UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

PROYECTO:

MÉTODOS DE ACCESO NO AUTORIZADOS DE WIFI

CÁTEDRA:

SISTEMAS OPERATIVOS DE REDES

CATEDRÁTICO:

ING. MANUEL FLORES VILLATORO

PRESENTADO POR:

Carnet	Apellidos	Nombres	Participación
RG01133698	Reyes García	José Alfredo	100%
SJ01133616	Serpas Jiménez	Edwin Antonio	100%
ZV01133710	Zelaya Villalta	Jerson Ernesto	100%

San Salvador, 2 de junio de 2018

Índice

Contenido

Índice de tablas

Índice de figuras

Agradecimientos

Agradecemos a Dios por el don de la vida, la salud y la sabiduría que nos ha dado para poder elaborar el presente proyecto: Métodos de Acceso No Autorizados de la catedra de: Sistemas Operativos de Redes, a nuestros padres con la confianza, por el apoyo incondicional y la motivación que recibimos constantemente que nos alienta a seguir luchando por nuestras metas trazadas; al Ing. Manuel Flores, que comparte con cada uno de nosotros los conocimiento de la materia antes mencionada, por la paciencia, por la entrega, por la constancia, la orientación y la motivación que recibimos en cada una de sus clases, que alimentan nuestras espíritu de perseverancia. A nuestros compañeros y amigos que siempre están dispuestos a ayudarnos cuando lo hemos requerido, a todos los antes mencionados nuestros más sinceros agradecimientos, ya que sin ellos este proyecto no sería una realidad.

Resumen (abstract)

En el presente proyecto se pretende mostrar los diferentes cifrados y contraseñas que pueden tener nuestras redes wi-fi, así como los diferentes métodos por los cuales nuestras redes puede ser vulneradas, también presentamos las herramientas más utilizadas comúnmente por las personas que buscan irrumpir la seguridad de las redes inalámbricas; también una breve descripción y conceptualización de la red wi fi y el funcionamiento de esta. Esperamos que con la información presentada en este proyecto se aclaren muchas dudas referentes a las redes inalámbricas y su funcionamiento. También están explicadas las diferentes bandas por las cuales funcionan nuestras redes inalámbricas y la forma en la cual podemos protegerlas no en un 100% pero si de una forma efectiva ante los diferentes ataques de personas que buscan infiltrarse en nuestras redes inalámbricas.

Palabras claves

1. WPA,WPE,WPA-PSK,HANDSHACKE,HostSpot,IVs

Introducción

Las redes inalámbricas brindan grandes beneficios tanto en lo laboral como en lo domestico, todos en algún momento nos habremos conectado un punto de acceso a internet WIFI, ya sea en nuestras casas o en nuestro trabajo y es en este lugar donde toma un poco más de importancia el tema de seguridad de la red.

Las redes inalámbricas pueden ser vulnerables a diversos ataques realizados por personas con malas intenciones, pero también hay personas que utiliza los mismos ataques con el fin de encontrar una vulnerabilidad y tratar de erradicarla o disminuirla.

Dichas herramientas pueden ejecutarse en diferentes sistemas operativos (Linux, MacOS, Windows), en la actualidad los sistemas operativos que más se han popularizado son los sistemas Linux dedicados a la auditoria de redes inalámbricas.

Entre estos tenemos Kali Linux, Wifislax, BackTrack, todas ellas con muchas herramientas para romper los protocolos de seguridad en las redes wifi, entre estas herramientas esta la Suite Aircrack-ng siendo esta la suite más popular y más usada en la auditoria de redes inalámbricas.

En el presente trabajo además de mencionar los diferentes protocolos de seguridad también se hablará un poco de este conjunto de herramientas.

Objetivos

General

- Conocer y comprender en funcionamientos de diferentes métodos de acceso no autorizados de wifi.

Especifico

- Investigar los métodos más usados para obtener acceso no autorizado en una red inalámbrica.
- Realizar pruebas con el software utilizado para penetrar las redes inalámbricas.

Marco Teórico

Redes Inalámbricas

Definición de red inalámbrica

Es la interconexión de distintos dispositivos con la capacidad de compartir información entre ellos, pero sin un medio físico de transmisión. Estos dispositivos pueden ser de muy variadas formas y tecnologías entre ellos:

- Computadoras de escritorio.
- Teléfonos celulares.
- Asistentes digitales personales (PDA).
- *Access Point* (encargado de permitir a los dispositivos inalámbricos el acceso a la red).
- Computadoras portátiles: *Laptop*, *Netbook* y *Notebook*

Figura 1 Ejemplo de dispositivos interconectados sin necesidad de cables

Tecnologías actuales para red inalámbrica

Wi-Fi ("*Wireless Fidelity*"): en lenguajes español significa literalmente fidelidad sin cables. También se les denomina WLAN ("*Wireless Local Area Network*") o redes de área local inalámbricas. Se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio con muy buena calidad de emisión para distancias cortas (hasta teóricamente 100 m). Este tipo de transmisión se encuentra estandarizado por la IEEE, siglas en inglés del Instituto de Ingenieros en Electricidad y Electrónica, la cuál es una organización internacional que define las reglas de operación de ciertas tecnologías.

Figura 2 Logo Wifi

Para la transmisión es necesario el uso de antenas integradas en las tarjetas, además este tipo de ondas son capaces de traspasar obstáculos sin necesidad de estar frente a frente el emisor y el receptor.

Actualmente son 3 estándares básicos:

Tabla 1 Estándares Básicos

Nombre	Tecnología	Velocidad de Transmisión	Características
Wireless B	IEEE 802.11b	11 Mbps (Megabits por segundo)	Trabaja en la banda de frecuencia de 2.4 GHz solamente, compatible con velocidades menores.
Wireless G	IEEE 802.11g	11 / 22 / 54 Mbps	Trabaja en la banda de frecuencia de 2.4 GHz solamente.
Wireless N	IEEE 802.11n	300 Mbps	Utiliza una tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente.

