eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Ingeniaritza Goi Eskola Teknikoa
Escuela Técnica Superior de Ingeniería
Bilbao

Trabajo Fin de Grado

Grado en Ingeniería en Tecnología de Telecomunicación

Antikörper

Diseño e Implementación de un Sistema de Detección de Intrusos Inalámbrico basado en Network IDS

Autor

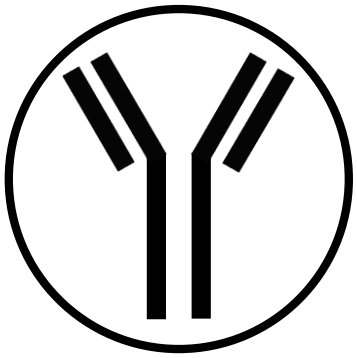
Josu Barrientos Bahamonde

Director

Luis Zabala Alberdi

Curso Académico

2014/2015



Antikörper

Diseño e Implementación de un Sistema de Detección de Intrusos Inalámbrico basado en Network IDS

Autor

Josu Barrientos Bahamonde

Director

Luis Zabala Alberdi

Licencia

Antikörper: Diseño e Implementación de un Sistema de Detección de Intrusos Inalámbrico basado en Network IDS

Abstract

This Project, fruits of my Final Year Project, aims to describe the most relevant aspects of the **W**ireless **I**ntrusion **D**etection **S**ystems (WIDS), such as its history, performance, architectures, deployment and future. After this, the main aim of the project will be exposed. The proposal of a generic WIDS architecture and the development of Antikörper, a Network IDS based fully functional WIDS, which covers all the needs of the actual Wireless LAN networks and which is adaptable for future revisions.

Este proyecto, fruto de mi Trabajo Fin de Grado, pretende describir los aspectos más relevantes de los **W**ireless **I**ntrusion **D**etection **S**ystem (**WIDS**), tales como su historia, funcionamiento, arquitecturas, implementación o futuro. Tras esto, se expondrá el objetivo principal del proyecto. Proponer una arquitectura genérica para los WIDS y crear Antikörper, un WIDS basado en Network IDS completamente funcional, que cubra totalmente las necesidades de seguridad actuales en las redes Wireless LAN y sea adaptable a futuras revisiones.

Proiektu honek, nire Gradu Amaierako Lanaren fruituak bezala, **W**ireless **I**ntrusion **D**etection **S**ystems (WIDS)en alderdirik garrantzitsuenak aurkeztuko ditu, esaterako beraien historia, funtzionamendua, arkitektura, inplementazioa edo etorkizuna. Horren ondoren, proiektuaren funtsezko helburua aurkeztuko da. WIDSen arkitektura generiko baten proposamena eta Antikörperen garapena, Network IDSetan oinarrituko WIDSa, guztiz funtzionala, Wireless LAN sareetako segurtasun beharrak guztiz asetzen duena esta etorkizunerako berrikuzketentzat moldagarria izan dezakeena.

Agradecimientos

En primer lugar agradecer a Luis Zabala y Alberto Pineda, por el tiempo empleado, el apoyo transmitido y los conocimientos compartidos, sin los cuales habría sido imposible la realización de este proyecto.

A mis padres, Jesus y Tere, por su apoyo incondicional tanto en los buenos como en los malos momentos.

A mis amigos y compañeros, por sus ánimos, nos hayamos visto más o menos en este tiempo, y en especial a Egoitz Hernandez, por su ayuda en lo referente a los temas jurídicos relacionados con este trabajo y a Josu Amorebieta, por haber sido mi compañero de batalla en todas esas prácticas que parecían interminables.

Por último, agradecer a todos mis profesores por su dedicación y esfuerzo, quienes me han preparado, tanto a nivel profesional como personal, para acabar con éxito mis estudios.

Gracias a todos.

Notación y formato

Durante el desarrollo de este documento, se utilizarán anotaciones que ni ortográfica ni gramaticalmente son correctas. Esto se dará únicamente en lo relacionado a nombres de variables, funciones… y demás expresiones técnicas, pertenecientes al diseño e implementación del sistema a lo largo del documento.

Índice general

Índice de figuras

Índice de tablas

The only truly secure system is one that is powered off,
cast in a block of concrete and sealed in a lead-lined room with armed guards
- and even then I have my doubts.

Eugene "Gene" Howard Spafford

Capítulo 1

Introducción

1.1 Presentación

La seguridad informática se está convirtiendo en un tema de interés mundial, y la preocupación respecto al nivel de seguridad que tienen nuestros datos y comunicaciones se está cuestionando cada día con más preocupación. El sector de las auditorías de seguridad y el uso de herramientas de detección y prevención de intrusiones son cada vez más demandadas. Esto se debe a que no solo identifican y corrigen problemas de seguridad, sino que también ofrecen un nivel de estabilidad en las redes, el cual es de suma importancia para dar un nivel de confianza y una sensación de seguridad importante a los usuarios de la red.

La mayor parte de los expertos en seguridad coinciden en que es imposible diseñar un sistema completamente seguro, y partiendo de que el riesgo no puede eliminarse completamente, se debe reducir este lo máximo posible. Para que un sistema se pueda definir como seguro se definen cuatro características básicas.

- **Integridad** La información solo puede ser modificada por quien está autorizado.
- **Confidencialidad** La información solo debe ser entendible o descifrada por personas autorizadas.
- **Disponibilidad** El sistema debe estar disponible siempre que se lo necesite.
- **No Repudio (No-Rechazo o Irrefutabilidad)** Propiedad que evita que se pueda negar la autoría de cualquier acción realizada en el sistema.

Actualmente, gran cantidad de los ataques se deben a que un usuario no autorizado tiene acceso a la red a la que estamos conectados, a través de la cual transmitimos y recibimos datos que pueden estar llegando al intruso o atacante. En este contexto, se hace necesario el uso e implementación de distintas herramientas de seguridad, capaces de monitorizar e interpretar el flujo de datos en el interior de las redes para así poder detectar posibles intrusiones en su interior.

La monitorización de tráfico y la detección de intrusiones en redes será, por lo tanto, el aspecto fundamental en este proyecto. Toda esta problemática converge en la necesidad de implementar un Sistema de Detección de Intrusiones/**I**ntrusion **D**etection **S**ystem (**IDS**), más en concreto, un Sistema de Detección de Intrusiones Inalámbrico/**W**ireless **I**ntrusion **D**etection **S**ystem (**WIDS**), relacionado con la temática del proyecto. Dicho

IDS/WIDS será capaz de supervisar de forma exhaustiva todos los condicionantes de seguridad de una red LAN/WLAN y de proporcionar cierta garantía de seguridad a los usuarios de la red.

1.1.1 Intrusion Detection System (IDS)

Un Sistema Detector de Intrusos es un conjunto de herramientas software y hardware usadas para detectar accesos no autorizados a redes o sistemas de ordenadores. Estos sistemas monitorizan el tráfico buscando y detectando amenazas y avisando de estas a los encargados de mantenimiento de dichas redes, todo esto basándose en unas determinadas políticas de seguridad (1).

1.1.2 Contextualización del proyecto

Este proyecto se ha realizado bajo la dirección de personal investigador del grupo de investigación **N**etwork **Q**uality **a**nd **S**ecurity (**NQaS**) perteneciente a la **E**scuela **T**écnica **S**uperior de **I**ngeniería de **B**ilbao (**ETSIB**).

1.2 Definición del problema

El despliegue e implementación de sistemas IDS está actualmente bastante extendido y estudiado, esto se debe a que un IDS nos permite añadir un gran nivel de seguridad a las redes.

El problema surge cuando nos centramos en la seguridad de una red inalámbrica. Los sistemas de seguridad de estas redes están actualmente poco estudiados y extendidos, y esto se debe a dos cuestiones principales referentes al tráfico que viaja por la red.

- Necesidad de monitorización de un flujo de tráfico mayor que el de las redes cableadas.
- Tráfico de red encriptado en base a una serie de mecanismos de cifrado.

Si nos centramos en el diseño de un WIDS, nos surge la necesidad de cambios estructurales internos importantes al portar el diseño básico de un IDS común, orientado a redes cableadas. El cambio más significativo que sufrirá el WIDS será en la forma de capturar tráfico de la red.

1.2.1 Objetivo principal

Partiendo de este problema, el presente proyecto se enfoca al diseño e implementación de Antikörper, un Sistema de Detección de Intrusiones Inalámbrico, capaz de detectar la mayoría de ataques que puedan surgir en una red WLAN y de actuar frente a esos ataques como sea conveniente.

1.2.2 Objetivos parciales

Partiendo de la definición del problema al que nos enfrentamos, arriba enunciado, se exponen a continuación los objetivos parciales perseguidos con la realización de este proyecto.

- **Estudio del estándar IEEE 802.11 referente a las redes WLAN, arquitecturas de IDS y distintas soluciones y herramientas de seguridad**

  Se persigue obtener los conocimientos necesarios respectivos al contexto de la seguridad en las redes WLAN (2) y a las distintas herramientas disponibles para su protección, realizando así un análisis de alternativas que nos permita definir una solución óptima de WIDS.

- **Diseño de un arquitectura WIDS genérica**

  Se diseñará una arquitectura genérica sobre la que implementar un WIDS que cumpla con los requisitos impuestos al proyecto.

- **Implementación de Antikörper**

  Basándonos en la arquitectura definida anteriormente, se implementarán los módulos del sistema y se integrarán en conjunto, obteniendo así un sistema WIDS completamente funcional.

1.3 Beneficios

La realización de este proyecto conlleva una serie de beneficios que se agrupan de la siguiente manera:

- Beneficios técnicos
- Beneficios sociales
- Beneficios económicos

1.3.1 Beneficios técnicos

Como se verá en los capítulos posteriores, el sistema Antikörper estará basado en una arquitectura interna definida de manera modular. Esto permite que el sistema sea adaptable a evoluciones posteriores y a futuras ampliaciones, permitiendo así su uso en distintas líneas de investigación como puede ser la de la seguridad a través de sistemas IDS o la monitorización de tráfico a nivel 802.11 con diferentes fines.

1.3.2 Beneficios sociales

El producto de este proyecto conlleva una serie de beneficios sociales estrechamente relacionados con las futuras líneas de trabajo sobre Antikörper. Esto se debe a que el sistema puede servir de base para la implementación de nuevos sistemas y prototipos tanto a nivel educativo como empresarial.

1.3.3 Beneficios económicos

El sistema Antikörper, producto principal de este proyecto, está basado en su totalidad en código libre. Esto conlleva que su uso está libre de costes, exceptuando los costes derivados de despliegue, como pueden ser los costes de equipos o personal de mantenimiento. Esto es de extrema importancia debido a los altos costes que tienen los sistemas IDS/WIDS que ofertan diferentes empresas.

Por otro lado, debido a las licencias de código abierto sobre las que está basado el sistema, se permite que futuros desarrolladores puedan trabajar sobre este sin ningún tipo de coste y puedan usarlo como base para futuros proyectos.

1.4 Fases del proyecto

Para el desarrollo del proyecto se han considerado una serie de fases bien diferenciadas.

Definición del proyecto. Se realizará un análisis de la problemática a la que nos enfrentamos en el proyecto y se definirán las bases principales sobre las que se asentará este.

Especificación de requisitos. Se expondrán los requisitos que el proyecto debe cumplir.

Revisión del estado del arte. Se estudiará todo lo relacionado con el estándar IEEE 802.11 de WLAN, las diferentes arquitecturas de sistemas IDS/WIDS que existen en la actualidad y las diferentes alternativas y herramientas que existen actualmente relacionadas con los WIDS.

Diseño del sistema WIDS Antikörper. Se desarrollará una propuesta de diseño de WIDS genérica, y basándose en ella, se creará la arquitectura modular base del sistema Antikörper y se presentarán las funciones que deberán cumplir los diferentes módulos que lo componen.

Implementación del sistema WIDS Antikörper. Se implementarán las diferentes partes del sistema Antikörper y se integrará el conjunto para su posterior prueba en distribuciones basados en Linux.

Escenario de pruebas y rendimiento del sistema. Se harán una serie de pruebas sobre el sistema para probar así su correcto funcionamiento. Se comenzará con unas pruebas de caja negra sobre los módulos y se finalizará con unas pruebas de campo para validar el correcto funcionamiento del sistema y medir su rendimiento en diferentes situaciones.

Revisión del trabajo. Se realizará una revisión del trabajo documental generado a lo largo de las fases anteriores, de la cual se obtendrá la memoria final referente al proyecto. También se expondrán una serie de conclusiones y se establecerán las bases para futuras mejoras y ampliaciones del sistema.

Para llevar un control más preciso del alcance del proyecto, y como base para la planificación de este, se han utilizado una serie de herramientas para la gestión de proyectos.

1.4.1 Work Breakdown Structure (WBS)

La Estructura Desglosada de Trabajo/**W**ork **B**reakdown **S**tructure (**WBS)** es una técnica de planificación mediante la cual podemos definir y cuantificar el trabajo a realizar para nuestro proyecto. Se encuentra adjunto el WBS del proyecto en el *Anexo II – Estructuras de descomposición*, apartado *A2.1 Work Breakdown Structure (WBS)*.

1.4.2 Product Breakdown Structure (PBS)

La Estructura de Desglose de Productos/**P**roduct **B**reakdown **S**tructure (**PBS**) es una herramienta para analizar, documentar y comunicar los resultados del proyecto. En ella se especifican los documentos y los productos obtenidos en cada una de las tareas que

se indicaron en el WBS. Se encuentra adjunto el PBS del proyecto en el *Anexo II – Estructuras de descomposición*, apartado *A2.2 Product Breakdown Structure (PBS).*

1.5 Recursos

A continuación se expondrán los recursos a utilizar a lo largo del desarrollo del proyecto, los cuales se categorizarán en humanos, materiales e instalaciones.

1.5.1 Resource Breakdown Structure (RBS)

Para representar los recursos humanos y materiales del proyecto utilizaremos la estructura de desglose de recursos/**R**esource **B**reakdown **S**tructure (**RBS**), que es un árbol jerárquico que representa dichos recursos. En el *Anexo II – Estructuras de descomposición*, apartado *A2.3 Resource Breakdown Structure (RBS)* se encuentran los RBS correspondientes a los dos apartados siguientes.

1.5.2 Recursos humanos

- Prof. D. Luis Zabala Alberdi. Profesor del departamento de Ingeniería de Comunicaciones de la Escuela Técnica Superior de Ingeniería de Bilbao y personal investigador del grupo NQaS, como director del proyecto.
- D. Alberto Pineda Rodríguez. Investigador del grupo de investigación NQaS de la Escuela Técnica Superior de Ingeniería de Bilbao, como co-director del proyecto.
- D. Josu Barrientos Bahamonde. Alumno del Grado en Ingeniería en Tecnología de Telecomunicación de la Escuela Técnica Superior de Ingeniería de Bilbao, como realizador del proyecto.

1.5.3 Recursos materiales

1.5.3.1 Recursos hardware

Para el desarrollo del proyecto, sin contar los escenarios de pruebas que serán presentados en capítulos posteriores, se dispondrá de los siguientes recursos hardware:

- Ordenador portátil con procesador Intel Core i5-4200M, 2,5 GHz, 8 Gb de memoria RAM y 3 MB de memoria Caché.

- Tarjeta de red inalámbrica Alfa Network AWUS036NH con soporte IEEE 802.11b/g/n utilizada para la inyección de tráfico.
- Tarjeta de red inalámbrica TP-LINK TL-WN722N con soporte IEEE 802.11b/g/n para la captura de tráfico.
- Punto de Acceso WiFi TP-Link TL-WR841N.

1.5.3.2 Recursos software

Los recursos software utilizados en la implementación del sistema serán:

- Distribución Linux Ubuntu 12.04 (Precise Pangolin) y Ubuntu 14.04 (Trusty Tahr).
- Entorno de desarrollo integrado IDE Code::Blocks (3) C/C++ y Eclipse (4) Juno C/C++.
- Compiladores GNU GCC y G++ para C/C++.
- Suite Aircrack-ng (5).
- Sniffer Kismet (6).
- Herramienta Ettercap (7).
- Herramientas de inyección de tráfico theflOOdARP y theflOOdETH (creadas junto al sistema Antikörper para la realización de este proyecto), las cuales se expondrá en el *Anexo VII – Suite de herramientas theflOOd*.
- Suite ofimática Microsoft Office (8), utilizando Microsoft Word para la documentación del proyecto, Microsoft Project para la planificación del proyecto y Microsoft Visio para la creación de diagramas.

1.5.3.3 Material general

- Material de oficina.

1.5.3.4 Instalaciones

Utilización del laboratorio de investigación NQAS para el despliegue de la red a la hora de ejecutar las pruebas de funcionamiento y rendimiento.

Capítulo 2

Especificación de requisitos

En este capítulo se exponen los requisitos relativos al desarrollo del proyecto. Este proceso se conoce como Análisis de requisitos y nos ayudará a comprender cuál es el problema o necesidad que se pretende solucionar y cómo se afrontará.

Todos los requisitos se identificarán unívocamente mediante un código que constará de la codificación de la categoría a la que pertenece, un identificador de subcategoría y del número de orden. Este código será utilizado como referencia cada vez que sea necesario mencionarlo a lo largo del ciclo de vida del proyecto.

2.1 Requisitos funcionales

Los requisitos funcionales son aquellos que especifican cada funcionalidad del sistema, además de indicar como se ha de comportar la aplicación.

2.1.1 Sistema

2.1.1.1 RF.SIS.0/Usuarios y seguridad

El sistema debe garantizar que solo los usuarios autorizados a la máquina anfitrión tengan acceso a él. Esto garantiza que no se puedan modificar registros ni alterar el comportamiento del sistema.

2.1.1.2 RF.SIS.1/Interfaz de configuración

Se deberá disponer de un interfaz que permita al usuario autorizado arrancar y configurar el funcionamiento del sistema.

Dentro de esa configuración se debe poder escoger los diferentes dispositivos de captura de los que dispone el sistema.

2.1.1.3 RF.SIS.2/Interfaz de visualización de datos

El sistema deberá disponer un interfaz que permita a cualquier usuario visualizar en vivo las anomalías que se vayan detectando en la red, dando información referente a la máquina fuente de estas.

2.1.2 Datos de entrada

2.1.2.1 RF.ENT.0/Inserción, eliminación y modificación de datos de usuarios autorizados

El sistema ha de ser capaz de recibir, validar, cargar y modificar la información referente a los usuarios autorizados en la red. Estos deben encontrase registrados en el fichero correspondiente.

2.1.2.2 RF.ENT.1/Formato de registro de usuarios autorizados

El fichero de registro debe contener las direcciones MAC y un identificador único correspondiente a las máquinas autorizadas con el siguiente formato:

xx:xx:xx:xx:xx:xx+";"+identificación

2.1.2.3 RF.ENT.2/Inserción de datos referentes al Access Point de la red

El sistema ha de recibir la información referente al Access Point de la red a proteger para poder aplicar las correspondientes políticas de seguridad. Los datos a introducir han de ser los siguientes:

- **SSID** (**S**ervice **S**et **I**dentifier) de la red.
- **BSSID** (**B**asic **S**ervice **S**et **I**dentifier) de la red.

2.1.3 Informes y registros de incidencias

2.1.3.1 RF.INF.0/Registro de intrusos en la red

El sistema ha de ser capaz de registrar las incidencias surgidas en la red, debidas a los intrusos dentro de esta.

2.1.3.2 RF.INF.1/Formato de registro de intrusiones en la red

El fichero de registro generado y mantenido por el sistema ha de contener distintas entradas con la dirección MAC de la máquina intrusa y la fecha/hora de la intrusión.

xx:xx:xx:xx:xx:xx+";"+ "Y/m/d H:M:S"

La fecha/hora seguirán el formato correspondiente a la especificación ISO 8601 (9).

2.1.3.3 RF.INF.2/Registro de Access Point maliciosos

El sistema ha de ser capaz de registrar los Access Point maliciosos detectados en los alrededores de la red.

2.1.3.4 RF.INF.3/Formato de registro de Access Point maliciosos

El fichero de registro generado y mantenido por el sistema ha de contener la BSSID y SSID del Access Point que se anuncia en nombre de Access Point oficial y la fecha/hora del ataque.

"BSSID"+" "+xx:xx:xx:xx:xx:xx+";"+ "Y/m/d H:M:S"

La fecha/hora seguirán el formato correspondiente a la especificación ISO 8601 (9).

2.1.4 Respuestas frente a ataques

2.1.4.1 RF.PER.0/Respuesta frente a máquinas intrusas

El sistema ha de ser capaz de expulsar a los intrusos de la red.

2.1.4.2 RF.PER.1/Respuesta frente a Access Point maliciosos

El sistema ha de ser capaz de inhabilitar los Access Point maliciosos que detecte, evitando así que los usuarios puedan asociarse a este.

2.2 Requisitos no funcionales

Los requisitos no funcionales del proyecto son las restricciones impuestas por el cliente o que son inherentes a las características de la aplicación. Estas restricciones afectan al diseño del propio sistema y tienen relación directa con el rendimiento de la solución desarrollada.

2.2.1 Arquitectura

2.2.1.1 RNF.ARQ.0/Sistemas operativos

El sistema debe funcionar sobre sistemas operativos basados en GNU/Linux, independientemente de la arquitectura.

2.2.1.2 RNF.ARQ.1/Lenguaje de programación

C (10) será el lenguaje de programación utilizado debido a su alto rendimiento y disponibilidad al trabajar a nivel del hardware de la máquina.

2.2.1.3 RNF.ARQ.2/Arquitectura modular

La arquitectura base del sistema ha de gozar de un diseño modular que ofrezca facilidad a la hora de ejecutar modificaciones en futuras revisiones.

2.2.1.4 RNF.ARQ.3/Sistema centralizado

El sistema debe ser capaz de funcionar sobre un solo equipo que tenga acceso a la red que desea proteger.

2.2.2 Rendimiento y fiabilidad

2.2.2.1 RNF.REN.0/Rendimiento

El sistema ha de evitar saturar la máquina sobre la que está funcionando para así no causar parones no programados.

2.2.2.2 RNF.REN.1/Fiabilidad

El sistema ha de ser fiable en lo referente a su funcionamiento, ofreciendo así garantía de seguridad en la red sobre la que está desplegado.

2.2.3 Costes

2.2.3.1 RNF.COS.0/Coste de implementación

El sistema ha de basarse completamente en software libre, por lo que el coste de licencias y demás cuotas ha de ser nulo.

2.2.4 Compatibilidad

2.2.4.1 RNF.SOP.0/Versiones IEEE 802.11

El sistema debe ser compatible con todas las versiones de WLAN.

2.2.4.2 RNF.SOP.1/Mecanismos de seguridad

El sistema ha de soportar todas las opciones de configuración de cifrado de WLAN.

2.2.5 Detección de ataques

2.2.5.1 RNF.DET.0/Intrusos en red

El sistema ha de detectar intrusos en el interior de la red, los cuales puedan generar distintos ataques sobre las máquinas autorizadas.

2.2.5.2 RNF.DET.1/Access Point maliciosos

El sistema ha de detectar los Access Point que se anuncien con el BSSID de la red a proteger.

2.2.6 Escenarios de implantación

2.2.6.1 RNF.OPC.1/Redes domesticas

El sistema ha de poder desplegarse sobre una red doméstica, constituida por un Access Point y los equipos del usuario de la red. La Figura 2-1 representa la arquitectura de una red doméstica, la cual ofrece acceso a Internet a través de un punto de acceso inalámbrico. Basándonos en los sistemas centralizados, el WIDS se encontrará en uno de los equipos del cliente o uno dedicado, desde el cual monitorizará la red y sus alrededores en busca de amenazas.

2.2.6.2 RNF.OPC.2/Redes empresariales

El sistema ha de poder desplegarse sobre una red empresarial que no disponga de un tamaño importante o un servidor Radius (11) para el control de acceso de usuarios.

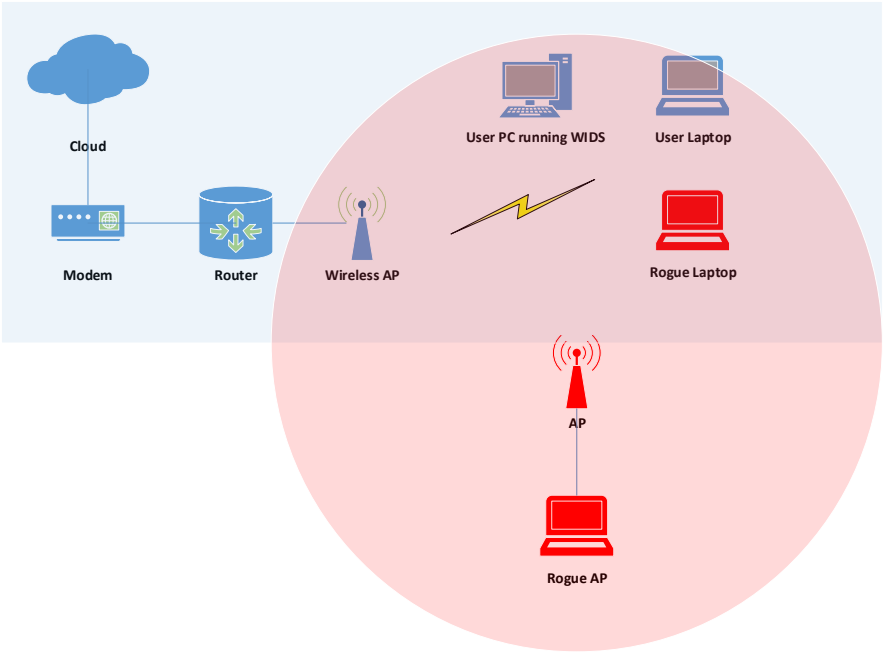


Figura 2-1: Red WLAN domestica con WIDS desplegado

Capítulo 3

Análisis de alternativas

En este capítulo se expone el análisis y la selección de las distintas alternativas con las que se contaba al inicio del proyecto. Para ello se han de tener en cuenta distintos determinantes como son el tipo de funcionamiento del WIDS y la arquitectura sobre la que basar su implementación para así optimizar el funcionamiento.

Con el fin de determinar de manera óptima los criterios de selección de las distintas alternativas, se ha llevado a cabo un extenso estudio del estado del arte de los sistemas WIDS. Este está incluido en el *Anexo III – Estudio del estado del arte*.

3.1 Selección del tipo de IDS

A continuación se expondrá la clasificación de los sistemas IDS/WIDS y se seleccionará la solución más conveniente al desarrollar Antikörper mediante distintos criterios de selección.

3.1.1 Metodología de detección de intrusos

Un WIDS puede realizar la detección de intrusiones de dos formas: basándose en una base de datos de firmas de anomalías (12) o bien detectando comportamientos anómalos en la red.

3.1.1.1 Basado en patrones/firmas

En este caso, el sistema cuenta con un registro de patrones de ataque, a través de los cuales es capaz de detectar diferentes ataques sobre la red. El problema de este método consiste principalmente en que solo se tiene registro de ataques conocidos, cuyos patrones están definidos en firmas de ataque. Esto conlleva a la imposibilidad de hacer frente a nuevos ataques que aún no han sido registrados o bien de los cuales es difícil definir un patrón genérico.

3.1.1.2 Basado en detección de anomalías

El funcionamiento basado en detección de anomalías no está muy implementado, ya que, aunque puede llegar a ser muy eficiente en la detección de intrusos, llega a generar gran cantidad de alarmas falsas. Lo principal en este método es desarrollar un perfil de funcionamiento correcto de la red y determinar un umbral de lo que cree el sistema que es tráfico normal y anormal. A partir de aquí, todo lo que supere el umbral resultará anómalo y generará alarmas.

3.1.1.3 Criterios de selección

A continuación se exponen los criterios utilizados al determinar el óptimo tipo de IDS a utilizar basándonos en su metodología de detección.

- Eficiencia (%40)

Bajo este criterio se valora la eficiencia de cada método, tomando en cuenta los beneficios y desventajas de cada uno de ellos.

- Complejidad de implementación (%40)

Teniendo en cuenta el tiempo del que se dispone en el proyecto para la implementación de Antikörper, se seleccionará una opción u otra dependiendo de la estimación de tiempo para su desarrollo.

- Coste de mantenimiento (%20)

Se ha de tener en cuenta los costes derivados del mantenimiento de cada uno de los métodos de detección, ya sea en la implementación de nuevos algoritmos de detección como en la creación y actualización de nuevas firmas de ataque.

3.1.1.4 Selección de la solución

La Tabla 3-1 presenta los resultados a la hora de seleccionar la solución relacionada con la forma de detección de intrusiones.

Criterio	Ponderación (%)	Basado en patrones/firmas	Basado en detección de anomalías
Eficiencia	40	35	15
Complejidad de implementación	40	35	20
Coste de mantenimiento	20	5	15
Total	100	75	50

Tabla 3-1: Selección de la metodología de detección

Se concluye que la solución óptima a la hora de seleccionar la metodología de detección de intrusiones del sistema sea el basado en patrones/firmas. Esto nos permitirá definir una serie de firmas de ataque que permitan al sistema detectar distintos tipos de ataques.

3.1.2 Lugar de despliegue y sistemas a monitorizar

Los sistemas WIDS pueden diseñarse de forma que capturen el tráfico de red de diferentes formas.

3.1.2.1 Network Based IDS (NIDS)

La principal estrategia que se plantea en estos WIDS es que se necesita monitorizar todos los datos de la red y, de manera paralela, realizar un análisis del tráfico para así, detectar diferentes patrones que puedan referirse a diferentes ataques a la red.

3.1.2.2 Host Based IDS (HIDS)

Estos están instalados en los host de la red y solo monitorizan el tráfico dirigido u originado en ese host.

3.1.2.3 Criterios de selección

A continuación se exponen los criterios utilizados al determinar el óptimo tipo de IDS basándonos en donde desplegarlo y que proteger.

- Eficiencia (%40)

Bajo este criterio se valora la eficiencia a la hora de detectar intrusos en función del número de intrusiones a detectar.

- Complejidad de implementación (%40)

Teniendo en cuenta el tiempo del que se dispone en el proyecto para la implementación de Antikörper, se seleccionara una opción u otra dependiendo de la estimación de tiempo para su desarrollo.

- Costes derivados del despliegue (%20)

Se ha de tener en cuenta los costes resultantes tras el despliegue del sistema, debido a las máquinas necesarias y al mantenimiento.

3.1.2.4 Selección de la solución

La Tabla 3-2 presenta los resultados a la hora de seleccionar la solución relacionada con el lugar donde desplegar el sistema y el número de elementos a proteger.

Criterio	Ponderación (%)	NIDS	HIDS
Eficiencia	40	35	10
Complejidad de implementación	40	20	30
Coste de despliegue	20	15	15
Total	100	70	55

Tabla 3-2: Selección de la forma de desplegar el sistema

Se concluye que la solución óptima a la hora de seleccionar el lugar donde desplegar el sistema y el número de elementos a proteger sea el basado en NIDS. Esto nos permitirá cubrir un rango de detección mucho más amplio y eficiente que si hubiésemos optado por HIDS, independientemente de la complejidad del sistema y de los costes.

3.1.3 Metodología de respuestas frente a intrusiones

Podemos clasificar los tipos de respuesta frente a intrusos en dos grupos.

3.1.3.1 Respuestas pasivas

Los sistemas notifican al administrador del sistema mediante alertas, etc., pero no actúan directamente sobre el ataque o atacante.

3.1.3.2 Respuestas activas

En este caso, el tipo de respuestas son acciones automáticas que se toman cuando una intrusión es detectada.

3.1.3.3 Criterios de selección

A continuación se exponen los criterios utilizados al determinar el óptimo tipo de IDS basándonos en su respuesta frente a intrusiones.

- Tiempo de respuesta (%60)

Se tiene en cuenta la velocidad de actuación del sistema frente a una amenaza.

- Rendimiento (%40)

Se evalúan las posibles caídas de rendimiento en la red a la hora de actuar frente a intrusiones.

3.1.3.4 Selección de la solución

La Tabla 3-3 presenta los resultados a la hora de seleccionar la solución relacionada con el tipo de respuesta frente a intrusiones.

Criterio	Ponderación (%)	Pasivas	Activas
Tiempo de respuesta	60	10	60
Rendimiento	40	35	20
Total	100	45	80

Tabla 3-3: Selección del tipo de respuesta frente a intrusiones

Se concluye que la solución óptima a la hora de seleccionar el tipo de respuesta que ha de tener el sistema frente a un intruso debe ser la respuesta activa. Esto nos permitirá actuar de manera rápida y eficiente frente a las amenazas que se puedan sufrir en la red a proteger.

3.2 Selección de la arquitectura de IDS

A la hora de seleccionar una arquitectura sobre la que implementar Antikörper, se ha de tener en cuenta que es posible trabajar sobre un sistema IDS libre, como podría ser Snort (13), manteniendo así los costes de software nulos que se especificaban en el proyecto. Por otro lado, también es posible plantear diseñar una nueva arquitectura.

3.2.1 Criterios de selección

A continuación, se exponen los criterios utilizados a la hora de seleccionar la arquitectura sobre la que implementar Antikörper.

- Complejidad (%30)

Determina la complejidad a la hora de basarnos sobre un sistema ya desarrollado aplicando modificaciones, o al diseñar e implementar desde cero.

- Libertad de implementación (%50)

Se tiene en cuenta las opciones de implementación que nos aportan ambas opciones.

- Costes de mantenimiento (%20)

El diseño seleccionado ha de derivar en unos costes mínimos a la hora de mantener el sistema. Esto puede traducirse en poder basarnos en una arquitectura que nos da las actualizaciones correspondientes o el tener que actualizar el sistema personalmente.

3.2.2 Selección de la solución

La Tabla 3-4 presenta los resultados a la hora de seleccionar la solución relacionada con la arquitectura del sistema.

Criterio	Ponderación (%)	Rediseño	Arquitectura nueva
Complejidad	30	20	10
Libertad de implementación	50	15	35
Costes de mantenimiento	20	5	15
Total	100	40	60

Tabla 3-4: Selección de la arquitectura del sistema

Se concluye que la solución óptima a la hora de seleccionar la arquitectura del sistema ha de ser un nuevo diseño de esta. Esto nos permitirá diseñar los módulos de la manera deseada para optimizar el funcionamiento del sistema.

3.3 Conclusión del análisis de alternativas

Se ha concluido, tras el análisis de alternativas arriba expuesto, que el sistema Antikörper ha de ser un sistema IDS inalámbrico basado en Network IDS, con detección de intrusiones mediante patrones de ataque y actuación activa frente a diferentes anomalías. En lo referente a la arquitectura, se diseñará partiendo de cero permitiendo optimizar así el funcionamiento del sistema que ha de albergar.

Capítulo 4

Diseño de WIDS basado en Network IDS

Como producto de lo realizado en los capítulos anteriores, se concluyó que el sistema debía satisfacer los requisitos definidos al inicio del proyecto y estar basado en una nueva arquitectura basada en Network IDS, con la metodología de detección de intrusiones mediante patrones. A continuación, se procederá a explicar las características y el diseño que se ha propuesto en este Trabajo de Fin de Grado para un WIDS.

