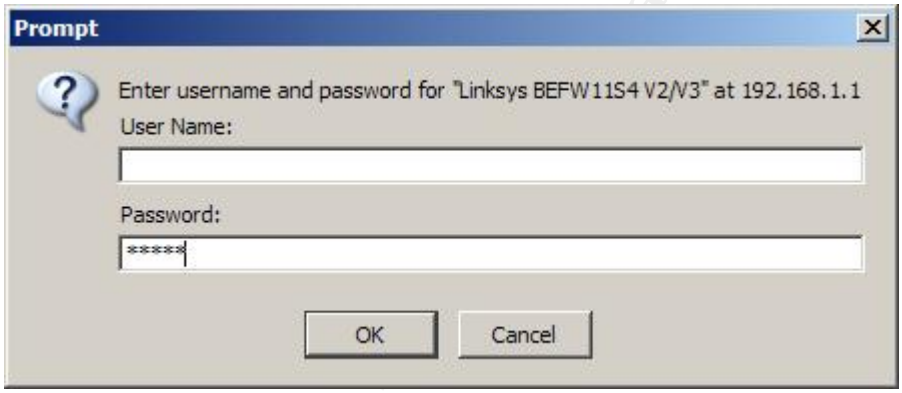

Figure 3.14: Linksys BEFW11S4 WEB management authentication

Asking the network administrator he confirmed that the password is periodically changed, about each 2 months, although the company policy specifies that the password for the network devices (wireless or wired) should at least be changed 2 times per year.

During the password testing an information leakage was discovered:

During the process of changing the password using the URL `http://192.168.1.1/Passwd.htm`, when the new password ("secret_gsna") is applied, it could be obtained in the Web administration page URL (on the top of the Web browser) (see figure 3.15):

`http://192.168.1.1/Gozila.cgi?sysPasswd=secret_gsna\&sysPasswdConfirm=secret_gsna\&UPnP_Work=1\&FactoryDefaults=0`

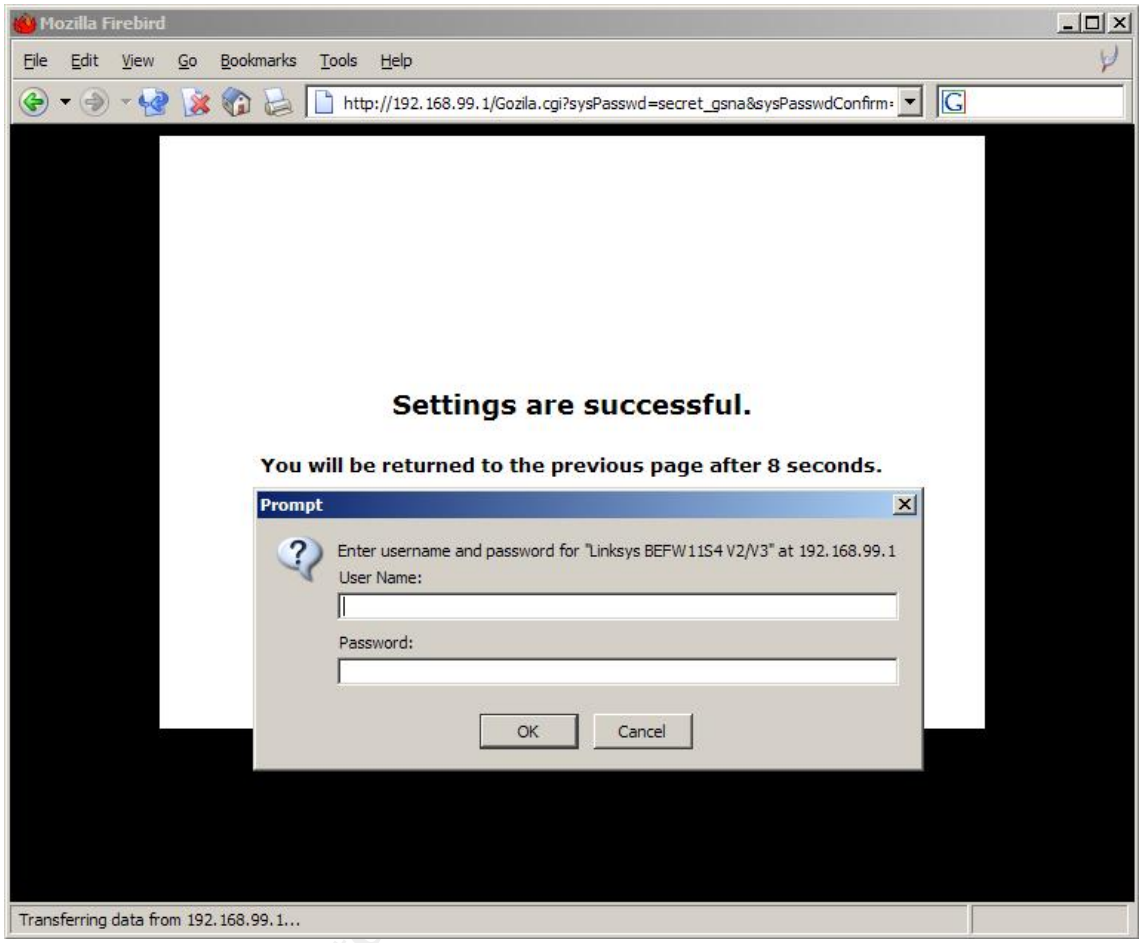

Figure 3.15: Linksys BEFW11S4 URL containing password

Therefore, any device logging the URL accessed is able to obtain it, such as a Web proxy or cache. Additionally, if someone is taking network traces this information travels in the clear (see figure 3.16).