Nombre	Tecnología	Velocidad de Transmisión	Características
Wireless AC	IEEE 802.11ac	433 Mbps / 1.3 Gbps	Trabaja sobre la banda de los 2.5 Ghz a 5 Ghz (MIMO) de 3 canales, múltiples antenas, tambien llamada Wi-Fi 5/5G

Para el uso de redes "Wireless" es necesario que los dispositivos dispongan de un emisor ya sea integrado o agregado para el uso de este tipo de red.

- ✓ **Computadoras de escritorio:** un emisor/receptor integrado en la Motherboard, una tarjeta PCI inalámbrica ó un adaptador USB para red inalámbrica.
- ✓ **Computadoras portátiles:** en caso de no tenerlo integrado se puede usar una tarjeta PCMCIA para red inalámbrica ó un adaptador USB para red inalámbrica.
- ✓ **PDA:** tiene integrada la tarjeta de red inalámbrica.
- ✓ **Celular:** tienen la tarjeta de red inalámbrica integrada.

Estándares y especificaciones de las redes Wi-Fi

Las redes Wi-Fi permiten la conectividad de equipos y dispositivos mediante ondas de radio. Existen distintos estándares que se han ido implementando con el paso del tiempo, con el objetivo de mejorar la conectividad y su rendimiento.
Todos son mejoras y parten del inicial estándar 802.11. Se espera que las mejoras continuaran durante años. Poseen características diferentes como la frecuencia que usan, el ancho de banda, la velocidad y el alcance o rango.
En los dispositivos casi siempre existe compatibilidad con los estándares anteriores y un adaptador inalámbrico, aunque admita varios estándares, siempre va a escoger y usar de ser posible el que más velocidad permita.

Los estándares más utilizados actualmente en las redes Wi-Fi son los siguientes:

802.11 Velocidad (teórica)	2 Mbit/s
Velocidad (práctica)	1 Mbit/s
Frecuencia	2,4 Ghz
Ancho de banda	22 MHz
Alcance	330 metros
Año de implementación	1997

Tabla 2 Estándar Wifi 802.11

a) 802.11a

Velocidad (teórica)	54 Mbit/s
Velocidad (práctica)	22 Mbit/s
Frecuencia	5,4 Ghz
Ancho de banda	20 MHz
Alcance	390 metros
Año de implementación	1999

Tabla 3 Estándar Wifi 802.11a

b) 802.11b

Velocidad (teórica)	11 Mbit/s
Velocidad (práctica)	6 Mbit/s
Frecuencia	2,4 Ghz
Ancho de banda	22 MHz
Alcance	460 metros
Año de implementación	1999

Tabla 4 Estándar Wifi 802.11b

c) 802.11g

Velocidad (teórica)	54 Mbit/s
Velocidad (práctica)	22 Mbit/s
Frecuencia	2,4 Ghz
Ancho de banda	20 MHz
Alcance	460 metros
Año de implementación	2003

Tabla 5 Estándar Wifi 802.11g

d) 802.11n

Velocidad (teórica)	600 Mbit/s
Velocidad (práctica)	100 Mbit/s
Frecuencia	2,4 Ghz y 5,4 Ghz
Ancho de banda	20/40 MHz
Alcance	820 metros
Año de implementación	2009

Tabla 6 Estándar Wifi 802.11n

Disponible en la mayoría de los dispositivos modernos. Puede configurarse para usar solo 20 MHz de ancho y así prevenir interferencias en una zona congestionadas.

e) **802.11ac**

Velocidad (teórica)	6.93 Gbps
Velocidad (práctica)	100 Mbit/s
Frecuencia	5,4 Ghz
Ancho de banda	80 o hasta 160 MHz
Año de implementación	2013

Tabla 7 Estándar Wifi 802.11ac

El estándar 802.11ac se está implementando desde el comienzo del 2014.

Los componentes que lo emplean consumen menos energía, por lo que es ideal para dispositivos portables, además ahora es posible transmitir datos idénticos a usuarios diferentes.

Usando la banda de 5 GHz el radio de alcance es menor, pero en la práctica se pueden alcanzar distancias mayores usando la tecnología "Beamforming" que focaliza la señal de radio.

802.11ac es mucho más rápido, la rapidez se debe a dos factores:

1) La posibilidad de usar canales de radio más anchos.

   En vez de usar 40 MHz de ancho de canal, AC puede funcionar con 80 o hasta 160 MHz.

   Otra posibilidad es la de usar la característica "Channel Bonding", es decir poder combinar dos canales independientes.

2) Antenas múltiples.

   Los routers actuales transfieren al mismo tiempo hasta seis flujos de datos (spatial streams) usando tres antenas. Con AC se pueden utilizar hasta cuatro antenas.

f) **802.11ad**

Velocidad (teórica)	7.13 Gbit/s
Velocidad (práctica)	Hasta 6 Gbit/s
Frecuencia	60 Ghz
Ancho de banda	2 MHz
Alcance	300 metros
Año de implementacion	2012

Tabla 8 Estándar Wifi 802.11ad

g) **802.11ah**

Frecuencia	0.9 Ghz
Ancho de banda	2 MHz
Alcance	1000 metros
Año de implementacion	2016
Conocida como Wi	Fi HaLow

Tabla 9 Estándar Wifi 802.11ah

El estándar 802.11ah o Wi-Fi HaLow, características y ventajas

IEEE 802.11ah es un nuevo protocolo de redes inalámbricas que comienza a implementarse en el 2016.