4.1 Arquitectura genérica de un WIDS

La arquitectura del WIDS propuesta constará de cuatro módulos principales: un módulo de interfaces de captura, un módulo de desencriptado de tráfico WLAN, un módulo de procesamiento del tráfico capturado y un módulo de actuación frente a intrusiones. Podemos ver un esquema de la arquitectura propuesta en la Figura 4-1.

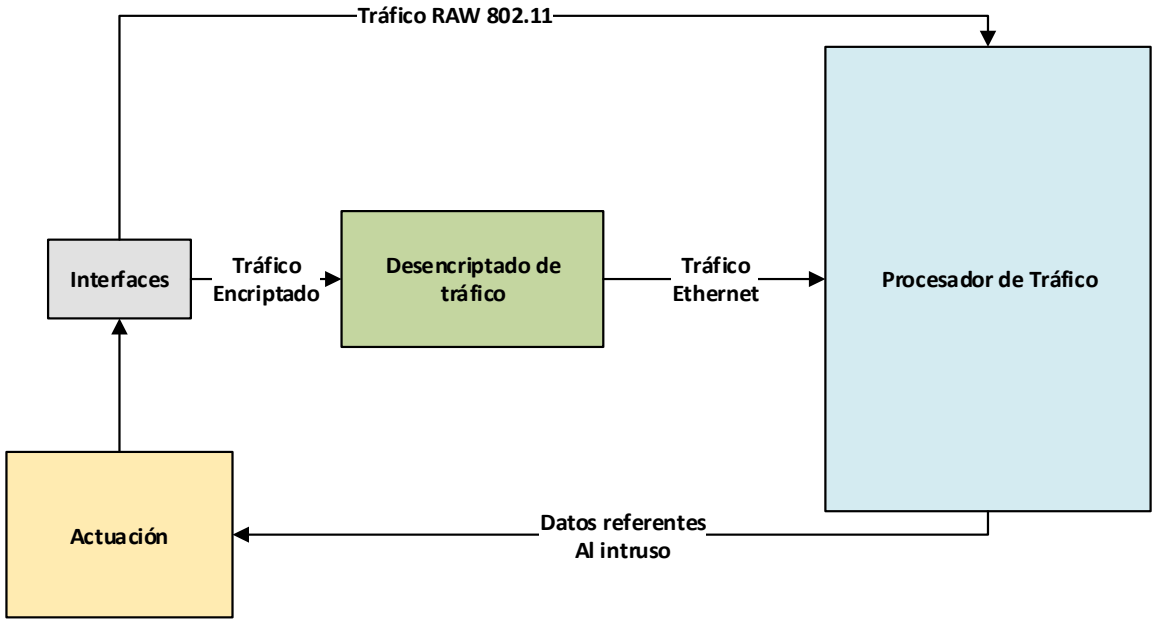


Figura 4-1: Propuesta de arquitectura genérica de WIDS

A continuación se explicará el flujo de datos que hay en el sistema.

El módulo de interfaces será el contacto que tendrá el sistema con la red a proteger. Este módulo contará con una serie de interfaces en modo monitor, a través de los cuales capturará el tráfico de red que pasará a los módulos posteriores para su análisis.

Este tráfico se bifurcará en dos caminos. Uno irá directamente al módulo de análisis que analizará el trafico 802.11 RAW analizando las tramas Beacon de los puntos de acceso, para así buscar posibles Puntos de Acceso maliciosos (a partir de ahora *Rogue APs* o *Access Point maliciosos*). Por otro lado, el tráfico pasará al módulo de desencriptación donde, mediante las claves de encriptado de la red, se encapsulará el tráfico a tramas Ethernet para que sean fácilmente manejables.

El módulo de análisis recibirá el tráfico, buscara anomalías y en caso de encontrar indicios de intrusiones, llamará al módulo de actuación que será el encargado de deshabilitar al intruso.

4.2 Diseño de arquitectura de Antikörper

Antikörper es un Wireless Intrusion Detection System basado en Network IDS y en el diseño previamente propuesto.

Basándonos en todo los analizado en capítulos anteriores, se ha diseñado la arquitectura base de Antikörper en base a los requerimientos que se impusieron en el *Capítulo 2 - Especificación de requisitos*.

Como se ha dicho anteriormente, el sistema está basado en arquitectura Network IDS siguiendo el esquema propuesto en la Figura 4-1. Esto permite que el sistema opere bajo todo un dominio de colisión, analizando no solo el tráfico que va dirigido al equipo sobre el que esta operado, sino el tráfico de todos los equipos de la red. Otro de los puntos importantes a cubrir por el sistema es la interoperabilidad con otros sistemas de seguridad que pueden existir en la red.

En la Figura 4-2 se puede ver la arquitectura final de Antikörper, en ella se puede observar los módulos finales de los que va a constar el sistema, cómo van a interoperar entre ellos y qué datos van a recibir y emitir.

A continuación se presenta el diseño de alto nivel del sistema Antikörper, en él se describen los módulos que lo componen junto a una descripción de sus características.

En el *Anexo IV – Diseño de bajo nivel* se adjunta el diseño de bajo nivel, en el que se explica más detalladamente el funcionamiento de los módulos de manera interna.

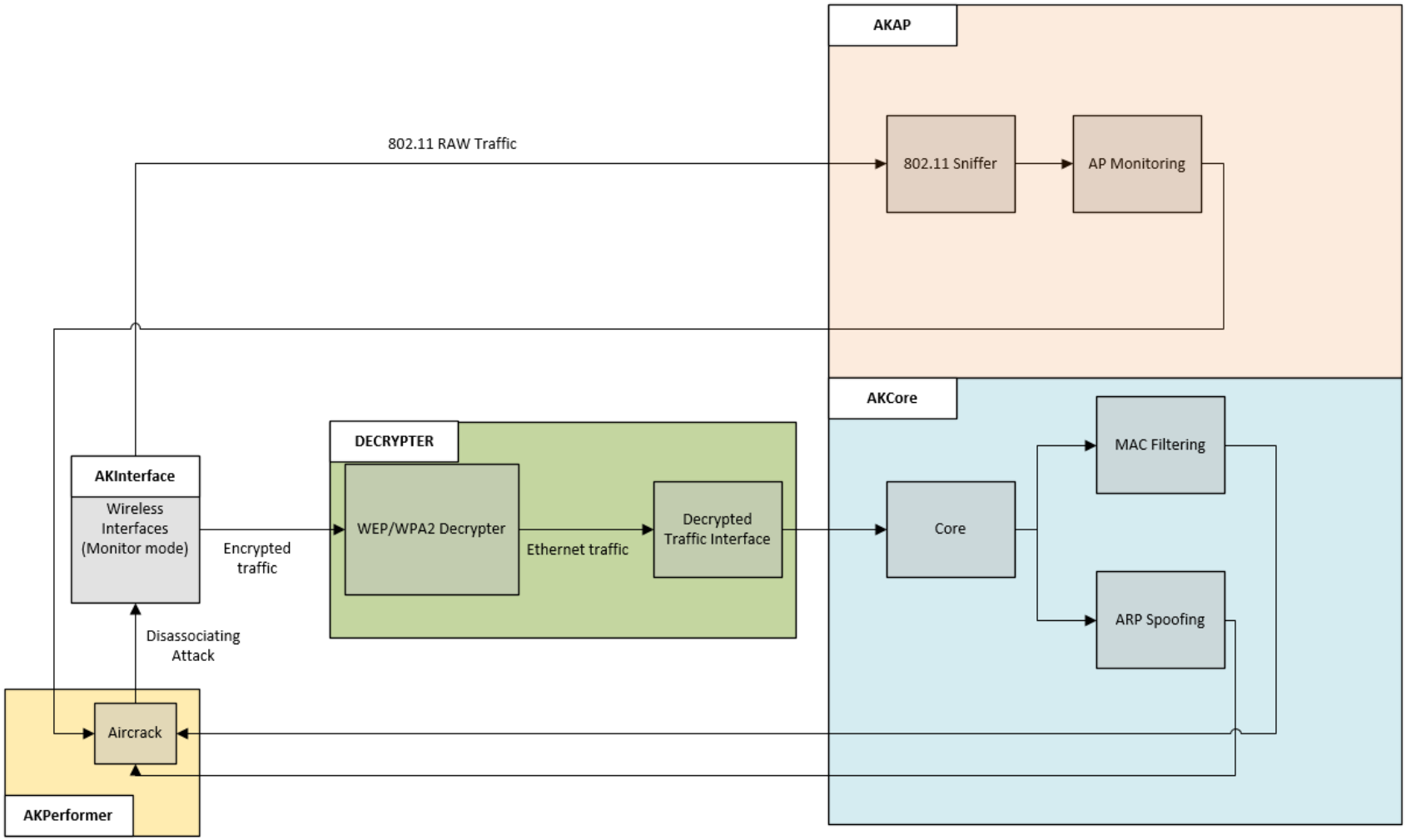


Figura 4-2: Arquitectura modular de Antikörper

Cabe destacar que el funcionamiento del sistema está separado en dos programas independientes, llamados AntikörperCore (dependiente principalmente del módulo AKCore) y AntikörperAP (dependiente principalmente del módulo AKAP), los cuales se encargarán de detectar intrusos dentro de la red y de detectar Rogue APs respectivamente. Esto permitirá una mayor libertad al arrancar el sistema, configurándolo en función de las necesidades del usuario.

4.2.1 *Módulo de interfaces - AKInterface*

El módulo de interfaces será el encargado de configurar los interfaces del sistema, los cuales serán la fuente de tráfico a analizar. Este módulo actuará a través del interfaz de configuración del sistema, el cual seleccionará el interfaz de captura automáticamente y lo configurará en modo monitor.

Características técnicas

- Tasa de captura de tráfico en función del hardware disponible.
- Numero de interfaces en función de las necesidades del cliente. Mínimo 2 interfaces con soporte monitor.

4.2.2 *Módulo de desencriptación de tráfico - Decrypter*

Una de las problemáticas principales a las que nos enfrentamos al diseñar un IDS inalámbrico, a diferencia de su homólogo cableado, es que el tráfico de la red viaja encriptado mediante una serie de mecanismos.

El no desencriptar el tráfico conlleva el no poder analizar una serie de paquetes de red que son de vital importancia a la hora de detectar ataques, como son los paquetes **ARP** (**A**ddress **R**esolution **P**rotocol*)* (14). Estos paquetes son la fuente de una inmensa cantidad de ataques como pueden ser los ARP Poisoning o los ataques MitM (Man in the Middle). Estos ataques han sido analizados en el estudio del estado del arte incluido en el *Anexo III – Estudio del estado del arte*. Debido a los problemas que trae consigo el analizar solo tráfico encriptado, se ve necesario incluir un módulo que se encargue de desencriptar este tráfico para así poder analizarlo correctamente.

El funcionamiento del módulo Decrypter es sencillo. El módulo requerirá un interfaz en modo monitor desde el que capturar tráfico, el cual será facilitado por el módulo AKInterface. Tras esto, con una información básica de red que incluirá el SSID y el BSSID, será capaz de encapsular el tráfico en tramas Ethernet fácilmente tratables.

En caso de que el protocolo de seguridad de la red sea **WEP** (**W**ired **E**quivalent **P**rivacy), el módulo desencriptará el tráfico de la red mediante la clave compartida en la red.

Por otro lado, en caso de usar el protocolo **WPA/WPA2** (**W**i-Fi **P**rotected **A**ccess), el módulo desautenticará a todos los usuarios de la red, deshabilitándola durante unos segundos, y comenzará a capturar tráfico a nivel 802.11. De esta forma, se esperará a capturar las Beacon Frames (15) enviadas del Access Point para así identificar las BSSID asociadas a cada SSID. Tras esto, esperará a los mensajes EAPOL (16) en los que, mediante el llamado EAPOL Handshake entre las estaciones y el Access Point, se obtendrán las claves con las que desencriptar el tráfico.

El nuevo tráfico desencriptado será enviado por un interfaz puente a través del cual el módulo de análisis recibirá el tráfico a analizar.

Características técnicas

- Desencriptación del tráfico WLAN mediante un sistema de registro de mensajes de configuración a nivel 802.11 (EAPOL Handshake).
- Creación de interfaz puente para redireccionar tráfico de red desencriptado.
- Soporte para todos los protocolos de seguridad WLAN.

4.2.3 *Módulo de análisis de tráfico 802.11 AKAP*

AKAP será el núcleo de AntikörperAP y será el encargado de procesar el tráfico capturado en busca de puntos de acceso maliciosos.

El módulo comenzará recibiendo el tráfico capturado por el módulo de interfaces AKInterface, y filtrará este en base a si las tramas recibidas son tramas Beacon o no. Por cada trama Beacon recibida, extraerá la información de anuncio del Access Point que la ha enviado y evaluará si el Access Point es un Rogue AP. Esto lo hará en base al patrón de si el Access Point se anuncia con el mismo nombre que el que estamos protegiendo pero lo hace con una SSID diferente; es decir, si intenta suplantar al Access Point oficial.

Tras esto, en caso de detectar un Rogue AP, llamará al módulo de actuación AKPerformer para que inhabilite el Access Point.

4.2.4 *Módulo de análisis de tráfico Ethernet AKCore*

Este módulo, a diferencia del módulo AKAP, será el encargado de buscar intrusiones en el interior de la red y será el núcleo de AntikörperCore.

El módulo comenzará recibiendo el tráfico desencriptado y encapsulado en tramas Ethernet que entrega el módulo Decrypter y analizará el tráfico trama por trama.

Comenzará extrayendo de la trama la información correspondiente a la máquina fuente, esto es su dirección MAC, y evaluará si pertenece a una máquina autorizada de la red. Para ello, hará uso de su registro de máquinas autorizadas. En caso de detectar una máquina intrusa, llamará al módulo AKPerformer para expulsarla de la red.

Tras analizar la trama en busca de intrusos mediante la dirección MAC, filtrará la trama en función de si esta encapsula un paquete ARP. En caso de detectar un paquete ARP, extraerá la información de cabecera de este y llevará a cabo un proceso de detección de envenenamiento ARP (ARP Poisoning). Este ataque es extremadamente peligroso, debido a que permite al atacante hacer de puente entre la víctima y el Access Point recibiendo todo el tráfico de la red, y es el primer paso de la mayoría de ataques que puedan surgir en una red WLAN.

La detección de ARP Poisoning se realizará mediante la búsqueda de respuestas ARP (ARP Reply) que anuncien que ellas son la salida hacia internet a través del Access Point, esto es, el Gateway de la red, haciendo así que la víctima cambie su tabla ARP y envíe el tráfico a este. En este proceso, el sistema buscará paquetes ARP Reply que anuncien direcciones IP del Gateway iguales a la oficial, pero con direcciones físicas (MAC) diferentes.

4.2.5 *Módulo de respuesta frente a intrusiones AKPerformer*

Mientras que los otros módulos se encargan de capturar, tratar y analizar el tráfico de la red, el módulo AKPerformer será el encargado de tomar acciones frente a las intrusiones y los atacantes.

Una vez invocado, ya sea por AKCore o AKAP, se encargará de tomar acciones mediante un ataque de disasociación a la entidad intrusa. Pudiendo ser esta un host de la red o un Access Point. En caso de ser un host de la red, generará un ataque de disasociación contra el host intruso obligando al Access Point a disasociar a este. En cambio, en caso de enfrentarnos a un Rogue AP, el AKPerformer inundará el entorno 802.11 físico de mensajes de disasociación en broadcast a todos los host de la red, para que sean incapaces de acceder a los servicios del Rogue AP.

4.2.6 Diseño de bajo nivel

En el *Anexo IV – Diseño de bajo nivel* se adjunta el diseño de bajo nivel del sistema. En él se detalla el funcionamiento de cada módulo y se describe el flujo datos que hay en ellos.

4.3 Implementación del sistema Antikörper

En el *Anexo IV – Diseño de bajo nivel*, apartado *A4.4 Diseño de los módulos del sistema* se adjunta la descripción de la implementación del sistema Antikörper.

Capítulo 5

Gestión del proyecto

A continuación se expone la planificación del proyecto y su presupuesto correspondiente.

5.1 Planificación

La planificación nos ayudará a obtener y repartir los recursos tanto materiales como humanos de los que disponemos para lograr los objetivos. Así mismo, nos ayudará a controlar el logro de los objetivos, fijar prioridades y a tratar posibles problemas en el transcurso del proyecto. La planificación del proyecto se ha gestionado con el software Microsoft Project 2013. Este nos ha ayudado en el desarrollo de planes, en la asignación de recursos a tareas, en dar seguimiento al progreso, en administrar el presupuesto y en el análisis de las cargas de trabajo.

5.1.1 Asignación de tareas

A continuación, se expone en la Tabla 5-1 la asignación temporal a las tareas definidas mediante el WBS adjunto en el *Anexo II – Estructuras de descomposición*, apartado *A2.1 Work Breakdown Structure (WBS)*.

Tareas	Duración	Inicio	Fin
1. Definición del proyecto	**16**	**04/10/2013**	**25/10/2013**
1.1 Descripción del problema	2	04/10/2013	07/10/2013
1.2 Definicion de los objetivos y los limitante	4	08/10/2013	11/10/2013
1.3 Especificación de requisitos	10	14/10/2013	25/10/2013
2. Revisión del estado del arte	**33**	**04/11/2013**	**18/12/2013**
3.1 Estudio del estándar IEEE 802.11	20	04/11/2013	29/11/2013
3.2 Análisis de arquitecturas IDS	4	02/12/2013	05/12/2013
3.3 Estudio de soluciones alternativas	9	06/12/2013	18/12/2013
3. Diseño	**40**	**03/02/2014**	**28/03/2014**
3.1 Propuesta de diseño	6	03/02/2014	10/02/2014
3.2 Diseño de Antikörper	34	11/02/2014	28/03/2014
4. Implementación	**47**	**22/09/2014**	**25/11/2014**
4.1 AKInterface	6	22/09/2014	29/09/2014
4.2 Decrypter	5	30/09/2014	06/10/2014
4.3 AKCore	20	07/10/2014	03/11/2014
4.4 AKAP	8	10/11/2014	19/11/2014
4.5 AKPerformer	1	20/11/2014	20/11/2014
4.6 Integración de módulos	3	21/11/2014	25/11/2014
5. Pruebas	**15**	**26/11/2014**	**16/12/2014**
5.1 Definición de pruebas	2	26/11/2014	27/11/2014
5.2 Pruebas de caja negra	4	01/12/2014	04/12/2014
5.3 Pruebas de integración	1	05/12/2014	05/12/2014
5.3 Pruebas de rendimientos	7	08/12/2014	16/12/2014
6. Gestión de proyecto	**41**	**17/12/2014**	**11/02/2015**
8.1 Tareas de gestión	4	17/12/2014	22/12/2014
8.2 Trabajo documental	37	23/12/2014	11/12/2015

Tabla 5-1: Tareas del proyecto

5.1.2 Diagrama de Gantt

Figura 5-1: Diagrama de Gantt – 1

Figura 5-2: Diagrama de Gantt - 2

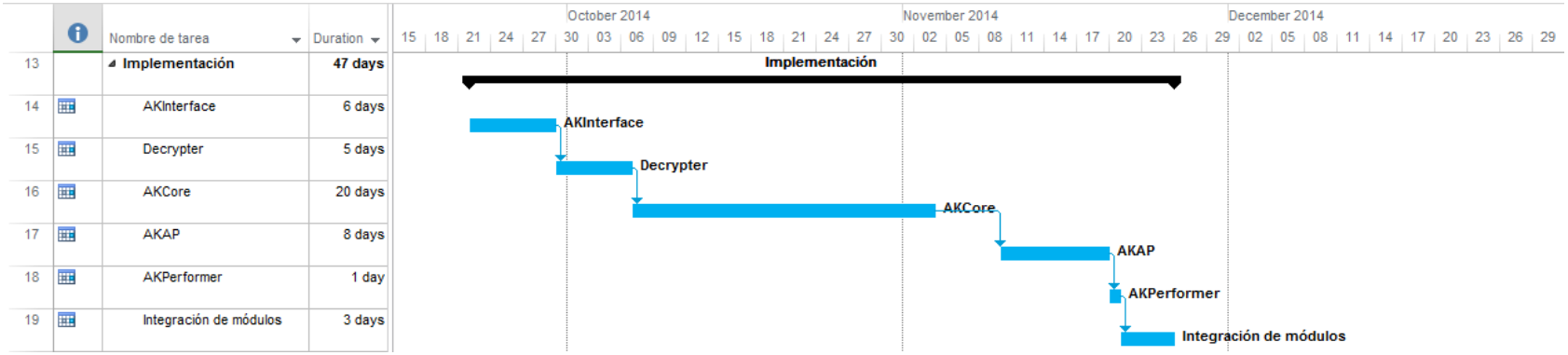


Figura 5-3: Diagrama de Gantt – 3

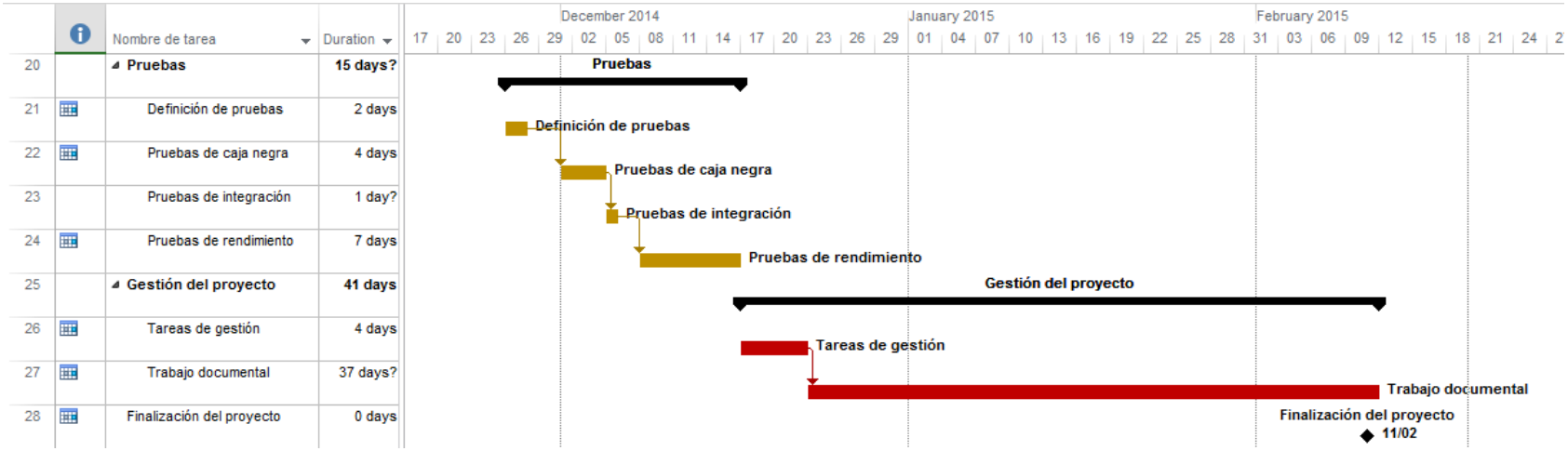


Figura 5-4: Diagrama de Gantt – 4

5.2 Presupuesto

Para poder estimar el presupuesto teórico, se ha planteado la situación de que el proyecto vinculado a este Trabajo Fin de Grado hubiese sido realizado en una empresa. Para ello, se supondrá que este proyecto ha sido realizado por un solo autor, cuyo nivel profesional podría corresponder a un ingeniero júnior, y la duración del proyecto ha sido de 8 meses contando los parones intermedios.

El desglose de presupuesto va a realizarse en dos bloques principales, por un lado, el coste en recursos humanos utilizado a lo largo del proyecto y el coste de materiales utilizados en el desarrollo de este.

5.2.1 Costes en recursos humanos

Para el cálculo de los costes en recursos humanos, se supondrá que un ingeniero júnior en la empresa supuesta tendrá un sueldo base de 800 euros mensuales por una jornada de trabajo media de 20 horas semanales.

*Coste de ingeniero júnior durante 8 meses (800€ * 8 meses)..... 6400 €*

Coste de Seguridad Social a cargo de la Empresa..... 1472 €

5.2.2 Costes materiales

Podemos dividir los costes materiales en dos grupos:

5.2.2.1 Costes hardware

Se tienen en cuenta los recursos materiales expuestos en el apartado 1.6.3.1.

Ordenador portátil..... 1250 €

Tarjeta de red inalámbrica Alfa Network..... 35 €

Tarjeta de red inalámbrica TP-LINK..... 13 €

Punto de Acceso WiFi TP-Link TL-WR841N..... 25 €

5.2.2.2 Costes software

Licencia Microsoft Office 2013, paquete Hogar&Empresa..... 228 €

5.2.2.2 Costes asociados a consumibles

Electricidad consumida..... 90 €

*Acceso a internet (30 € * 8 meses)..... 240 €*

Material de oficina..... 30 €

5.2.3 Costes totales

La Tabla 5-2 presenta el desglose total del presupuesto.

Concepto	Coste (en euros)
Recursos humanos	7872,00
Material	1911,00
Total	9783,00

Tabla 5-2: Presupuesto total del proyecto

Se observa que el coste teórico del proyecto en el ámbito empresarial será de 9783,00 euros.

5.3 Presupuesto de despliegue

Con el objetivo de evaluar los costes derivados del despliegue del sistema, se considera el presupuesto del proyecto de continuación. Este consiste en el despliegue del sistema Antikörper en una empresa. El *Anexo V – Presupuesto de despliegue* detalla dicho presupuesto.

Capítulo 6

Pruebas

En este capítulo se presenta un resumen del plan de pruebas adjunto en el *Anexo VI - Plan de pruebas y resultados obtenidos*. Estas pruebas han sido realizadas sobre el sistema implementado para comprobar que se satisfacen todos los requisitos especificados. Para ello, se hará una serie de pruebas de caja negra que permitirán validar el funcionamiento de los módulos, y tras esto, se integrarán los módulos y se probará el correcto funcionamiento del sistema en su conjunto. Por último, se realizará una serie de tests con el fin de probar el rendimiento del sistema en diferentes situaciones.

6.1 Pruebas de caja negra

El objetivo principal de estas pruebas es comprobar el correcto funcionamiento de los distintos elementos y componentes del sistema por separado, sin analizar la interacción que habrá entre ellos.

6.1.1 Pruebas en la apertura de interfaces

Identificador de la prueba	PRCN-01
Objetivos de la prueba	Comprobar que se configuran de manera correcta los interfaces de captura e inyección de tráfico del sistema
Resultados	Satisfactorios

Tabla 6-1: Resumen de prueba PRCN-01

6.1.2 Pruebas sobre el módulo Decrypter

Identificador de la prueba	PRCN-02
Objetivos de la prueba	Comprobar que el módulo Decrypter desencripta el tráfico correctamente e independientemente de la técnica utilizada
Resultados	Satisfactorios

Tabla 6-2: Resumen de prueba PRCN-02

6.1.3 Pruebas sobre el módulo AKCore

Identificador de la prueba	PRCN-03
Objetivos de la prueba	Comprobar que el módulo AKCore realiza de manera correcta el filtrado MAC y el análisis ARP
Resultados	Satisfactorios

Tabla 6-3: Resumen de prueba PRCN-03

6.1.4 Pruebas sobre el módulo AKAP

Identificador de la prueba	PRCN-04
Objetivos de la prueba	Comprobar que el módulo AKAP filtra las tramas Beacon y analiza su contenido en busca de Access Point maliciosos
Resultados	Satisfactorios

Tabla 6-4: Resumen de prueba PRCN-04

6.1.5 Pruebas sobre el módulo AKAP

Identificador de la prueba	PRCN-05
Objetivos de la prueba	Comprobar que el módulo AKPerformer genera ataques de disasociación como respuesta frente a las intrusiones
Resultados	Satisfactorios

Tabla 6-5: Resumen de prueba PRCN-05

6.1.6 Conclusión de pruebas de caja negra

La ejecución de estas pruebas nos muestra el correcto funcionamiento de los módulos que componen Antikörper, y nos da luz verde para poder realizar pruebas sobre el sistema con todos sus módulos funcionando en conjunto.

6.2 Pruebas de integración

Las pruebas de integración se realizaron una vez probado el funcionamiento correcto de los módulos que componen el sistema por separado.

Como se ha ido comentando en capítulos anteriores, el sistema Antikörper se compone de dos programas individuales, AntikörperCore y AntikörperAP. En las pruebas de integración se ejecuta cada programa por separado y se comprueba que ambos cumplen sus funcionalidades.

6.2.1 Pruebas sobre AntikörperCore

Para validar el funcionamiento de AntikörperCore, se realizan las siguientes pruebas.

Identificador de la prueba	PRIN-01
Objetivos de la prueba	Comprobar que AntikörperCore detecta intrusos dentro de la red
Resultados	Satisfactorios

Tabla 6-6: Resumen de prueba PRIN-01

Identificador de la prueba	PRIN-02
Objetivos de la prueba	Comprobar que AntikörperCore genera los ficheros de registro de intrusiones de manera correcta
Resultados	Satisfactorios

Tabla 6-7: Resumen de prueba PRIN-02

Identificador de la prueba	PRIN-03
Objetivos de la prueba	Comprobar que AntikörperCore recoge, almacena y modifica los datos de usuarios autorizados de manera correcta
Resultados	Satisfactorios

Tabla 6-8: Resumen de prueba PRIN-03

6.2.2 Pruebas sobre AntikörperAP

Para validar el funcionamiento de AntikörperAP, se realizan las siguientes pruebas.

Identificador de la prueba	PRIN-04
Objetivos de la prueba	Comprobar que AntikörperAP detecta Rogue APs en la red
Resultados	Satisfactorios

Tabla 6-9: Resumen de prueba PRIN-04

Identificador de la prueba	PRIN-05
Objetivos de la prueba	Comprobar que AntikörperAP genera los ficheros de registro de Rogue APs de manera correcta
Resultados	Satisfactorios

Tabla 6-10: Resumen de prueba PRIN-05

Tras ejecutar las pruebas de integración sobre los dos programas que componen Antikörper, se concluye que el sistema funciona de manera satisfactoria, cumpliendo las especificaciones y compromisos con los que fue concebido el proyecto.

6.3 Pruebas de rendimiento

Estas pruebas se han realizado con el objetivo de medir el rendimiento del sistema bajo situaciones de estrés. Para ello, se medirán los siguientes parámetros:

- Cantidad de tráfico recibido
- Cantidad de intrusiones detectadas
- Cantidad de actuaciones generadas frente a las intrusiones

Identificador de la prueba	PRREN-01
Objetivos de la prueba	Medir y evaluar la tasa de captura del sistema Antikörper.
Resultados	Satisfactorios
Rendimiento	99,83 %

Tabla 6-11: Resumen de prueba PRREN-01

Identificador de la prueba	PRREN-02
Objetivos de la prueba	Medir el número de intrusiones detectadas por el sistema a través de detecciones de envenenamiento ARP.
Resultados	Satisfactorios
Rendimiento	100 %

Tabla 6-12: Resumen de prueba PRREN-02

Identificador de la prueba	PRREN-03
Objetivos de la prueba	Medir el número de respuestas generadas por el sistema frente a máquinas intrusas en el interior de la red
Resultados	Satisfactorios
Rendimiento	100 %

Tabla 6-13: Resumen de prueba PRREN-03

6.3.1 Conclusión de pruebas de rendimiento

Tras la ejecución de estas pruebas concluimos que el sistema cumple con creces las necesidades de rendimiento impuestas. De esta forma concluimos que el sistema cumple la función de sistema de detección de intrusiones a la perfección bajo los requisitos que se impusieron en el inicio del proyecto.

Capítulo 7

Aspectos legales

Al implementar un sistema de seguridad es necesario llevar a cabo un estudio exhaustivo sobre la legislación vigente.

Al implementar un sistema de detección de intrusiones, el cual es el tema que se abarca en este proyecto, hay que ser especialmente cuidadosos al cumplir toda la normativa de manera íntegra. Esto se debe a que el cumplir con estos condicionantes permite que la información recogida por el sistema sea de relevancia ante un proceso judicial.

A continuación expondremos los aspectos legales más significativos que podemos encontrar en España que rodean los sistemas de detección de intrusiones y la seguridad informática en general.

7.1 Legislación

Se entiende como delito informático a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estos delitos se recogen en la Ley Orgánica 10/1995, de 23 de noviembre, del ***Código Penal*** (17). Estos, como norma general, tienen la misma pena que sus homólogos no informáticos. Por ejemplo, se aplica la misma pena para una intromisión en el correo electrónico que para una intromisión en el correo postal.

A la hora de proceder a su investigación, debido a que una misma acción puede tener consecuencias en diferentes fueros, comenzará la investigación aquel partido judicial que primero tenga conocimiento de los hechos delictivos cometidos a través de un medio informático, si durante el transcurso de la investigación, se encuentra al autor del delito y pertenece a otro partido judicial, se podrá realizar una acción de inhibición a favor de este último para que continúe con la investigación del delito.

7.2 Clasificación de delitos

Aunque los delitos informáticos no están contemplados como un tipo especial de delito en la legislación española, existen varias normas relacionadas con este tipo de conductas (sin ser ilícitos penales):

- Ley Orgánica de Protección de Datos de Carácter Personal.
- Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.
- Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley General de Telecomunicaciones.
- Ley de Propiedad Intelectual.
- Ley de Firma Electrónica.

Además de estas normas, en el Código Penal español, se incluyen multitud de conductas ilícitas relacionadas con los delitos informáticos. Las que más se aproximan a la clasificación propuesta por el "Convenio sobre la Ciberdelincuencia" se reflejan en los siguientes artículos:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

El **Artículo 197** contempla las penas con las que se castigará:

- A quien, con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apodere de cualquier documentación o efecto personal, intercepte sus telecomunicaciones o utilice artificios de escucha, transmisión, grabación o reproducción de cualquier señal de comunicación (delito de descubrimientos de secretos).

- Al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado (delito de manipulación de datos reservados registrados en ficheros o soportes informáticos).

- El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años (delito de intromisión informática).

- Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos.

El delito de descubrimiento de secretos del artículo 197.1 CP constituye un atentado contra la intimidad que puede realizarse de dos formas distintas: apoderándose de documentos o efectos o mediante la intromisión en ámbitos reservados de la víctima.

La primera modalidad mencionada, consiste, desde el punto de vista objetivo, en apoderarse de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales de una persona. Por lo tanto, también puede ser cometido por vía informática mediante, por ejemplo, la apoderación de un mensaje de correo electrónico ajeno.

La segunda modalidad (castigada con la misma pena que la primera), consiste objetivamente en interceptar las telecomunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación. Este tipo delictivo tiene su base en el derecho fundamental recogido en el artículo 18.3 del secreto de las comunicaciones, y aunque pareciera que normalmente se comete por vía telefónica, no hay que descartar el ámbito informático como medio para su comisión.

Sobre el artículo 197.2, contiene el delito de manipulación de datos reservados registrados en ficheros o soportes informáticos, el cual supone un atentado contra la intimidad. El objeto del delito son los datos reservados de carácter personal o familiar, es decir, han de ser informaciones cuyo conocimiento está limitado a las personas autorizadas (datos indisponibles sin autorización) y deben incidir en la esfera personal o familiar.