3.1.10 Management interfaces (AC-6-2)

It was confirmed through the device documentation that it can only be administered using the Web management interface. With the idea of evaluating its security, network traces were taken during the authentication process and for an administration session (see figure 3.17).

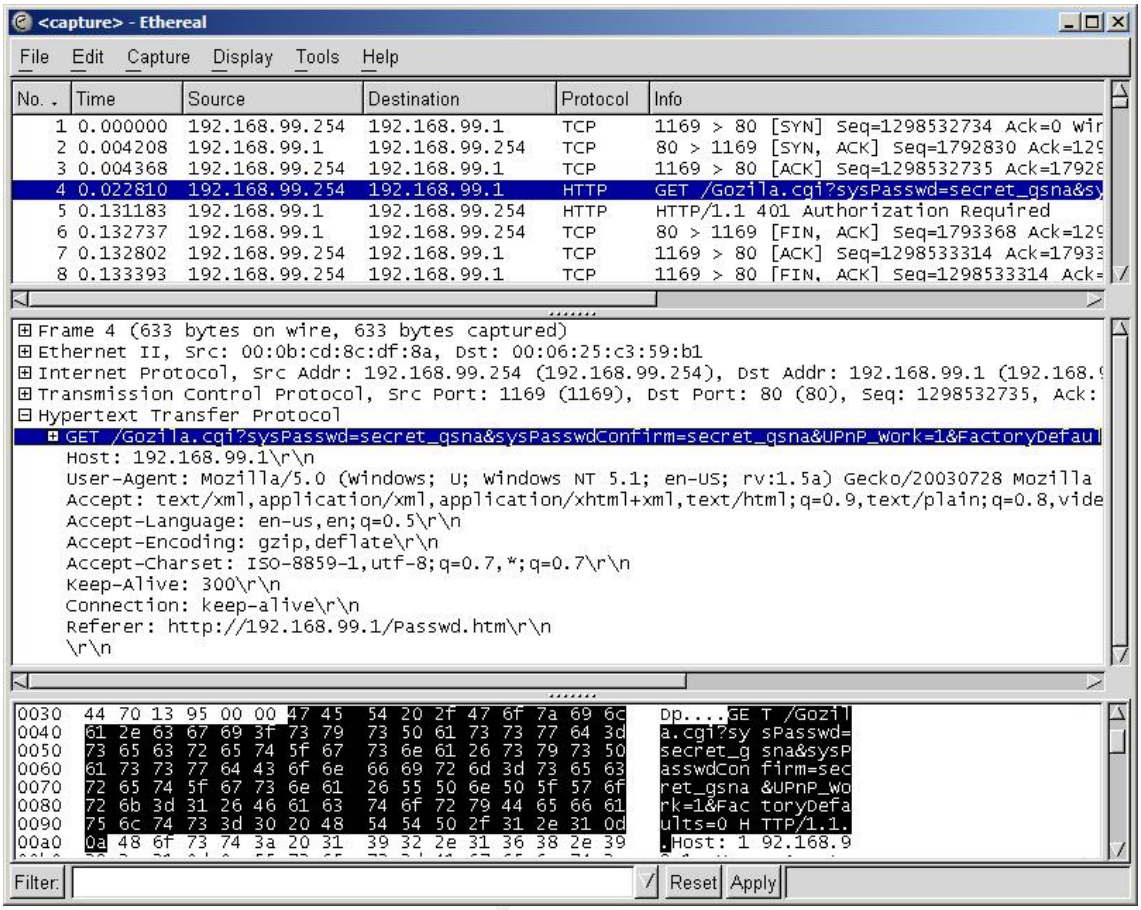

Figure 3.16: Linksys BEFW11S4 changing password

The transport protocol used is HTTP, but on its unencrypted version (not HTTS), therefore all the traffic is available to anyone administering the network. Due to the fact that it is not possible with the model analyzed to avoid the administration through the wireless network, only through the WAN link, this leaves the access point in a highly vulnerable state.

This weakness is ratified with the stimulus test developed in the previous check, AC-6-1, when changing the administrator password.

3.1.11 TCP portscan (AC-7-2)

The TCP portscan over the audited Linksys model provided the following opened TCP ports (see figure 3.18).