Surge a causa de los constantes requerimientos de la tecnología, la información y el mercado.

Se diferencia de los anteriores por usar frecuencias inferiores a 1 GHz y permite aumentar el rango de alcance de estas redes, hasta alrededor de 1000 metros.

Esto facilita en la práctica su distribución en áreas rurales, usando torres de telefonía con sensores para compartir la señal.

También ofrece el beneficio de un menor consumo de energía.

Este protocolo es un competidor del popular Bluetooth usado en dispositivos pequeños.

Wi-Fi alliance anuncio que 802.11ah se conocería con el nombre Wi-Fi HaLow, que se pronuncia "HAY-Low".

Información de un dispositivo Wi-Fi usando el comando NETSH

Otra de las formas de obtener información de cualquier dispositivo, es con el comando NETSH en Windows.

Haz lo siguiente:

1. Abre una ventana de la consola de CMD o Símbolo del sistema.

   Para eso abre la herramienta Ejecutar mediante las teclas Windows + R, escribe CMD y presiona Enter.

2. Escribe en la ventana de la consola lo siguiente y presiona la tecla Enter. netsh wlan show drivers

   Se mostrará toda la información disponible del adaptador inalámbrico.

   Busca la línea: "Tipos de radio admitidos" como se muestra en la siguiente imagen.

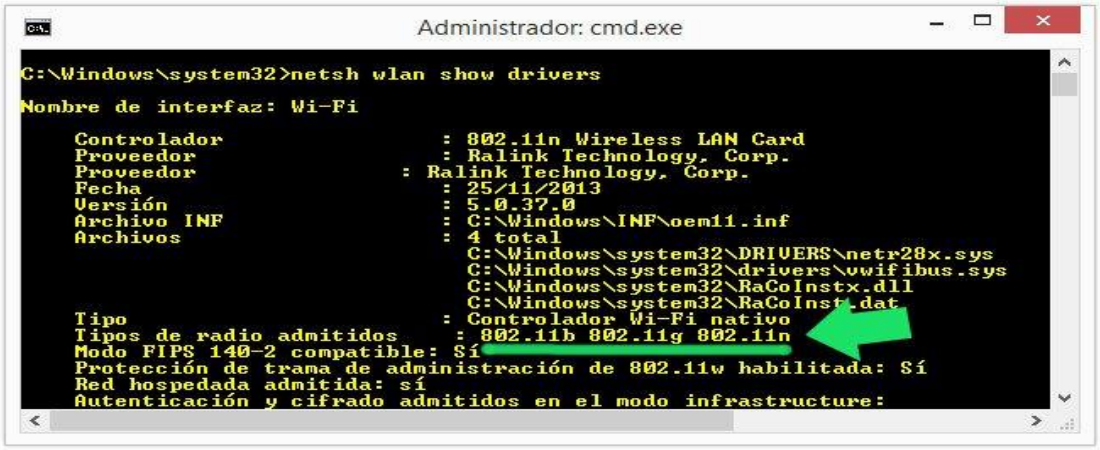

Figura 3 Comando NETSH

Modos de conexiones Wi-Fi

Existen dos tipos de conexiones Wi-Fi: el modo "infraestructura" y el modo "ad hoc".

a) El primero de ellos es la conexión que se efectúa entre un equipo o dispositivo y un punto de acceso inalámbrico (AP) ya sea un router o un punto público.

   Existen redes abiertas y protegidas. Algunas son públicas y otras privadas.

b) El segundo, el modo ad-hoc es la conexión que se establece entre dos equipos o dispositivos de forma independiente. Esta conexion solo permite algunos metros de alcance.

¿Que son las redes ad hoc?

Con Wi-Fi podemos crear una conexión entre dos computadoras o entre una computadora y un dispositivo portable, sin mediar un punto de acceso inalámbrico.

Incluso de esa forma podemos compartir una conexión de internet, funcionando uno de los equipos como un router, AP o HotSpot.

Este tipo de red virtual es llamada "red ad hoc".

Windows Vista y 7 incluye opciones para crearla en el asistente de crear una nueva red. En Windows 8 es necesario usar la línea de comandos.

¿Qué es Wi-Fi Direct?

Wi-Fi Direct es la tecnología que permite crear una conexión entre dos dispositivos por Wi-Fi, de forma similar a una red ad hoc.

Los dispositivos que la admiten ya traen integrado un pequeño punto de acceso, por lo que no es necesario depender de una computadora para crear la red y todo se hace más sencillo y seguro.

Es importante conocer que solo es necesario que uno de los dispositivos admita Wi-Fi Direct, además no importa que sean de fabricantes diferentes.

Con Wi-Fi Direct se puede conectar teléfonos, tabletas, impresoras, cámaras, protegidos mediante la autentificación WPA2.

Por ejemplo, de esa forma podemos compartir la conexión de internet en un teléfono celular con otro dispositivo ya sea un teléfono, tableta una computadora de escritorio o una Laptop.

Todo sin necesidad de instalar ninguna aplicación.

La gran mayoría de los teléfonos celulares smartphone de gama media y alta ya incluyen Wi-Fi Direct. Algunos son: Samsung Galaxy S9, HTC One, Nexus, etc.

Figura 4 Wifi Direct en android

¿Qué es la certificación o certificado Wi-Fi?

El certificado Wi-Fi (Wi-Fi CERTIFIED™) es un logotipo que incluyen todos los dispositivos debidamente certificados y aprobados por la Wi-Fi Alliance® grupo industrial propietario de la marca registrada Wi-Fi, que indica que cumple con todos los estándares para el uso de estas redes.

Antes de adquirir cualquier dispositivo asegúrate que lo incluya.