Los datos reservados se protegen cuando están almacenados a través de un sistema informático, electrónico o telemático o en cualquier otro tipo de archivo en registro público o privado.

Este artículo, recoge dos grupos de comportamientos que, aunque son distintos, en ocasiones pueden superponerse. Por un lado, castiga a quien se apodere, utilice, o modifique datos reservados de carácter personal o familiar. Por otro lado, también castiga el denominado ``espionaje electrónico´´, es decir, el acceso a datos reservados y también su alteración o utilización, Sin embargo, en este caso, los comportamientos irían dirigidos a los ficheros o soportes informáticos y no a los datos (para no repetirse).

Por último, el apoderamiento, modificación o utilización de los datos han de realizarse en perjuicio de tercero y el acceso, alteración o utilización de ficheros o soportes informáticos en perjuicio del titular de los datos o de un tercero, lo cual es lo mismo.

Por otro lado, el artículo 197.3 prevé el delito de intromisión informática, consistente en acceder sin autorización a datos o programas informáticos contenidos en un sistema informático o mantenerse en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Supondría un delito de allanamiento de morada pero referido a un acceso virtual (modificación con origen en el convenio del consejo de Europa sobre ciberciminalidad de Budapest de 2001 y la decisión marco 2005/222/ JAI del consejo de la UE que insta a los estados miembros a tipificar como delito el acceso no autorizado.

El bien jurídico protegido (valor) sería el honor y la intimidad personal y familiar de los ciudadanos.

Este delito tiene 2 modalidades típicas (conductas castigadas). La primera consiste en acceder a datos o programas informáticos contenidos en un sistema informático o en parte del mismo (hacking, sin más requisitos que la ausencia de autorización del titular). La segunda consiste en mantenerse en el sistema contra la voluntad de quien tenga el legítimo derecho a excluirlo. Obviamente, antes ha de haber un acceso autorizado por el titular, el cual lo revoca.

Por último, está el delito de revelación de secretos del artículo 197.4 CP, que tan solo supone revelar los datos que se han conseguido mediante las formas anteriores (y está más castigado). Si el que revela los datos es otra persona que no los ha descubierto, habrá de saber el origen ilegal de los mismos para que se le pueda aplicar este delito.

Además, hay que añadir que se castigan más gravemente estos delitos anteriores si se dan ciertas circunstancias recogidas en el artículo 197 y 198 CP.

En el **artículo 278.1** se exponen las penas con las que se castigará a quien lleve a cabo las mismas acciones expuestas anteriormente, pero con el fin de descubrir secretos de empresa.

El **Artículo 264.2** trata de las penas que se impondrán al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Simplemente es una vertiente del delito de daños, el denominado delito de daños informáticos que trata de extender la protección a cosas inmateriales con contenido económico.

Delitos informáticos

Los artículos 248 y 249 tratan las estafas. En concreto el **artículo 248.2** considera las estafas llevadas a cabo mediante manipulación informática o artificios semejantes. Una variante del delito de estafa en la cual se intenta proteger la seguridad en la informática.

El artículo 256 CP castiga al que usare cualquier equipo terminal de telecomunicación sin consentimiento de su titular. Es importante aclarar aquí que la cuantía defraudada habrá de ocasionar un perjuicio superior a 400 euros, ya que, si no, estaremos ante una mera falta del artículo 623.4CP).

Delitos relacionados con el contenido

El **artículo 186** cita las penas que se impondrán a aquellos, que por cualquier medio directo, vendan, difundan o exhiban material pornográfico entre menores de edad o incapaces. Lo cual puede realizarse mediante la informática.

El **artículo 189** trata las medidas que se impondrán a quien utilice a menores de edad o a incapaces con fines exhibicionistas o pornográficos, y quien produzca, venda, distribuya, exhiba o facilite la producción, venta, distribución o exhibición de material pornográfico, en cuya elaboración se hayan utilizado menores de edad o incapaces.

El artículo 183 bis CP prevé el delito de ciberacoso sexual: el que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 (delitos contra la libertad sexual) y 189 (el anterior), siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento. Las penas correspondientes a los delitos en su caso cometidos se acumulan las penas a las de este delito. Las penas se impondrán de forma agravada cuando el acercamiento se obtenga mediante coacción, intimidación o engaño. (INTRODUCIDO EN 2010).

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines

El **Artículo 270** enuncia las penas con las que se castigará a quienes reproduzcan, distribuyan o comuniquen públicamente, una parte o la totalidad de una obra literaria, artística o científica, con ánimo de lucro y en perjuicio de terceros.

El **artículo 273** trata las penas que se impondrán a quienes sin consentimiento del titular de una patente, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio, objetos amparados por tales derechos, con fines comerciales o industriales.

Capítulo 8

Conclusiones y trabajo futuro

A continuación se exponen las conclusiones obtenidas de la realización de este proyecto, así como el trabajo futuro que se pretende realizar tras la realización de este.

8.1 Conclusiones

Las conclusiones extraídas de este proyecto han sido más que satisfactorias. El proyecto ha concluido en el diseño y la implementación de Antikörper, un sistema de detección de intrusiones orientado a redes inalámbricas completamente funcional. Dicho sistema ha logrado equipararse a sus equivalentes cableados a pesar de la problemática derivada de la naturaleza inalámbrica del entorno que pretende proteger.

Además, se han logrado alcanzar todos los objetivos propuestos al inicio del proyecto junto con el cumplimiento de todos los requisitos impuestos al sistema.

En general, con la realización del proyecto, se ha logrado lo siguiente:

- Se ha diseñado una arquitectura de IDS inalámbrico genérica, la cual se compone de todos los módulos necesarios para cubrir todas las necesidades que demandan las redes WLAN. Entre ellas se encuentran la monitorización de todo el tráfico de la red y la desencriptación del tráfico.
- Se ha implementado un sistema IDS inalámbrico basado en Network IDS con respuesta activa frente a intrusiones con el cual ofrecer seguridad en las redes inalámbricas.
- Se ha llevado a cabo un estudio de las vulnerabilidades de las redes WLAN, el cual nos ha permitido definir las políticas y las necesidades de seguridad que optimicen el sistema en lo referente a la detección de intrusos.
- Se ha diseñado un sistema de configuración y monitorización a través del cual el usuario sea capaz de configurar todas las funcionalidades del sistema y obtener la información referente a los ataques que se han sufrido en la red.
- Se han llevado a cabo una serie de pruebas de funcionamiento y rendimiento, las cuales han sido todas satisfactorias y nos han confirmado que el sistema obtenido del proyecto es un sistema potente y fiable.

8.2 Trabajo futuro

Aunque el resultado de la implementación del sistema ha sido satisfactorio, se pretende llevar a cabo una serie de ampliaciones y mejoras al sistema Antikörper. Entre estas ampliaciones y mejoras predominan las siguientes:

- Permitir la implementación y la integración de complementos que amplíen las funcionalidades del sistema fácilmente, sin que conlleven cambios en el código.
- Añadir funciones de medición **QoS** (**Q**uality **o**f **S**ervice) en el sistema.
- Distribuir el funcionamiento del sistema, de manera que se integren en las máquinas a proteger pequeñas aplicaciones que informen de la situación de la red e informen de alertas, pudiendo llegar a tomar acciones en la propia máquina. Todo esto manteniendo el núcleo del sistema con los procesadores de tráfico en una máquina independiente.
- Integrar en el sistema una base de firmas más extensa y fácilmente ampliable, junto con un procesador de tráfico heurístico.

Bibliografía

1. Bace, R. *Intrusion Detection*. s.l. : Sams Publishing, 2000.

2. *IEEE 802.11™: Wireless LANs*. s.l. : IEEE Standards.

3. Code::Blocks. [En línea] The Code::Blocks Team. http://www.codeblocks.org/.

4. Eclipse. [En línea] Eclipse Foundation. https://eclipse.org/.

5. d'Otreppe, Thomas. Aircrack-ng. [En línea] http://www.aircrack-ng.org/.

6. Kershaw, Mike. Kismet. [En línea] https://www.kismetwireless.net/.

7. Ornaghi, Alberto y Valleri, Marco. Ettercap. [En línea] http://ettercap.github.io/ettercap/about.html.

8. Microsoft Office. [En línea] Microsoft. https://www.office.com/start/default.aspx.

9. ISO 8601. [En línea] http://www.iso.org/iso/home/standards/iso8601.htm.

10. Kernighan, Brian W. y Ritchie, Dennis M. *The C Programming Language*. 1978.

11. (IETF), Internet Engineering Task Force. *Remote Authentication Dial In User Service (RADIUS)*. 1997.

12. Kumar, Ajoy. Fernandez, Eduardo B. *Security Pattern for Intrusion Detection System*. 2012.

13. Snort. The Open Source Network Intrusion Detection System. [En línea] https://www.snort.org/.

14. *Address Resolution Protocol (ARP)* . s.l. : Internet Engineering Task Force (IETF).

15. Geier, Jim. *802.11 Beacons Revealed*.

16. -. *Extensible Authentication Protocol (EAP)*. s.l. : Internet Engineering Task Force (IETF).

17. *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*. s.l. : Jefatura del Estado.

18. *Open System Interconnection (OSI)*. s.l. : International Organization for Standardization (ISO).

19. *IEEE Std 802-1990: IEEE Standards for Local and Metropolitan Networks: Overview and Architecture*. s.l. : IEEE Standards Association, 1990.

20. *802.3-2012*. s.l. : IEEE Standards Association.

21. Peterson, W. W. Brown, D. T. *Cyclic Codes for Error Detection*. 1961.

22. [En línea] Wi-Fi Alliance. http://www.wi-fi.org/.

23. *Advanced Encryption Standard (AES)*. s.l. : National Institute of Standards and Technology (NIST), 2001.

24. Peslyak, Alexander. John the Ripper. [En línea] http://www.openwall.com/john/.

25. Requirements for Internet Hosts -- Communication Layers. [En línea] Internet Engineering Task Force (IETF). http://tools.ietf.org/html/rfc1122.

26. AirMagnet. [En línea] Fluke Networks. http://es.flukenetworks.com/products/airmagnet-survey.

27. AirDefense Services Platform. [En línea] Motorola. http://www.motorolasolutions.com/US-EN/Business+Product+and+Services/Software+and+Applications/WLAN+Management+and+Security+Software/AirDefense+WIDS+WIPS.

28. MySQL. [En línea] Sun Microsystems. http://www.mysql.com/.

29. Fontanini, Matias. dot11decrypt. [En línea] https://github.com/mfontanini/dot11decrypt.

30. libtins: packet crafting and sniffing library. [En línea] http://libtins.github.io/.

31. Anderson, James P. *Computer Security Threat Monitoring and Surveillance*. 1980.

32. Natarajan Meghanathan, Selma Boumerdassi, Nabendu Chaki, Dhinaharan Nagamalai. *Recent Trends in Network Security and Applications*. s.l. : Springer Science & Business Media, 2010.

33. (IETF), Internet Engineering Task Force. [En línea] http://www.ietf.org/rfc/rfc0826.txt.

Glosario

Alarmas: Señal con la cual se informa sobre la presencia real o inminente de una amenaza.

Anómalo: Todo aquello que está fuera de lo que se considera como normal.

Ataque Activo: Ataques que interfieren de alguna forma en el flujo de datos de la red.

Ataques de Descubrimiento De Contraseña: Se basan en tratar de descubrir contraseñas de acceso al sistema o claves de cifrado de los datos que viajan por la red.

Ataques De Fuerza Bruta: Se crea un procedimiento que intenta romper un cifrado mediante la prueba de todas las combinaciones posibles.

Ataques Pasivos: El atacante monitoriza la red obteniendo así información referente a ella.

Auditorias De Seguridad: Comprende el análisis y gestión de sistemas llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Autenticación: Es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

Base de Datos De Firmas de Anomalías: Registro de patrones de anomalías conocidas.

Cifrado: procedimiento que utiliza un algoritmo de cifrado con cierta clave transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.

Código Abierto: Expresión con la que se conoce al software distribuido y desarrollado libremente.

Desencriptación: Proceso contrario a la encriptación.

Dirección IP: Número único e irrepetible con el cual se identifica una máquina conectada a una red IP.

Dirección MAC: identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

Distros: Distribución Linux, es una distribución de software basada en el núcleo Linux.

Encriptación: Utilización de cifrado.

Espectro: Distribución energética del conjunto de las ondas electromagnéticas.

Estándar IEEE 802.11: Define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

Fuentes De Tráfico: Origen de tráfico de red.

Hexadecimal: Es un sistema de numeración posicional que tiene como base el 16.

IDS Basados En Patrones: Mantienen una base de datos de ataques conocidos y sus correspondientes patrones de ataques, mediante los cuales son capaces de identificar un ataque.

IDS Estadístico: Detecta usuarios o comportamientos del sistema anómalos. Para ello, realiza un perfil de cada usuario de la red y, a raíz de esto, analiza el comportamiento de cada usuario en busca de algún tipo de desviación frente a su comportamiento normal.

Interfaz de red: Periférico que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras.

Modo Monitor: Modo de funcionamiento de las tarjetas de red inalámbricas con el cual un equipo es capaz de recibir todo el tráfico de la red, sea dirigido a él o no, sin estar asociado a ningún punto de acceso.

Modo Promiscuo: Igual al modo Monitor, pero siendo necesaria la asociación al punto de acceso.

Multiplataforma: Capaz de funcionar sobre diferentes sistemas.

Paquetes de red: Bloques en que se divide, en el nivel de Red, la información que enviar.

Patrones De Comportamiento: Modo de comportamiento típico de un elemento.

Preprocesador: Programa separado que es invocado por el compilador antes de que comience la traducción real.

Protocolo de Comunicaciones: Conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física.

Punto de Acceso inalámbrico: Dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica.

Redes De Ordenadores: Conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Redes Privadas: Una *Red privada* es una red que utiliza un espacio de direcciones IP privado. Por ejemplo, en redes domésticas o empresariales.

Seguridad Informática: Área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

Servidor: Nodo que, formando parte de una red, provee servicios a otros nodos denominados clientes.

Servidor Radius: Servidor que utiliza el protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP conocido como Radius (*Remote Authentication Dial-In User Service*).

Sistemas Detectores de Intrusos: Programa usado para detectar accesos no autorizados a un computador o a una red

Tarjeta de Red: Véase "Interfaz de red".

Trabajo De Fin De Grado (TFG): Consiste en un trabajo original que el alumno, con ayuda de un tutor, deberá realizar al final de su carrera y con el que deberá demostrar que ha adquirido los conocimientos, capacidades y aptitudes previstas en el plan de estudios de su titulación.

Glosario de términos anglosajones

Access Point (AP): Véase "Punto de Acceso Inalámbrico".

Address Resolution Protocol (ARP): Protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

Advanced Encryption Standard (AES): Esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Adoptado como método de codificación en WPA2.

American Standard Code for Information Interchange (ASCII): Código de caracteres basado en el alfabeto latino, tal como se usa en inglés moderno.

Bandwidth: Medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él (ciento setenta y dos, Mbit/s, entre otros).

Basic Service Set Identifier (BSSID): Nombre de identificación único de todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. Se forma con la dirección MAC (Media Access Control) formada por 48 bits (6 bloques hexadecimales), del Punto de acceso inalámbrico.

Beacon Frames: Uno de los marcos de administración en redes inalámbricas WLAN basadas en IEEE 802.11. Los Beacon Frames contienen toda la información sobre la red inalámbrica y son transmitidos periódicamente para anunciar la presencia de la red WLAN.

Denial of Service (DoS): Ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Dynamic Host Configuration Protocol (DHCP): Protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

Extensible Authentication Protocol over IEEE 802 (EAPOL): Provee algunas funciones comunes y negociaciones para el o los mecanismos de autenticación escogidos. Estos mecanismos son llamados métodos EAP. Utilizadas en autenticación en WLAN sobre WPA2.

Gateway: Equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation).

Hijacking: Generalmente secuestro de una conexión TCP/IP.

Host: Se refiere a las computadoras conectadas a una red.

Host Based IDS: IDSs instalados en los host de la red y solo monitorizan el tráfico dirigido u originado en ese host.

Internet: Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

Internet Protocol (IP): Protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI.

Intrusion Detection System (IDS): Véase "Sistemas Detectores de Intrusos".

IP Spoofing: Suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.

Jamming: Uso de una señal de alta potencia para así interferir en el espectro e inhabilitar distintos servicios inalámbricos.

MAC Filtering: Método de control de acceso mediante el filtrado de la autenticación de usuario en función de sus direcciones MAC.

Man in the Middle (MiTM): Ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

Managed Security Service Provider (MSSP): ISP que ofrece servicios de seguridad de distintos tipos.

Network Based IDS: IDSs colocados estratégicamente en una red para detectar cualquier ataque contra los host de esa red.

Node: Máquinas dentro de una red de computadores.

Open System Interconnection (OSI): Marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

Password: Forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

Rogue AP: Punto de acceso sin autorización que se ha conectado a una red segura existente. Estos se convierten en una fuente de todo tipo de ataques debido a que permiten una conexión sin ningún tipo de seguridad a través de ellos.

Service Set Identifier (SSID): Nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

Smurf: Ataque en el que el atacante envía grandes cantidades de tráfico ICMP a la dirección de broadcast, todos ellos teniendo la dirección de origen cambiada a la dirección de la víctima. De este modo los ordenadores responderán aumentando el tráfico de la red y pudiendo llegar a inhabilitar la red.

Software: Es el soporte lógico e inmaterial que permite que la computadora pueda desempeñar tareas inteligentes, dirigiendo a los componentes físicos o hardware con instrucciones y datos a través de diferentes tipos de programas.

Spoofing: Uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Structured Query Language (SQL): Lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas.

TCP/IP: Conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.

TKIP (Temporal Key Integrity Protocol): También llamado hashing de clave WEP/WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos.

Warchalking: Lenguaje de símbolos normalmente escritos con tiza en las paredes que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.

Wardriving: Búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento.

Wi-fi Protected Access (WPA): Sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP).

Wired Equivalent Privacy (WEP): Sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

Wireless Local Area Network (WLAN): Sistema de comunicación inalámbrica flexible, muy utilizada como alternativa a las redes de área local cableada o como extensión de estas.

Recursos

Productos

Kismet

http://www.kismetwireless.net/

Aircrack

http://www.aircrack-ng.org/

NetStumbler

http://www.netstumbler.com/

AirMagnet

http://es.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Survey

AirDefense

http://www.motorolasolutions.com/USEN/Services/Run/Network+Infrastructure+Management/IT/AirDefense_Services_Platform

dot11decrypt

https://github.com/mfontanini/dot11decrypt

Organizaciones

SANS institute

http://www.sans.org/

Computer Security Institute

http://urlm.co/www.gocsi.com

Information Systems Audit and Control Association

https://www.isaca.org/

Information Systems Security Association

https://www.issa.org/

International Information Systems Security Certification Consortium

https://www.isc2.org/

Internet Engineering Task Force

https://www.ietf.org/

Institute of Electrical and Electronics Engineers (IEEE)

http://standards.ieee.org/about/get/802/802.11.html

Páginas de Noticias

InfoSysSec

www.infosyssec.com/

elhacker.NET

www.elhacker.net/hacking.html

Underc0de

http://underc0de.org/

Anexo I – Manual de usuario

A continuación se incluyen las instrucciones para el uso del Sistema de Detección de Intrusiones *Antikörper*.

El sistema se separa en dos programas independientes, AntikörperCore y AntikörperAP, los cuales ofrecen detección de intrusos dentro de la red y detección de Rogue APs respectivamente. Cada uno de ellos dispone un interfaz de configuración y un interfaz de visualización de datos que permiten al usuario la utilización sencilla de todas las funcionalidades del sistema.

Antikörper incluye soporte para todas las versiones del protocolo 802.11 y todos los mecanismos de seguridad existentes.

A1.1 Requisitos del Sistema

A continuación, se presentan los requisitos software y hardware que precisa el sistema para su funcionamiento.

A1.1.1 Requisitos software

El sistema precisa de los siguientes componentes software.

- Sistema operativo GNU/Linux
- Compilador GNU GCC
- Compilador GNU G++ (solo para AntikörperCore)
- Librería libpcap 1.3 o superior
- Librería libtins (solo para AntikörperCore)
- 25 MB de espacio libre en el disco duro

A1.1.2 Requisitos hardware

Los siguientes requisitos hardware son los recomendados para el sistema tras haber probado el rendimiento de este en equipos con distintas características.

- Procesador: 2.0 GHz o superior
- Memoria: 4GB RAM
- Interfaz WLAN 802.11 b/g/n con soporte monitor para la captura de tráfico

- Interfaz WLAN 802.11 b/g/n con soporte monitor para la inyección de tráfico

A1.2 Instalación

El sistema Antikörper se distribuye en un paquete .tar.gz, el cual contiene tanto el programa AntikörperCore como AntikörperAP. Para descomprimir el paquete se puede hacer uso de las herramientas disponibles en Linux.

```
$ tar -xzvf Antikorper.tar.gz
$ ls
Antikorper  Antikorper.tar.gz
$ cd Antikorper
$ ls
AntikorperAP  AntikorperCore
```

Una vez descomprimida la carpeta, se han de instalar ambos programas por separado. Para ello, se hará uso del script *configure*, el cual comprobará que se disponen en el equipo de todos los requisitos necesarios para el funcionamiento del sistema. Se realizará de la siguiente manera:

```
$ cd AntikorperCore
$ ./configure

$ cd AntikorperAP
$ ./configure
```

A continuación, se compilará el código fuente de cada programa desde su directorio correspondiente:

```
$ make
```

Por último se instalarán los programas de la siguiente manera, ejecutando el comando como administrador:

```
# make install
```

En caso de necesitar desinstalar alguno de los programas, se ejecutará el siguiente comando desde el directorio donde se encuentra su código fuente:

```
# make uninstall
```

A1.3 Guía de uso de Antikörper

A continuación, se muestra la guía de uso del sistema Antikörper, la cual se encuentra dividida en dos manuales. En el primero, se encontrará el manual de AntikörperCore, y en el segundo, el correspondiente a AntikörperAP.

A1.3.1 Manual de AntikörperCore

AntikörperCore será el programa encargado del análisis del tráfico WLAN perteneciente a la red sobre la que está desplegado.

Se arrancará el programa con el siguiente comando:

```
# antikorpercore
```

AntikörperCore arrancará solicitando información referente a la red a proteger.

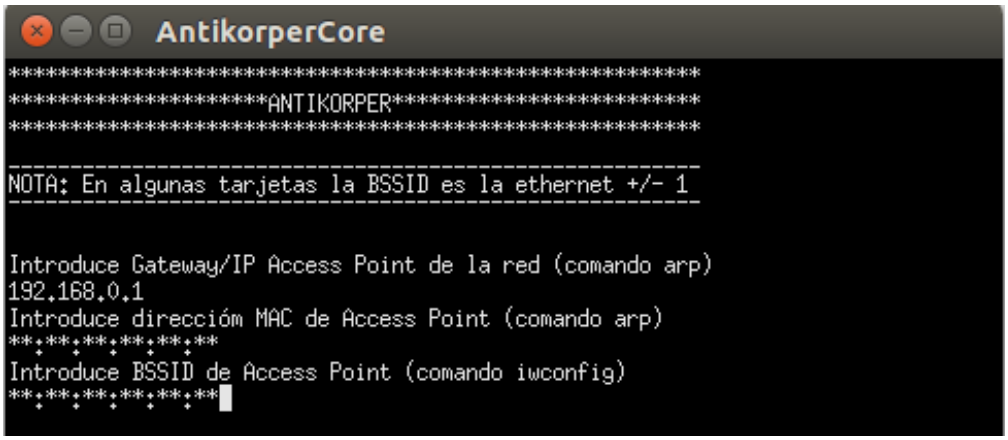


Figura A1-1: Configuración de AntikörperCore

La Figura A1-1 muestra el interfaz de configuración que facilita el sistema, a través del cual se pedirá al usuario la dirección IP del Gateway y las direcciones físicas del AP.

Una vez introducida la configuración, se mostrará un menú con las distintas opciones a las que puede acceder el usuario. Este se puede observar en la Figura A1-2.

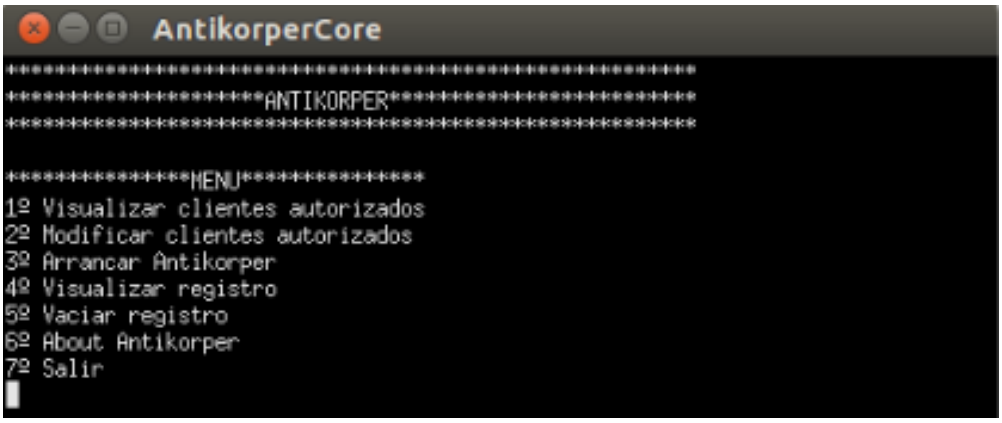


Figura A1-2: Menú de selección de AntikörperCore

El menú nos permite elegir entre las siguientes opciones:

1. **Visualizar clientes autorizados.** Se mostrará un listado con las direcciones MAC pertenecientes a las máquinas autorizadas en la red.
2. **Modificar clientes autorizados.** Permite la inserción, la modificación y la eliminación de las entradas pertenecientes a las máquinas autorizadas en la red.
3. **Arrancar Antikörper.** Se iniciará la búsqueda de intrusos en la red.
4. **Visualizar registro.** Mostrará el registro de intrusiones detectadas por el sistema.
5. **Vaciar registro.** Vaciará el registro de intrusiones
6. **About Antikörper.** Muestra información referente al sistema.
7. **Salir.** Nos permite apagar el sistema.

Una vez seleccionemos la opción *Arrancar Antikörper*, el menú mostrado en la Figura A1-3 pedirá al usuario que seleccione el interfaz desde el que capturar el tráfico a analizar.

Figura A1-3: Menú de selección de interfaz de AntikörperCore

Al seleccionar el interfaz, el sistema comenzará a analizar el tráfico de la red en busca de máquinas intrusas y envenenamiento ARP. En caso de encontrar alguna anomalía, mostrará a través del interfaz de visualización mostrado en la Figura A1-4 y en la Figura A1-5 cuál es la incidencia.

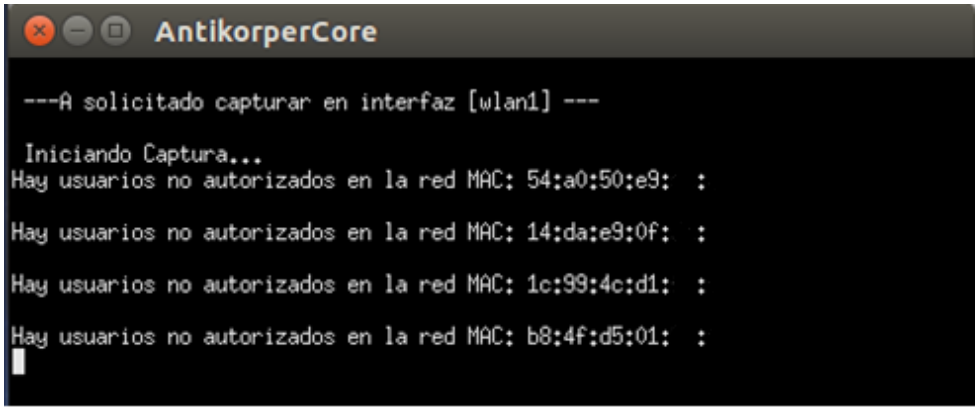


Figura A1-4: Detección de máquinas intrusas

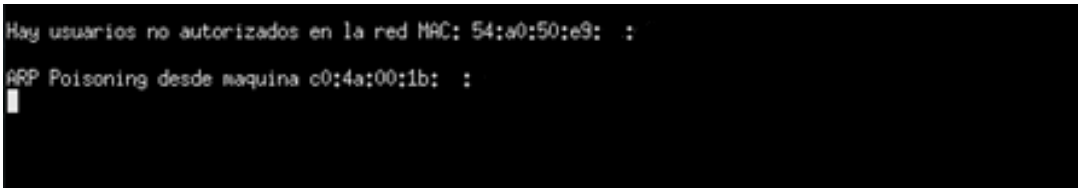


Figura A1-5: Detección de ARP Spoofing

A1.3.2 Manual de AntikörperAP

AntikörperAP será el programa encargado del análisis del tráfico RAW 802.11 en busca de Access Point maliciosos.

Podremos arrancar el programa con el siguiente comando:

```
# antikorperap
```

AntikörperAP arrancará solicitando información referente a la red a proteger.

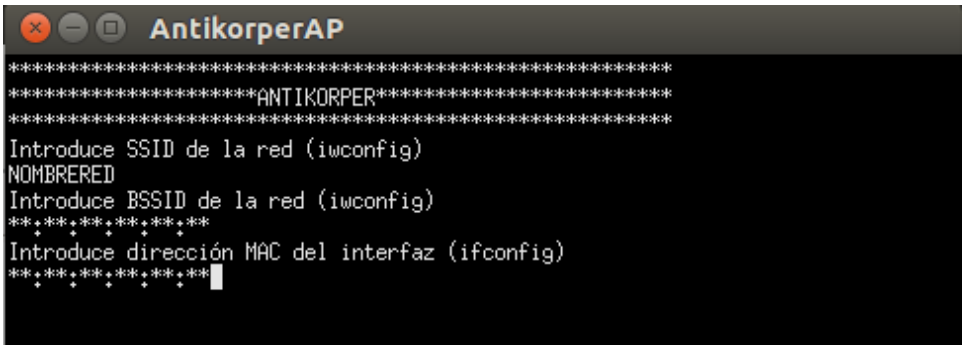


Figura A1-6: Configuración de AntikörperAP

La Figura A1-6 muestra el interfaz de configuración de AntikörperAP, a través del cual se solicita el SSID y el BSSID del Access Point oficial de la red, junto a la dirección física del interfaz de respuesta frente a intrusiones.

Una vez introducida la configuración, se mostrará un menú con las distintas opciones a las que puede acceder el usuario. Este se muestra en la Figura A1-7.

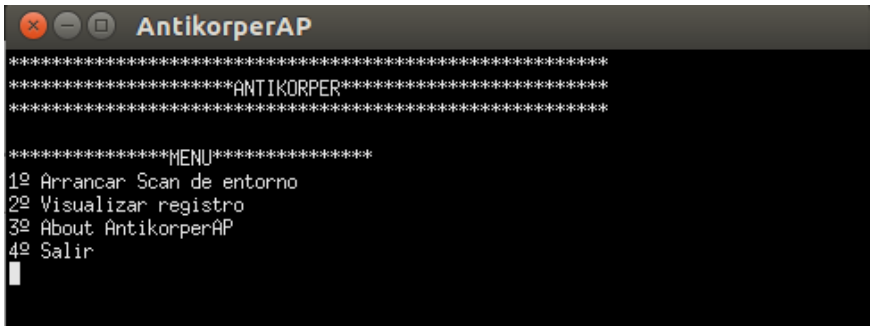


Figura A1-7: Menú de selección de AntikörperAP

El menú nos permite elegir entre las siguientes opciones:

1. **Arrancar Scan de entorno.** Se iniciará la captura y el análisis de tráfico RAW 802.11 en busca de Rogue APs.
2. **Visualizar registro.** Mostrará el registro de Rogue APs detectados por el sistema.
3. **About Antikörper.** Muestra información referente al sistema.
4. **Salir.** Nos permite apagar el sistema.

Una vez seleccionemos la opción Arrancar Scan de entorno, el menú mostrado en la Figura A1-8 pedirá al usuario que seleccione el interfaz desde el que capturar el tráfico a analizar.

Figura A1-8: Menú de selección de interfaz de AntikörperAP

Al seleccionar el interfaz, el sistema comenzará a analizar el tráfico en busca de Rogue APs. En caso de encontrar alguna anomalía, mostrará a través del interfaz de visualización mostrado en la Figura A1-9 la información referente al ataque.