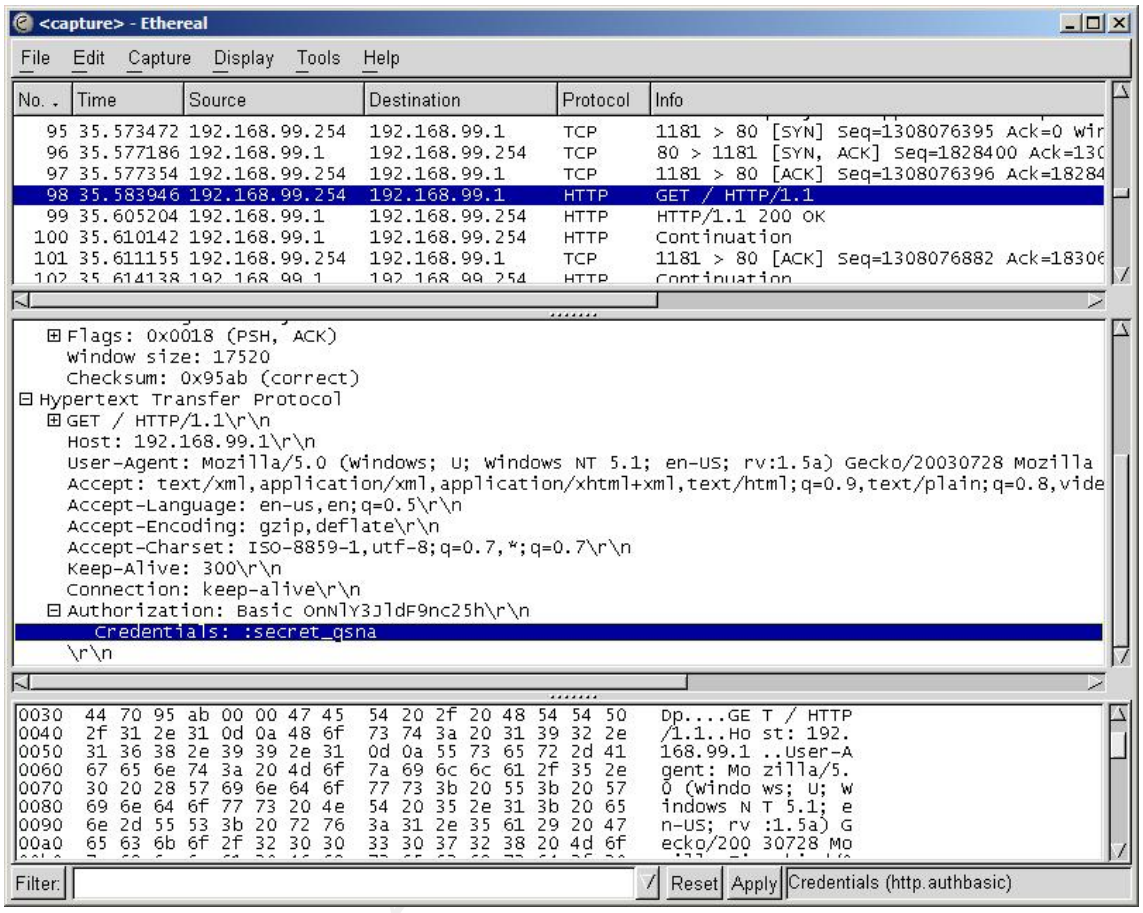

Figure 3.17: Network traces of a Linksys BEFW11S4 WEB admin session

```
# nmap -sT -p 1-65535 192.168.1.1

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-14 21:22 CET
Interesting ports on 192.168.1.1:
(The 65531 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
80/tcp   open  http
2468/tcp open  unknown
5678/tcp open  unknown
6688/tcp open  unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 769.776 seconds
#
```

Figure 3.18: nmap TCP portscan output

The well-known port is associated to the Web management interface (http). Several Google [1] references show that these ports are typically opened in the

[1] http://www.google.com

Linksys devices.

IANA [2] shows that port 2468 corresponds to "qip_msgd", 5678 to "rrac" and 6688 is not reserved.

A deepest analysis showed that accessing all them, for example using `nc` no string was displayed and the ports are closed after a 5 second timeout if no activity is detected. Linksys should be contacted in order to know the purpose of these TCP ports because no info was found in the Linksys support Web page.

Finally, port 5678 is referenced in a Linksys vulnerability where the remote management interface is opened although it had been disabled in the AP settings: http://www.securiteam.com/securitynews/5OP022K7GE.html. However, the AP doesn't have a Web server listening in this port.

3.1.12 UDP portscan (AC-7-3)

The UDP portscan over the audited Linksys model provided the following opened UDP ports (see figure 3.19).

```
# nmap -sU -p 1-65535 192.168.1.1

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-14 21:42 CET
Interesting ports on 192.168.1.1:
(The 65529 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
53/udp   open  domain
67/udp   open  dhcpserver
69/udp   open  tftp
520/udp  open  route
1900/udp open  UPnP
1901/udp open  unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 2593.578 seconds
#
```

Figure 3.19: nmap UDP portscan output

Although several features of the access point has been disabled, the associated ports are showed as opened. From the list above, only the DNS port (53) should be opened because all the other services were not configured. All them were verified:

- DHCP server (67): disabled in the `DHCP` configuration tab.
- TFTP server (69): it is supposed to be associated to the firmware upgrade features, not active at the moment the UDP scan took place. Available in the `Help` configuration tab, under the `Upgrade Firmware` link.

[2] http://www.iana.org/assignments/port-numbers

- RIP (520): the dynamic routing capabilities were disabled in the `Advanced` tab, under the `Dynamic Routing` tab.
- UPnP (1900): the Universal Plug and Play option was disabled in the `Password` tab.
- Finally, the UDP port 1901 seems to be officially associated to the "Fujitsu ICL Terminal emulator program" based on the IANA information. The Linksys implementation uses this port for UPnP as a client port, sending packets from it to the multicast address `239.255.255.250`, port 1900.

Again, it is recommended to contact Linksys for specific information about why these ports are opened when they are configured to be closed.

3.1.13 ICMP typescan (AC-7-4)

These are the responses obtained from the BEFW11S4 model to the 3 different ICMP types tested:

As can be seen in figure 3.20 the device replied only to the ECHO requests, ignoring the TIMESTAMP or NETWORK MASK requests.

3.1.14 Operating System fingerprinting (AC-7-5)

After running the `nmap` operating system fingerprinting functionality it identified the Linksys BEFW11S4 model as the exact WAP model it is (see figure 3.21). To do so it just used the HTTP port as the reference/testing port.

The `nmap` accurate results must be considered because any remote attacker will be able to identify the device and use specific exploits against well-known vulnerabilities associated to the Linksys BEFW11S4 model.

3.1.15 Device Firmware (AC-11-1)

The Linksys BEFW11S4 analyzed is running the firmware revision 1.44.2. The binary file is publicly available at http://www.linksys.com/download/firmware.asp?fwid=17.

Searching into the Linksys download page [3] there are 5 different BEFW11S4 models: version 4, no-version, v3, version 2 and version 3.2; besides, there are 3 additional models: BEFW11S4-AT v2, CA(FR) v4 and v2.