Figura 5 Logo Wi-Fi Certified

Alcance de las redes Wi-Fi

El alcance de las redes Wi-Fi es limitado.

Un punto de acceso usando 802.11b puede llegar hasta los 100 metros (exterior).

Usando 802.11n se puede llegar hasta los 200 metros.

El alcance puede extenderse hasta algunos kilómetros, usando antenas direccionales.

Las redes que usan la banda de 5 GHz (802.11ac) poseen un menor alcance, aunque menos interferencia.

Vulnerabilidades de WEP, WPA, y WPA2

WEP

El lanzamiento del estándar IEEE 802.11 para conexiones inalámbricas que se ratificó en 1997 incluyó un apartado para la seguridad de esas conexiones: el llamado Wired Equivalent Privacy (WEP) —curioso que el acrónimo haga uso de la palabra "Wired" y no "Wireless", por cierto— planteaba un algoritmo de seguridad para proteger la confidencialidad de los datos de forma similar a la que se proporcionaba a redes de cable.

El protocolo WEP hacía uso del cifrado RC4 y del mecanismo CRC-32 para la integridad, y el sistema estándar de 64 bits hacía uso de una clave de 40 bits que se concatenaba con un vector de inicialización (IV) de 24 bits para conformar la clave RC4. A cualquiera que haya usado este protocolo le resultarán familiares esas clave WEP de 64 bits, pero en formato hexadecimal, que hacían que al conectarnos a una red WiFi con esa seguridad tuviésemos que introducir esos diez caracteres hexadecimales (números del 0 al 9, letras de la A a la F).

Aquel protocolo demostró su debilidad en 2001, cuando Scott R. Fluhrer, Itsik Mantin y Adi Shamir publicaron un estudio sobre los problemas del cifrado RC4 y cómo descifrar esas

claves era posible en un tiempo reducido espiando una de estas conexiones e inspeccionando los paquetes que se iban intercambiando un cliente conectado a un punto de acceso. De hecho, si el tráfico era bajo, era posible inyectar y "estimular" paquetes de respuesta que servían para lograr que la cantidad de IVs permitiese luego encontrar la clave de acceso WiFi.

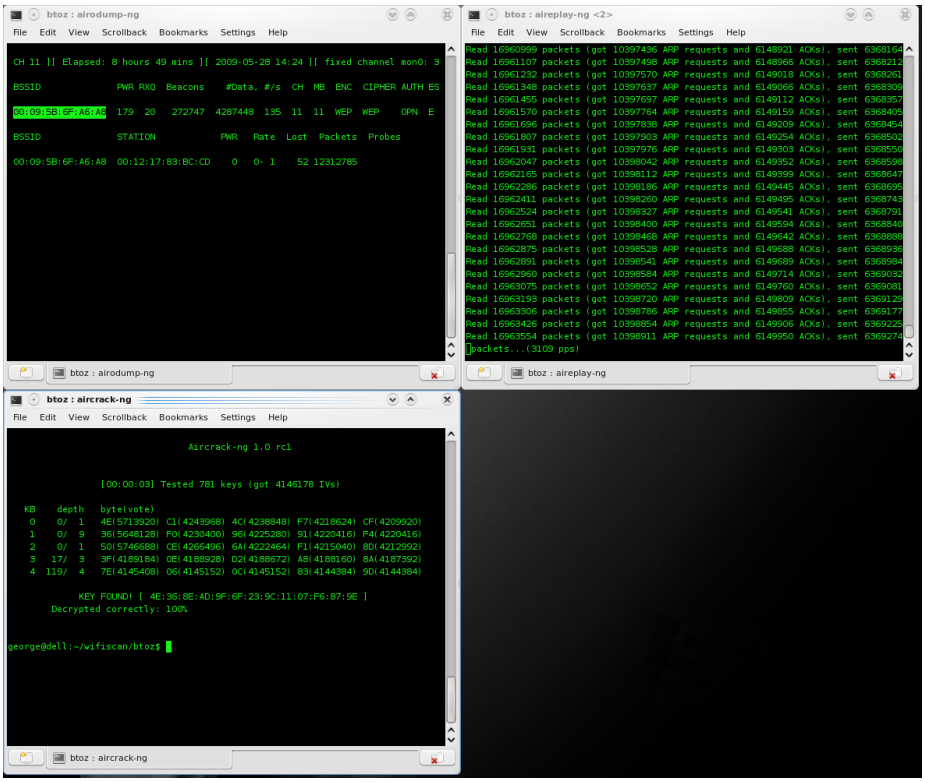

Figura 6 Captación de IVs

Aquel tipo de ataque se volvió uno de los clásicos de los aficionados al hacking WiFi, y suites de seguridad como la archiconocida aircrack-ng permitieron crackear una conexión WiFi con el protocolo WEP en apenas unos minutos.

A pesar de que la vulnerabilidad se conocía ampliamente, las operadoras mantuvieron su validez durante años, predefiniendo redes WiFi en los routers que suministraban a los clientes en las que se usaba el protocolo WEP por defecto.

El propio FBI acabó mostrando lo fácil que era romper la seguridad esas redes en 2005, pero el verdadero detonante del caos WEP fue la brecha de seguridad en TJ Maxx, uno de los gigantes comerciales de Estados Unidos. Allí un hacker llamado Albert Gonzalez —capturado y condenado a 20 años de cárcel— lograron robar más de 100 millones de cuentas de usuario, lo que le supuso unas pérdidas estimadas que rondaron los 1.000 millones de dólares.