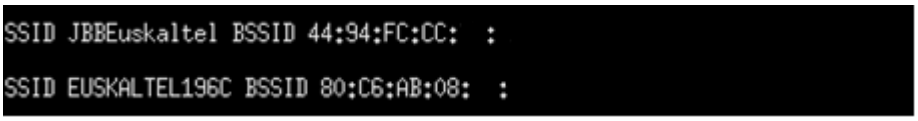


Figura A1-9: Detección de Rogue APs

Anexo II – Estructuras de descomposición

A2.1 Work Breakdown Structure (WBS)

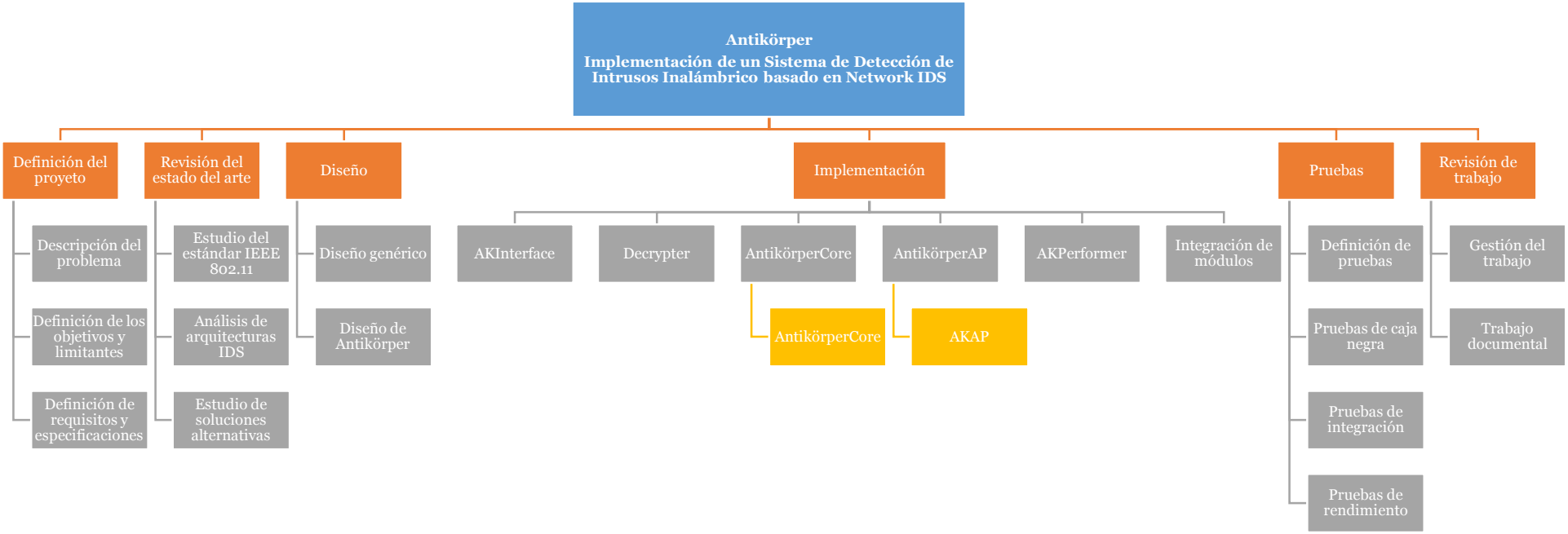


Figura A2-1: Work Breakdown Structure (WBS)

A2.2 Product Breakdown Structure (PBS)

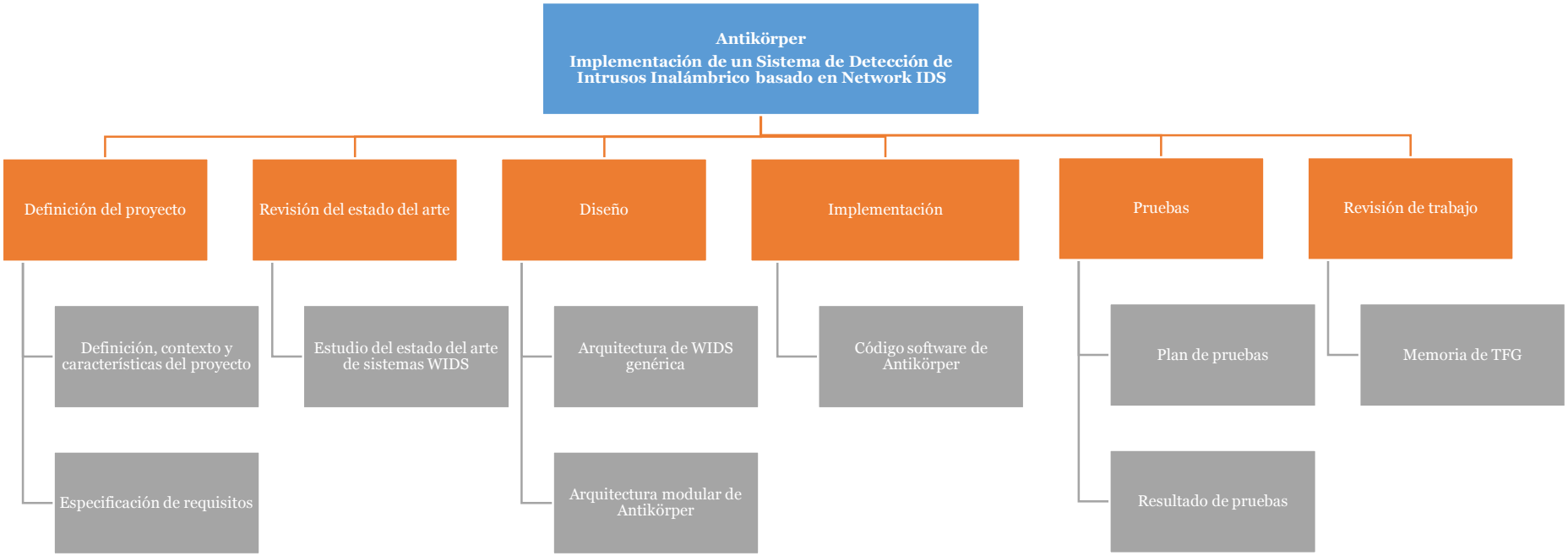


Figura A2-2: Product Breakdown Structure (PBS)

A2.3 Resource Breakdown Structure (RBS)

A2.3.1 Recursos humanos

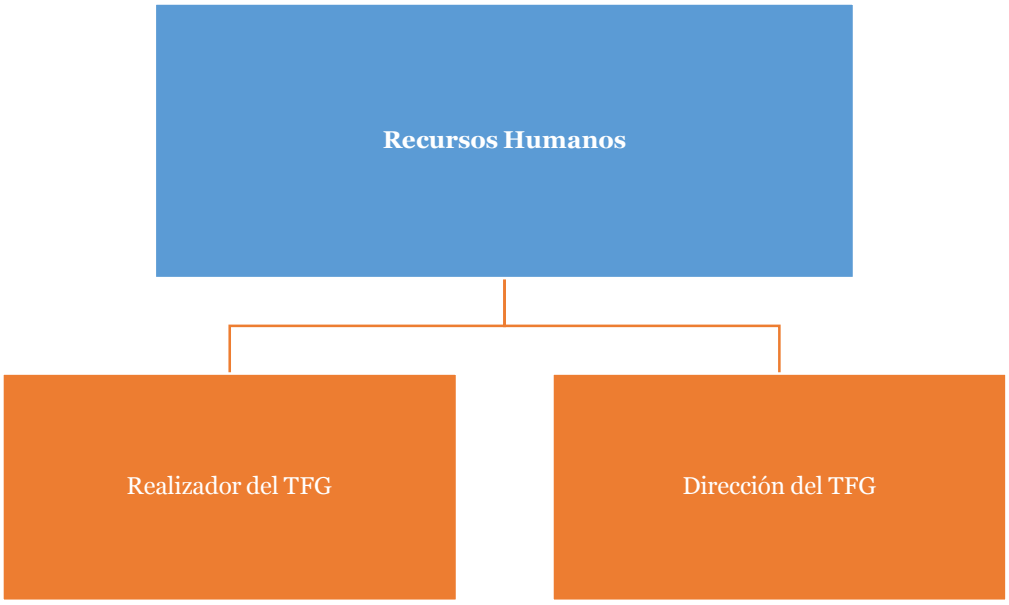


Figura A2-3: Resource Breakdown Structure (RBS) – Recursos humanos

A2.3.2 Recursos materiales

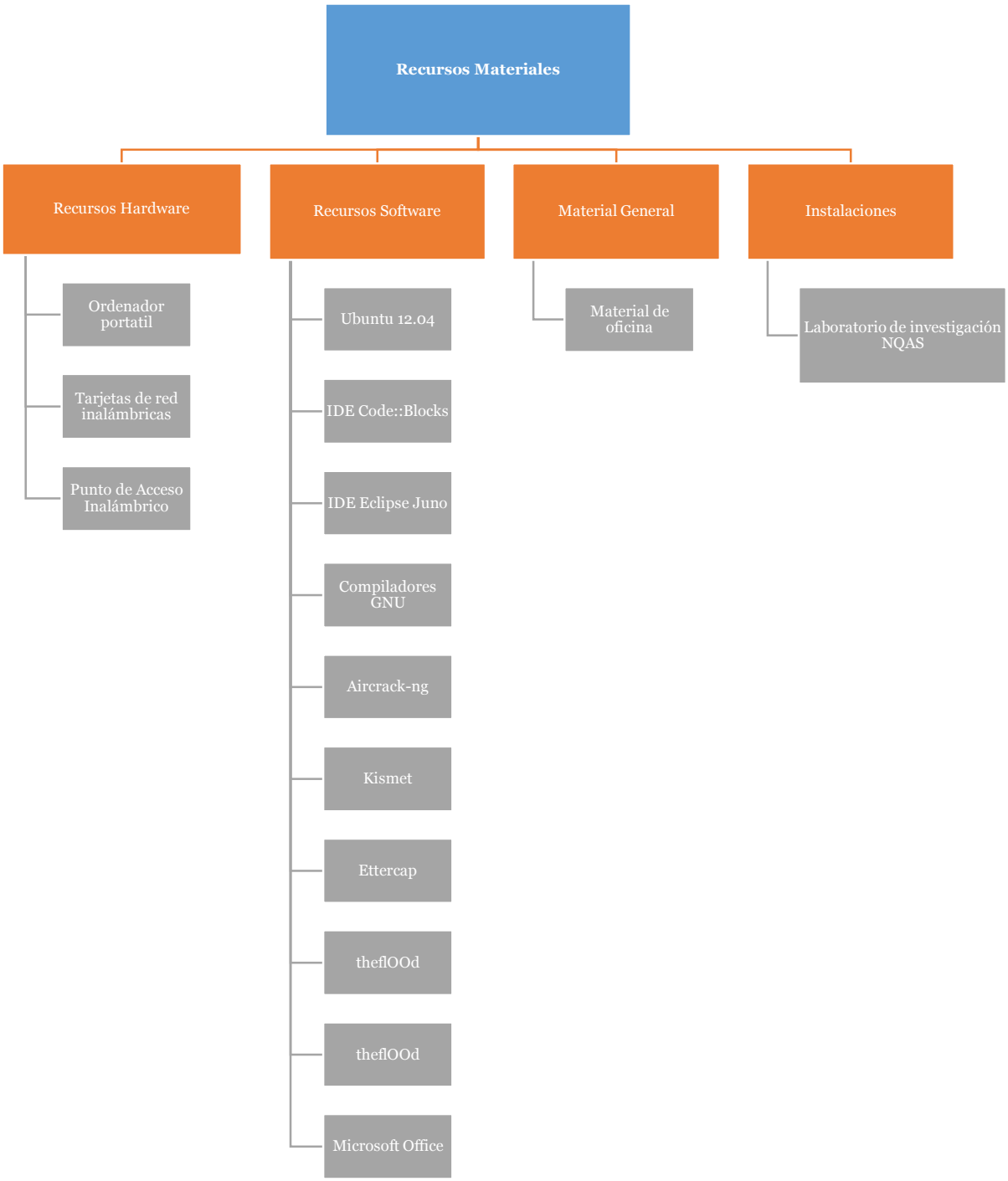


Figura A2-4: Resource Breakdown Structure (RBS) – Recursos materiales

Anexo III – Estudio del estado del arte

A continuación se procederá a introducir el estado actual de las redes **W**ireless **LAN** (**WLAN**) junto con una clasificación de los ataques que se pueden llegar a sufrir en ellas. Tras ello, se hará una clasificación de los sistemas que proporcionan servicios de detección de intrusiones en estas redes.

A3.1 Escenario de las redes WLAN

En 1997 fue aprobado el estándar 802.11 (2), un estándar que regulaba las transmisiones inalámbricas de datos en redes locales permitiendo así la interconexión de diversos equipos. Este fue el primero de una serie de estándares los cuales, en cada versión, iban añadiendo importantes funcionalidades a esta tecnología. Hoy en día, podemos encontrar la tecnología WLAN basada en 802.11 en su versión ac, la cual permite la interconexión de innumerables equipos permitiendo unas velocidades de transmisión teóricas de 1 Gbit/s.

Actualmente, esta tecnología esta implementada en la mayoría de las redes locales, debido a su facilidad de implementación y la opción de movilidad que tanto se requiere hoy en día. Esto se debe a que cualquier equipo, ya sea un PC, tablet o teléfono móvil, que posea una tarjeta de red inalámbrica, nos da acceso a este tipo de redes.

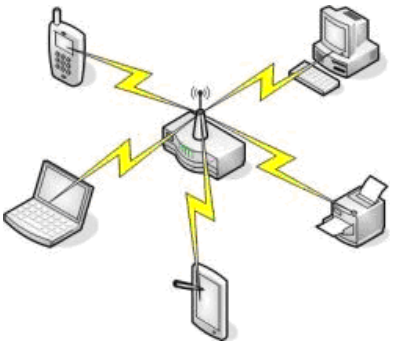


Figura A3-1: Escenario genérico de red WLAN

Hasta aquí las redes inalámbricas parecen tener solo beneficios frente a las redes cableadas, pero uno de los principales problemas de las redes WLAN es precisamente la seguridad, ya que cualquier usuario con un terminal inalámbrico podría comunicarse con un punto de acceso privado, si no se disponen de las medidas de seguridad adecuadas.

En lo referente a la autenticación, un usuario o estación móvil debe identificarse antes de asociarse a un **A**ccess **P**oint (**AP**) o router de banda ancha, para así obtener acceso a la red inalámbrica local. Este proceso se realiza a nivel 2 del modelo OSI (18). Por otro lado, los mecanismos cifrados aseguran que no sea posible decodificar el tráfico de usuario.

Esto parece solucionar los compromisos a la seguridad de WLAN, pero debemos tener en cuenta que estas técnicas no son perfectas y un atacante con conocimiento suficiente puede atravesarlas y acceder a la red para hacer uso de ella, acceder a los equipos que se encuentran en esta y ver el tráfico que se transmite por la red.

Tras ver los problemas que conlleva sufrir un ataque en una red WLAN, se ve necesario un sistema capaz de detectar a estos intrusos que intentan acceder a esta, ya sea para monitorizar el tráfico o para realizar cualquier ataque activo.

A3.2 Evolución del estándar IEEE 802.11

802.11 es un miembro de la familia 802 de IEEE (19), la cual agrupa una serie de especificaciones para redes de área local (LAN). En concreto, el grupo de 802.11 define una serie de protocolos de nivel de enlace y físico para redes inalámbricas. A lo largo del desarrollo de esta tecnología apreciamos distintos hitos, donde los más importantes son los siguientes:

- 802.11 (1997): Primera publicación del estándar que define control de acceso al medio **MAC** (**M**edia **A**ccess **C**ontrol) y nivel físico.
- 802.11a y 802.11b (1999): Mayores velocidades, la primera trabaja en la banda de los 5 GHz con una velocidad máxima de 48 Mbit/s y la segunda en la de los 2.4 GHz con velocidad máxima de 11 Mbit/s.
- 802.11g (2003): Evoluciona de 802.11b (misma banda de frecuencia) y es retrocompatible. Alcanza una velocidad máxima teórica de 54 Mbit/s, con una media de 22 Mbit/s.
- 802.11n (2008, ratificado en 2009): Actualmente el más extendido. 10 veces más rápido que 802.11a y 802.11g, con velocidades máximas teóricas de alrededor de 500 Mbit/s y velocidades reales de 100Mbit/s. Opera tanto en la banda de 5 GHz como en la de 2.4 GHz.
- 802.11ac (2014): Mejora de 802.11n, velocidades teóricas de 1 Gbit/s.
- 802.11ad, 802.11ah (Actualmente en desarrollo).

Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna technologies	Maximum data rate
1997	802.11	2.4	20	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4, 5	20, 40	OFDM	MIMO, up to four spatial streams	600 Mbits/s
2012 (expected)	802.11ad	60	2160	SC, OFDM	Beamforming	6.76 Gbits/s
2013 (expected)	802.11ac	5	40, 80, 160	OFDM	MIMO, MU-MIMO, up to eight spatial streams	6.93 Gbits/s

Tabla A3-1: Estándares 802.11 de capa física

A3.3 Elementos de una red WLAN

Las redes 802.11 están compuestas principalmente por cuatro componentes físicos, estos se pueden apreciar en la Figura A3-1:

- **Estaciones (STA, Station)**

Las estaciones son los elementos básicos que hacen uso de las redes para transferir datos. Estos, al encontrarse en un entorno inalámbrico, han de disponer de una tarjeta de interfaz de red inalámbrica Las estaciones son dispositivos informáticos con interfaces de red inalámbrica.

- **Puntos de acceso (AP, Access Point)**

Los puntos de acceso son las puertas de enlace de las estaciones a Internet. Realizan la función de puente entre la red inalámbrica y la cableada.

- **Medio inalámbrico (WM, Wireless Medium)**

Para mover las tramas de una estación a otra, el estándar 802.11 utiliza el medio inalámbrico mediante ondas electromagnéticas. Este contempla tres capas físicas: 2 capas físicas de radiofrecuencia y una de infrarrojos, aunque las capas RF han resultado ser mucho más populares.

A3.4 Tramas MAC 802.11

El estándar IEEE 802.11 define varios tipos de tramas, de las cuales cada una tiene un objetivo específico. En las redes WLAN encontramos la necesidad de anunciar los puntos de acceso, asociar estaciones, autenticar clientes y otras funciones. Todas estas funciones normalmente se gestionan mediante unas tramas especiales, a parte de las tramas propias de transmisión de datos. A continuación se expondrán las principales características de las tramas 802.11 y se hará especial hincapié en las tramas de control, debido a su importancia en el desarrollo del proyecto.

A3.4.1 Formato de la trama

Para cubrir las necesidades de un enlace inalámbrico, la capa MAC se vio obligada a adoptar una serie de características únicas, como es el uso de 4 campos de dirección. Sin embargo no todas las tramas hacen uso de los 4 campos de dirección, y el valor de dichos campos depende además del tipo de trama MAC. La Figura A3-2 muestra la estructura de una trama 802.11 MAC genérica:

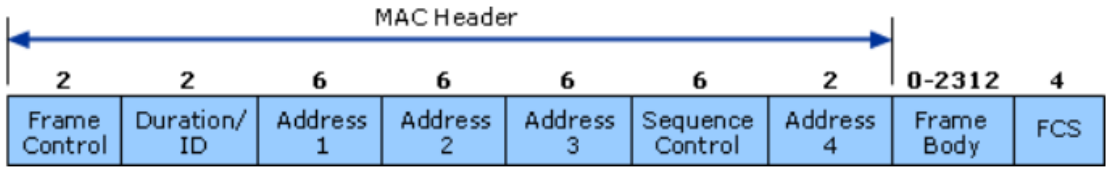


Figura A3-2: Trama 802.11 MAC genérica

- **Frame Control**

El campo Control Frame, que se muestra en la Figura A3-3, contiene información de control que se utiliza para definir el tipo de trama 802.11 MAC y proporciona la información necesaria para saber cómo procesar la trama MAC.

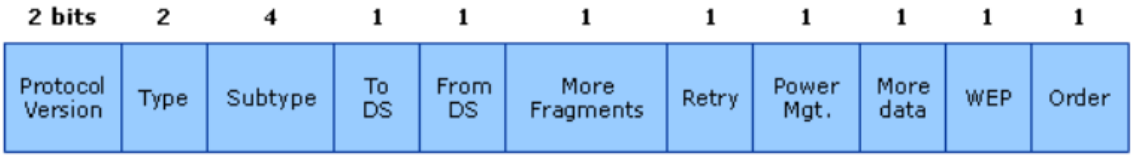


Figura A3-3: Campo Frame Control de trama 802.11

- **Duration/ID**

El campo Duration indica el tiempo mínimo restante para recibir la siguiente trama.

- **Address Fields**

Dependiendo del tipo de trama, los cuatro campos de dirección contendrán una combinación de los siguientes tipos de direcciones:

- **B**asic **S**ervice **S**et **I**dentifier **(BSSID).** La dirección BSSID identifica inequívocamente el tráfico de una red. Cuando la trama proviene de una STA, la BSSID es la dirección MAC del AP.

- **D**estination **A**ddress **(DA).** La dirección DA indica la dirección MAC del destinatario final de la trama.

- **S**ource **A**ddress **(SA).** La dirección SA indica la dirección MAC de la Fuente original que creó y transmitió la trama.

- **R**eceiver **A**ddress **(RA).** La dirección RA indica la dirección MAC de la siguiente STA de la WLAN en recibir la trama.

- **T**ransmitter **A**ddress **(TA).** La dirección TA indica la dirección MAC de la STA que introdujo la trama en el medio inalámbrico STA.

- **Sequence Control**

El campo Sequence Control contiene dos subcampos, el campo Sequence Number y el campo Fragment Number, como se muestra en la Figura A3-4.

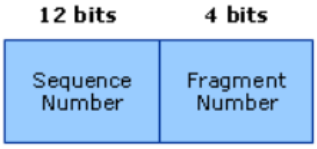


Figura A3-4: Campo Sequence Control de trama 802.11

- **Sequence Number** indica el número de secuencia de cada trama. El número de secuencia es la misma para cada trama enviada aunque esté fragmentada.

- **Fragment Number** indica el número de cada trama enviada de una trama fragmentada. El valor inicial se establece a 0 y luego se incrementa en uno por cada trama subsiguiente enviada de la trama fragmentada.

- **Frame Body**

Desplaza la carga útil de la capa superior de una estación a otra.

- **FCS (Frame Check Sequence)**

La trama 802.11, se cierra con una secuencia de comprobación de trama (**FCS**, **F**rame **C**heck **S**equence) (20). Normalmente, FCS se conoce como comprobación de redundancia cíclica (**CRC**, **C**yclic **R**edundancy **C**heck) (21), debido a las operaciones matemáticas subyacentes. FCS permite a las estaciones comprobar la integridad de las tramas recibidas. Todos los campos en el encabezado MAC y en el cuerpo de la trama se incluyen en la FCS. Cuando se envían tramas a la interfaz inalámbrica, se calcula la FCS antes de que dichas tramas se envíen sobre el enlace inalámbrico. Los receptores pueden calcular posteriormente la FCS a partir de la trama recibida y compararla con la FCS recibida. Si las dos secuencias coinciden, existe una probabilidad muy alta de que la trama no se haya dañado durante el tránsito.

A3.4.2 Tipos de Tramas

- **Tramas de datos**

Las tramas de datos transportan datos de protocolo de nivel superior en el cuerpo de la trama.

- **Tramas de control**

Las tramas de control ayudan a la entrega de datos. Administran el acceso al medio inalámbrico y proporcionan funcionen de fiabilidad de la capa MAC.

- **Tramas de administración**

Debido a la importancia de estas tramas en el desarrollo del proyecto, haremos especial hincapié en ellas.

La administración es un componente importante en la especificación 802.11. En una red Ethernet la administración es muy sencilla, solo implica buscar la toma adecuada en la pared. 802.11 desglosa el procedimiento en tres componentes. Las estaciones móviles en busca de conectividad, primero, tienen que localizar una red inalámbrica disponible para el acceso. A continuación, la red tiene que autenticar las estaciones móviles para establecer que la identidad autenticada permita conectarse a la red. En la red con cable esto es automático, la red con cable equivalente se proporciona a través de la propia red. Por último, las estaciones móviles tienen que asociarse a un AP para obtener acceso a la red troncal, un proceso equivalente a conectar el cable a la red con cable. Todos los subtipos de tramas de

administración tienen el mismo encabezado. Las tramas de administración utilizan elementos de información, pequeños fragmentos de datos con una etiqueta numérica, para comunicar la información al resto de sistemas.

Este tipo de trama es bastante flexible. La mayoría de los datos contenidos en el cuerpo utilizan campos de longitud fija denominados campos fijos y campos de longitud variable conocidos como elementos de información. Cada elemento de información está etiquetado con un número de tipo y un tamaño y se entiende que un elemento de información de un tipo determinado tiene su propio campo de datos interpretado de una manera determinada.

Los campos fijos y los elementos de información se utilizan en el cuerpo de las tramas de administración para la comunicación. Existen diversos tipos de tramas de administración que se utilizan en distintas funciones de mantenimiento de la capa de enlace:

- **Beacon**: las tramas Beacon (15) anuncian la existencia de una red y constituyen un elemento importante para muchas tareas de mantenimiento de la red. Se transmiten a intervalos regulares (intervalo Beacon) para permitir a las estaciones móviles buscar e identificar una red así como parámetros de comparación para unirse a la misma. En una infraestructura de red, el AP es el responsable de transmitir las tramas Beacon. El área en la que aparecen estas tramas define el área de servicio básico.

- **Petición de Prueba (Probe Request)**: las estaciones móviles utilizan las tramas de petición de prueba para examinar un área en busca de redes 802.11 existentes.

- **Respuesta de Prueba (Probe Response)**: si una petición de prueba encuentra una red con parámetros compatibles, la red envía una trama de respuesta de prueba. El AP que envió la última Beacon es el responsable de responder a las pruebas entrantes (red infraestructura).

- **Autenticación (Authentication)**: las estaciones se autentican utilizando una clave compartida e intercambiando tramas de autenticación. Pueden coexistir distintos algoritmos de autenticación. El campo número de algoritmo de autenticación se utiliza para la selección de algoritmo. El proceso de autenticación puede implicar seguir diversos pasos (dependiendo del algoritmo), por lo que existe un número de secuencia para cada trama en el intercambio de autenticación.

- **Petición de Asociación (Association Request)**: cuando las estaciones móviles identifican una red compatible y la autentican pueden intentar unirse a la red enviando una trama de petición de asociación. El campo información de capacidad se utiliza para indicar el tipo de red al que desea unirse la estación móvil. Antes de que el conjunto de acceso acepte una

Petición de Asociación, comprueba que la información de capacidad, el **SSID** (**Service S**et **ID**entifier) y las velocidades admitidas coinciden con los parámetros de la red.

- **Respuesta de Asociación (Association Response)**: cuando las estaciones móviles intentan asociarse a un punto de acceso, este responde con una trama de Respuesta de Asociación. Todos los campos de la trama son obligatorios. Como parte de la respuesta, el AP asigna un ID de asociación.

- **Disociación y Desautenticación (Disassociation and Deauthentication)**: las tramas de Disociación se utilizan para finalizar una relación de asociación y las tramas de Desautenticación, para finalizar una relación de autenticación. Ambas tramas incluyen un solamente campo fijo, el código de razón. Los campos de control son diferentes, porque se trata de dos tipos diferentes de tramas.

TIPO Bits (3-2)	Descripción	Subtipo Bits (7-6-5-4)	Descripción
00	Administración	0000	Solicitud de asociación
00	Administración	0001	Respuesta asociación
00	Administración	0010	Solicitud re-asociación
00	Administración	1010	Disociación
00	Administración	1011	Autenticación
00	Administración	1100	Des-autenticación
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
10	Datos	0000	Datos

Tabla A3-2: Clasificación de tramas MAC 802.11

A3.5 Servicios de acceso y seguridad en redes WLAN

Estos servicios los podemos agrupar en 2 bloques principales:

A3.5.1 Autenticación

Un usuario o estación móvil debe identificarse antes de asociarse a un AP o router de banda ancha, para así obtener acceso a la red inalámbrica local. Este proceso se realiza a nivel 2 del modelo OSI (Open System Interconnection).

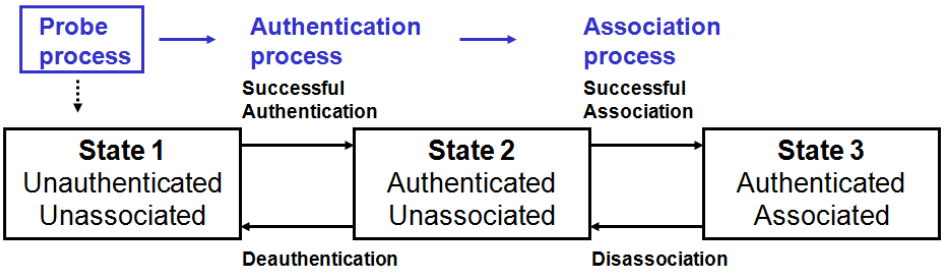


Figura A3-5: Procedimiento de asociación

En la Figura A3-5 podemos ver el procedimiento que sigue un host para obtener conectividad con un AP. En ella observamos como el host se autentica frente al AP, y tras eso, se asocia al AP obteniendo así acceso completo a la red.

Podemos diferenciar dos métodos de autenticación en la redes WLAN: Open System Authentication (OSA) y Shared Key Authentication (SKA):

A3.5.1.1 **O**pen **S**ystem **A**uthentication (**OSA**)

Esta autenticación consiste en dos pasos sencillos como podemos observar en la Figura A3-6. El primero es una petición de autenticación por parte del cliente que contiene la BSSID del AP. Esto es seguido por una respuesta de autenticación del AP portando un mensaje de éxito o de fallo. Un ejemplo de fallo puede ser cuando la dirección MAC del cliente está en la lista de excluidos del AP (MAC Filtering).

Figura A3-6: Procedimiento de asociación mediante OSA

A3.5.1.2 **S**hared **K**ey **A**uthentication (**SKA**)

Esta autenticación se basa en una clave que conocen tanto el host como el AP. El AP, para identificar una estación, envía un desafío en texto plano al host, el cual encripta el desafío utilizando la clave compartida. El AP encripta el mensaje también y cuando recibe el desafío encriptado del host los comparará, determinando si el host está autorizado o no. Podemos observar el procedimiento entre las dos entidades en la Figura A3-7.

Figura A3-7: Procedimiento de asociación mediante SKA

Aunque a priori podamos pensar que la SKA tiene ventajas en cuanto a seguridad frente a la OSA, en realidad es más insegura. Esto se debe a que cualquier intruso que consiga detectar el paquete de desafío (Authentication Challenge) y el mismo paquete cifrado con la clave compartida (Authentication Response) es capaz de generar la respuesta a cualquier desafío a pesar de desconocer la clave.

A3.5.2 Encriptaciones y mecanismos de seguridad

Son diversos los mecanismos de seguridad que se pueden aplicar en redes WLAN para evitar los ataques anteriormente descritos. Y como se puede observar en la Figura A3-8, actúan en diferentes capas del modelo OSI.

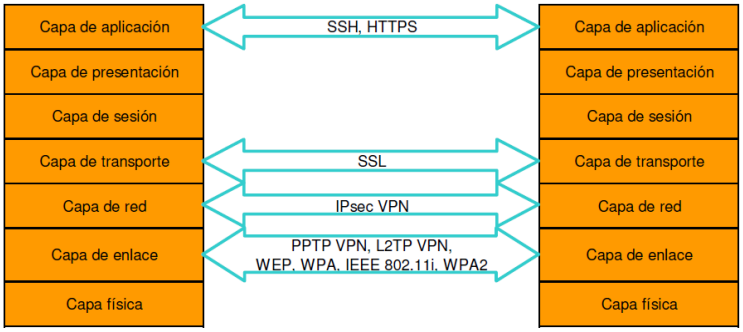


Figura A3-8: Mecanismos de seguridad por capas OSI

Nos centraremos en analizar los mecanismos de seguridad basados en el nivel de enlace.

A3.5.2.1 Mecanismos de seguridad a nivel de enlace

Como hemos explicado anteriormente, la seguridad en redes WLAN puede ser comprometida en dos aspectos: autenticación y cifrado. Los mecanismos de autenticación se emplean para identificar un usuario inalámbrico ante un punto de acceso y viceversa, mientras que los mecanismos cifrados aseguran que no sea posible decodificar el tráfico de usuario. Con ese objetivo, desde la aparición de las redes WLAN los protocolos del nivel de enlace desarrollados específicamente para dotarlas de seguridad han sido WEP, **WPA** (**W**i-Fi **P**rotected **A**ccess) y **WPA2** (**W**i-Fi **P**rotected **A**ccess v**2**).

- WEP

WEP es un protocolo de cifrado a nivel de enlace contenido en la especificación original de estándar IEEE 802.11. WEP permite cifrar los datos que se transfieren a través de una red inalámbrica y autenticar los dispositivos móviles que se conectan a sus puntos de acceso. Como se ha observado previamente, la autenticación se hace tanto en OSA como SKA, pero la utilidad del cifrado WEP se basa en que, aunque en OSA, se lleve a cabo la asociación y la autenticación, no se podrán transmitir paquetes porque no se conocerá la clave WEP con la que desencriptarlo. Por otro lado, en la SKA, la clave de autenticación será la clave WEP, por lo tanto, en caso de no conocerla no se podrá autenticar frente el AP.

En cuanto a la encriptación, WEP usa el algoritmo de cifrado RC4, este se basa en la concatenación de 24 bits del vector inicialización y 40 o 104 bits de la clave.

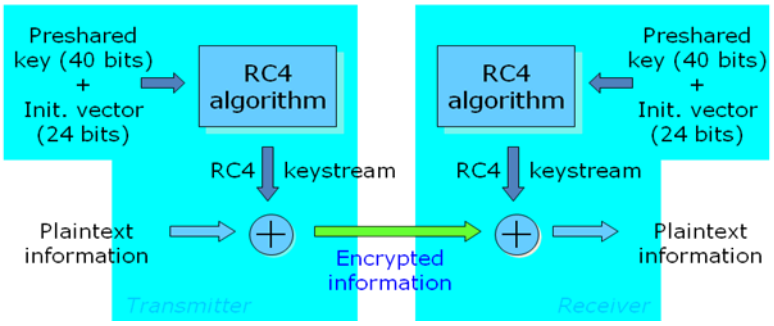


Figura A3-9: Algoritmo de cifrado WEP

- WPA

WPA fue desarrollado por la Wi-Fi Alliance (22) para mejorar el nivel de codificación existente en WEP, así como para incorporar un método de autenticación. Los aspectos que se intentan optimizar mediante el uso de WPA son el proceso de autenticación y el de cifrado.

Las principales características de WPA son las siguientes:

- Distribución dinámica de claves.
- Utilización más robusta del vector de inicialización (mejora de la confidencialidad).
- Nuevas técnicas de integridad y autenticación (aplicable en entornos residenciales y empresariales).
- Actualización de equipamiento radio a WPA mediante software.

Podemos encontrar WPA en dos entornos, el **P**re-**S**hared **K**ey (**PSK**) Mode (entornos domésticos) y el Enterprise Mode (entornos empresariales).

- **Entornos domésticos**

Se usa una autenticación WPA-PSK. En estos entornos no es posible contar con un servidor de autenticación centralizado o un marco **EAP** (***E**xtensible **A**uthentication **P**rotocol*) (16). En estos casos WPA se ejecuta en un modo especial conocido como "home mode" o **P**re-**S**hared**K**ey (**PSK**) que permite la utilización de claves configuradas manualmente y facilitar así el proceso de configuración al usuario residencial.

El usuario únicamente debe introducir una passphrase de entre 8 y 63 caracteres, conocida como clave maestra, en su punto de acceso o modem ADSL o cable módem inalámbrico residencial, así como en cada uno de los dispositivos que desea conectar a la red WLAN. De esta forma la clave permite, en primer lugar, conectarse a la red únicamente

a aquellos dispositivos con la clave adecuada, lo que evita ataques basados en escuchas así como acceso de usuarios no autorizados, y en segundo lugar, la contraseña provee una relación de acuerdo único para generar el cifrado **TKIP** (***T**emporal **K**ey **I**ntegrity **P**rotocol*) en la red.

Por lo tanto, la passphrase inicial para la autenticación es compartida por todos los dispositivos de la red, pero no lo son las claves de cifrado, que son diferentes para cada dispositivo, lo que es una mejora con respecto al mecanismo WEP.

- **Entornos empresariales**

Los requerimientos estrictos de cifrado y autenticación hacen que sea más adecuada la utilización de WPA con los mecanismos IEEE 802.1x y el protocolo de autenticación extensible EAP, que disponen de procedimientos de gestión de claves dinámicamente. En este entorno WPA utiliza el estándar IEEE 802.1x y EAP. EAP se emplea como transporte extremo-a-extremo para los métodos de autenticación entre el dispositivo de usuario y los puntos de acceso. Mientras que IEEE 802.1x se emplea como marco para encapsular los mensajes EAP en el enlace radio .El conjunto de estos dos mecanismos juntos con el esquema descifrado forman una fuerte estructura de autenticación que utiliza un servidor de autenticación centralizado. En cuanto al cifrado, WPA emplea el protocolo de integridad de clave temporal (TKIP) para codificar los datos.

TKIP comienza el proceso mediante una clave semilla de 128 bits compartida temporalmente entre los usuarios y los puntos de acceso. Después esa clave temporal se combina con la dirección MAC del usuario y se le añade un vector de inicialización de 16 bits para producir la clave que cifrará los datos.