[3] http://www.linksys.com/download/

```
- ICMP ECHO requests:

# hping2 192.168.1.1 -1 -C 8 -c 5
HPING 192.168.1.1 (eth1 192.168.1.1): icmp mode set, 28 headers + 0 data bytes
46 bytes from 192.168.1.1: icmp_seq=0 ttl=254 id=32646 rtt=4.4 ms
46 bytes from 192.168.1.1: icmp_seq=1 ttl=254 id=32647 rtt=4.2 ms
46 bytes from 192.168.1.1: icmp_seq=2 ttl=254 id=32648 rtt=4.6 ms
46 bytes from 192.168.1.1: icmp_seq=3 ttl=254 id=32649 rtt=5.5 ms
46 bytes from 192.168.1.1: icmp_seq=4 ttl=254 id=32650 rtt=5.0 ms

--- 192.168.1.1 hping statistic ---
5 packets tramitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.2/4.8/5.5 ms
#

- ICMP TIMESTAMP requests:

# hping2 192.168.1.1 -1 -C 13 -c 5
HPING 192.168.1.1 (eth1 192.168.1.1): icmp mode set, 28 headers + 0 data bytes

--- 192.168.1.1 hping statistic ---
5 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

- ICMP network MASK requests:

# hping2 192.168.1.1 -1 -C 17 -c 5
HPING 192.168.1.1 (eth1 192.168.1.1): icmp mode set, 28 headers + 0 data bytes

--- 192.168.1.1 hping statistic ---
5 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
#
```

Figure 3.20: nmap ICMP typescan output

```
# nmap -O 192.168.1.1

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-14 22:36 CET
Interesting ports on 192.168.1.1:
(The 1658 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
Device type: WAP|broadband router
Running: Linksys embedded
OS details: Linksys BEFW11S4 WAP or BEFSR41 router

Nmap run completed -- 1 IP address (1 host up) scanned in 71.277 seconds
#
```

Figure 3.21: nmap OS fingerprint output

Looking at the latest versions, given that the model analyzed is version 3, these are the available firmwares and its main security features:

- **BEFW11S4 version 4**: Latest firmware version is 1.50.10 (1/16/2004). Its

main features are [4]:

- "Filter Internal NAT Redirection": to filter internal communication based on the IP address.
- Added WPA support (since version 1.50, previous one).
- Some vulnerabilities have been fixed: URL commands, lock up issue and some pass-through features.

- **BEFW11S4 version 3.2, 3** (the exact model analyzed here) **and 2**: Latest firmware version is 1.45 (2/28/2003). Its main features are [5]:
  - A new backup and restore configuration function has been added.
  - This new firmware includes a new upgrade utility with Zone Alarm support for Windows users.

3.1.16 Linksys long password field vulnerability (AC-12-1)

The long password field was sent using the Mozilla Web browser version 1.5 over Red Hat Linux 9.0.

When authenticating through the Web management interface with a packet length over 5000 bytes the BEFW11S4 device was not affected. Therefore the vulnerability that appeared in the BEFW11S4 version 2 has been resolved in version 3.

3.1.17 Linksys DoS vulnerability (AC-12-4)

The empty string in a HTTP GET request was sent as indicated by the audit item and again, the access point was not affected. Instead it generated a message requiring the user authentication (see figure3.22).

3.2 Measure residual Risk

The audit has helped in identifying some areas with an associated residual risk. Some actions will be recommended to mitigate this risk and evaluate its cost.

[4] http://www.linksys.com/download/vertxt/befw11s4v4_ver.txt
[5] http://www.linksys.com/download/vertxt/befw11s4_ver3.2z.txt

```
# nc 192.168.1.1 80
GET
HTTP/1.1 401 Authorization Required
WWW-Authenticate: Basic realm="Linksys BEFW11S4 V2/V3"
Content-type: text/html
Expires: Thu, 13 Dec 1969 10:29:00 GMT
Connection: close
Pragma: no-cache

<html><head><title>401 Authorization Required</title></head>
<body bgcolor=red text=white><h1>401 Authorization Required</h1>
This server could not verify that you are authorized to access.
Either you supplied the wrong credentials(e.g., bad password), or
your browser doesn't understand how to supply the credentials
required.</body></html>
#
```

Figure 3.22: Checking the AC-12-4

One of the risks that should be analyzed in detail is the limit of the wireless network, defined by the range covered by the wireless signal. A great effort should be spent in trying to reduce the signal strength and limiting it as much as possible inside the company facilities. The cost to reduce it is low (if the signal is able to cover all the required service area) and it just requires some trial and error tests involving the device configuration and the orientation of the antennas. If one device is not enough to cover the service area, the cost will be increased because additional hardware should be acquired.

The possibility of cracking WEP exposes the whole network infrastructure. Is therefore necessary to use a more robust solution, such as WPA. To do so, a new hardware version and firmware revision is needed. The associated costs are not too high due to the low cost of the access point model studied.

One of the top vulnerabilities found is the lack of security of the unique management interface (HTTP), where all the traffic travels in clear. The risk associated to anyone capturing and obtaining the administration password and, therefore, the device control is too high and cannot be fixed; HTTPS cannot be used. Thus, to mitigate it other encryption solutions such as the ones mentioned in the previous paragraph must be used.

Although the device was customized, some factory default settings still reside in the configuration, increasing the exposure of the access point because they are typically the first element checked by a potential attacker. These values can be easily changed for a low cost and will mitigate the associated threats and the risk of the whole network being compromised.

It was identified a lack of security policies related with the wireless environment. The company only have general IT policies, for example, to renew the administration passwords for all systems and network devices, or password policies for end

users, but there is no difference based on the type of device and its particularities. It is recommended to define specific policies for the wireless environment.