Aquello fue la gota que colmó el vaso, y la industria y los usuarios por fin tomaron conciencia del peligro y se comenzó a dejar de usar el protocolo WEP por parte de fabricantes de equipos de comunicaciones y operadoras. Aquellas vulnerabilidades se trataron de parchear con claves más largas de hasta 256 bits o variaciones como WEP2 o WEPplus, pero el protocolo que trataría de atajar los problemas —sin lograrlo— ya estaba funcionando desde hacía años. WPA parecía la solución a nuestros problemas, pero claro, no lo era.

WPA

Aquellos enormes fallos al concebir un protocolo de seguridad para las comunicaciones inalámbricas trataron de corregirse con el desarrollo del estándar IEEE 802.11i, que no llegaría hasta un año después. La urgencia de la situación hizo que la Wi-Fi Alliance sacara una versión preliminar de ese estándar, y es así como en 2003 apareció en escena el protocolo Wi-Fi Protected Access (WPA).

Una de las ideas de WPA era poder ser aplicable como una actualización del firmware de muchos routers y otros equipos de comunicaciones, pero resultó que los puntos de acceso y routers necesitaban contar con algunos requisitos adicionales, lo que hizo que muchos routers "antiguos" no pudieran ser actualizados.

El protagonista de ese protocolo WPA que cumplía con parte de la especificación IEEE 802.11i era el llamado Temporal Key Integrity Protocolo (TKIP), que se diferenciaba del protocolo WEP en un tema clave: mientras que la clave tradicional WEP de 64 o 128 bits no cambiaba, con TKIP se implementaba una "clave por paquete", lo que hacía que se generara una nueva clave de 128 bits por cada paquete, algo que evitaba que este protocolo fuera vulnerable a los ataques que afectaban al protocolo WEP.

En este protocolo se usaba además un Message Integrity Check (MIC) de 64 bits —conocido popularmente como MICHAEL—, que servía para proporcionar integridad a todo el sistema, pero de nuevo se comprobó que aquello no era suficiente para asegurar estas conexiones. Martin Beck —uno de los creadores de la suite aircrack-ng— y Erik Twes —de la Universidad Técnica de Darmstadt— desmotraron en 2008 cómo los ataques a las redes WPA eran factibles haciendo uso de parte de lo que ya se había logrado en los célebres ataques Chopchop a las redes WEP. Su documento 'Practical attacks against WEP and WPA" (PDF) se convirtió en todo un referente en este tipo de estudios, pero este documento solo fue el principio.

Pronto aparecerían variaciones como la de Mathy Banhoef y Frank Piessens, que con su 'Practical Verification of WPA-TKIP Vulnerabilities" (PDF) fueron aún más allá y lograron demostrar cómo era posible inyectar paquetes y descifrarlos, algo que podía ser aprovechado para "secuestrar una sesión TCP" e inyectar código malicioso.

Cifrados inseguros para nuestra red Wi-Fi

Sin cifrado o red Wi-Fi abierta

Las redes sin cifrado, o abiertas, son aquellas que no tienen ninguna contraseña y que permiten a cualquier usuario conectarse a ellas sin necesidad de nada más. Estas redes son totalmente inseguras ya que, además de permitir a cualquiera conectarse al router, la conexión no cuenta con ningún tipo de cifrado, por lo que cualquier usuario podría capturar los paquetes que enviamos y obtener así toda nuestra información.

Este sistema es, sin duda, el menor recomendable.

Cifrado WEP

El cifrado WEP fue uno de los primeros cifrados utilizados para proteger las redes inalámbricas. Este cifrado es débil y vulnerable y, aunque en el pasado podía servir más o menos, actualmente con la potencia de los sistemas informáticos domésticos y las

aplicaciones desarrolladas para explotar este tipo de cifrado, finalmente se considera un cifrado “inseguro” y es posible obtener su clave en tan solo unos minutos capturando paquetes mediante falsas solicitudes de acceso. El cifrado WEP ofrece una protección insuficiente, por lo que no es recomendable su uso.

Cifrados seguros para nuestra red Wi-Fi

Cifrado WPA

El cifrado WPA nació a partir de la necesidad de solucionar los problemas del cifrado WEP. Este sistema de cifrado ofrece una serie de variantes según la finalidad que se le vaya a dar:

- ✓ WPA-Personal: Utiliza un sistema de claves PSK o claves precompartidas donde el administrador especifica su propia contraseña y todos los usuarios se conectan a la red con ella, de manera que sea más fácil recordarla.
- ✓ RADIUS: Enfocado a empresas, este sistema de seguridad se basa en un servidor en el que los usuarios deben autenticarse con un usuario y una contraseña diferente para cada uno en vez de conectarse todos con una contraseña global.

Cifrado WPA2

El cifrado WPA2 es la actualización del cifrado WPA y mejora tanto la seguridad como el rendimiento de este. Este sistema también cuenta con las variantes de claves personales PSK y sistemas RADIUS para la gestión de redes, aunque el cifrado es muy superior al de WPA.

Tipo de cifrado (TKIP / AES) en WPA / WPA2

Las contraseñas WPA y WPA2 pueden utilizar dos tipos de cifrado diferente: TKIP y AES. Los usuarios que buscan compatibilidad con dispositivos antiguos (por ejemplo, una

Nintendo DS) deben utilizar WPA con cifrado TKIP, sin embargo, recientemente se han detectado varias vulnerabilidades en este cifrado, por lo que, salvo en casos de extrema necesidad, no es recomendable utilizarlo.

Si lo que queremos es asegurarnos de tener la máxima seguridad en nuestra red a la vez que le mejor rendimiento debemos elegir el cifrado AES ya que, además de la mejora en la seguridad, este algoritmo soporta mayores velocidades que TKIP.