- WPA2

Es una evolución del mecanismo WAP, el cual utiliza un nuevo algoritmo de encriptación AES (Advanced Encryption Standard) (23), aunque puede seguir usando TKIP. AES es mucho más complejo y no sufre de los problemas asociados a RC4, pero por otro lado, a diferencia de TKIP, el cifrado AES requiere una gran capacidad de procesado que se realiza mediante aceleración hardware. Esta aceleración hardware la debe realizar un chip dedicado y no es compatible con algunos equipos existentes actualmente, esto obliga a los fabricantes a cambiar el hardware para soportarlo.

Podemos observar la evolución entre los mecanismos de encriptación utilizados en WLAN en la Tabla A3-3.

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
IV Size	24 bits	48 bits	48 bits
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-Based	EAP-Based

Tabla A3-3: Comparación entre mecanismos de encriptación

A3.6 Ataques en redes WLAN

Para poder diseñar un sistema de seguridad, es prioritario conocer las estrategias de ataques que se pueden sufrir en los elementos que deseamos proteger.

Podemos clasificar las amenazas típicas de WLAN en dos grandes grupos, los ataques pasivos y los ataques activos.

- Ataques pasivos: En esta clase de ataques el principal objetivo del atacante es el de monitorizar la red obteniendo así información referente a ella.

- Ataques activos: A diferencia de los ataques pasivos, estos interfieren de alguna forma en el flujo de datos de la red. Esto puede usarse para obtener información que fluye dentro de la red o interferir de algún modo en el funcionamiento de la red.

Una vez definidos los dos grandes grupos, pasaremos a introducir los ataques que se dan en cada uno de ellos.

A3.6.1 Ataques pasivos

Dentro de los ataques pasivos podemos encontrar los siguientes ataques:

- **Sniffing**

Es el ataque pasivo más típico dentro de las redes inalámbricas. Se basan principalmente en monitorizar el flujo de datos de la red obteniendo así información de la capa de red y de la capa de enlace junto con información de los actores que toman parte en cada flujo, entre ellos direcciones IP origen y destino o direcciones MAC. Dentro de los

mensajes que se escuchan mediante el sniffing podemos encontrar información tan crítica como pueden ser password de diferentes servicios o claves de seguridad entre muchos otros datos.

Este tipo de ataques no son más que el paso inicial de los ataques activos, cuyos procedimientos se basan en usar la información obtenida mediante el sniffing realizando así ataques como los de suplantación de identidad.

Estos ataques son peligrosos debido a la facilidad de llevarlos a cabo. Cualquier equipo con una tarjeta de red inalámbrica, haciendo uso de herramienta de análisis de tráfico de red, podría monitorizar toda la información que viaja a través de la red WLAN. Para esto su tarjeta inalámbrica ha de soportar el modo monitor, el cual funciona no discriminando ninguno de los paquetes de datos que llegue a la interfaz de red, ya que una tarjeta en su funcionamiento normal solo acepta paquetes que vayan dirigidos a ella. En la Figura A3-10 se muestra un ejemplo de sniffing con Wireshark.

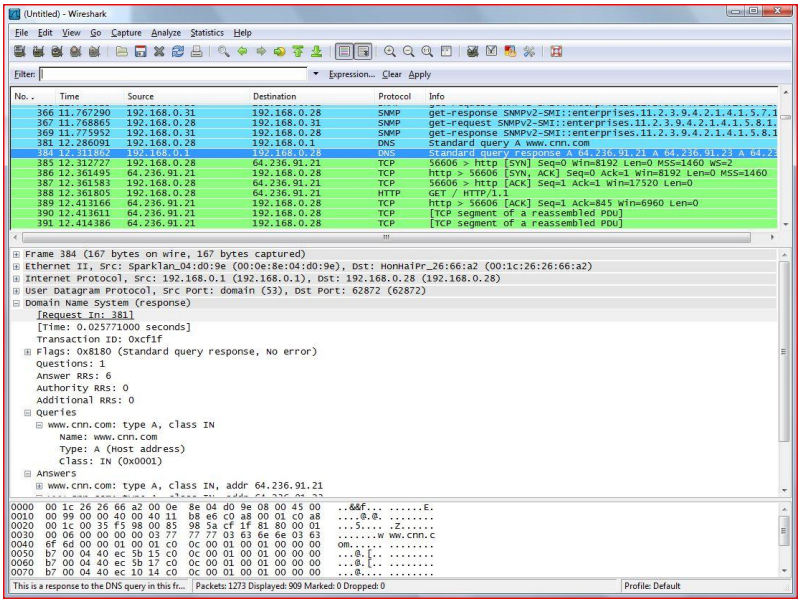


Figura A3-10: Captura de tráfico mediante Wireshark

- **Wardriving**

Es una extensión del ataque de sniffing, en el cual el atacante recorre zonas en coche tratando de localizar puntos de acceso inalámbricos. Para ello, solo es necesario un equipo portátil con una tarjeta inalámbrica y una antena para poder obtener una cobertura mayor.

- **Warchalking**

Más que un ataque es un método de información a atacantes. Se basa en un lenguaje de símbolos normalmente escritos con tiza en las paredes, para así informar a los posibles interesados de la existencia de una red inalámbrica en ese punto. La información que dan estos mensajes son el SSID de la red, el estado de la red (abierta, cerrada o WEP) y la velocidad de esta. En la Figura A3-11 podemos ver un ejemplo de cómo trasmite la información referente al estado de la red.

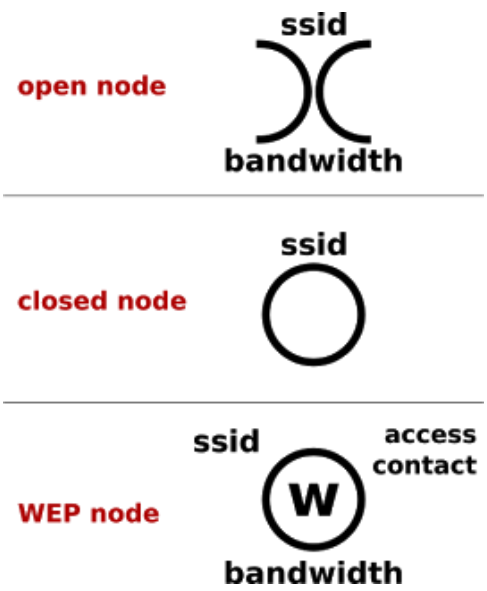


Figura A3-11: Nomenclatura Warchalking

- **Ataques de descubrimiento de contraseña**

Se basan en tratar de descubrir contraseñas de acceso al sistema o claves de cifrado de los datos que viajan por la red. Esto se realiza tras un proceso de monitorización de la información.

En el proceso de obtención de contraseñas, podemos encontrar dos tipos de técnicas: las de fuerza bruta y las de obtención por diccionario. Cuando se implementó el sistema de cifrado WEP en las redes WLAN, se desarrollaron herramientas software que probaban a gran velocidad posibles contraseñas, combinando ataques estadísticos con ataques de fuerza bruta.

En los ataques de fuerza bruta, básicamente se crea un procedimiento que intenta romper un cifrado mediante la prueba de todas las combinaciones posibles. La ventaja de este ataque es que siempre se consigue romper el cifrado, pero su gran problema es el consumo de recursos y tiempo que conlleva este, ya que se puede disparar dependiendo del

tamaño de la clave. También entran como factor importante el tipo de sistema de seguridad, debido a que este ha ido evolucionando con el paso del tiempo, comenzando con WEP a WPA y a su evolución, WPA2, haciéndose más segura debido al aumento de tamaño del vector de inicialización y a la encriptación usada.

Los ataques por diccionario, parecidos a los de ataques de fuerza bruta, no utilizan todas las combinaciones posibles, sino que se reducen el rango de comprobaciones a un listado de palabras probables. Esto hace que el tiempo del proceso de comprobación se reduzca considerablemente comparado con el de ataque por fuerza bruta. Uno de los diccionarios típicos en este tipo de ataques es el diccionario "John the Ripper" (24).

A3.6.2 Ataques activos

Dentro de los ataques activos podemos encontrar los siguientes ataques:

- **Rogue AP**

Un Rogue AP es un punto de acceso sin autorización que se ha conectado a una red segura existente. Estos se convierten en una fuente de todo tipo de ataques debido a que permiten una conexión sin ningún tipo de seguridad a través de ellos. Esto conlleva que sean unos de los ataques más peligrosos que se pueden encontrar en redes WLAN. En general estos AP suelen usar una potencia de señal mayor para que la conexión de los usuarios sea automática a ellos debido a las políticas de asociación de las redes WLAN. En la Figura A3-12 se muestra un ejemplo de funcionamiento de un ataque Rogue AP.

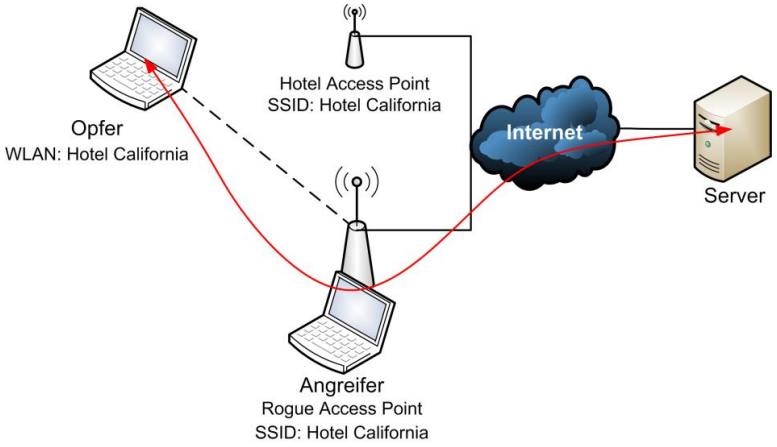


Figura A3-12: Ejemplo de Rogue AP

- **Spoofing**

Consisten en el uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Estos ataques se pueden clasificar dependiendo de la

tecnología utilizada y el tipo de identificador suplantado. Entre ellos podemos encontrar los siguientes tipos de Spoofing:

- **IP spoofing**: Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP (25) por otra dirección IP a la cual se desea suplantar.

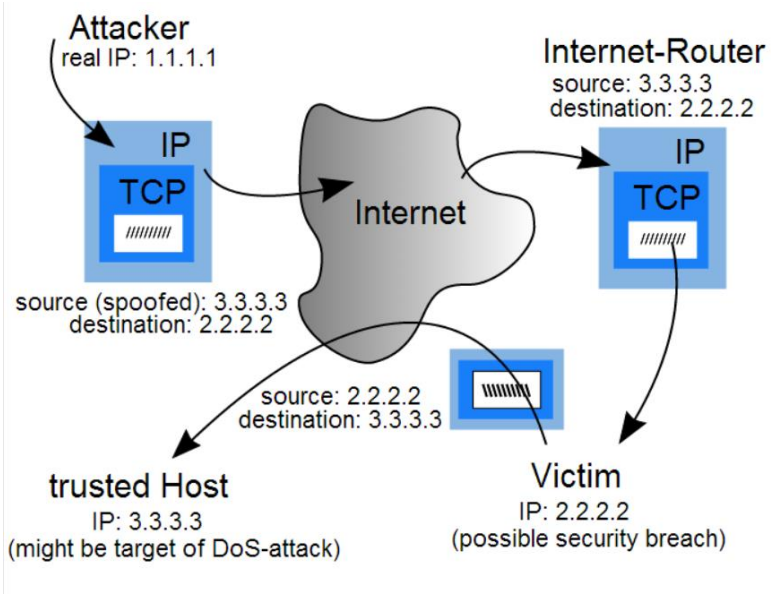


Figura A3-13: Ejemplo IP Spoofing

En la Figura A3-13 podemos observar un ataque típico de suplantación IP, en ella el atacante adopta la dirección 3.3.3.3 y envía un paquete a 2.2.2.2, por último, 2.2.2.2 contestara al verdadero 3.3.3.3. Si varias máquinas desde el exterior llevan a cabo este ataque, puede llegar a darse el caso en el que los mensajes de respuesta inunden la red mediante un ataque DoS y dejen inutilizable la máquina 3.3.3.3.

- **ARP Spoofing:** Suplantación de identidad por falsificación de tabla **ARP** (**A**ddress **R**esolution **P**rotocol) (14). Se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.

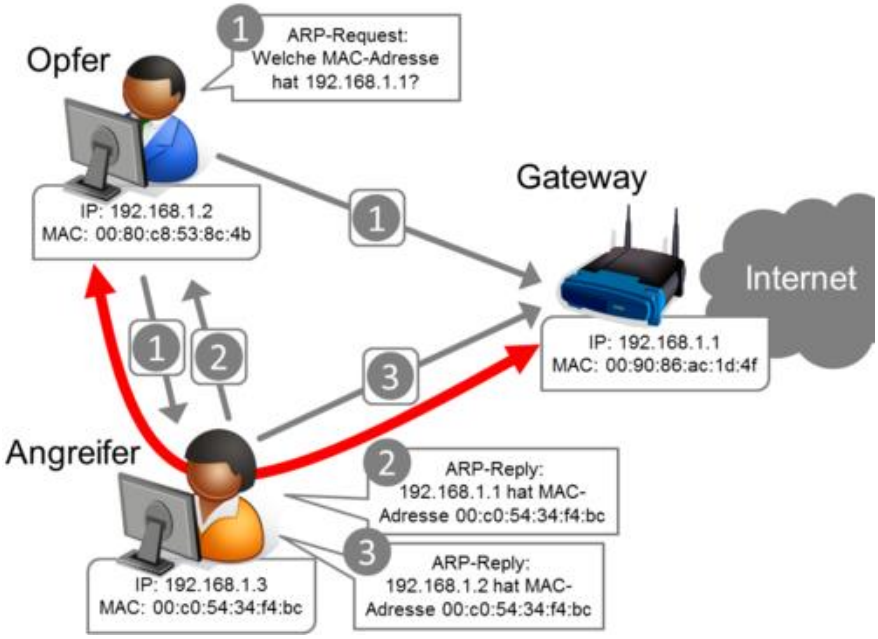


Figura A3-14: ARP Spoofing y MitM attack

En la Figura A3-14 se muestra el ejemplo típico de una suplantación de mensajes ARP, en el ejemplo, podemos ver como el atacante con IP 192.168.1.3 intercepta el envío del ARP-Request del usuario 192.168.1.2, en la cual pregunta por el Gateway con 192.168.1.1. Tras esto, el atacante ha de ser más rápido contestando que el Gateway, para así contaminar la cache ARP del usuario. Tras esto, el tráfico destinado al Gateway pasara por el atacante, generando así un ataque **M**an **i**n **t**he **M**iddle (**MitM**).

Estos son los dos ataques de spoofing que son más nocivos en las redes WLAN. También sirven de base para otros ataques que utilizan previamente las técnicas de suplantación.

- **Man In the Middle**

Ataque basado en spoofing. El atacante selecciona una serie de entidades, con las cuales intercambia mensajes modificados para suplantar sus identidades, como podría ser un ARP Poisoning, de esta forma se le permite servir de puente en la comunicación entre las entidades. Un escenario típico sería un MitM entre una estación y un AP, de esta forma todo el tráfico que la estación envié y se le envíe hacia y desde el exterior pasará por el equipo atacante, ya que este simula ser el Gateway para la estación y la estación autorizada para el AP. Para esto el atacante ha debido modificar los mensajes de ARP para envenenar las tablas de ARP de las víctimas. (Véase Figura A3-14).

- **Hijacking**

Basado en spoofing. Se sirve de "robar" una sesión de una víctima haciéndose pasar por ella. Para ello, realizara un sniffing de la red para conocer la situación, entonces

disasociará a la víctima y tomará su lugar asociándose al punto de acceso con la MAC de la víctima y los identificadores de la sesión.

- **Denial of Service (DoS)**

El objetivo de este ataque no está orientado a acceder a la red o suplantar identidades, sino a inutilizar la red para que no se pueda hacer uso de ella. A continuación, se explican los ataques DoS principales.

- **Wireless DoS:** Hace uso de las tramas de disociación estandarizadas en 802.11 debido a que no están protegidas por privacidad ni autenticidad. El proceso consiste en inundar la red con tramas de disociación para evitar que se pueda hacer uso de ella.

- **Jamming:** Hace uso de una señal de alta potencia para así interferir en el espectro e inhabilitar el servicio.

- **Smurf:** El atacante envía grandes cantidades de tráfico **ICMP** (**I**nternet **C**ontrol **M**essage **P**rotocol) a la dirección de broadcast, todos ellos teniendo la dirección de origen cambiada a la dirección de la víctima. De este modo los ordenadores responderán aumentando el tráfico de la red y pudiendo llegar a inhabilitar la red.

- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **DoS**: El atacante suplanta la identidad del servidor DHCP asignando IP falsas a las estaciones que se quieran conectar a la red.

Con esto concluimos la sección de ataques, en la que hemos podido ver una clasificación al detalle de los ataques y lo dañinos que pueden resultar si se llevan a cabo.

A continuación se expondrán las diferentes arquitecturas que podemos encontrar en los IDS y sus correspondientes beneficios e inconvenientes.

A3.7 Clasificación de los IDS

Los sistemas IDS se pueden clasificar en función de tres premisas:

A3.7.1 Metodología de detección de intrusos

Un WIDS puede realizar estas tareas de dos formas: basándose en una base de datos de firmas de anomalías (12) o bien detectando comportamientos anómalos en la red.

A3.7.1.1 Basado en patrones/firmas

En este caso, el sistema cuenta con un registro de patrones de ataque, a través de los cuales es capaz de detectar diferentes ataques sobre la red. El problema de este método es que se basa principalmente en que solo se tiene registro de ataques conocidos, cuyos patrones están definidos en firmas de ataque. Esto conlleva a la imposibilidad de hacer frente a nuevos ataques que aún no han sido registrados o bien de los cuales es difícil definir un patrón genérico. Se puede observar un modelo de estos sistemas en la Figura A3-15.

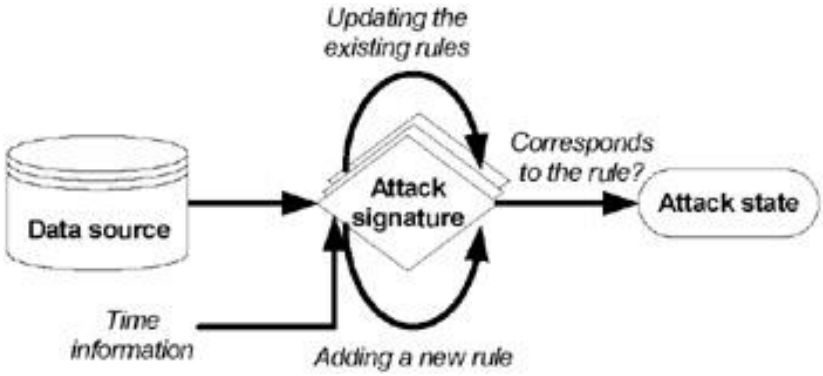


Figura A3-15: Modelo de un detector basado en firmas

A3.7.1.2 Basado en detección de anomalías

El funcionamiento basado en detección de anomalías no está muy implementado, ya que, aunque puede llegar a ser muy eficiente en la detección de intrusos, llega a generar gran cantidad de alarmas falsas. Lo principal en este método es desarrollar un perfil de funcionamiento correcto de la red y determinar un umbral de lo que cree el sistema que es tráfico normal y anormal. A partir de aquí, todo lo que supere el umbral resultará anómalo y generará alarmas. Se puede observar un modelo de estos sistemas en la Figura A3-16.

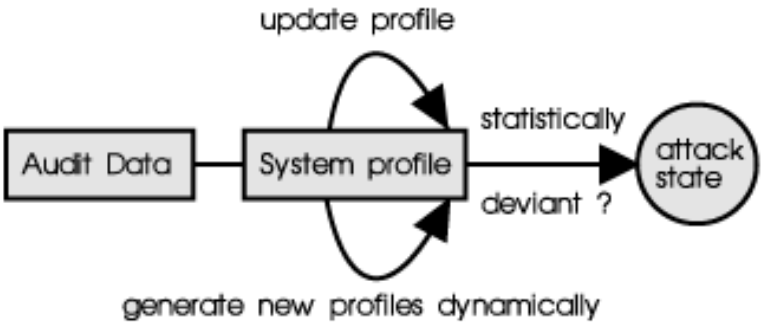


Figura A3-16: Modelo de un detector basado en anomalías

A3.7.2 Lugar de despliegue y sistemas a monitorizar

Los sistemas WIDS pueden instalarse de forma que capturen el tráfico de red de diferentes formas.

A3.7.2.1 Network Based IDS (NIDS)

Este tipo de IDS están colocados estratégicamente en una red para detectar cualquier ataque contra los hosts de esa red. Hay que ser cuidadoso al posicionar el IDS para poder recoger el mayor volumen de tráfico posible tanto de entrada o de salida. También es posible colocar algunos IDS cerca de las posiciones estratégicas de la red interna, dependiendo del nivel de seguridad necesario en la red. La principal estrategia que se plantea en estos IDS es que se necesita monitorizar todo el tráfico de la red y, de manera paralela, realizar un análisis de este para así detectar diferentes patrones que puedan referirse a diferentes ataques a la red. Podemos observar un ejemplo de estas redes en la Figura A3-17.

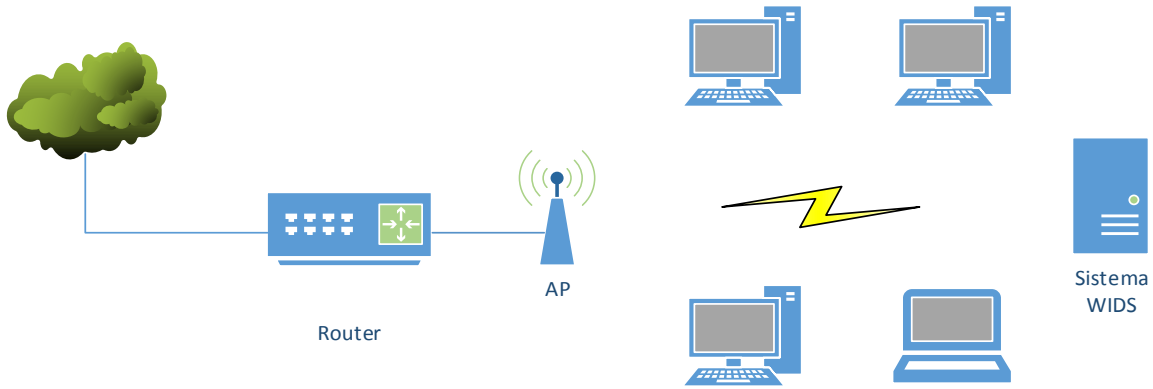


Figura A3-17: Arquitectura Network Based IDS

A3.7.2.2 Host Based IDS (HIDS)

Están instalados en los hosts de la red y solo monitorizan el tráfico dirigido u originado en ese host. Podemos ver un ejemplo de despliegue de estos sistemas en la Figura A3-18. Aparte del análisis de tráfico de red, también implementan técnicas de seguridad correspondientes al análisis del sistema de archivos de un host, las actividades de inicio de sesión de los usuarios, los procesos en ejecución, la integridad de datos. En lo referente a sus ventajas, son capaces de identificar ataques en el interior del host, pueden analizar el tráfico descifrado y se pueden implementar en un equipo de usuario, sin necesidad de

infraestructura adicional. Por otro lado, sus desventajas principales se basan en que el sistema se verá comprometido tan pronto como la máquina host sufra algún ataque o fallo.

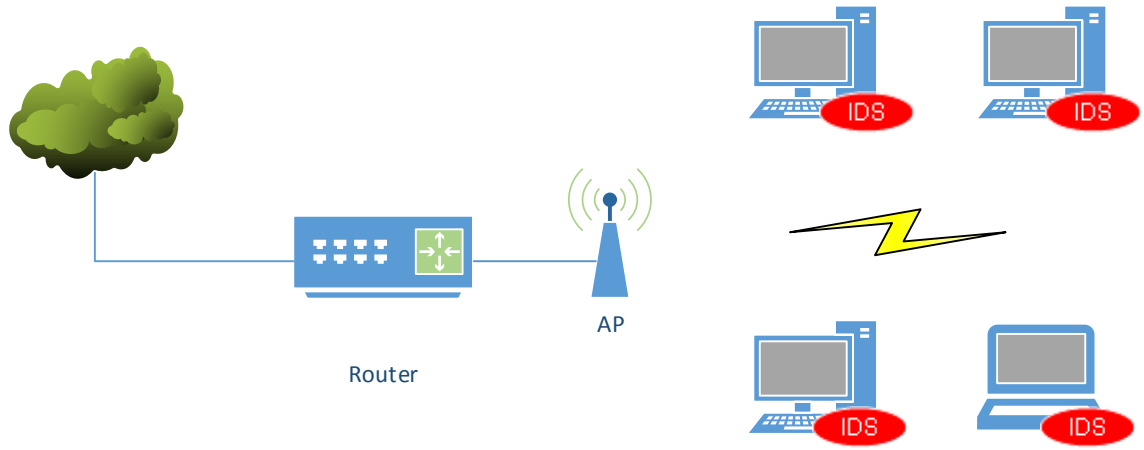


Figura A3-18: Arquitectura Host Based IDS

A3.7.3 Metodología de respuestas frente a intrusiones

Podemos clasificar los tipos de respuesta frente a intrusos en dos grupos.

A3.7.3.1 Respuestas pasivas

Los sistemas notifican al administrador del sistema mediante alertas, etc., pero no actúan directamente sobre el ataque o atacante.

A3.7.3.2 Respuestas activas

Este tipo de respuestas son acciones automáticas que se toman cuando una intrusión es detectada.

A3.8 Arquitectura de los IDS

Las arquitecturas de IDS se han puesto con el objetivo de facilitar la interoperabilidad y reutilización de los módulos, así como la reducción de la complejidad en la gestión y configuración de los IDS. Gracias a la aprobación de protocolos de comunicación específicos, es posible lograr el intercambio de datos entre elementos de distintos fabricantes que pueden formar parte de un IDS. De este modo, se facilita la captura

de eventos generados por distintas fuentes, proporcionando una imagen más amplia y detallada de las actividades maliciosas en un determinado entorno.

Las arquitecturas de IDS más importantes son CIDF e IDWG.

A3.8.1 CIDF (Common Intrusion Detection Framework)

Es una arquitectura promovida por la Agencia Federal de Estados Unidos **DARPA** (**D**efense **A**dvanced **R**esearch **P**rojects **A**gency) y finalizada en 1999, que ha tenido una escaza aceptación comercial. Esta arquitectura está constituida por los siguientes elementos:

- Generador de eventos: obtención y descripción de eventos mediante objetos denominados **GIDO**s (**G**eneralized ***I**ntrusion **D**etection **O**bjets*).
- Analizador de eventos: incorpora los algoritmos de detección de ataques.
- Base de datos de eventos: se utiliza el lenguaje **CISL** (**C**ommon ***I**ntrusion **S**pecification **L**anguage*) para expresar los diferentes eventos.
- Unidades de respuesta: se encargan de cerrar las conexiones, terminar procesos, bloquear el acceso a los servidores, etcétera.

A3.8.2 IDWG (Intrusion Detection Working Group)

Propone el formato **IDEF** (**I**ntrusion ***D**etection **E**xchange **F**ormat*) para facilitar el intercambio de información sobre los incidentes de seguridad. En este caso se distinguen los módulos Sensor, Analizador, Fuente de Datos y Manager.

- El Analizador es el componente que analiza los datos recolectados por el Sensor, buscando señales de actividad no autorizada o indeseada.
- El Sensor recolecta datos de la Fuente de Datos: paquetes de red, "*logs*" de auditoría del sistema operativo, "*logs*" de aplicaciones… (información que el IDS emplea para detectar cualquier actividad indeseada o no autorizada).
- El Manager es el componente desde el cual se administran los restantes elementos del IDS: se encarga de la configuración de los sensores y analizadores, de la consolidación de datos, de la generación de informes, etcétera.

La arquitectura IDWG ha definido un modelo de datos orientado a objetos basado en el lenguaje XML para describir los eventos, conocido como **IDMEF** (**I**ntrusion ***D**etection **M**essage **E**xchange **F**ormat*). Así mismo IDWG prevé dos mecanismos de comunicaciones: el protocolo **IAP** (**I**ntrusion ***A**lert **P**rotocol*), para intercambiar datos de alertas de intrusiones de forma segura entre las entidades de detección, y el protocolo **IDXP** (**I**ntrusion ***D**etection **E**xchange **P**rotocol*), que permite intercambiar datos en general entre las entidades de detección de intrusiones.

A3.8.3 Elementos de un IDS

A continuación se numeran los elementos principales y mínimos que debería tener un IDS/WIDS.

- **Fuentes de tráfico** Son los elementos del sistema que tienen contacto directo con la red. Son los encargados de capturar tráfico de red para su posterior análisis en el sistema. Podemos tener distintas topologías en lo referente a la localización de las fuentes de tráfico:
  - **Centralizada** Las fuentes van montadas junto al equipo anfitrión del sistema, por ejemplo una tarjeta de red.
  - **Descentralizada** Se colocan varios sensores en la red, los cuales se encargan de capturar tráfico y enviarlo al sistema para su procesamiento.

- **Unidades de procesamiento** Son los elementos del sistema encargados de procesar la información obtenida de los sensores y, basándose en las políticas configuradas, tomarán distintas decisiones, por ejemplo, almacenar las incidencias o avisar a los administradores de la red de estas.

Como ya se ha comentado anteriormente, el diseño y arquitectura genérica de los sistemas detectores están basados para redes cableadas. Esto se debe a que la inmensa mayoría de los sistemas detectores está diseñado para este tipo de redes y los WIDS no están tan estudiados. Aun así, nos basaremos en las configuraciones anteriormente explicadas para proponer un WIDS que se adapte perfectamente a las diferencias en configuración y diseño que precisan las redes inalámbricas Wireless LAN.

A continuación se va a mostrar distintos tipos de sistemas detectores de intrusos orientados a redes inalámbricas.

A3.9 Wireless intrusion detection system (WIDS) comerciales

Después de ver una clasificación de los ataques orientados a las redes WLAN, procederemos a mostrar los distintos tipos de WIDS comerciales que podemos encontrar actualmente.

Lo primero a tener en cuenta es quién va a gestionar el detector de intrusos. Si la entidad es lo suficientemente grande, habrá un grupo de técnicos que se encarguen de la gestión de la red. En este caso, productos como AirMagnet Distributed, AirDefense Enterprise o el conjunto de productos de Red -M son soluciones que están disponibles.

Sin embargo, si estamos intentando implementar un WIDS en una red doméstica, en una organización pequeña o mediana, entonces es más probable que un **M**anaged **S**ecurity **S**ervice **P**rovider (**MSSP**) del servicio de WIDS. Un MSSP no es más que un **I**nternet **S**ervice **P**rovider (**ISP**) que ofrece monitorización de red y de alerta de diversos tipos junto con un servicio técnico 24x7. La gran ventaja que tienen los ISP es que disponen de la infraestructura para dar este servicio. Volviendo al software comercial, podemos ver a Motorola con AirDefense junto a la cooperación de IBM y Fluke con AirMagnet. En esto vemos cómo las empresas no solo están comenzando a entrar en el mercado de la seguridad inalámbrica, sino que están cooperando entre ellas para dar estos servicios.

A3.9.1 AirMagnet

Los sensores de AirMagnet (26) reportan información sobre el rendimiento de la red y alertas a un servidor de gestión dentro de una base de datos **SQL** (**S**tructured **Q**uery **L**anguage), la cual se controla a través de una consola de administración. También nos permite la detección de APs maliciosos para obtener la posición geográfica en la que se encuentran.

AirMagnet actualmente tiene un precio de 1.800 euros en su opción más básica.

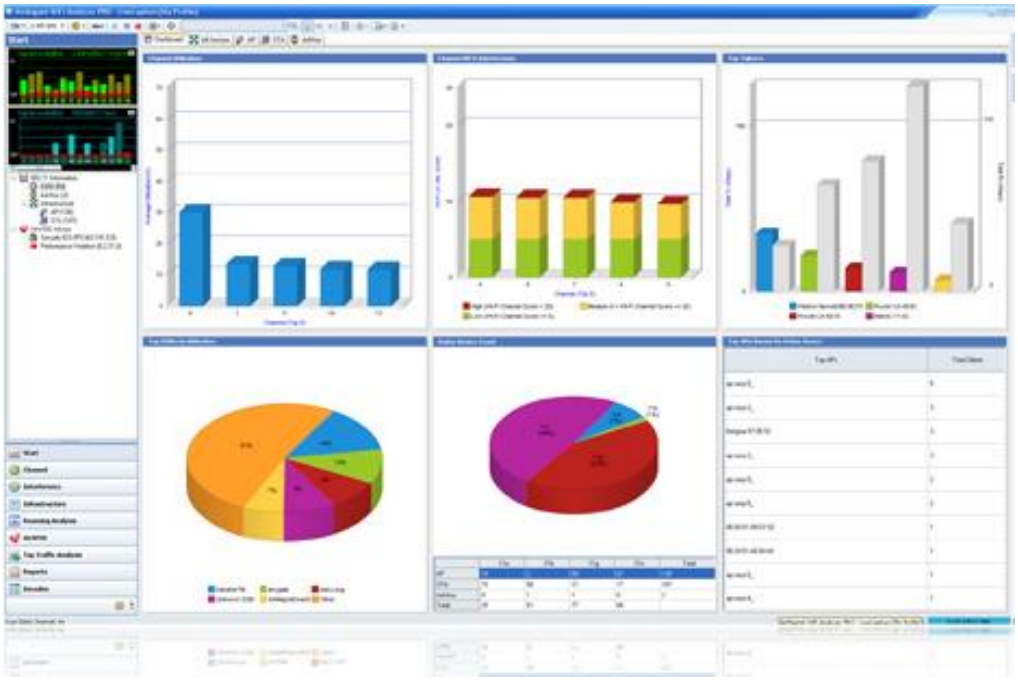


Figura A3-19: Interfaz de administración AirMagnet

En la Figura A3-19 se muestra el interfaz de administración a través del cual el usuario puede interactuar con el sistema.

A3.9.2 AirDefense

El sistema de AirDefense (27) consiste en un servidor que ejecuta Red Hat Linux con una serie de sensores inalámbricos AP y una consola Web basada en Java. La comunicación entre los distintos elementos del sistema se realiza mediante un canal seguro a través de un servidor propio.

AirDefense actualmente tiene un precio de 6.500 euros en su opción más básica.