Another risk introduced by the device features is the relationship between the built-in wired ports and the wireless network. Due to the fact that all them reside in the same subnet, it is recommended not to use the wired connectors for production servers. There is no cost associated to this measure and the protection is increased when setting the server in the internal network (far from the AP).

Finally, in order to mitigate some of the risks described, it is recommended to isolate the access point under the control of a filtering device. This solution requires to change the network topology and a new design and its implication should be evaluated.

All the mentioned changes don't require high cost expenses and it is worth the benefit obtained based on the business requirements for the existence of the wireless network and based on the loss associated to the network being compromised.

3.3 Is the system auditable?

The auditing processes was successful and helped to identify different improvements in the device configuration and the network environment that will increase the security level of the company network.

During the auditing process some aspects couldn't be audited due to device or environment constraints. It is well worth to mention all them in order to know the BEFW11S4 access point limitations:

Wireless security protocols:

The following list shows the nowadays available wireless security standards in the 802.11 arena:

- **WECA**: WEP (802.11b), WPA (802.11i).
- **IEEE**: EAP (802.1X): MD5, LEAP (Cisco), TLS (MS XP), TTLS (Funk SW), PEAP (Cisco,XP).

There are two main organizations regulating all the 802.11 aspects, the WECA, also called the WiFi Alliance [WIFI1], responsible of the 802.11 security evolutions, and the IEEE [IEEE1], responsible of the 802.1X and EAP authentication protocols.

As was noted in the initial section, it would be interesting to evaluate the latest security mechanism in order to ensure the highest protection level for

the wireless network and the access point. The analyzed model and firmware version running don't implement the latest features, so it was not possible to check them.

As a conclusion, to be able to test the WPA and 802.1X protection methods, at least the BEFW11S4 version 4 model and the 1.50 firmware revision should be used.

Access point purpose:

Some features provided by the access point analyzed were not checked because they are not relevant for the device when acting as an wireless AP for flexible connectivity, but they could be interesting when the access point acts as the Internet company gateway, such as:

- the `Port Range Forwarding`, very useful when placing wireless servers accessed from Internet and some kind of port or/and address translation is required.
- the `Dynamic routing`, because in this case the AP acts as a very simple router, using static information, not dynamic protocols as RIP.
- the `DMZ Host` feature, to bypass all the traffic to a unique system.

WEP configuration:

Although it was mentioned as a prerequisite, several audit items require to know the WEP key if WEP is enabled, thus the administrator provided it in order to run the audit.

As an extra exercise the `airsnort` tool was used trying to crack the 40-bits WEP key used during the audit process.

This test has not been extensively documented because it has been already probed and described in lots of references included in `assignment 1`.

To sum up, it was possible to break the WEP key (lowest encryption level, 40 bits) in 6 hours and 25 minutes based on the wireless network activity during the auditing process. This step could be strictly required for situations were the company is interested in testing it and the WEP key is not provided to run the whole audit.

Another comment about the WEP implementation of the BEFW11S4 is that it is not possible to configure the recommended configuration, that is, multiple WEP keys of 128 bits. It only support multiple WEP keys of 40 bits or one key of 128 bits.

SNMP logging and management:

Generally speaking, it should be possible and recommendable to log the AP activity through the SNMP protocol [GAST1] [POTT1]. SNMP trap messages could be generated by the device alerting about anomalous events. Apart from being used to send alerts, the SNMP protocol can be used to manage the network device. The type and details of the information associated to the wireless 802.11 SNMP agent, called MIB, can be obtained from the IEEE [IEEE1].

Having an SNMP management host to receive the SNMP packets is required, and it is possible to interact with the SNMP agent through the `net-snmp` commands [6], such as `snmpget, snmpset, snmpwalk`...

The Linksys model analyzed doesn't have a configurable SNMP agent, thus this relevant management element cannot be audited.

However, this AP seems to include some SNMP functionality because when the device is booting it generates an SNMP trap from its IP address, using an ephemeral port, to the IP broadcast address (255.255.255.255), destination UDP port 162:

```
Simple Network Management Protocol
  Version: 1 (0)
  Community: public
  PDU type: TRAP-V1 (4)
  Enterprise: 1.3.6.1.4.1.3955.2.2.1 (iso.3.6.1.4.1.3955.2.2.1)
  Agent address: 192.168.1.1 (192.168.1.1)
  Trap type: ENTERPRISE SPECIFIC (6)
  Specific trap type: 1
  Timestamp: 141
  Object identifier 1: 1.3.6.1.4.1.3955.1.1.0 (iso.3.6.1.4.1.3955.1.1.0)
  Value: STRING: "Wireless: Status=1, MAC=0002dd8902fa, ESSID=linksys,
  Domain=10, Channel=6, WEP=1."
```

As can be seen, lot of configuration and relevant information is included in this UDP packet: `MAC address, ESSID, Domain/Channel, WEP status`.

[6] http://net-snmp.sourceforge.net

ASSIGNMENT 4 - AUDIT REPORT

4.1 Executive summary

This report summarizes the results obtained from the security audit of the Linksys BEFW11S4 access point router used to provide wireless connectivity to telecommuters, mainly sales and engineering staff, inside the analyzed company.

Most audit controls and objectives were achieved through the auditing and testing process described in the previous sections, and the scope of the audit was completely covered, analyzing all the technical security aspects of the mentioned device given its purpose. The running configuration and environment is safe against some generic wireless risks but some weaknesses still prevail.

Given that the access point analyzed provides access to the internal resources and to Internet, it is a critical network piece and, if compromised, it could provoke attacks over the whole network infrastructure.

The nowadays security status of the device could be considered as **medium** but some important risk are associated to it. Through a set of predefined and specific recommendation steps it is possible to remarkably provide a highly secure environment.