Principales herramientas usadas para encontrar vulnerabilidades en una red WIFI

Aircrack-ng

Figura 7 Logo Aircrack-NG

El Aircrack es una de las herramientas más populares para romper cifrado WEP/WPA/WPA2. La suite de Aircrack-ng contiene herramientas para capturar paquetes y apretones de manos para autenticar a clientes conexión generando tráfico y herramientas para realizar ataques de fuerza bruta y diccionario. El Aicrack-ng es un todo-en-uno que cuenta con las siguientes herramientas (entre otros):

- Aircrack-ng para agrietarse de la contraseña;
- Aireplay-ng para generar tráfico y autenticación de cliente;
- Airodump-ng para capturar paquetes;
- airbase-ng para configurar puntos de acceso falsos.

suite Aicrack-ng está disponible para Linux y viene por defecto en Kali Linux. Si va a utilizar esta herramienta, usted tiene que asegurarse de que su tarjeta Wi-Fi es capaz de inyección de paquetes.

Reaver

Figura 8 Logo Reaver

Realiza ataques de fuerza bruta contra los pernos de la configuración protegida WiFi (WPS) para recuperar la contraseña WPA/WPA2. Puesto que muchos fabricantes de routers y liguam de ISPs el WPS por defecto, muchos routers son vulnerables a este tipo de ataques.

para utilizar reaver, se necesita una buena señal para el router inalámbrico y también la configuración correcta. En promedio de 4 a 10 horas, raver puede recuperar contraseñas de router vulnerables, dependiendo de la intensidad de la señal de punto de acceso y el PIN propio. Estadísticamente, tienes 50% de probabilidades de romper un PIN de WPS en mitad del tiempo.

PixieWPS

Figura 9 Logo Pixie WPS

PixieWPS está escrito en C y se utiliza para fuerza bruta en WPS pines sin conexión, explorar la baja o ninguna entropía de los puntos vulnerables de acceso. Este ataque es conocido como polvo de pixie (polvo de duende o hada). Los PixieWPS requiere una versión modificada del Get o Wifite para trabajar eficazmente.

Wifite

Figura 10 Logo Wifite

Es una herramienta automatizada para atacar varias redes WiFi encriptadas con WEP/WPA/WPA2 y WPS. En la puesta en marcha Wifite, requiere algunos parámetros para trabajar, pero el Wifite hará todo el trabajo duro. Se captura handshakes de WPA, autenticar clientes conectados automáticamente, suplantar la dirección MAC y mantener contraseñas seguras agrietadas.

Wireshark

Figura 11 Logo Wireshark

Es una de las mejores herramientas de protocolo de red de análisis disponibles si no el mejor. Con Wireshark, puede analizar una red con mayor detalle para ver lo que está sucediendo. Wireshark puede ser utilizado para la captura de paquete vivo, inspección profunda de cientos de protocolos, búsqueda y filtro de paquetes y es multiplataforma.

Las contraseñas WiFi, talón de Aquiles de WPA (y WPA2)

A este protocolo le fallaba otra pata: la de las contraseñas. Aunque los fabricantes de equipos de comunicaciones (routers, puntos de acceso) establecían contraseñas relativamente fuertes por defecto para proteger las redes WiFi predefinidas en sus equipos, los usuarios acababan renombrando sus redes y cambiándoles las contraseñas por otras fáciles de recordar.

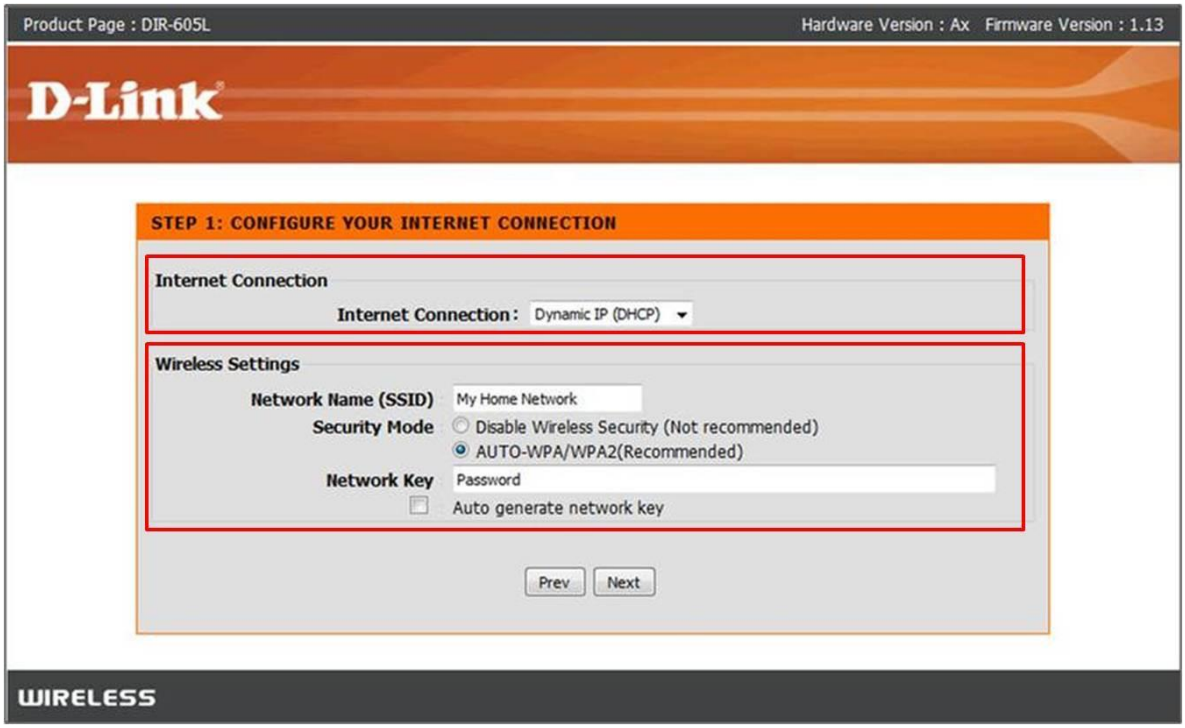

Figura 12 Página de configuración del Router D-link

Esas contraseñas débiles acababan siendo el verdadero problema de unas redes WiFi que quedaban desprotegidas ante los ataques de fuerza bruta con diccionario. Las suites como aircrack-ng y las distribuciones Linux dedicadas a la auditoría de seguridad se hicieron famosas por integrar herramientas capaces de atacar redes WiFi que usaran el protocolo WPA.