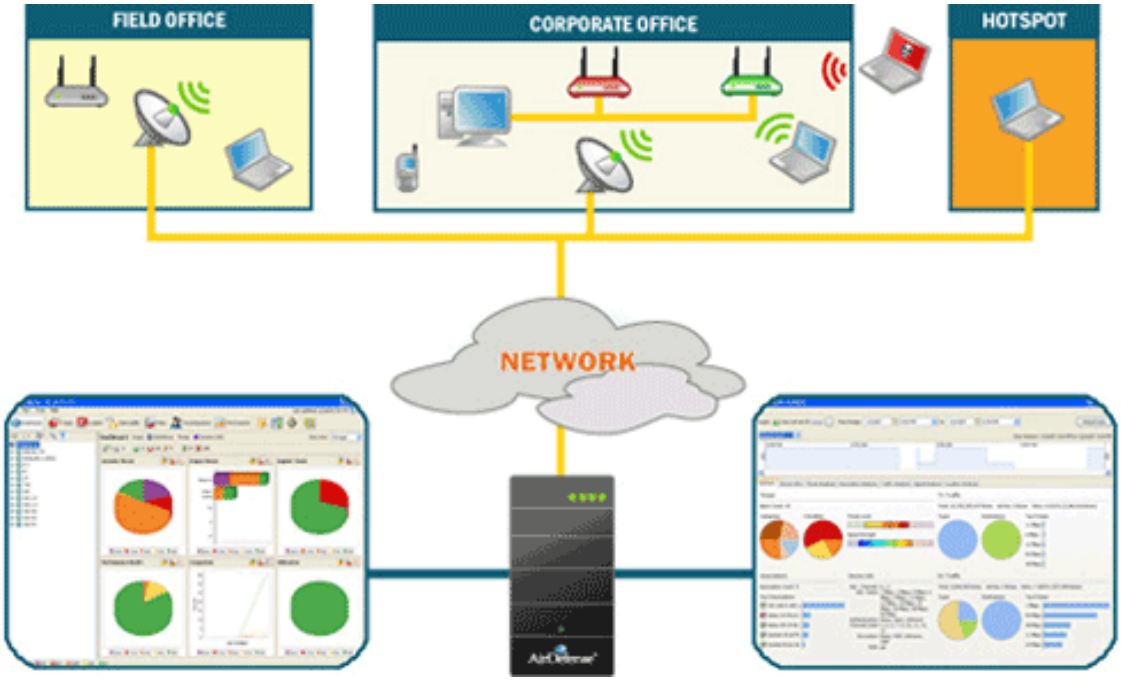


Figura A3-20: Arquitectura del sistema AirDefense

La Figura A3-20 muestra como los distintos elementos de la red se comunican entre sí creando un sistema cerrado entre todos los componentes de este.

En conclusión, podemos ver cómo estos dos sistemas ofrecen un servicio de IDS bastante completo, teniendo como único problema los altos precios que cuesta desplegar el sistema.

A3.10 Scanners e IDS de redes cableadas e inalámbricas de código abierto

Estos programas nos ofrecen un escaneo de la redes WLAN a nivel de enlace. De esta forma podemos ver lo que está pasando constantemente en nuestra red al controlar los BSSID de los AP, las estaciones que están conectadas a esos AP y los mensajes que se envían. Dentro de este grupo destacan Kismet, NetStumbler y Snort.

A3.10.1 Kismet

Kismet (6) es un sniffer para redes inalámbricas 802.11. Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización RAW (paquetes 802.11), y puede rastrear tráfico 802.11b, 802.11a, 802.11g y 802.11n.

El programa corre bajo Linux, FreeBSD, NetBSD, OpenBSD y Mac OS X. El cliente puede también funcionar en Windows, aunque la única fuente entrante de paquetes compatible es otra sonda.

Kismet tiene tres partes diferenciadas: una Sonda que puede usarse para recoger paquetes, que son enviados a un servidor para su interpretación, un servidor que puede o bien ser usado en conjunción con una sonda o bien consigo mismo, interpretando los datos de los paquetes, extrapolando la información inalámbrica y organizándola. El cliente se comunica con el servidor y muestra la información que el servidor recoge.

Aparte de darnos información "live", también creará ficheros de registro en los que irá almacenando la información para poder ser analizada en otro momento junto con otros ficheros de alertas que nos comunicarán diversos ataques sobre las redes WLAN. En la Figura A3-21 se observa el interfaz vía consola desde el cual se puede configurar Kismet y a través del cual nos devuelve los datos referentes al estado de la red.

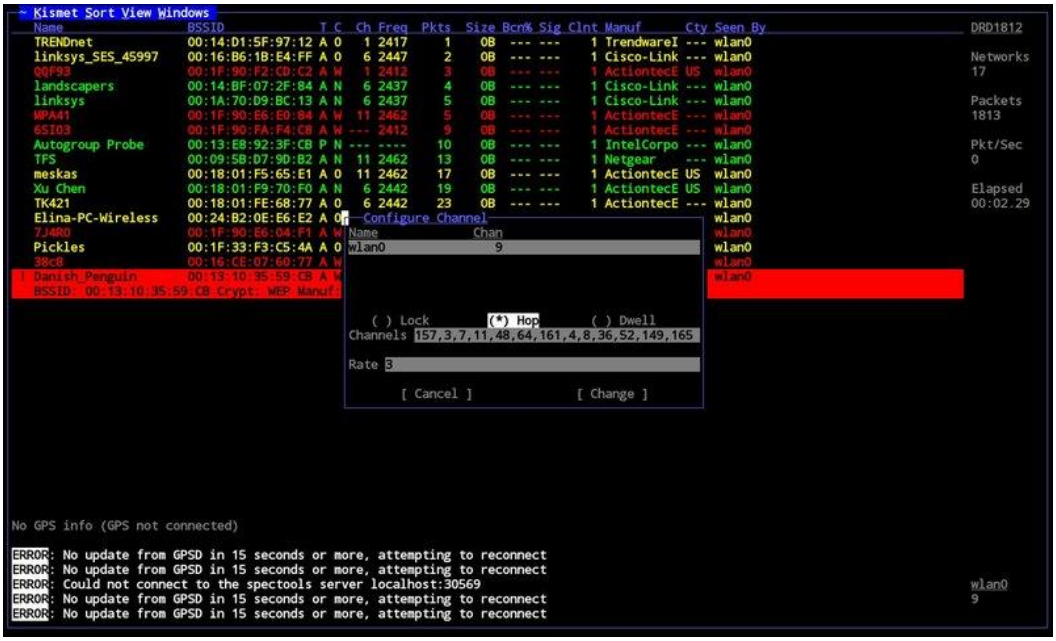


Figura A3-21: Interfaz de usuario de Kismet vía consola

A3.10.2 NetStumbler

Es el sniffer más popular en sistemas operativos Windows. Funciona mandando mensajes "request" a la red 802.11 y visualizando datos referentes a los equipos que responden. En la Figura A3-22 se observa el interfaz gráfica de NetStumbler para plataformas Windows.

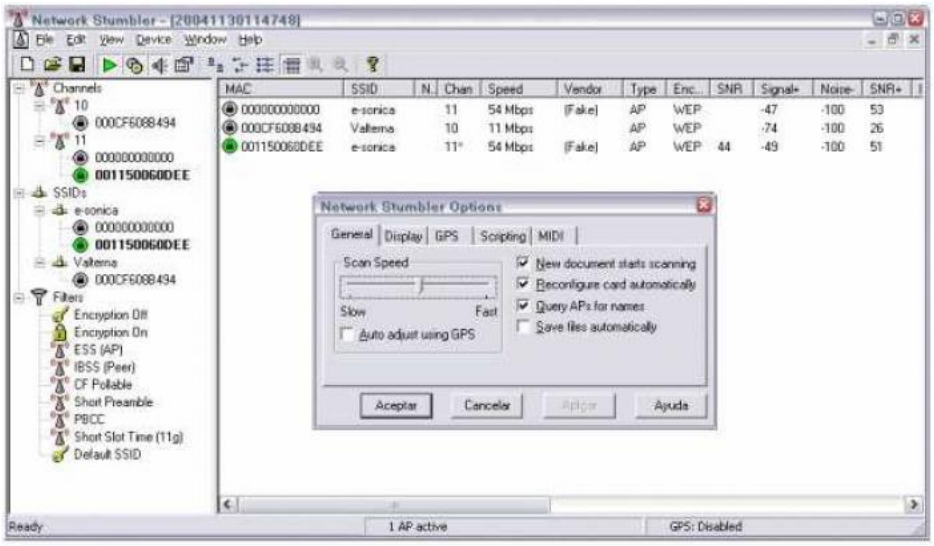


Figura A3-22: Interfaz de usuario NetStumbler

A3.10.3 Snort

Snort (13) es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL (28). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un Sistema Detector de Intrusos (IDS).

Este IDS implementa un lenguaje de creación de reglas flexibles, potentes y sencillas. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, DDoS, finger, FTP, ataques web, CGI y NMap entre otras.

Puede funcionar como sniffer o como un IDS. En la Figura A3-23 podemos observar la arquitectura general de Snort.

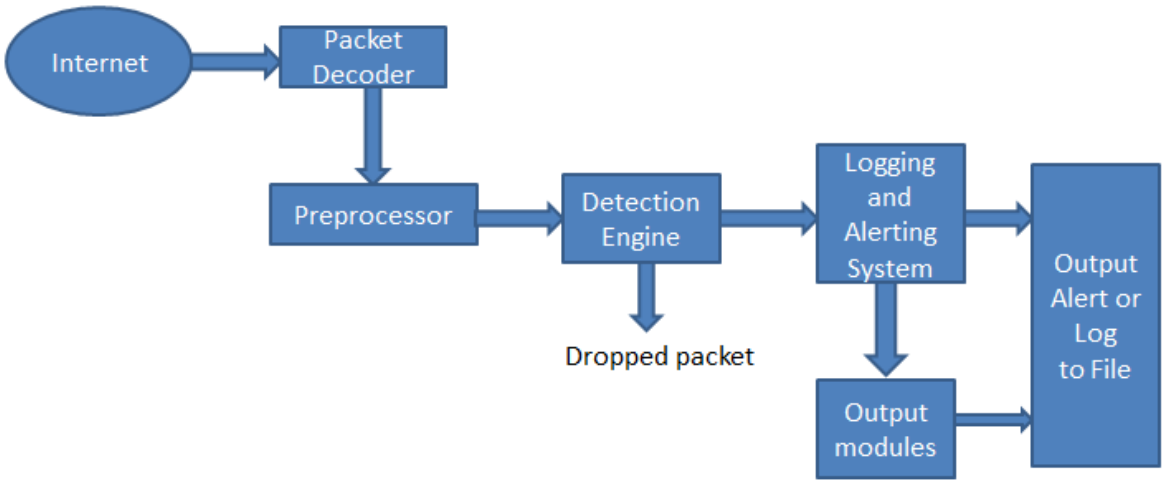


Figura A3-23: Arquitectura de Snort

Aquí acabamos el análisis de los sistemas IDS/WIDS que están comercializados actualmente y de los scanners de red a nivel de enlace más completos que podemos encontrar.

Anexo IV – Diseño de bajo nivel

A continuación se expone el diseño de bajo nivel del sistema Antikörper. En él se explica de manera detallada su funcionamiento mediante diferentes diagramas.

Debido a que el sistema está principalmente desarrollado en el lenguaje de programación C (el módulo Decrypter está basado en la herramienta dot11decrypt (29) desarrollada en C++), y debido a la naturaleza estructurada de este, se ha optado por la utilización de diagramas de flujo.

En la Figura A4-1 se puede ver la arquitectura final de Antikörper. En ella se puede observar los módulos de los que va a constar el sistema, cómo van a interoperar entre ellos y qué datos van a recibir y emitir.

A4.1 Diagramas de flujo de AntikörperCore

En la Figura A4-2 podemos ver la primera fase en el arranque de Antikörper Core, en la que se inicializa el sistema y se ofrecen diferentes opciones al usuario.

En el diagrama podemos observar las siguientes fases:

- **Inicialización de variables.** El sistema incluirá los ficheros de cabecera en la directiva del preprocesador, inicializará las diferentes estructuras de datos con las que se va a trabajar y se declararán una serie de variables globales de tipo especial que serán necesarias para hacer uso de las librerías utilizadas en la implementación. Todo esto será explicado más en detalle en el capítulo de implementación.

- **Carga de configuración y listas blancas.** El sistema cargará de los correspondientes ficheros de configuración su configuración más básica y cargará en memoria la lista blanca de usuarios autorizados en la red.

- **Petición de datos al usuario.** El sistema pedirá datos referentes a la configuración básica de la red, entre los que se encontrarán la dirección del Gateway de la red y el BSSID de la red a proteger.

- **Menú de selección.** Mostrará al usuario distintas opciones:

  - **Visualizar registro de intrusiones.** Permitirá al usuario visualizar los registros de intrusiones generados anteriormente por el sistema, de los que mantendrá un fichero en un formato dado.

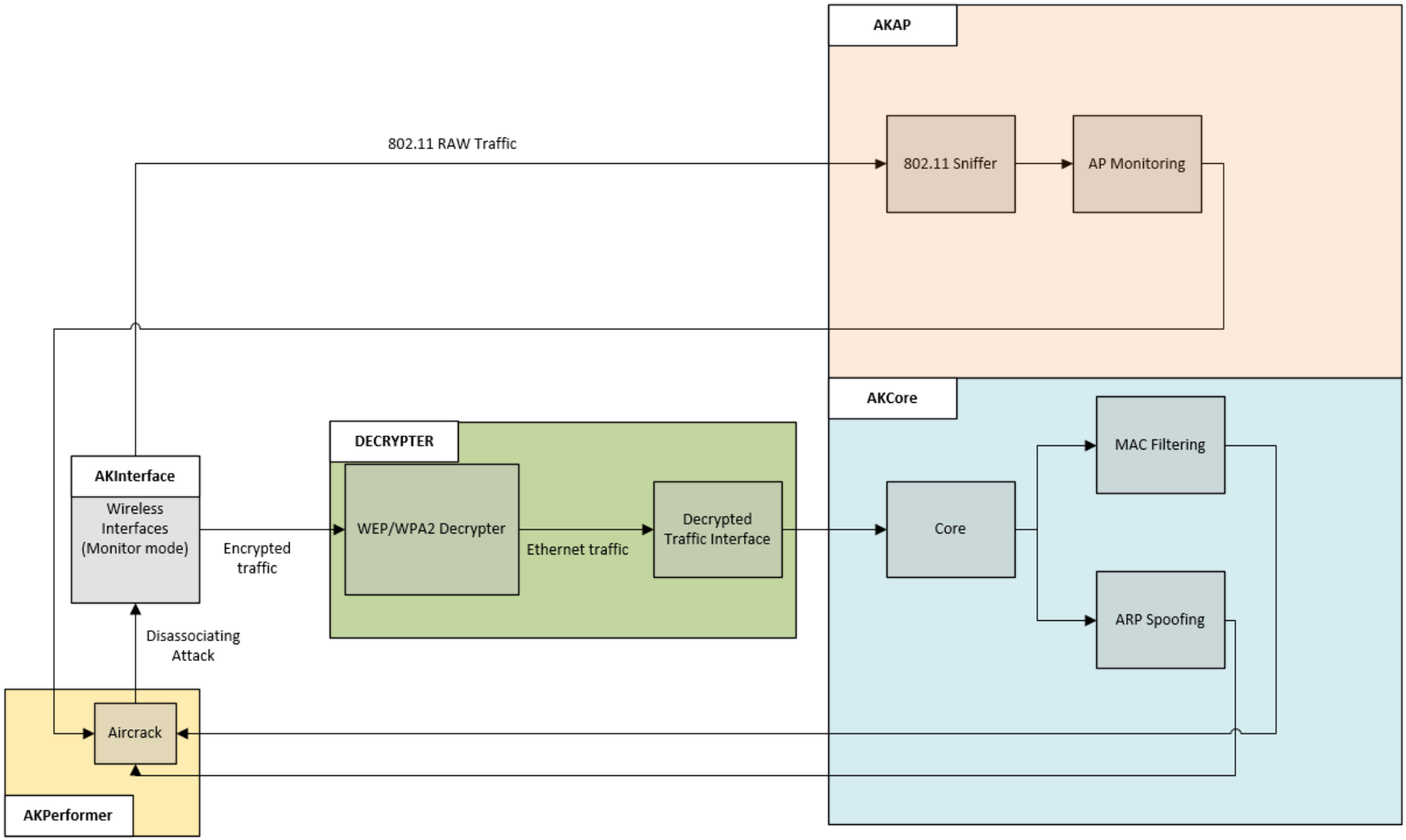


Figura A4-1: Arquitectura modular de Antikörper

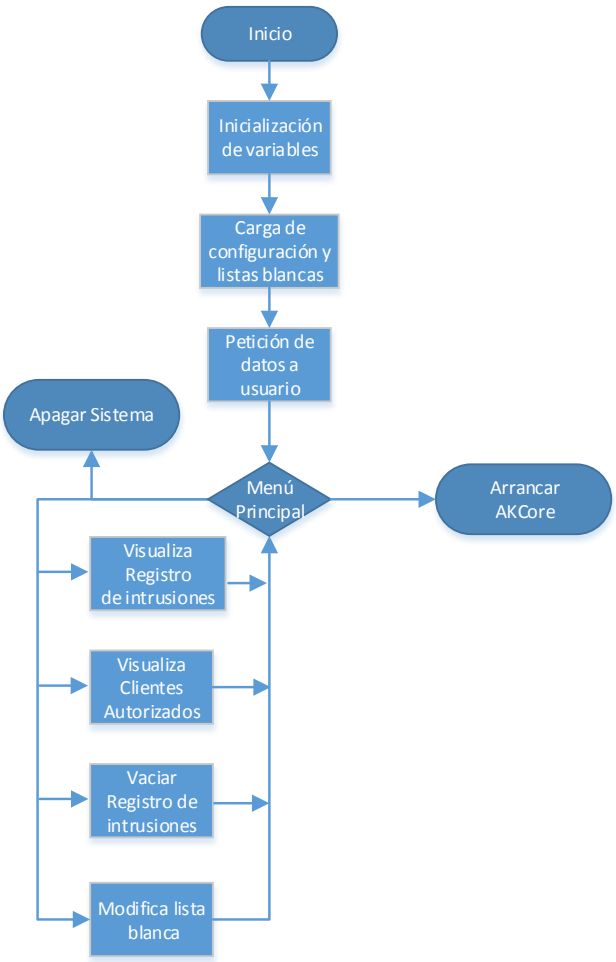


Figura A4-2: Diagrama de flujo de 1º Fase de AntikörperCore

- **Visualizar clientes autorizados.** Permitirá al usuario visualizar la lista blanca de usuarios autorizados en las que se contendrá la dirección MAC de estos.

- **Vaciar registro de intrusiones.** Permitirá reiniciar los registros mantenidos de sesiones anteriores.

- **Modificar lista blanca.** Permitirá introducir o eliminar usuarios autorizados de la lista blanca que mantiene el sistema.

- **Arrancar AKCore.** Arrancará el módulo de análisis principal del programa, que se encargara de analizar el tráfico obtenido por los interfaces de red. Se expondrá su diagrama en la Figura A4-3.

- **Apagar Sistema.** El sistema se apagará guardando toda la configuración y los ficheros de registro generados.

Como podemos observar en el diagrama, el sistema se mantendrá en un ciclo de menú siempre que no seleccionemos la opción de Arrancar AntikörperCore o Apagar Sistema.

A4.1.1 Diagrama de flujo interno de AntikörperCore

En el diagrama de la Figura A4-3 se muestra el funcionamiento interno del módulo AKCore, así como todos los procesos que va ejecutando.

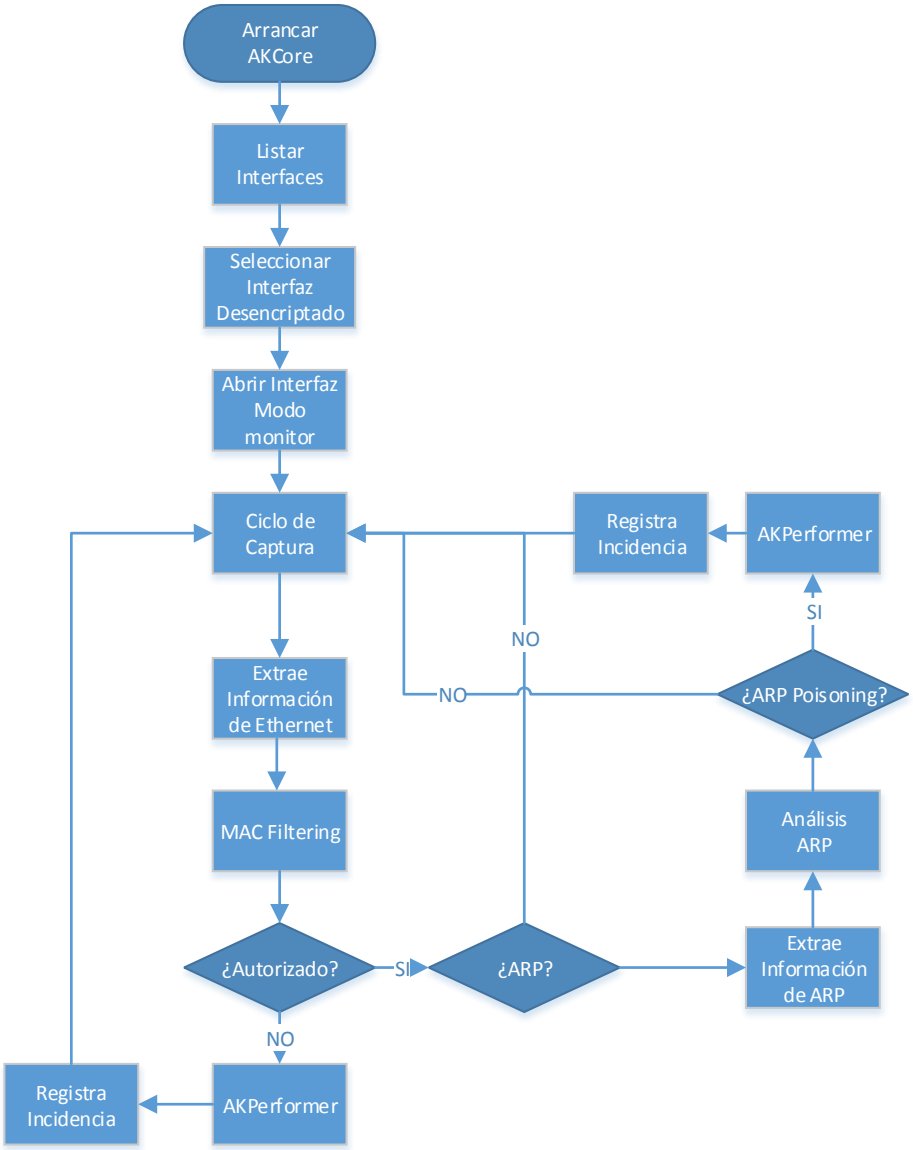


Figura A4-3: Diagrama de flujo de 2º Fase de AntikörperCore

- **Listar interfaces.** El sistema buscara e inicializara todos los interfaces disponibles en el equipo anfitrión.

- **Seleccionar interfaz de desencriptado.** El interfaz a seleccionar en este caso será en creado por el módulo de desencriptación, que no será más que un interfaz puente entre el tráfico encriptado y el desencriptado.
- **Abrir interfaz en modo monitor.** El sistema preparará el interfaz seleccionado para la captura del tráfico para su análisis posterior.

- **Ciclo de captura.** El sistema capturará los paquetes de tráfico uno a uno e irá generando un proceso de análisis por cada uno de ellos.

- **Extrae información Ethernet.** Se volcará la cabecera Ethernet de cada paquete a una de las estructuras de datos generadas anteriormente.

- **Mac Filtering.** Se realiza un filtrado MAC basándonos en las direcciones de la cabecera del paquete y la lista blanca que mantiene el sistema.

Una vez llegado a este punto evaluará si la máquina origen del paquete está autorizada a estar en la red, en caso de que no lo esté, registrará la incidencia y llamará al módulo AKPerformer. Tras esto volverá a esperar la llegada de un nuevo paquete.

En caso de que la máquina origen este autorizada, analizará si es un paquete ARP. En caso de no serlo, volverá a esperar un nuevo paquete. En caso de que sea un paquete ARP:

- **Extrae información ARP.** Se volcará la cabecera ARP del paquete a una de las estructuras de datos definidas.

- **Análisis ARP.** Se analizará la existencia de un posible envenenamiento ARP mediante una firma genérica de ataque.

Aquí se evaluará si existe ARP Poisoning. En caso de que exista, se llamará al módulo AKPerformer, se registrará la incidencia y se volverá a esperar un nuevo paquete. En caso de que no hubiese ARP Poisoning, se esperaría un paquete directamente.

Estos serán los pasos que seguirá Antikörper Core en su funcionamiento. Se analizará su diseño a nivel bajo en el Capítulo de Implementación.

A4.2 Diagramas de flujo de AntikörperAP

AntikörperAP será la parte del sistema encargada de analizar el tráfico RAW 802.11 en busca de posibles Rogue APs. La Figura A4-4 muestra la primera fase en el arranque de AntikörperAP, en la que se inicializa el sistema y se ofrecen diferentes opciones del funcionamiento al usuario.

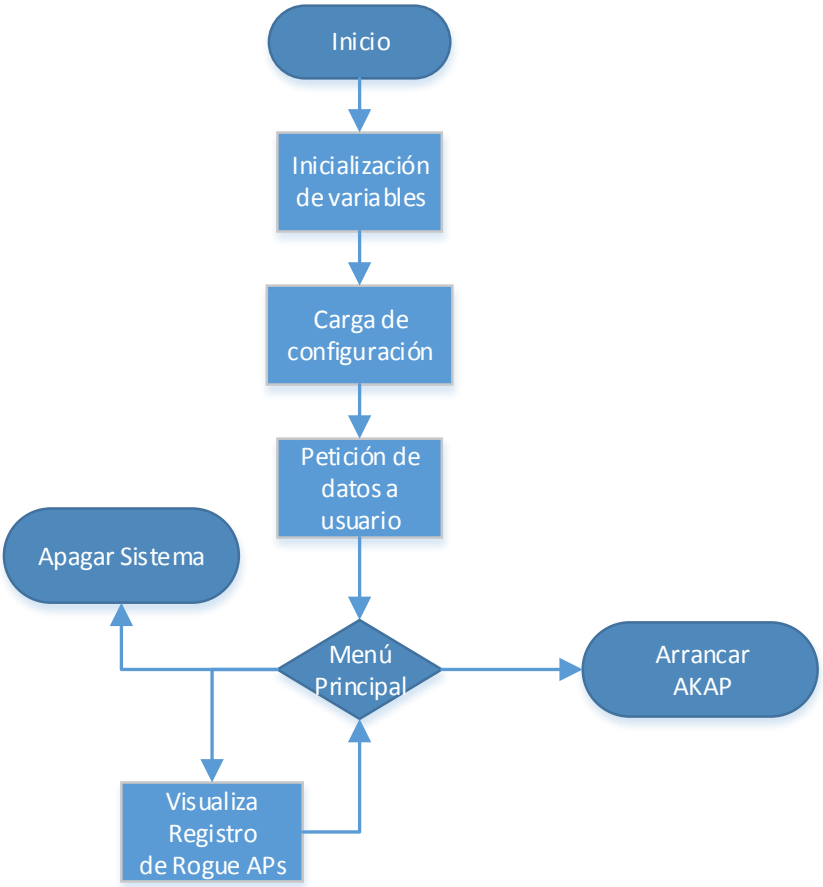


Figura A4-4: Diagrama de flujo de 1º Fase de AntikörperAP

- **Inicialización de variables.** El sistema incluirá los ficheros de cabecera en la directiva del preprocesador, inicializará las diferentes estructuras de datos con las que se va a trabajar y se declararán una serie de variables globales de tipo especial que serán necesarias para hacer uso de las librerías utilizadas en la implementación. Todo esto será explicado más en detalle en el capítulo de implementación.

- **Carga de configuración y listas blancas.** El sistema cargará de los correspondientes ficheros de configuración su configuración básica.

- **Petición de datos al usuario.** El sistema pedirá datos referentes a la configuración básica de la red a proteger, entre los que se encontrará la BSSID y la SSID de la red.

- **Menú de selección.** Mostrará al usuario distintas opciones:

- **Visualizar registro de Rogue APs.** Permitirá al usuario visualizar los registros de los Rogue APs detectados en sesiones anteriores.
- **Arrancar AKAP.** Arrancará el módulo de análisis principal de AntikörperAP, que se encargará de analizar el tráfico 802.11 RAW obtenido por los interfaces de red. Se expondrá su diagrama en la Figura A4-5.

- **Apagar Sistema.** El sistema se apagara guardando toda la configuración y los ficheros de registro generados.

Como podemos observar en el diagrama, el sistema se mantendrá en un ciclo de menú siempre que no seleccionemos la opción de Arrancar AntikörperAP o Apagar Sistema.

A4.2.1 Diagrama de flujo interno de AntikörperAP

En la Figura A4-5 se muestra el funcionamiento interno del módulo AntikörperAP, así como todos los procesos que va ejecutando.

- **Listar Interfaces.** El sistema buscarán e inicializarán todos los interfaces disponibles en el equipo anfitrión.

- **Seleccionar Interfaz.** El interfaz a seleccionar en este caso será un módulo en modo monitor que sea capaz de capturar tráfico RAW 802.11.

- **Abrir interfaz Modo monitor.** El sistema preparará el interfaz seleccionado para la captura del tráfico para su análisis posterior.

- **Ciclo de Captura.** El sistema capturarán los paquetes de tráfico uno a uno e irá generando un proceso de análisis por cada uno de ellos.

- **Extrae información RadioTAP.** Se volcará la cabecera RadioTAP de cada trama a una estructura de datos de tráfico 802.11.

Con esa información de cabecera, el sistema ha de analizar basándose en la estructura de cabecera 802.11 si esa trama es una trama Beacon, la cuales nos interesan ya que son las que portan información de los AP.

En caso de que sea una trama distinta a una de tipo Beacon Frame, se esperará una nueva trama. Si es una trama Beacon:

- **Extrae BSSID y SSID.** Se extraerá la BSSID y SSID que anuncian los AP a través de las tramas.

A partir der aquí, se hará un análisis en dos pasos:

1. Se comparará la SSID anunciada en la trama con la SSID oficial de nuestra red. En caso de que no sea la de nuestra red, se esperará una nueva trama de anuncio.
2. Se comparara el BBSID anunciada en la trama con la BBSID de nuestro punto de acceso oficial. En caso de que sean iguales querrá decir que la trama proviene de nuestro AP. En cambio, si las BSSIDs son diferentes, querrá decir que hay un AP anunciándose con nuestro nombre, por lo que será un Rogue AP. Por lo tanto, se llamará al módulo AKPerformer y se registrará la incidencia.

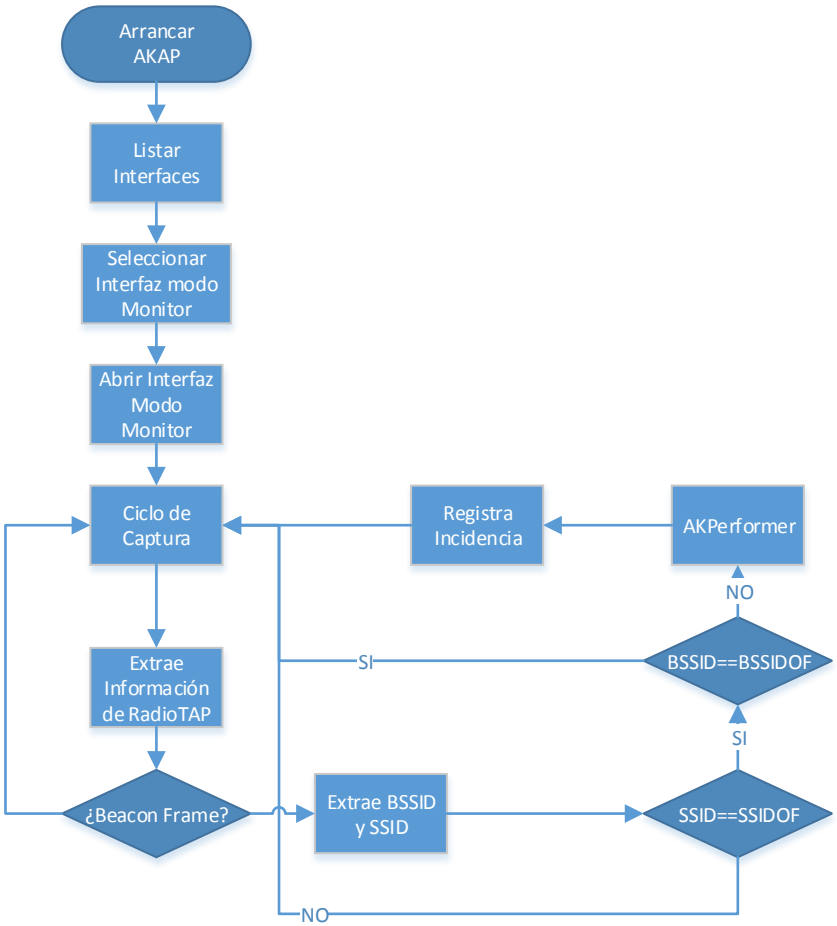


Figura A4-5: Diagrama de flujo de 2º Fase de AntikörperAP

A4.3 Diagramas de flujo de AKPerformer

Este será el módulo de actuación frente a amanezcas. Se apoyará en la suite de herramientas Aircrack-ng, más concretamente en aireplay-ng, para inyectar tráfico de disasociación en la red, inhabilitando así la amenaza. Podemos observar el diagrama de flujo del módulo en la Figura A4-6.

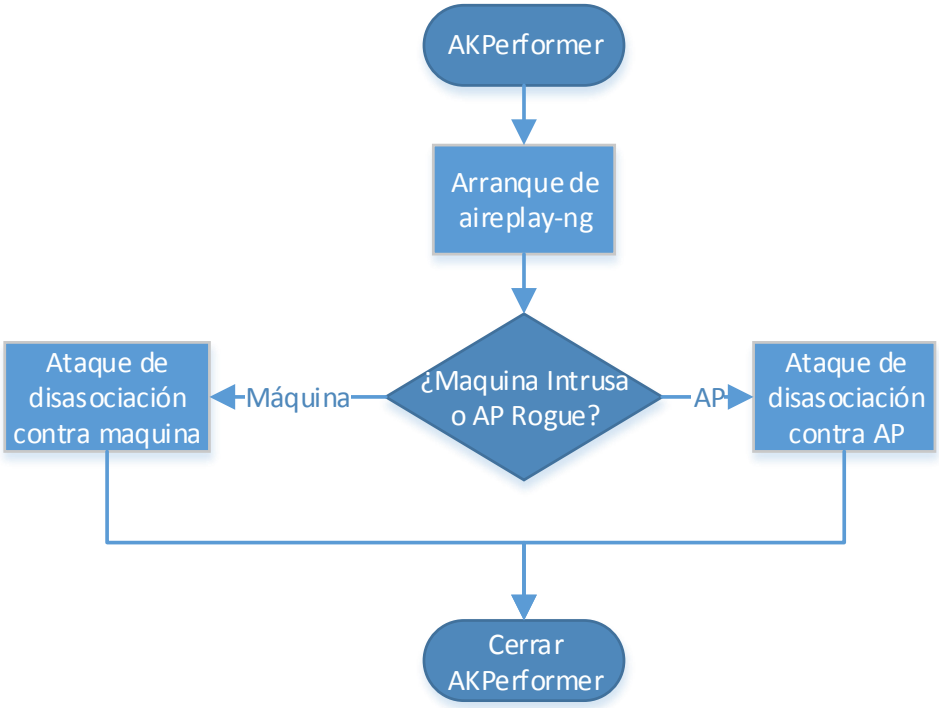


Figura A4-6: Diagrama de flujo de módulo AKPerformer

Debido a que la herramienta aireplay-ng no requiere demasiados recursos y se desea enviar flujo de unas pocas tramas de disasociación para no saturar la red, se ha visto conveniente no tener el modulo arrancado en todo momento.