In order to increase the security of the wireless network infrastructure two actuation phases have been identified: first one is a low-cost, fast deployment phase, that tries to increase the security in the short term, while second one is focused on more advanced solutions and its associated cost is greater; it could be applied in the medium-long term.

1. **Phase 1**: apply changes in the configuration settings and upgrade the firmware access point version.
2. **Phase 2**: define new security policies, acquire new equipment and change the network topology and protocols used (VPNs).

From an economic point of view, the recommended investment is well worth compared with the potential monetary loss if an incident takes place.

4.2 Audit findings

In order to sum up the most relevant security audit findings obtained during the audit process, two groups of check items have been created:

- First one focuses on those checks for which a default value is available; then, the default value, the audited value and the recommended value will be showed (see table 4.1). In general, default values should be avoided because they are well known and used during network attacks.
- Second set includes all the more general relevant check items without a clearly defined default value (see table 4.2).

The details about the results obtained can be get from the previous `assignment 3` section.

AC	Description	default	audited	recommended
AC-1-1	Interoperability range	very broad	very broad	reduce the signal power
AC-3-1	Broadcasting SSID	yes	no	no
AC-3-2	Default SSID	linksys	linksys	different
AC-4-1	MAC address ACLs	no	no	yes
AC-4-2	IP filters and other options	no	no	yes
AC-5-1	WEP encryption level	no WEP	40-bits WEP	128-bits WEP
AC-5-2	Multiple WEP keys	no WEP	yes (40-bits)	yes (128-bits) (*)
AC-6-1	Default admin password	admin	another	another
AC-6-3	Configuration backup/restore	no	no	yes, upgrade firmware
AC-7-1	DHCP server	yes	yes	no
AC-7-5	OS fingerprinting	identify	identify	obfuscate
AC-8-1	Logging	no	no	yes
AC-9-2,3	WPA and 802.1X	no	no	yes, upgrade firmware

(*): The model analyzed doesn't support multiple WEP 128-bits keys.

Table 4.1: Audit findings for the BEFW11S4 wireless AP (default values)

The audit process found that the access point was customized, avoiding some vulnerabilities associated to certain default values, like the default admin password or the fact of broadcasting the network existence. Besides, additional security features have been configured, such as WEP using 40-bits keys. Additionally, checking the device configuration non vulnerable changes were detected, indicating that an special care had been taken when changing and manipulating the multiple device options.

However, the audit performed reflected the following main security exposures:

AC	Description	audited	recommended
AC-1-3	Rogue access points	1 found	research its location
AC-1-4	Physical security	good	tight controls
AC-2-1	Network topology	weak	AP “protected” by a firewall
AC-2-2	Wired and wireless built-in nets	same subnet	(*)
AC-3-3	Change the SSID frequently	no policy	yes, policy based
AC-5-4	Change the WEP keys frequently	no policy	yes, policy based
AC-6-2	Management interfaces (Web)	insecure	use WPA
AC-7-2,3	TCP and UDP portscans	several ports	check with Linksys
AC-9-1	VPN usage	no	yes
AC-10-1	Wireless security policies	no	yes

(*): Non changeable; it is based on the device implementation.

Table 4.2: Audit findings for the BEFW11S4 wireless AP (non default values)

- **Default values**: there are several access point features that keep the factory default values, such as the SSID value or the DHCP server.
- **Not supported features**: based on the firmware revision and hardware version running, some highly recommended security features are not available, like the configuration backup/restore functionality or the WPA support.
- **Misconfiguration**: some of the security features available have not been configured, such as the MAC address ACLs or the IP filters.
- **Security policies**: there is a relevant lack of wireless security policies, specifying the methods and procedures associated to the access point support and maintenance.
- **Network**: the network topology and the location of the access point should be reviewed. It is also recommended to evaluate the usage of VPN solutions.

4.3 Background/risk

Analyzing the non-compliant audit checks from the previous section, several risks were identified. Most them could be mitigated applying small and low-cost changes (see the `Cost` section bellow) that will improve the overall security state.

The following list describes the identified risks and its impact on the company IT infrastructure:

- The wireless network signal is very powerful, so it is available from outside the company facilities. An attacker could verify the existence of the network during a reconnaissance process and even connect to it (based on other configuration aspects); this is the first step to develop more advanced attacks.

- The default SSID value is used, so it is well known for an attacker. Although it is not being broadcasted, an attacker could try to use it and find the company wireless network.

  Having WEP enabled reduces this risk because the WEP key must be known to connect to the network.

- The DHCP server is enabled, therefore an attacker could be able to obtain all the required network information to connect to the company communication infrastructure: IP address and mask, DNS server, default gateway...

- Not limiting the end station access through filters could lead to a situation in which anyone, using any address, will be able to generate traffic to and through the wireless segment. The filtering definitions help in limiting the actions a potential attacker can perform, at the layer 2 (MAC addresses) and layer 3 (IP addresses).

- Due to the fact that WEP is available, if the highest level is not used or the same keys are used during long periods, an attacker could easily obtain the WEP key, being able to intercept and acquire all the wireless traffic and even manipulate it. A weak encryption solution could compromise the whole network, facilitating other attacks and increasing its associated risks.

  This is probably one of the weakest elements in the infrastructure, because if its security is broken, the network is opened for other mentioned vulnerabilities to be exploited, such as the lack of encryption associated to the Web management interface. The attacker could obtain the administrator password and obtain full control of the access point, thus of the wireless network.

- If an attacker is able to compromise the network, due to the lack of logging capabilities, the risk of not having enough information about the incident and the events taking place exists. The attacker activities couldn't be traced.