Estas suites permitían forzar a un cliente a desconectarse para volver a negociar la conexión con el punto de acceso, algo que daba acceso al llamado 4-way TKIP handshake, resultado de esa negociación y suficiente para tratar de descifrar la contraseña WiFi por fuerza bruta a través (normalmente) del uso de un diccionario.

Figura 13 Script ejecutado en Tablet Android

Estos diccionarios contienen habitualmente millones de palabras del lenguaje normal, pero también se pueden generar a partir de combinaciones de todo tipo de caracteres para formar palabras de cualquier longitud. Esos diccionarios permiten comparar el handshake con cada palabra del diccionario, y si está en ellos, el atacante logra obtener la contraseña.

El proceso es habitualmente largo y costoso en potencia de computación, y no siempre es efectivo: la clave está en el uso de contraseñas fuertes, y esos ataques de diccionario y fuerza bruta están destinados a descifrar contraseñas WiFi de redes WPA (y WPA2) que son débiles por longitud o por usar palabras muy populares. La capacidad de cálculo necesaria para acelerar los cálculos ha hecho que hayan aparecido herramientas que usan GPUs en lugar de CPUs para hacer esos cálculos (hashcat es una de las más conocidas), y existen servicios como GPUhash o OnlineHashCrack que te ayudan a descifrar esos handshakes de forma gratuita y sin que uses tus propios recursos.

WPS, buenas intenciones, implementación desastrosa

Uno de los problemas que imponían las conexiones WiFi era lo incómodo que era conectar cierto tipo de dispositivos para que aprovechasen esta capacidad. Las impresoras, por ejemplo, planteaban la necesidad de facilitar el sistema de conexión basado en introducir la contraseña WiFi en cada momento.

Así es como nació Wi-Fi Protected Setup (WPS), un estándar para crear una red inalámbrica doméstica segura que la Wi-Fi Alliance lanzó en el año 2006. La idea era estupenda, porque hacía que, si el router y el cliente disponían de esta capacidad, que uno se conectase al otro fuera cuestión de pulsar un botón.

Sin embargo, WPS acabó convirtiéndose en una condena más para la seguridadde las conexiones WPA y WPA2. Una vulnerabilidad detectada en diciembre de 2011 por parte de Stefan Viehböck dejaba claro que aquel protocolo estaba expuesto a un ataque que permitía conseguir la clave WiFi sin necesidad de diccionarios o del proceso con el que hasta entonces se podían atacar a las redes WPA y WPA2.

En su documento 'Brute forcing Wi-Fi Protected Setup" (PDF) este investigador demostraba cómo un ataque por fuerza bruta hacía factible superar la seguridad de los protocolos WPA y WPA2, y concluía con una recomendación a los usuarios: desactivar WPS, algo que de hecho no todos los routers facilitaban o incluso hacían posible.

Ese ataque online tuvo una alternativa offline con el ataque "Pixie Dust" descubierto en 2014 por Dominique Bongard, que no estaba siempre disponible pero que sí afectaba a unos cuantos fabricantes de chips WiFi. Tanto el uno como el otro fueron integrados en sucesivas versiones de suites de seguridad y auditoría con herramientas como pixieWPS o Reaver que permitían atacar a este tipo de redes de forma automática y transparente para los usuarios.

creíamos que estábamos a salvo, pero no era así

Hace la friolera de 13 años que tenemos teórico protocolo seguro para nuestras redes WiFi. Fue en 2004 cuando se lanzó por fin WPA2, la segunda versión de WPA que era de hecho la implementación del estándar IEEE 802.11i.

Figura 14 Whiphisher

Las herramientas para realizar auditorías automatizadas a redes WiFi de todo tipo son cada vez más avanzadas y más sencillas de usar.

Wifiphisher corriendo sobre Wifislax es un buen ejemplo de estas soluciones.

En WPA2 se sustituyen tanto TKIP como el cifrado RC4 que se usó tanto en WEP y en WPA con dos alternativas de cifrado y autenticaciones más fuertes. En primer lugar, el Advanced Encryption Standard (AES), y en segundo, el llamado Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). Era además posible configurar WPA2 con TKIP como forma de mantener la compatibilidad hacia atrás.

El protocolo ha demostrado ser mucho más resistente a ataques que sus predecesores, pero eso no significa que sea inmune. La vulnerabilidad llamada Hole196 aprovecha la implementación del Group Temporal Key (GTK), que teóricamente hacía uso de un sistema aleatorio que impedía ataques a esa parte del sistema. Sin embargo, el uso de un generador de números aleatorios (RNG) específico utilizado por ciertos fabricantes hacía predecible ese GTK, lo que a su vez hacía vulnerable el protocolo.

A ese problema se le suman al menos otros dos. El primero, una vez más, el uso de contraseñas débiles que pueden también ser descifradas mediante ataques de fuerza bruta como los anteriormente descritos. El segundo, el uso de métodos alternativos de ingeniería social que engañen al usuario.