Una vez el modulo sea llamado, este seleccionara automáticamente el interfaz inyector en modo monitor e interpretará el comando enviado por AntikörperCore o AntikörperAP. En caso de que la amenaza provenga de un máquina intrusa en nuestra red, se enviara tráfico de disasociación a esa máquina obligándola a disasociarse e imposibilitando que acceda a los servicios de la red.

En caso de que la amenaza provenga de un Rogue AP, se inundara el nivel 802.11 físico con tráfico de disasociación proveniente de ese AP para que las posibles víctimas no puedan asociarse al punto de acceso.

A4.4 Diseño de los módulos del sistema

A continuación se expone la implementación de un prototipo de Antikörper completamente funcional que satisfaga todas las especificaciones que se impusieron a la hora de definir el proyecto.

A4.4.1 Módulos principales

A continuación se expondrán cada uno de los módulos que componen Antikörper y se dará una explicación exhaustiva de su funcionamiento y desarrollo.

A4.4.1.1 AKInterface

Los interfaces de red serán los únicos elementos del sistema que interaccionarán con la red a proteger y sus usuarios. Dependiendo del tamaño de la red, deberemos incluir un número indeterminado de interfaces, siendo dos el número mínimo de interfaces para hacer funcionar el sistema de manera correcta, y pudiendo aumentar el número en caso de que la red disponga de varios puntos de acceso y necesitemos cubrir un rango de protección mayor.

Las necesidades técnicas referentes a los interfaces vienen dadas por el uso de ese interfaz por el sistema:

- **Interfaces de captura de tráfico.** Interfaces básicos con soporte para modo monitor.
- **Interfaces de actuación frente a intrusos.** Interfaces con soporte para modo monitor, preferiblemente interfaces preparados para la inyección de tráfico.

Como se ha dicho previamente, independientemente del uso que le vayamos a dar al interfaz, es necesario ponerlo en modo monitor. Para ello:

```
iwconfig [interface] mode monitor
```

En caso de utilizar Aircrack-ng como herramienta:

```
airmong start [interface]
```

Antikörper permitirá escoger al usuario el interfaz desde el que arrancar el sistema mediante.

A4.4.1.2 Decrypter

Este módulo será el encargado de capturar el tráfico y desencriptarlo en vivo, soportando WEP/WPA2 (AES y TKIP) y creando un interfaz puente al que redireccionar el tráfico ya desencriptado para el procesado en módulos posteriores.

- **Funcionamiento**

El módulo requerirá un interfaz en modo monitor desde el que capturar tráfico. Tras esto, con una información básica de la red entre los que serán necesarios el SSID y el BSSID de la red será capaz de encapsular el tráfico en tramas Ethernet fácilmente tratables.

En caso de que el protocolo de seguridad de la red sea WEP, el módulo desencriptará el tráfico de la red mediante la clave compartida en la red.

Por otro lado, en caso de usar el protocolo WPA/WPA2, el módulo desautenticará a todos los usuarios de la red deshabilitándola durante unos segundo y comenzará a capturar tráfico a nivel 802.11. De esta forma, se esperará a capturar las Beacon Frames para así identificar las BSSID asociadas a cada SSID. Tras esto, esperará a los mensajes EAPOL en los que, mediante el llamado EAPOL Handshake entre las estaciones y la Access Point, se obtendrán las claves con las que desencriptar el tráfico.

- **Desarrollo**

El desarrollo de este módulo se realizara mediante la librería multiplataforma basada en C++ **libtins** (30) y el software dot11decrypt (29) modificado y actualizado para funcionar con Antikörper.

A4.4.1.3 AntikörperCore/AntikörperAP

Estos serán los programas de los que constará Antikörper y serán los encargados de trabajar con el tráfico capturado por el módulo Decrypter y el módulo de interfaces.

- **Funcionamiento**

AntikörperCore recibirá el tráfico enviado por el módulo Decrypter y lo analizará en busca de algún ataque ARP Poisoning, así evitando los ataques derivados de este. A la vez, realizara un MAC Filtering mediante un fichero de direcciones MAC de los equipos autorizados en la red, introducidas por el usuario en el sistema.

AntikörperAP analizará el tráfico capturado directamente del interfaz a nivel 802.11 y filtrara las Beacon Frames, obteniendo de estas la SSID y la BSSID de todos los puntos de acceso en el rango del sistema. Tras esto buscará la existencia de ataques AP Rogue de estos Access Point.

- **Desarrollo**

Estos dos programas han sido desarrollados en su totalidad mediante el lenguaje de programación C y la librería **libpcap**. Se ha optado por el lenguaje C debido a su alto rendimiento y disponibilidad al trabajar a nivel del hardware de la máquina.

AKCore

AKCore será el núcleo de AntikörperCore y será el encargado de procesar el tráfico capturado en busca de amenazas. Para su implementación:

Lo primero será incluir el fichero de cabecera de libpcap pcap.h en la directiva del preprocesador:

```
#include <pcap.h>
```

Con el objetivo de poder filtrar los paquetes dependiendo del tipo que sean, definiremos los tipos de la siguiente manera:

```
//Tipos de definiciones de paquetes ethernet
#define     ETHERTYPE_PUP           0x0200      /* Xerox PUP */
#define     ETHERTYPE_IP            0x0800      /* IP */
#define     ETHERTYPE_ARP           0x0806      /* Address resolution */
#define     ETHERTYPE_REVARP        0x8035      /* Reverse ARP */
```

También será necesario definir las cabeceras sobre las que será volcada la información del paquete, para ello:

Ethernet header

```
/* Ethernet header */
struct sniff_ethernet {
    u_char ether_dhost[ETHER_ADDR_LEN]; /* Destination host address */
    u_char ether_shost[ETHER_ADDR_LEN]; /* Source host address */
    u_short ether_type;                 /* IP? ARP? RARP? etc */
      };
```

ARP header

```
/* ARP Header, (assuming Ethernet+IPv4)            */
#define ARP_REQUEST 1   /* ARP Request             */
#define ARP_REPLY 2     /* ARP Reply               */
typedef struct arphdr {
    u_int16_t htype;    /* Hardware Type           */
    u_int16_t ptype;    /* Protocol Type           */
    u_char hlen;        /* Hardware Address Length */
    u_char plen;        /* Protocol Address Length */
    u_int16_t oper;     /* Operation Code          */
    u_char sha[6];      /* Sender hardware address */
    u_char spa[4];      /* Sender IP address       */
    u_char tha[6];      /* Target hardware address */
    u_char tpa[4];      /* Target IP address       */
}arphdr_t;
```

A continuación se declararán una serie de variables globales de tipo especial para pcap las cuales serán necesarias para trabajar con la librería:

```
char *dev;                    /*Fichero desde el que monitorizar*/
char errbuf[PCAP_ERRBUF_SIZE]; /*Cadena de error*/
pcap_t* descr;                /*Descriptor de la sesion*/
struct bpf_program fp;         /* En caso de querer aplicar filtros */
bpf_u_int32 pMask;             /* Mascara de subred propia */
bpf_u_int32 pNet;              /* Dirección IP propia*/
pcap_if_t *alldevs, *d; /*Lista de volcado de interfaces*/
```

Lo primero que hará el software será pedir al usuario la dirección IP del Gateway, la dirección MAC del Access Point y la BSSID del Access Point.

NOTA: En Access Points de bajo coste, los fabricantes utilizan diferentes BSSID y direcciones Ethernet del Gateway (Fusión Router-Modem), por lo que BSSID es la Ethernet +/- 1, p.e. 00-04-01-ad-cf-45 para la Ethernet y 00-04-01-ad-cf-46 para la BSSID.

Una vez pedidos los datos al usuario, cargará a una lista enlazada las direcciones MAC de las estaciones autorizadas. Tras esto el sistema comenzará a analizar el equipo en busca de interfaces desde los cuales monitorizar y volcará los interfaces a la lista previamente declarada:

```
if (pcap_findalldevs(&alldevs, errbuf) == -1)
    {
        fprintf(stderr,"Error in pcap_findalldevs: %s\n", errbuf);
        exit(1);
    }
```

Mostrará al usuario por pantalla los interfaces disponibles:

```
printf("\nLista de dispositivos disponibles en el sistema:\n\n");
    for(d=alldevs; d; d=d->next)
    {
        printf("%d. %s", ++i, d->name);
        if (d->description)
            printf(" (%s)\n", d->description);
        else
            printf("(Sorry,   No   description   available   for   this
device)\n");
    }
```

Pedirá al usuario la selección de uno de los interfaces, donde el usuario deberá introducir el nombre completo del interfaz:

```
printf("\n Interfaz desde el que capturar tráfico : ");
    getchar();
    fgets(dev_buff, sizeof(dev_buff)-1, stdin);
```

Analizará si se ha introducido correctamente el interfaz y si este existe:

```
if(strlen(dev_buff))
    {
        dev = dev_buff;
        printf("\n ---A solicitado capturar en interfaz [%s] ---\n\n
Iniciando Captura...",dev);
    }
if(dev == NULL)
    {
        printf("\n[%s]\n", errbuf);
        return -1;
    }
```

Una vez declarado el interfaz desde el que capturar el tráfico, se obtendrá la información básica del interfaz, entre ella la dirección IP y la máscara de subred:

```
pcap_lookupnet(dev, &pNet, &pMask, errbuf);
```

Y por último se abrirá el interfaz para capturar el tráfico desde el:

```
descr = pcap_open_live(dev, BUFSIZ, 0,-1, errbuf);
    if(descr == NULL)
    {
        printf("pcap_open_live() failed due to [%s]\n", errbuf);
        return -1;
    }
```

Entre los argumentos de la función tendremos:

1. El interfaz desde el que capturar.
2. Tamaño del buffer.
3. Si se debe establecer el modo promiscuo en el interfaz (0 si, -1 no).
4. Read timeout de la captura (-1 por defecto).
5. Buffer de error.

Una vez abierto el interfaz, cada vez que se reciba un paquete se deberá procesar, para ello se utilizara la siguiente función:

```
pcap_loop(descr,-1, callback, NULL);
```

Sus argumentos serán:

1. Descriptor de la sesión.
2. Numero de paquetes a recibir (-1 sin límite).
3. Función para tratar el paquete.
4. NULL.

Hasta aquí el software irá recibiendo paquetes de manera indefinida y pasándole el paquete a una función cíclica de trata de paquetes:

```
void callback(u_char *useless,const struct pcap_pkthdr* pkthdr,const
u_char* packet)
```

La función callback recibirá diferentes punteros apuntando a los paquetes recibidos y a las cabeceras de estos. Definiremos un puntero a la cabecera Ethernet declarada en libpcap, para así poder extraer las direcciones MAC y demás información para realizar el MAC Filtering:

```
ethernet = (struct sniff_ethernet*)(packet); /*Puntero a cabecera
ethernet*/
```

Definiremos un puntero a la cabecera ARP declarada en libpcap, para así poder extraer las direcciones MAC de los paquetes ARP y demás información para realizar la detección ARP Poisoning:

```
arpheader = (struct arphdr *)(packet+14); /*Puntero a cabecera ARP*/
```

Pasaremos a analizar el paquete en busca de ARP Poisoning en caso de que el paquete sea de tipo ETHERTYPE_ARP.

```
if (ntohs (ethernet->ether_type) == ETHERTYPE_ARP)
```

En caso de que sea un paquete de tipo ARP, extraeremos de la cabecera las direcciones IP (fuente y destino) y las direcciones MAC (fuente y destino). Para ello deberemos convertirlas de formato hexadecimal a **ASCII** (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange).

```
sprintf(ipARPFuente,"%d.%d.%d.%d",arpheader->spa[0],arpheader-
>spa[1],arpheader->spa[2],arpheader->spa[3]);

sprintf(macARPFuente,"%02X:%02X:%02X:%02X:%02X:%02X",arpheader-
>sha[0],arpheader->sha[1],arpheader->sha[2],arpheader-
>sha[3],arpheader->sha[4],arpheader->sha[5]);

sprintf(ipARPDestino,"%d.%d.%d.%d",arpheader->tpa[0],arpheader-
>tpa[1],arpheader->tpa[2],arpheader->tpa[3]);

sprintf(macARPDestino,"%02X:%02X:%02X:%02X:%02X:%02X",arpheader-
>tha[0],arpheader->tha[1],arpheader->tha[2],arpheader-
>tha[3],arpheader->tha[4],arpheader->tha[5]);
```

Una vez obtenida la información del paquete ARP, se analizará si existe un envenenamiento ARP.

```
arppoisoning(ipARPFuente,macARPFuente);

void arppoisoning(char *datoip,char *datomac)
{
    //Evalua si las IP del ARP y del AP coinciden
    if(strcmp(datoip,ipAP)==0)
    {

        //Evalua si las MAC del ARP y del AP son diferentes
        if(strcmp(datomac,macAP)!=0)
        {
            savefile(datomac,1);
            actuador(datomac);
            printf("\nARP Poisoning en maquina %s\n",datomac);

        }
    }
}
```

Primero comparará que el paquete que anuncia ser el Gateway de la red y, en caso de serlo, evalúa si la dirección MAC fuente del mensaje es la oficial de la red. En caso de no serlo, se concluirá que es un ARP Poisoning, se registrara la incidencia y se generará un ataque de disasociación para expulsar de la red al atacante.

Tras analizar si el paquete recibido es ARP o no, extraeremos de la cabecera las direcciones MAC (fuente y destino) del paquete Ethernet. Para ello deberemos convertirlas de formato hexadecimal a ASCII.

```
sprintf(fuenteMAC,"%02X:%02X:%02X:%02X:%02X:%02X",ethernet-
>ether_shost[0],ethernet->ether_shost[1], ethernet->ether_shost[2],
ethernet->ether_shost[3],ethernet->ether_shost[4], ethernet-
>ether_shost[5]);

sprintf(destinoMAC,"%02x:%02x:%02x:%02x:%02x:%02x\n",ethernet-
>ether_dhost[0],ethernet->ether_dhost[1], ethernet->ether_dhost[2],
ethernet->ether_dhost[3],ethernet->ether_dhost[4], ethernet-
>ether_dhost[5]);
```

Tras obtener las direcciones MAC del paquete Ethernet, se llamará a una función que buscara la existencia de la dirección fuente del paquete en la lista enlazada contenedora de las direcciones MAC de las estaciones autorizadas.

```
/*Evalua si las direcciones MAC estan autorizadas*/
if(cicloanalisis(lista,fuenteMAC)!=1)
{
        savefile(fuenteMAC,0);

        printf("Hay usuarios no autorizados en la red MAC:
%s\n",fuenteMAC);
        actuador(fuenteMAC);
}
```

En caso de que la función nos comunique que la dirección MAC no está entre las autorizadas, registrara la incidencia y generara un ataque de disasociación contra el intruso.

AKAP

AKAP será el núcleo de AntikörperAP y será el encargado de procesar el tráfico capturado en busca de puntos de acceso maliciosos. Para su implementación:

Al igual que en AKCore, lo primero será incluir el fichero de cabecera de **libpcap** pcap.h en la directiva del preprocesador:

```
#include <pcap.h>
```

La funciones de captura usan el tipo de dato **uint8_t** que viene con el fichero de cabecera netinet/in.h. Este formato es necesario para trabajar sobre el tráfico RAW a nivel del protocolo 802.11.

```
#include <netinet/in.h>
```

La funcionalidad principal de AKAP es la de escanear el entorno inalámbrico en busca de puntos de acceso. Para ello, debe trabajar con el trafico 802.11, en concreto, los Beacon Frames enviados por los APs. Estos contienen toda la información sobre la red inalámbrica y son transmitidos periódicamente para anunciar la presencia de la red WLAN.

La información con la que están formados los Beacon Frames es la siguiente:

```
SSID
Rangos soportados
Frequency-hopping (FH)
Direct-Sequence (DS)
Contention-Free (CF)
IBSS
Mapa de indicación de tráfico (TIM)
```

Debido a la complejidad al tratar con estas tramas, debemos trabajar con las longitudes de los campos de la cabecera. Para ello, necesitamos un tipo de datos de estructura para reunir el valor uint8_t antes comentado.

```
//Para el valor it_len
struct radiotap_header {
uint8_t it_rev;
uint8_t it_pad;
uint16_t it_len;
};
```

Al igual que en AKCore, el usuario deberá introducir una serie de datos necesarios para hacer funcionar el software correctamente. Estos datos son:

- SSID de la red
- BSSID de la red
- Dirección MAC del interfaz sobre el que trabaja AKAP.

Tras esto, utilizando las mismas funciones usadas en AKCore, AKAP arrancará una captura de tráfico desde el interfaz solicitado. Al recibir un nuevo paquete de datos, utilizará una función cíclica para tratar estos. Dentro de ella comenzaremos definiendo los punteros de la información que queremos obtener:

```
const u_char *bssid;
const u_char *essid;
```

Creamos un puntero y lo asignamos a una estructura de tipo **radiotap_header**. Mediante esa estructura seremos capaces de calcular la longitud del **offset**:

```
rtaphdr = (struct radiotap_header *) packet;
offset=rtaphdr->it_len;
```

Una vez tengamos el offset, podemos filtrar los paquetes en busca de los Beacon Frames:

```
if(packet[offset] == 0x80)
```

A continuación extraeremos del paquete la SSID y la BSSID. Esto lo haremos tras analizar teóricamente la estructura de los Beacon Frames de 802.11, donde la BSSID está a 36 bytes de distancia desde el inicio y la ESSID/SSID está a 64 bytes.

```
bssid = packet + 36;
essid = packet + 64;
```

El BSSID es fácil de extraer, debido a que corresponde a los 6 bytes de los que está compuesta la dirección MAC del AP. En cambio, el ESSID/SSID puede tener una longitud aleatoria, por lo que, tras analizar la estructura de los Beacon Frames, sabemos que este campo acaba en un byte terminado igual que 0x1. Para ello recorremos el paquete hasta encontrarlo:

```
while(essid[i] > 0x1)
{
        ssid[i] = essid[i];
        i++;
}
```

Esto nos volcará la ESSID a una variable SSID en la que quedará registrada la SSID del punto de acceso origen del Beacon Frame. Por último desharemos el formato hexadecimal de la BSSID para poder trabajar con ella:

```
sprintf(macAP,"%02X:%02X:%02X:%02X:%02X:%02X\n",bssid[0],bssid[1],bssi
d[2],
bssid[3], bssid[4], bssid[5]);
```

Una vez tengamos toda la información del Beacon Frame, realizaremos un análisis de la información obtenida en busca de un ataque Rogue AP. Para ello:

```
void cicloanalisis(char *data1,char *data2)
{                   //ssid      //bssid
        //mismos nombres
       if(strstr(data1,ssidof)!=NULL)
       {
            //diferentes macs
            if(strstr(data2,bssidof)==NULL)
            {
                printf("Rogue AP en %s\n",data2);
                savefile(ssid);
                actuador();
            }
       }
}
```

En el algoritmo arriba expuesto, comenzaremos evaluando si la SSID anunciada en el Beacon Frames es la misma que al oficial del Access Point de la red que queremos proteger. En caso de serlo, compararemos las BSSID del Beacon Frame y las de Access Point oficial, y en caso de ser distintos, concluiremos que el Beacon Frame proviene de un Rogue

AP. Tras eso registraremos la incidencia y se llamará al módulo AKPerformer para deshabilitar el Rogue AP.

A4.4.1.4 AKPerformer

Mientras que los otros módulos se encargan de capturar, tratar y analizar el tráfico de la red, el módulo AKPerformer será el encargado de tomar acciones frente a las intrusiones y los atacantes.

- **Funcionamiento**

Una vez invocado, ya sea por AKCore o AKAP, se encargará de tomar acciones mediante un ataque de disasociación a la entidad intrusa. Pudiendo ser esta un host de la red o un Access Point. En caso de ser un host de la red, generará un ataque de disasociación contra el host intruso obligando al Access Point a disasociar a este. En cambio, en caso de enfrentarnos a un Rogue AP, el AKPerformer inundará el entorno 802.11 físico de mensajes de disasociación en broadcast a todos los host de la red, para que sean incapaces de acceder a los servicios del Rogue AP.

- **Desarrollo**

Para el desarrollo de este módulo, nos hemos apoyado en la herramienta Aircrack-ng. Para ello, hemos utilizado la funcionalidad airplay de Aircrack que nos ofrece la capacidad de realizar ataques de disasociación mediante el envío de tramas de disasociación a la red.

Se invocará a Aircrack mediante una llamada en segundo plano al Bash de Linux. Los comandos tendrán la siguiente estructura:

Disasociación de un host de la red

```
void actuador(char *data)
{
    char cmd[100];
    sprintf(cmd, "sudo aireplay-ng -0 5 -a %s -c %s mon0 --ignore-
negative-one > /dev/null",etherAP,data);
    system(cmd);

}
```

Haciendo uso de la función system(), ejecutaremos un comando en donde se lanzará un comando que enviará cinco tramas (número suficiente para que no haya problemas de perdidas) de disasociación a través del interfaz en modo monitor, en donde el primer argumento dinámico será la dirección MAC del Access Point y el segundo es la dirección MAC del host a expulsar.

Esto nos permite mantener de manera rápida y sencilla a los intrusos excluidos de la red sobre la que está funcionando Antikörper. Donde en caso de que el intruso vuelva a conectarse a la red, en cuanto se detecten sus tramas de asociación al Access Point se le volverá a expulsar de la red.

Deshabilitar Rogue Access Point

```
void actuador()
{

    char cmd[100];
    sprintf(cmd, "aireplay-ng --deauth 10 -a %s -h %s mon0 -D >
/dev/null",bssidof,macinter);
    system(cmd);
}
```

Al igual que antes, utilizaremos la función system () para ejecutar un comando el cual lanzara 10 mensajes de disasociación cada vez que se detecte algo de tráfico proveniente del Rogue Access Point. En este caso el primer argumento dinámico será la dirección MAC del Rogue Access Point y el segundo será el interfaz monitor sobre el que trabaja Antikörper.

A4.4.2 Conclusión

El desarrollo del prototipo Antikörper ha concluido en un sistema estable, potente y capaz de cubrir la inmensa mayoría de los ataques que puedan surgir en una red WLAN. Aparte de ser un WIDS completamente funcional, tiene los valores añadidos de existir en un sector como el inalámbrico donde escasean lo IDS, ser semiautónomo con una sencilla configuración por parte del usuario, la capacidad de actuar automáticamente ante cualquier anomalía y ser fácilmente actualizable en futuras revisiones. Las capacidades de Antikörper se pondrán a prueba en el capítulo de pruebas de validación y rendimiento.

Anexo V – Presupuesto de despliegue

En este anexo se presenta un presupuesto de despliegue del sistema en la red interna de empresa pequeña, el cual se ha planteado como proyecto de continuación de este trabajo. Se comenzó con un estudio de la problemática del cliente, donde se realizó un mapa de la red de la empresa y tras su análisis, se aprobó el poder desplegar el sistema en la red. La red de la empresa se presenta en la Figura A5-1.

A5.1 Planificación

A continuación, se muestra la planificación y la asignación de tareas que se han de llevar a cabo para el despliegue completo del sistema, suponiendo que el cliente contrató el servicio a fecha 13 de abril del 2015.

A5.1.1 Asignación de tareas

A continuación, se expone en la Tabla A5-1 la asignación temporal de las tareas a llevar a cabo en el despliegue.

Tareas	Duración	Inicio	Fin
1. Estudio del entorno	**3**	**15/04/2015**	**17/10/2015**
1.1 Medidas de señal inalámbrica	1	15/04/2015	15/04/2015
1.2 Estudio de despliegue	2	16/04/2015	17/04/2015
2. Despliegue	**5**	**20/04/2015**	**24/04/2015**
2.1 Montaje de elementos de red	2	20/04/2015	21/04/2015
2.2 Instalación del sistema	2	22/04/2015	23/04/2015
2.3 Configuración del sistema	1	24/04/2015	24/04/2015
3. Fase de pruebas	**3**	**27/04/2015**	**29/04/2015**
3.1 Pruebas de funcionamiento	1	27/04/2015	27/04/2015
3.2 Pruebas de rendimiento	2	28/04/2015	29/04/2015
4. Entregas	**1**	**30/04/2015**	**30/04/2015**
4.1 Entrega del manual	1	30/04/2015	30/04/2015

Tabla A5-1: Tareas del despliegue

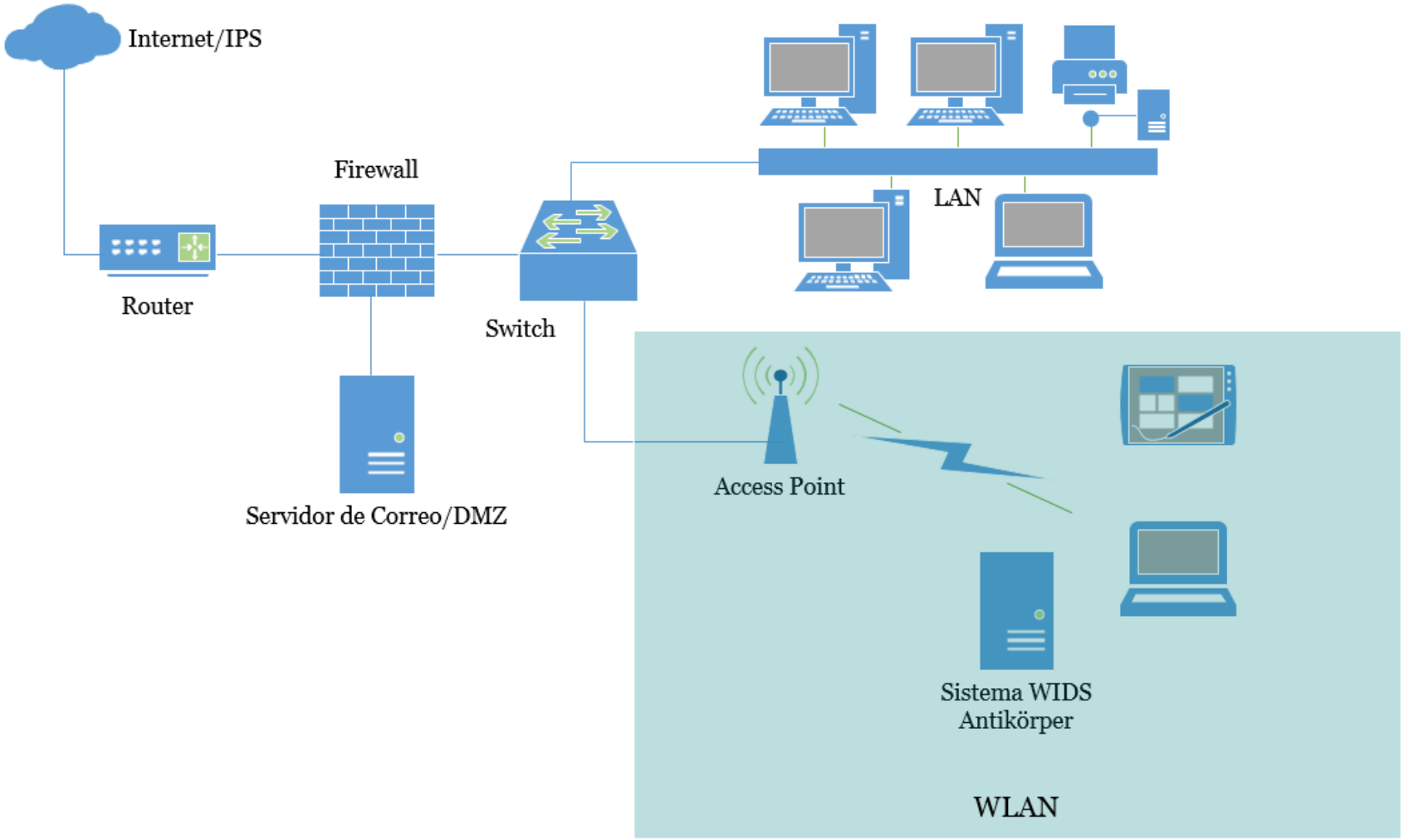


Figura A5-1: Red de empresa

A5.1.2 Diagrama de Gantt

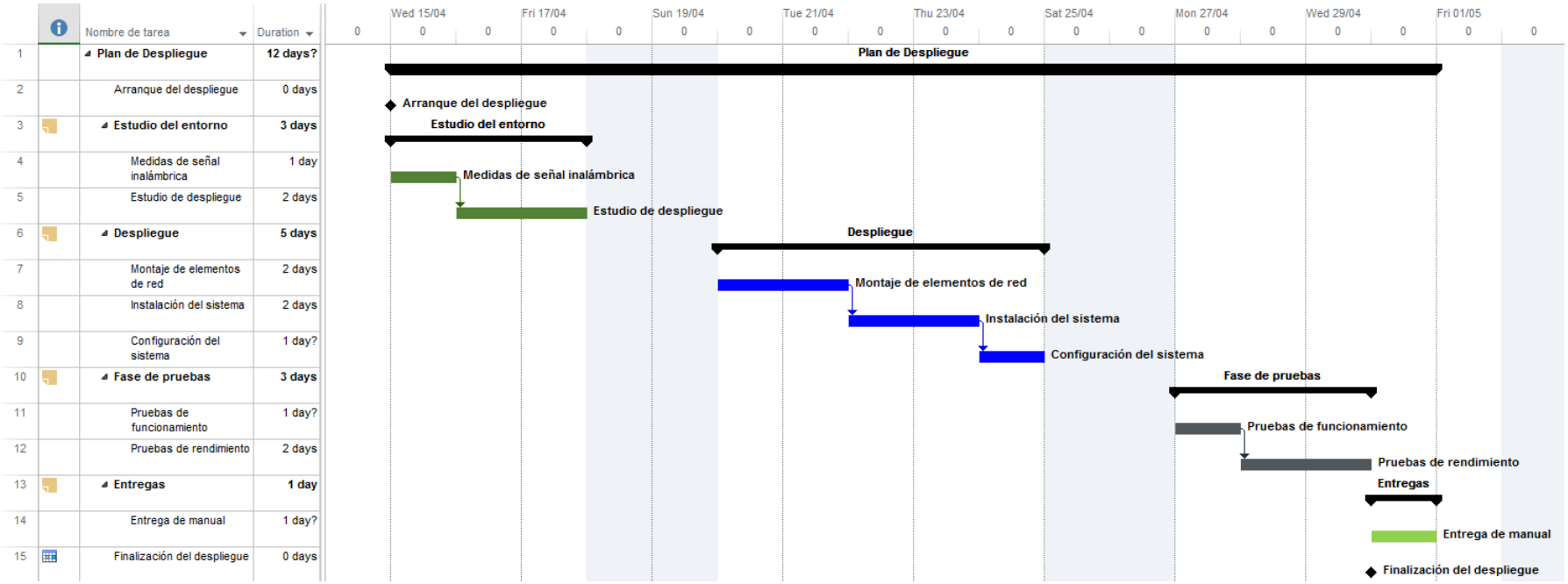


Figura A5-2: Diagrama de Gantt

A5.2 Presupuesto

El desglose de presupuesto va a realizarse en tres bloques principales, por un lado, el coste en recursos humanos utilizados en el despliegue, el coste de materiales utilizados en este y las subcontratas realizadas.

A5.2.1 Costes en recursos humanos

Para el cálculo de los costes en recursos humanos, se supondrá que un ingeniero júnior, con un sueldo base de 800 euros mensuales por una jornada de trabajo media de 20 horas semanales, será el encargado del estudio del entorno, de la instalación y configuración del sistema y de las pruebas sobre este.

*Costes de ingeniero júnior durante 9 días (800€/mes * 9 días)..... 300€*

Coste de Seguridad Social a cargo de la Empresa..... 69 €

A5.2.2 Costes materiales

Podemos dividir estos en dos grupos:

A5.2.2.1 Costes hardware

Se tienen en cuenta los recursos materiales utilizados en la instalación del sistema, contando los que la subcontrata ha de montar en la empresa del cliente.

Dell OptiPlex 7020..... 550 €

Tarjetas de red inalámbricas dedicadas ..... 50 €

A5.2.2.2 Costes software

Debido a que el sistema está basado en su totalidad en software libre, los costes de software son nulos.

A5.2.2.3 Costes asociados a consumibles

Material de oficina..... 15 €

A5.2.3 Subcontrataciones

Se subcontratará a una empresa que se encargará del montaje del equipo anfitrión del sistema y las obras necesarias para su despliegue (tomas eléctricas…).

Subcontrataciones..... 250 €

A5.2.4 Costes totales

La Tabla A5-2 presenta el desglose total del presupuesto.

Concepto	Coste (en euros)
Recursos humanos	369,00
Material	615,00
Subcontrataciones	250,00
Total	1234,00

Tabla A5-2: Presupuesto total del proyecto

Se observa que el coste de despliegue del proyecto en un entorno empresarial será de 1234,00 euros.

Anexo VI - Plan de pruebas y resultados obtenidos

A continuación se presenta el plan de pruebas realizado para el sistema Antikörper. Para ello, se harán una serie de pruebas de caja negra que permitirán validar el funcionamiento de los módulos y tras esto se integrarán los módulos y se probará el correcto funcionamiento del sistema en un escenario de red real. Por último, se realizará una batería de pruebas de campo con el fin de probar el rendimiento del sistema bajo distintas situaciones.

Cada prueba realizada se presenta en una tabla que contiene un identificador inequívoco y el procedimiento y la verificación de la prueba. Tras cada apartado, se recogerá en una tabla los resultados obtenidos tras la realización de cada prueba.

A6.1 Escenario de pruebas

El escenario de pruebas es similar a cualquier red real sobre la que se podría desplegar el sistema. La Figura A6-1 muestra el escenario de pruebas utilizado.