- The access point is directly connected to the company internal network. If the wireless segment is compromised, the risk of an easy and direct access to the wired corporate network exists. A potential attacker would be able to access the production systems without a filtering device trying to block him.

- The risk associated to the lack of security policies is that employees don't know how to behave and the actions they should perform when managing

and working in a wireless environment. This could lead to the appearance of rogue access points, misconfigured and acting as backdoors into the corporate network.

All these specific threats, vulnerabilities and risks could lead to more generic risks, such as an attacker getting all the network traffic in the clear, thus reading company confidential information, such as passwords, credit card numbers and other relevant pieces of data.

Once the attacker has accessed the wireless network, he could consume excessive network resources associated to the uplink connection, Internet, reducing the bandwith for the company legitimate usage. And it shouldn't be forgot the company legal responsibilities if an intruder launch attacks against third party organizations from the company network and/or systems.

The network traffic could also be modified, therefore obtaining access to the internal servers through more advanced attacks. The risk is similar to having the attacker sit into one of the company meeting rooms, plugged into the network without being watched.

4.4 Audit recommendations

Analyzing the list of risk previously presented a set of recommendations is proposed with the goal of mitigating and even reducing to a minimum the company network exposure.

The physical values of the access point wireless configuration should be modified in order to reduce the 802.11 signal and limit its existence to the service area inside the building.

A lack of company security policies related with the wireless environment was identified. Therefore, policies should be defined containing all the relevant procedures that ensure a safe wireless network, like frequency for changing configuration values, periodic basic audits to find rogue access points, physical security aspects...

The default SSID network name should be changed and periodically modified based on the previously recommended company defined policies.

The device firmware version should be upgraded in order to obtain the configuration backup/restore function (AC-6-3) and to avoid well known vulnerabilities (AC-12-2). But it is even more important, not only to upgrade the firmware, but to upgrade to a newer hardware version, version 4, in order to have WPA support (AC-9-3), a very relevant wireless security standard.

Disabling the DHCP server (it was found enabled during the audit) requires users to have an IP address previously assigned, so it is more difficult for an attacker to access the network. Besides, if the default network IP subnet is changed (nowadays in use), then although the attacker knows that a Linksys access point is being used he couldn't access the default 192.168.1.0/24 value.

With the goal of increasing the controls over the trusted wireless users and in accordance with the previous recommendation, once fixed IP addresses are used and assigned per user, it is recommended to apply filters for an specific IP address range and for specific MAC addresses.

Although WEP has been probed to be a weak encryption solution, it must be used in its highest encryption level, 128 bits. Its keys should be periodically changed per security policy definition.

The WPA solution mentioned above would increase the WEP robustness, complementing both, the authentication and the encryption mechanisms. To authenticate the trusted users it uses advanced methods based on credentials that must be validated by an external authentication server, such as a username and password, two factor authentication or a digital certificate.

If an incident occurs, it is desired to have enough information recorded to be able to figure out what was going on during the attack period. The most used method to extract these events is the logging capabilities of the devices. The analyzed access point can be configured to log anomalous events to a remote system.

As a more advanced recommendation, the usage of VPN solutions to transport all the traffic traveling over the wireless segment should be considered. All the nowadays available solutions, HTTPS (SSL), IPSec, SSH, use strong encryption algorithms.

In relationship with the protocol used over the network, the wireless segment should be considered a non-secure area, therefore the network topology should be changed to include the access point in an individual DMZ of the company external firewall (see figure 1.2). This will allow to apply external filters to and from all the traffic associated to the wireless subnet.

Finally, based on the portscan audits developed, it would be recommended to contact Linksys about why some UDP and TCP ports were found opened.

4.5 Costs

In order to evaluate the working costs it has been considered that the average price per day of a senior engineer capable of deploying all the required changes is $480 ($60 per hour).

There are several configuration issues, that involve changing the default values or adding new security settings in the access point, with an associated low cost:

- Changing default configuration settings: wireless range, default SSID, disabling DHCP (and assigning addresses to end stations), increase the WEP level to 128 bits (1 day): $480.
- Upgrading the firmware version and enabling the backup/restore feature and the logging capabilities, and deploy the migration of users to 128-bits WEP (1 day): $480.
- Design and apply new MAC and IP filters, and conclude the migration to WEP 128-bits (1 day): $480.

There are some medium cost activities that added to the previous changes will increase the network security:

- Defining the initial wireless security policies based on the information provided in this report (2 days): $960.
- Acquire a new access point hardware version, ver. 4: $100 per system (initially only one device is required).
- Deploy the new hardware, applying the latest firmware version and the defined advanced security settings, such as WPA (2 days): $960.

The long term activities are the ones with a highest cost and a longer dedication:

- Reviewing the wireless security policies (2 days): $960.
- Design and deploy of the new network topology, involving the corporate firewall, and assigning a new network subnet (3 days): $1440.
- It could be required to add an additional network card to the firewall system for the new wireless DMZ segment: $100.
- Analyze and design the usage of VPN solutions (deployment not included) as a complement or replacement of the nowadays protocols (2 days): $960.

Phase	Cost ($)	working days
Short term	1440	3
Medium term	2020	4
Long term	3460	7
TOTAL	6920	14

Table 4.3: Recommendation costs based on the deployment phases

To sum up, the proposed investment seems to be justified by the previously mentioned risks and the costs associated to them.

4.6 Compensating controls

Due to the fact that some of the recommended actions require to get a new hardware piece or involve the company policies not defined yet, it is possible to mitigate some of the risk identified using a monitoring solution, instead of a corrective control.

Like in the wired world, it is possible to use two types of detection countermeasures to identify potential attackers and evil activity.

The most simpler one is based on configuring a NIDS, Network Intrusion Detection System, to analyze and process the wireless traffic, like `Snort` [1].