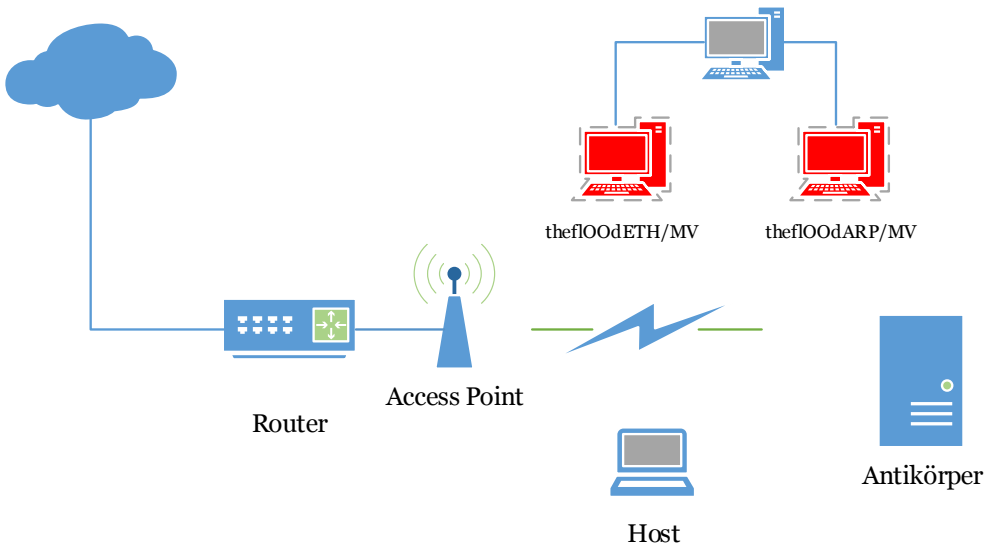


Figura A6-1: Escenario de pruebas

Observamos que el escenario de pruebas se compone de un Access Point que da servicio a una red WLAN. Entre las máquinas que se encuentran en la red tenemos el sistema Antikörper, una máquina host y un equipo con dos máquinas virtuales que ejecutan las herramientas theflOOdETH y theflOOdARP.

A6.2 Pruebas de caja negra

Estas pruebas tienen como objetivo principal el comprobar el correcto funcionamiento de los distintos elementos y componentes del sistema por separado, sin analizar la interacción que habrá entre ellos (esto se llevará a cabo en el apartado de Pruebas de Integración).

ID	PRCN-01
Objetivo	El objetivo de esta prueba será el comprobar que podemos configurar de manera correcta los interfaces de captura e inyección de tráfico del sistema
Procedimiento	▪ Se arranca el sistema Antikörper ▪ Se selecciona el interfaz desde el que capturar tráfico
Verificación	De manera manual se debe observar que los interfaces están configurados en modo monitor

Tabla A6-1: Prueba PRCN-01

ID	PRCN-02
Objetivo	El objetivo de esta prueba será el comprobar que el módulo Decrypter desencripta el tráfico independientemente de la técnica utilizada
Procedimiento	▪ Se configura distinta encriptación en el Access Point ▪ Se arranca el módulo y se introduce de manera manual la información referente a la red
Verificación	Se captura mediante cualquier sniffer de red el interfaz puente creado y se evalúa si el tráfico ha sido desencriptado

Tabla A6-2: Prueba PRCN-02

ID	PRCN-03
Objetivo	El objetivo de esta prueba será el comprobar que el módulo AKCore realiza de manera correcta el filtrado MAC y el análisis ARP
Procedimiento	▪ Se arranca un interfaz inalámbrico de los disponibles en el sistema a través de Antikörper ▪ Se manda tráfico mediante una máquina no autorizada en la red ▪ Se genera un ataque ARP Poisoning mediante la herramienta theflOOdARP
Verificación	Se visualiza mediante el interfaz de usuario si el sistema detecta las intrusiones

Tabla A6-3: Prueba PRCN-03

ID	PRCN-04
Objetivo	El objetivo de esta prueba será el comprobar que el módulo AKAP filtra las tramas Beacon y analiza su contenido en busca de Access Point maliciosos
Procedimiento	▪ Se arranca un interfaz inalámbrico de los disponibles en el sistema a través de Antikörper ▪ Se introduce la información referente a la red a proteger pero con una SSID errónea (para así simular un Rogue AP)
Verificación	Se visualiza mediante el interfaz de usuario cómo el sistema detecta el Access Point como malicioso

Tabla A6-4: Prueba PRCN-04

ID	PRCN-05
Objetivo	El objetivo de esta prueba será el comprobar que el módulo AKPerformer genera ataques de disasociación como respuesta frente a las intrusiones
Procedimiento	▪ Se arranca el módulo ▪ Se introduce la información de la máquina intrusa de manera manual
Verificación	Se visualiza mediante un sniffer de nivel 802.11 las tramas de disasociación y se ve cómo la máquina destino se desconecta de la red

Tabla A6-5: Prueba PRCN-05

A6.2.1 Resultados de pruebas de caja negra

ID	Resultado	Descripción del fallo (si procede)
PRCN-01	Satisfactorio	
PRCN-02	Satisfactorio	
PRCN-03	Satisfactorio	
PRCN-04	Satisfactorio	
PRCN-05	Satisfactorio	

Tabla A6-6: Resultados de pruebas PRCN

La ejecución de estas pruebas nos muestra el correcto funcionamiento de los módulos que componen Antikörper y nos da luz verde para poder realizar pruebas sobre el sistema con todos sus módulos funcionando en conjunto.

A6.3 Pruebas de integración

Las pruebas de integración se realizan una vez probado el funcionamiento correcto de los módulos que componen el sistema por separado.

Para realizar estas pruebas se despliega la red WLAN mostrada en la Figura A6-1 con una serie de máquinas contenedoras de diferentes herramientas para probar el rendimiento del sistema.

Como se ha ido comentando en capítulos anteriores, el sistema Antikörper se compone de dos programas individuales, AntikörperCore y AntikörperAP. En las pruebas de integración se ejecutará cada programa por separado y se comprobará que ambos cumplen sus funcionalidades.

ID	PRIN-01
Objetivo	El objetivo de esta prueba es el comprobar que AntikörperCore detecta intrusos dentro de la red
Requerimientos	Se requiere el funcionamiento de los módulos AKInterface, Decrypter, AKCore y AKPerformer
Procedimiento	▪ Se arranca el módulo Decrypter de manera separada configurando un interfaz puente por el que se emita el tráfico desencriptado. ▪ Se arranca AntikörperCore y se selecciona la opción de arranque del sistema desde el menú. ▪ Se selecciona el interfaz puente creado por el módulo Decrypter. ▪ Se introduce la BSSID y el SSID de la red en el sistema. ▪ Se generan ataques desde otras máquinas de red mediante las herramientas theflOOdARP y theflOOdETH
Verificación	Se visualiza mediante el interfaz de usuario si el sistema detecta las intrusiones y cómo las máquinas intrusas se disasocian de la red

Tabla A6-7: Prueba PRIN-01

ID	PRIN-02
Objetivo	El objetivo de esta prueba será el comprobar que AntikörperCore genera los ficheros de registro de intrusiones de manera correcta
Requerimientos	Se requiere el funcionamiento de los módulos AKInterface, Decrypter, AKCore y AKPerformer
Procedimiento	▪ Se genera de nuevo la prueba PRIN-01 ▪ Se apaga el sistema ▪ Se arranca el sistema
Verificación	Se selecciona mediante el menú de selección del interfaz de usuario visualizar el registro de intrusiones

Tabla A6-8: Prueba PRIN-02

ID	PRIN-03
Objetivo	El objetivo de esta prueba será el comprobar que AntikörperCore recoge, almacena y modifica los datos de usuarios autorizados
Requerimientos	Se requiere el funcionamiento de los módulos AKInterface, Decrypter, AKCore y AKPerformer
Procedimiento	▪ Se arranca AntikörperCore y se selecciona la opción de añadir un nuevo usuario autorizado en la lista blanca ▪ Se selecciona en el menú la opción de modificar la lista blanca ▪ Se borra un usuario autorizado ▪ Se apaga el sistema ▪ Se arranca el sistema ▪ Se visualiza la lista blanca
Verificación	Se ha de ver cómo el fichero de registro de usuarios autorizados va recogiendo los cambios

Tabla A6-9: Prueba PRIN-03

ID	PRIN-04
Objetivo	El objetivo de esta prueba será el comprobar que AntikörperAP detecta Access Point maliciosos en la red
Requerimientos	Se requiere el funcionamiento de los módulos AKInterface, AKAP y AKPerformer
Procedimiento	▪ Se arranca AntikörperAP y se selecciona la opción de arranque del sistema desde el menú. ▪ Se selecciona un interfaz que el sistema pone automáticamente en modo monitor. ▪ Se introduce la BSSID y el SSID de la red en el sistema junto a la dirección MAC del interfaz sobre el que está trabajando AntikörperAP. ▪ Se introduce la BSSID de la red a proteger de forma errónea para que el sistema detecte tráfico procedente de un AP con la misma SSID y diferentes BSSID, tratándolo así como un Rogue AP.
Verificación	Se visualiza mediante el interfaz de usuario si el sistema informa del Rogue AP y cómo no se nos permite conectarnos a esa red

Tabla A6-10: Prueba PRIN-04

ID	PRIN-05
Objetivo	El objetivo de esta prueba será el comprobar que AntikörperAP genera los ficheros de registro de Rogue APs de manera correcta
Requerimientos	Se requiere el funcionamiento de los módulos AKInterface, AKAP y AKPerformer
Procedimiento	▪ Se vuelve a realizar la prueba PRIN-04 ▪ Se apaga el sistema ▪ Se arranca el sistema ▪ Se selecciona en el menú la opción de visualizar el registro de Rogue APs
Verificación	Se ha de visualizar el registro del Rogue AP.

Tabla A6-11: Prueba PRIN-05

A6.3.1 Resultados de pruebas de integración

ID	Resultado	Descripción del fallo (si procede)
PRIN-01	Satisfactorio	
PRIN-02	Satisfactorio	
PRIN-03	Satisfactorio	
PRIN-04	Satisfactorio	
PRIN-05	Satisfactorio	

Tabla A6-12: Resultados de pruebas PRIN

Tras ejecutar las pruebas de integración sobre los dos programas que componen Antikörper, se ha concluido que el sistema funciona de manera satisfactoria cumpliendo las especificaciones y compromisos con los que fue concebido el proyecto.

A6.4 Pruebas de rendimiento

En este tipo de pruebas nos centraremos en medir el rendimiento del sistema base a una serie de parámetros:

- Cantidad de tráfico recibido
- Cantidad de intrusiones detectadas
- Cantidad de actuaciones generadas frente a las intrusiones

La metodología de estas pruebas será la de ejecutar el sistema y realizar las mediciones correspondientes en situaciones de estrés, como puede ser el inundar la red con tráfico inyectado o ataques generados mediante distintas herramientas.

A6.4.1 Características del entorno

A continuación, se detallan las características del equipo anfitrión sobre el que se llevan a cabo las pruebas de rendimiento.

Sistema

- Sistema IDS inalámbrico Antikörper (Prototipo)

Especificaciones técnicas

- Intel Core i5-4200M, 2, 5 GHz, 8 Gb de memoria RAM
- Interfaz red inalámbrico inyector 802.11b/g/n a 150 Mbps y antena de 5dBi
- Interfaz red inalámbrico de captura 802.11b/g/n a 150 Mbps y antena de 4dBi
- OS Ubuntu 14.0.1 (Trusty Tahr).

Dimensiones físicas

- Altura: 220 mm (4 RU)
- Anchura: 383 mm
- Profundidad: 249 mm
- Peso: 2,4 kg

Requisitos de alimentación

- Alimentación: 1,7 A entre 115-220 V~ y 6,15 A a 19,5V =
- Frecuencia: 50-60 Hz

A6.4.2 Tasa de captura de tráfico

Esta prueba se basa en medir el rendimiento del sistema en base a las tramas 802.11 que captura. De esta forma seremos capaces de determinar la fiabilidad del sistema.

ID	PRREN-01
Objetivo	El objetivo de esta prueba será el medir y evaluar la tasa de captura del sistema Antikörper.
Requerimientos	Sistema Antikörper y máquina externa de mediciones
Procedimiento	▪ Arranque del sistema Antikörper ▪ Arranque en otro equipo de la red la herramienta Wireshark capturando en modo monitor ▪ Ejecutar la prueba durante 10 minutos
Verificación	El sistema ha de capturar y procesar un 95 % del tráfico de la red

Tabla A6-13: Prueba PRREN-01

A6.4.3 Tasa de detección de ataques

Esta prueba se basa en determinar el número de ataques detectados mediante la utilización de la herramienta theflOOdARP creada para ese fin.

ID	PRREN-02
Objetivo	El objetivo de esta prueba será el medir el número de intrusiones detectadas por el sistema a través de detecciones de envenenamiento ARP.
Requerimientos	Sistema Antikörper, máquina generadora de ataques y máquina víctima de ataques
Procedimiento	▪ Arranque del sistema Antikörper ▪ Arranque de herramienta theflOOdARP ▪ Configuración de la herramienta ARP para generar ataques de envenenamiento ARP contra una máquina de la red ▪ Generar 500 paquetes de envenenamiento
Verificación	El sistema ha de detectar un 90 % de los ataques

Tabla A6-14: Prueba PRREN-02

A6.4.4 Tasa de respuestas frente a intrusiones

Esta prueba se basa en determinar la capacidad de respuesta frente a intrusiones del sistema. Para ello se hará uso de la herramienta theflOOdETH creada para ese fin.

ID	PRREN-03
Objetivo	El objetivo de esta prueba será el medir el número de respuesta generadas por el sistema frente a máquinas intrusas en el interior de la red
Requerimientos	Sistema Antikörper, máquina de mediciones y máquina atacante
Procedimiento	▪ Arranque del sistema Antikörper ▪ Arranque en otro equipo de la red la herramienta Wireshark capturando en modo monitor ▪ Arranque de herramienta theflOOdETH ▪ Generar 500 tramas de red con diferentes direcciones fuente no autorizadas
Verificación	El sistema ha de responder a un 95 % de los ataques

Tabla A6-15: Prueba PRREN-03

A6.4.5 Resultados de pruebas de rendimiento

ID	Resultado	Medidas	
PRREN-01	Satisfactorio	**Tramas 802.11 en red**	14.789 tramas
		Tramas capturadas	14.765 ±15 tramas
		Rendimiento	99,83 %
PRREN-02	Satisfactorio	**Ataques generados**	500
		Ataques detectados	500
		Rendimiento	100 %
PRREN-03	Satisfactorio	**Intrusos en red**	500
		Intrusos expulsados	500
		Rendimiento	100 %

Tabla A6-16: Resultados de pruebas PRREN

Podemos ver que el sistema cumple con creces los criterios de rendimiento que se han impuesto. Por lo que concluimos que el sistema cumple la función de sistema de detección de intrusiones a la perfección bajo los requisitos que se impusieron a inicio del proyecto.

Anexo VII – Suite de herramientas theflOOd

theflOOd es una suite de herramientas implementadas en el lenguaje de programación C diseñadas para inyectar diferentes tipos de tráfico en redes cableadas e inalámbricas.

Estas herramientas fueron desarrolladas en paralelo al *proyecto Antikörper: Diseño e Implementación de un Sistema de Detección de Intrusos Inalámbrico basado en Network IDS,* con el objetivo inicial de probar el funcionamiento y medir el rendimiento del sistema. Aparte, son de utilidad como herramientas de seguridad debido a las características con las que fueron concebidas.

A continuación se exponen las dos herramientas que componen la suite actualmente.

A7.1 theflOOdARP

La herramienta theflOOdARP permite inyectar tráfico ARP sintético, permitiendo configurar tanto el tipo de paquete (Request o Reply) como la información de fuente y destino del paquete. Además permite seleccionar el número de paquetes a enviar así como el tiempo entre paquetes sucesivos.

Esta herramienta es interesante debido a que, aparte de permitir inyectar tráfico, permite llevar a cabo ataques de envenenamiento ARP y MitM (Man in the Middle) de una forma sencilla y rápida.

Aunque hay herramientas que realizan las mismas funciones que theflOOdARP, como por ejemplo Ettercap, se ha optado por la implementación de esta herramienta y su uso debido a que ofrece una mayor libertad al inyectar tráfico. Estas otras herramientas necesitan de una fase de auditoría previa para llevar a cabo los ataques y no permiten configurar el número de paquetes ni el tiempo sucesivo entre ellos.

A7.2 theflOOdETH

La herramienta theflOOdETH permite inyectar tramas Ethernet sintéticas dando libertad a la hora de configurar la información fuente y destinos de las tramas. Además, permite seleccionar el número de tramas a enviar así como el tiempo entre tramas sucesivas.

Esta herramienta es interesante como herramienta de seguridad debido a que incluye una opción que permite generar tramas con direcciones MAC aleatorias para poder simular la existencia de una gran cantidad de máquinas en la red.

Anexo VIII - GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the

text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright (C) YEAR YOUR NAME.
> Permission is granted to copy, distribute and/or modify this document
> under the terms of the GNU Free Documentation License, Version 1.3

or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with ... Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Anexo IX - Licencia de Documentación Libre GNU (Traducción)

Version 1.2, November 2002

This is an unofficial translation of the GNU Free Documentation License into Spanish. It was not published by the Free Software Foundation, and does not legally state the distribution terms for software that uses GNU FDL-only the original English text of the GNU FDL does that. However, we hope that this translation will help Spanish speakers understand the GNU FDL better.

Equipo de documentación de GIMP

1. PREÁMBULO

El propósito de esta licencia es hacer un manual, libro de texto, u otro documento funcional y útil "libre" con el sentido de libertad: para asegurar a todos la libertad efectiva para copiarla y redistribuirla, con o sin modificaciones, tanto comercialmente como no comercialmente. En segundo lugar, esta licencia preserva para el autor y el editor una manera de acreditar su trabajo, sin considerarlos responsables de las modificaciones hechas por otros.

Esta licencia es de tipo "copyleft", lo que significa que los trabajos derivados del documento deben ser libres de la misma manera. Complementa la licencia pública general GNU, que es una licencia copyleft diseñada para el software libre.

Se ha diseñado esta licencia para usarla en manuales de software libre, ya que el software libre necesita documentación libre: un programa libre debe venir con manuales que ofrezcan las mismas libertades que da el software. Pero esta licencia no se limita a manuales de software; sino que se puede usar para cualquier trabajo de texto, sin tener en cuenta su temática o si se publica como libro impreso. Se recomienda esta licencia principalmente para trabajos cuyo fin sea instructivo o de referencia.

2. APLICACIÓN y DEFINICIONES

Esta licencia aplicada a cualquier manual o a otro trabajo, en cualquier medio, que contiene una nota colocada por el propietario del copyright diciendo que se puede distribuir bajo los términos de esta licencia. Tal nota garantiza en todo el mundo, una licencia libre de derechos, sin límite de duración, para usar ese trabajo bajo las condiciones estipuladas en este documento. El siguiente "Documento" se refiere a cualquier manual o trabajo. Cualquier miembro del público tiene licencia y se le trata como "usted". Vd. acepta la licencia si copia, modifica o distribuye el trabajo de un modo que requiera permiso bajo la ley de los derechos de autor.

Una "Versión modificada" del documento significa cualquier trabajo que contenga el documento o una porción de él, tanto copiado literalmente, como con modificaciones y/o traducciones a otro idioma.

Una "Sección secundaria" es un apéndice con título o una sección preliminar del documento que trata exclusivamente de la relación entre los editores o autores del documento al tema general del Documento (o temas relacionados) y que no contiene nada que entre directamente en dicho tema general. (Así, si el documento es en parte un texto de matemáticas, una sección secundaria puede no explicar nada de matemáticas.) La relación puede ser una conexión histórica con el tema o temas relacionados, o una opinión legal, comercial, filosófica, ética o política sobre ellos.

Las "Secciones invariantes" son ciertas secciones secundarias cuyos títulos son designados, como son las de las secciones invariantes, en la nota que indica que el documento se libera bajo esta licencia. Si una sección no entra en la definición anterior de secundaria, entonces no puede designarse como invariante. El documento puede no tener secciones invariantes. Si el documento no identifica ninguna Sección Invariante, es que no las tiene.

Los "Textos de cubierta" son ciertos pasajes cortos de texto que se listan, como textos de cubierta delantera o textos de cubierta trasera, en la nota que indica que el documento se libera bajo esta licencia. Un texto de cubierta delantera puede tener como mucho 5 palabras, y uno de cubierta trasera puede tener hasta 25 palabras.

Una copia "Transparente" del documento significa una copia para lectura en máquina, representada en un formato cuya especificación está disponible para el público en general, apto para que los contenidos se puedan revisar directamente con editores de texto genéricos o (para imágenes compuestas por píxeles) con programas genéricos de manipulación de imágenes o (para dibujos) con algún editor de dibujos ampliamente disponible, y que sea adecuado como entrada para formateadores de texto o para su traducción automática a formatos adecuados para formateadores de texto. Una copia hecha en un formato definido como transparente, pero cuyo marcado o ausencia de él se haya diseñado para impedir o dificultar modificaciones posteriores por parte de los lectores no es transparente. Un formato de imagen no es transparente si se usa para una cantidad de texto sustancial. Una copia que no es "Transparente" se denomina "Opaca".

Ejemplos de formatos adecuados para copias transparentes incluyen ASCII puro sin marcado, formato de entrada de Texinfo, formato de entrada de LaTeX, SGML o XML

usando una DTD disponible públicamente, y HTML, PostScript o PDF simples, que sigan los estándares diseñados para que los modifiquen personas. Ejemplos de formatos de imagen transparentes son PNG, XCF y JPG. Los formatos opacos incluyen formatos propietarios que pueden ser leídos y editados únicamente en procesadores de texto propietarios, SGML o XML para los cuáles las DTD y/o herramientas de procesamiento no estén ampliamente disponibles, y HTML, PostScript o PDF generados por algunos procesadores de texto solo como salida.

La "Portada" es, en un libro impreso, la página de título, más las páginas siguientes que sean necesarias para mantener legible, el material que esta licencia requiere que aparezca en la página del título. Para trabajos en formatos que no tienen portada como tal, "Portada" significa el texto cercano a la aparición más prominente del título del trabajo, precediendo el comienzo del cuerpo del texto.

Una sección "Titulada XYZ" significa una parte del documento cuyo título es precisamente XYZ o que contiene XYZ entre paréntesis a continuación de texto que traduce XYZ a otro idioma (aquí XYZ se refiere a nombres de sección específicos mencionados más abajo, como "Agradecimientos", "Dedicatorias" , "Aprobaciones" o "Historia". "Conservar el título" de tal sección cuando se modifica el documento significa que permanece una sección "Titulada XYZ" según esta definición

El documento puede incluir limitaciones de garantía cercanas a la nota donde se declara que al documento se le aplica esta licencia. Se considera que estas limitaciones de garantía están incluidas por referencia en esta licencia, pero solo en cuanto a limitaciones de garantía: cualquier otra implicación que estas limitaciones de garantía puedan tener es nula y no tiene efecto en el significado de esta licencia.

3. COPIA LITERAL

Usted puede copiar y distribuir el documento en cualquier soporte, sea en forma comercial o no, siempre y cuando esta licencia, las notas de copyright y la nota que indica que esta licencia se aplica al documento se reproduzcan en todas las copias y que usted no añada ninguna otra condición a las expuestas en esta licencia. Usted no puede usar medidas técnicas para obstruir o controlar la lectura o copia posterior de las copias que usted haga o distribuya. Sin embargo, usted puede aceptar compensación a cambio de las copias. Si distribuye un número suficientemente grande de copias también deberá seguir las condiciones de la sección 4.

Usted también puede prestar copias, bajo las mismas condiciones establecidas anteriormente, y puede exhibir copias públicamente.

4. COPIADO EN CANTIDAD

Si publica copias impresas del documento (o copias en soportes que tengan normalmente cubiertas impresas) que sobrepasen las 100, y la nota de licencia del documento exige textos de cubierta, debe incluir las copias con cubiertas que lleven en forma clara y legible todos esos textos de cubierta: textos de cubierta delantera en la cubierta delantera y textos de cubierta trasera en la cubierta trasera. Ambas cubiertas deben

identificarlo a Usted de forma clara y legible como editor de tales copias. La cubierta delantera debe mostrar el título completo con todas las palabras igualmente prominentes y visibles. Además puede añadir otro material en las cubiertas. Las copias con cambios limitados a las cubiertas, siempre que conserven el título del documento y satisfagan estas condiciones, pueden considerarse como copias literales.

Si los textos requeridos para la cubierta son muy voluminosos para que ajusten de forma legible, debe colocar los primeros listados (tantos como sea razonable colocar) en la verdadera cubierta y situar el resto en páginas adyacentes.

Si publica o distribuye copias opacas del documento cuya cantidad exceda las 100, debe incluir una copia transparente, que pueda ser leída por una máquina, con cada copia opaca, o bien mostrar, en cada copia Opaca, una dirección de red donde cualquier usuario de la misma tenga acceso por medio de protocolos públicos y estandarizados a una copia transparente del documento completa, sin material adicional. Si hace uso de la última opción, deberá tomar las medidas necesarias, cuando comience la distribución de las copias opacas en cantidad, para asegurar que esta copia transparente permanecerá accesible en el sitio establecido por lo menos un año después de la última vez que distribuya una copia opaca de esa edición al público (directamente o a través de sus agentes o distribuidores).

Se solicita, aunque no es requisito, que se ponga en contacto con los autores del documento antes de redistribuir gran número de copias, para darles la oportunidad de que le proporcionen una versión actualizada del documento.

5. MODIFICACIONES

Puede copiar y distribuir una versión modificada del documento bajo las condiciones de las secciones 3 y 4 anteriores, siempre que libere la versión modificada bajo esta misma licencia, con la versión modificada haciendo el rol del documento, por lo tanto dando licencia de distribución y modificación de la versión modificada a quienquiera posea una copia de la misma. Además, debe hacer lo siguiente en la versión modificada:

a. Usar en la portada (y en las cubiertas, si hay alguna) un título distinto al del documento y de sus versiones anteriores (que deberían, si hay alguna, estar listadas en la sección de historia del documento). Puede usar el mismo título de versiones anteriores al original siempre y cuando quien las publicó originalmente otorgue permiso.
b. Listar en la portada, como autores, una o más personas o entidades responsables de la autoría de las modificaciones de la versión modificada, junto con por lo menos cinco de los autores principales del documento (todos sus autores principales, si hay menos de cinco), a menos que le eximan de tal requisito.
c. Mostrar en la portada el nombre del editor de la versión modificada, como editor.
d. Preservar todas las notas del copyright del documento.
e. Añadir una nota de copyright apropiada a sus modificaciones, adyacente a las otras notas de copyright.

f. Incluir, inmediatamente después de las notas de copyright, una nota de licencia dando el permiso para usar la versión modificada bajo los términos de esta licencia, como se muestra en el Apéndice más abajo.
g. Conservar en esa nota de licencia el listado completo de las secciones invariantes y los textos de cubierta requeridos en la nota de la licencia del documento.
h. Incluir una copia sin modificación de esta licencia.
i. Conservar la sección titulada "Historia", conservar su título y añadirle un elemento que declare al menos el título, el año, los nuevos autores y el editor de la versión modificada, tal como figuran en la portada. Si no hay una sección titulada "Historia" en el documento, crear una estableciendo el título, el año, los autores y el editor del documento, tal como figuran en su portada, añadiendo además un elemento describiendo la versión modificada, como se estableció en la oración anterior.
j. Conservar la dirección en red, si la hay, dada en el documento para el acceso público a una copia transparente del mismo, así como las otras direcciones de red dadas en el documento para versiones anteriores en las que estuviese basado. Pueden ubicarse en la sección "Historia". Puede omitir la ubicación en red de un trabajo que haya sido publicado por lo menos cuatro años antes que el documento mismo, o si el editor original de dicha versión da permiso.
k. En cualquier sección titulada "Agradecimientos" o "Dedicatorias", conservar el título de la sección y conservar en ella toda la sustancia y el tono de los agradecimientos y/o dedicatorias incluidas por cada contribuyente.
l. Conservar todas las secciones invariantes del documento, sin alterar su texto ni sus títulos. Los números de sección o el equivalente no son considerados parte de los títulos de la sección.
m. Borrar cualquier sección titulada "Aprobaciones". Tales secciones no pueden estar incluidas en las Versiones Modificadas.
n. No cambiar el título de ninguna sección existente en "Aprobaciones" ni a uno que entre en conflicto con el de alguna sección invariante.
o. Conservar todas las limitaciones de garantía.

Si la versión modificada incluye secciones o apéndices nuevos que se califiquen como secciones secundarias y no contienen material copiado del documento, puede opcionalmente designar algunas o todas esas secciones como invariantes. Para hacerlo, añada sus títulos a la lista de secciones invariantes en la nota de licencia de la versión modificada. Tales títulos deben ser distintos de cualquier otro título de sección.

Puede añadir una sección titulada "Aprobaciones", siempre que contenga únicamente aprobaciones de su versión modificada por otras fuentes, por ejemplo, observaciones de peritos o que el texto ha sido aprobado por una organización como la definición oficial de un estándar.

Puede añadir un pasaje de hasta cinco palabras como texto de cubierta delantera y un pasaje de hasta 25 palabras como texto de cubierta trasera en la versión modificada. Una entidad solo puede añadir (o hacer que se añada) un pasaje al texto de cubierta delantera y

uno al de cubierta trasera. Si el documento ya incluye un textos de cubiertas añadidos previamente por usted o por la misma entidad que usted representa, usted no puede añadir otro; pero puede reemplazar el anterior, con permiso explícito del editor que agregó el texto anterior.

Con esta Licencia ni los autores ni los editores del documento dan permiso para usar sus nombres para publicidad ni para asegurar o implicar aprobación de cualquier versión modificada.

6. COMBINACIÓN DE DOCUMENTOS

Usted puede combinar el documento con otros documentos liberados bajo esta licencia, bajo los términos definidos en la sección 5 anterior para versiones modificadas, siempre que incluya en la combinación todas las secciones invariantes de todos los documentos originales, sin modificar, y listadas todas como secciones invariantes de su trabajo combinado en su nota de licencia, y así mismo debe incluir la limitación de garantía.

El trabajo combinado necesita contener solamente una copia de esta licencia, y puede reemplazar varias secciones invariantes idénticas por una sola copia. Si hay varias secciones invariantes con el mismo nombre pero con contenidos diferentes, haga el título de cada una de estas secciones único añadiéndole al final del mismo, entre paréntesis, el nombre del autor o editor original de esa sección, si es conocido, o si no, un número único. Haga el mismo ajuste a los títulos de sección en la lista de secciones invariantes de la nota de licencia del trabajo combinado.

En la combinación, debe combinar cualquier sección titulada “Historia” de los documentos originales, formando una sección titulada “Historia”; de la misma forma combine cualquier sección titulada “Agradecimientos”, y cualquier sección titulada “Dedicatorias”. Debe borrar todas las secciones tituladas “Aprobaciones”.

7. COLECCIONES DE DOCUMENTOS

Puede hacer una colección que conste del documento y de otros documentos liberados bajo esta licencia, y reemplazar las copias individuales de esta licencia en todos los documentos por una sola copia que esté incluida en la colección, siempre que siga las reglas de esta licencia para cada copia literal de cada uno de los documentos en cualquiera de los demás aspectos.

Puede extraer un solo documento de una de tales colecciones y distribuirlo individualmente bajo esta licencia, siempre que inserte una copia de esta licencia en el documento extraído, y siga esta licencia en todos los demás aspectos relativos a la copia literal de dicho documento.

8. AGREGACIÓN CON TRABAJOS INDEPENDIENTES

Una recopilación que conste del documento o sus derivados y de otros documentos o trabajos separados e independientes, en cualquier soporte de almacenamiento o distribución, se denomina un agregado si el copyright resultante de la compilación no se usa

para limitar los derechos de los usuarios de la misma más allá de lo que los de los trabajos individuales permiten. Cuando el documento se incluye en un agregado, esta licencia no se aplica a otros trabajos del agregado que no sean en sí mismos derivados del documento.

Si el requisito de la sección 4 sobre el texto de cubierta es aplicable a estas copias del documento y el documento es menor que la mitad del agregado entero, los textos de cubierta del documento pueden colocarse en cubiertas que enmarquen solamente el documento dentro del agregado, o el equivalente electrónico de las cubiertas si el documento está en forma electrónica. En caso contrario deben aparecer en cubiertas impresas enmarcando todo el agregado.

9. TRADUCCIÓN

La traducción se considera como un tipo de modificación, por lo que usted puede distribuir traducciones del documento bajo los términos de la sección 5. El reemplazo de las secciones invariantes con traducciones requiere permiso especial de los dueños de los derechos de autor, pero usted puede añadir traducciones de algunas o todas las secciones invariantes a las versiones originales de las mismas. Puede incluir una traducción de esta licencia, de todas las notas de licencia del documento, así como de las limitaciones de garantía, siempre que incluya también la versión en inglés de esta licencia y las versiones originales de las notas de licencia y limitaciones de garantía. En caso de desacuerdo entre la traducción y la versión original en inglés de esta licencia, la nota de licencia o la limitación de garantía, la versión original en Inglés prevalecerá.

Si una sección del documento se titula “Agradecimientos”, “Dedicatorias”, o “Historia”, el requisito (sección 5) de Conservar su título (sección 2) requerirá, típicamente, cambiar su título.

10. TERMINACIÓN

Usted no puede copiar, modificar, sublicenciar o distribuir el documento salvo por lo permitido expresamente por esta licencia. Cualquier otro intento de copia, modificación, sublicenciamiento o distribución del documento es nulo, y dará por terminados automáticamente sus derechos bajo esa licencia. Sin embargo, los terceros que hayan recibido copias, o derechos, de usted bajo esta licencia no verán terminadas sus licencias, siempre que permanezcan en total conformidad con ella.

11. REVISIONES FUTURAS DE ESTA LICENCIA

La Fundación de software libre puede publicar versiones nuevas y revisadas de la licencia de documentación libre GNU. Tales versiones nuevas serán similares en espíritu a la presente versión, pero pueden diferir en detalles para solucionar nuevos problemas o intereses. Consulte http://www.gnu.org/copyleft/.

Cada versión de la licencia tiene un número de versión que la distingue. Si el documento especifica que se aplica una versión numerada en particular de esta licencia “o cualquier versión posterior”, usted tiene la opción de seguir los términos y condiciones de la versión especificada o cualquiera posterior que haya sido publicada (no como borrador)

por la fundación de software libre. Si el documento no especifica un número de versión de esta licencia, puede elegir cualquier versión que haya sido publicada (no como borrador) por la fundación de software libre.

12. ADENDA: cómo usar esta licencia en sus documentos

Para usar esta licencia en un documento que usted haya escrito, incluya una copia de la licencia en el documento y ponga el siguiente copyright y nota de licencia justo después de la página de título:

Copyright (c) 2011 Equipo de traducción de GNOME al Español. Se otorga permiso para copiar, distribuir y/o modificar este documento bajo los términos de la licencia de documentación libre de GNU, Versión 1.2 o cualquier otra versión posterior publicada por la fundación de software libre; sin secciones invariantes ni textos de cubierta delantera ni textos de cubierta trasera. Una copia de la licencia está incluida en la sección titulada “Licencia de documentación libre GNU”.

Si tiene secciones invariantes, textos de cubierta delantera y textos de cubierta trasera, reemplace la frase “con…textos.” por esto:

Siendo las secciones invariantes LISTE SUS TÍTULOS, siendo los textos de cubierta delantera LISTAR, y siendo sus textos de cubierta trasera LISTAR.

Si tiene secciones invariantes sin textos de cubierta o cualquier otra combinación de los tres, mezcle ambas alternativas para adaptarse a la situación.

Si su documento contiene ejemplos de código de programa no triviales, se recomienda liberar estos ejemplos en paralelo bajo la licencia de software libre que usted elija, como la licencia pública general de GNU, para permitir su uso en software libre.