The most complex and innovative solution is based on creating a wireless honeypot [2] [3], which main goal will be to identify the fraudulent attempts or usage of the wireless environment. For general information about the honeypots purposes and features see http://www.honeynet.org.

It is very common that all the evil activities suffered over the wireless honeypot, whose only purpose is to wait for attacks or reconnaissance actions, are also performed over the wireless production environment.

[1] http://www.snort.org
[2] http://www.incident-response.org/WISE.htm
[3] http://www.securityfocus.com/infocus/1761

Bibliography

[ARBA1] *"An Initial Security Analysis of the IEEE 802.1X Protocol". William Arbaugh. University of Maryland.* http://www.cs.umd.edu/~waa/1x.pdf (3 November 2003)

[ARPS1] *"Real World ARP Spoofing". Raúl Siles Peláez. August 2003.* http://www.giac.org/practical/GCIH/Raul_Siles_GCIH.pdf (1 Nov. 2003)

[BORI1] *"Intercepting Mobile Communications: The Insecurity of 802.11". Nikita Borisov, Ian Goldberg, and David Wagner.* http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf (1 September 2003)

[CENT1] *"Intel Centrino Mobile Technology". Intel.* http://www.intel.com/products/mobiletechnology/ (1 December 2003)

[CORA1] *"Topics in Auditing - High Level Review of WLAN (Version 2)". Philip J. Coran. GSNA Practical v2.0.* http://www.giac.org/practical/Philip_Coran_GSNA.doc (17 January 2004)

[DILL1] *"Initial Wireless Networking Audit for Higher Educational Institutions. John Dillons."* http://www.auditnet.org/docs/wireless.doc (1 February 2004)

[1] *"Wireless LAN Security FAQ". Christopher W. Klaus (ISS).* http://www.iss.net/wireless/WLAN_FAQ.php

[FLUH1] *"Weaknesses in the Key Scheduling Algorithm of RC4". Scott Fluhrer, Itsik Mantin and Adi Shamir.* http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps, http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf (4 November 2003)

[GAST1] *"802.11 Wireless Networks. The Definitive Guide". Matthew S. Gast. O'Reilly. ISBN: 0-596-00183-5.* (April 2002)

[GOLD1] *"The Insecurity of 802.11. An analysis of the WEP protocol". Black Hat Briefings. Ian Goldberg, 2001.* http://www.cypherpunks.ca/bh2001/ (17 December 2003)

[GRIP1] *"Auditing the Cisco Aironet 340 Wireless Access Point". Mark Griparis. GSNA Practical v2.0.* http://www.giac.org/practical/GSNA/Mark_Gryparis_GSNA.pdf (17 January 2004)

[IEEE1] *"IEEE 802.11 WLAN Group". IEEE.* http://grouper.ieee.org/groups/802/11/, http://standards.ieee.org/getieee802/802.11.html (5 January 2004)

[LINK1] *"Wireless Access Point Router with 4-port Switch: User Guide". BEFW11s4 ver. 3. Linksys. Included in the CD delivered with the product.*

[LOEB1] *"Roaming charges: Out with the WEP, in with the WPA". Larry Loeb. IBM developerWorks.* http://www-106.ibm.com/developerworks/wireless/library/wi-roam11/ (3 October 2003)

[LOON1] *"Auditing the Wireless environment: A mobile wireless LAN used for training in multiple sites on a corporate WAN". Angela Loonis. GSNA Practical v2.0.* http://www.giac.org/practical/Angela_Loomis_GSNA.doc (17 January 2004)

[LOWD1] *"Auditing the Cisco Aironet 1200 Wireless AP In a Small to Medium Business Environment (SMB)". Ryan Lowdermilk. GSNA Practical v2.1.* http://www.giac.org/practical/GSNA/Ryan_Lowdermilk_GSNA.pdf (17 January 2004)

[MARC1] *"Auditing a Wireless Access Point: The Orinoco Outdor Router 1000 Configured as a Wireless Access Point". Slawomir Marcinkowski. GSNA Practical v1.2.* http://www.giac.org/practical/Slawomir_Marcinkowski_GSNA.doc (17 January 2004)

[NETC1] *"Netcat (nc)".* http://www.atstake.com/research/tools/network_utilities/, http://netcat.sourceforge.net (3 September 2003)

[NEWS1] *"Craking WEP keys". Tim Newsham. @stake.* http://www.lava.net/~newsham/wlan/WEP_password_cracker.ppt (17 December 2003)

[POTT1] *"802.11 Security". Bruce Potter & Bob Fleck. O'Reilly. ISBN: 0-596-00290-4.* (December 2002)

[STAL1] *"Auditing a Cisco Aironet Wireless Network". Ryan Stall. GSNA Practical v2.1.* http://www.giac.org/practical/GSNA/Ryan_Stall_GSNA.pdf (17 January 2004)

[VIIT1] *"An Audit of a Wireless Demonstration network Implementing Cisco Aironet 1200". Oliver Viitamaki. GSNA Practical v2.1.* http://www.giac.org/practical/GSNA/Oliver_Viitamaki_GSNA.pdf (17 January 2004)

[WALK1] *"Unsafe at any key size; An analysis of the WEP encapsulation". Jesse R. Walker.* http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip (23 October 2003)

[WIFI1] *"Wi-Fi (Wireless Fidelity, 802.11) Alliance".* http://www.wi-fi.com (10 December 2003)

[WIFI2] *"Securing Wi-Fi Wireless Networks with Today Technologies". Wi-Fi Alliance. February 6, 2003.* http://www.80211info.com/publications/page289-655794.asp

[WPA1] *"WPA- Wifi Protected Access".* http://www.wi-fi.com/OpenSection/protected_access.asp (20 December 2003)