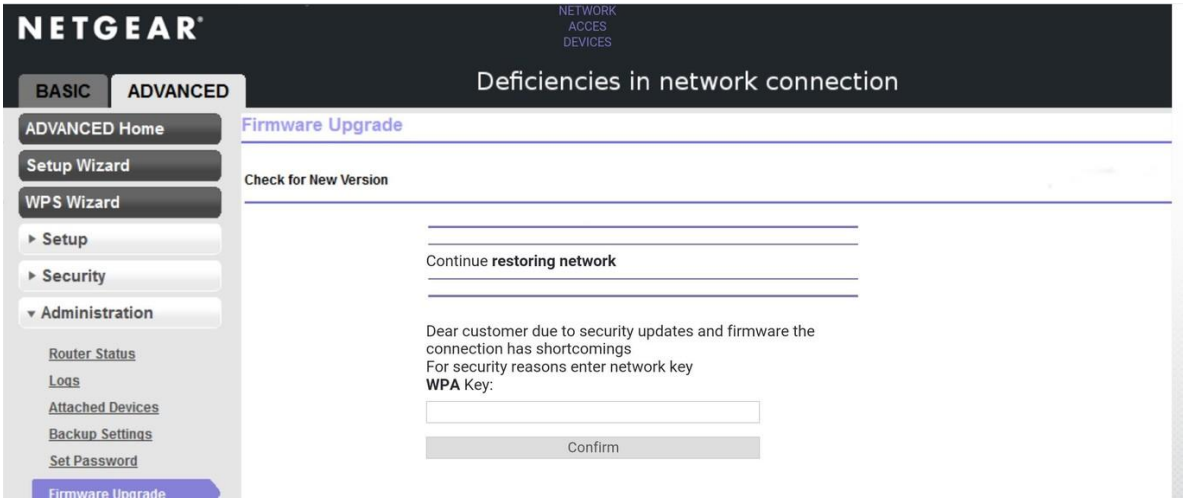

Figura 15 Página que imita la del router para el robo de contraseña

Es algo así como "si no puedes capturar la contraseña directamente, pídesela al usuario". Un atacante puede usar herramientas como Fluxion para desconectar a un cliente (usuario) de su red WiFi y generar una página web que simule la que generaría su router. Esto haría creer al usuario que se ha perdido la conexión por algún conflicto y que con introducir la contraseña a su red WiFi desaparecerá el problema: lo que está haciendo en realidad es confesarle al atacante esa contraseña WiFi sin darse cuenta.

El anuncio de hoy del investigador de seguridad Mathy Vanhoef vuelve no obstante a demostrar que nuestras conexiones WiFi siguen sin estar protegidas aun cuando usemos el protocolo WPA2. Los llamados KRACKs (Key Reinstallation AttaCKs) permiten que los atacantes puedan "acceder a la información que hasta ahora se asumía que estaba cifrada de forma segura".

El ataque permite por tanto acceder a información sensible que transmitimos a través de nuestras conexiones WiFi, tal como números de tarjetas de crédito, contraseñas, mensajes de chat, correos o fotos, y "funciona con todas las redes WiFi", siendo además posible en algunas de ellas "inyectar y manipular los datos".

¿Hay solución? Sí: la de que los fabricantes ofrezcan una actualización del firmware de sus equipos de comunicaciones y los responsables de nuestros dispositivos móviles (portátiles, smartphones y tablets sobre todo) también ofrezcan esos parches para atajar el problema. Lamentablemente es probable que en muchos casos esas actualizaciones tarden en llegar o incluso no lleguen nunca, por lo que hacer uso de mecanismos adicionales (VPNs, conexiones seguras HTTPS) también ayudará a proteger nuestros datos sensibles.

Materiales

- Para las pruebas de intrusión se usarán don equipos portátiles con características diferentes.

Equipos utilizados para las pruebas		
Equipo #1		
Marca y modelo	Características	
ASUS. X453S.	Procesador	Intel Celeron 3050. 2,16 GHz
	Memoria RAM	4 GB
	Disco duro	500 GB
	Tarjeta inalámbrica	Realtek rtl8723be
	GPU	Gráficos HD Intel® para el procesador Intel® Celeron® serie N3000
	S.O	Wifislax LIVE 64bits
Equipo # 2		
Marca y modelo	Características	
ACER ASPIRE ES1-411	Procesador	Intel Celeron N2840 2,58 GHz
	Memoria RAM	2 GB
	Disco duro	500 GB
	Tarjeta inalámbrica	Broadcom bcm94313hmgb
	GPU	Gráficos HD Intel® para procesadores Intel Atom® serie Z3700
	S.O	Kali linux

Figura 16 Características de los Equipos usados

Tabla 10 Características de los Equipos usados en las pruebas

- Modem Huawei modelo E5330 utilizando una configuración de seguridad WPA.
- Adaptador WIFI USB: D-Link® Tarjeta de Red USB WiFi N150 DWA-123.
- Adaptador WIFI USB: Realtek RTL8188EU Wireless LAN 802.11n USB 2.0.
- Sistema operativo destinado a la auditoria de redes WIFI: Wifislax , Kali Linux

Dichos sistemas con la Suite Aircrack-ng.

Metodología

En nuestro proyecto nos hemos guiado mediante las siguientes etapas:

Investigación bibliográfica: esta primera etapa es de vital importancia para poder comprender cuales son los diferentes requerimientos que necesitamos para la planificación y ejecución del proyecto mediante toda la teoría que esto implica.

Instalación de herramientas: Con los requerimientos determinados en el punto anterior se procede a la instalación de herramientas que sirven para realizar las diferentes pruebas, entre estas podemos mencionar: Aircrack-ng.

Realización de pruebas: Mediante los diferentes ataques para comprobar los niveles vulnerabilidades que tienen de los protocolos de seguridad.

Obtención de resultados: como resultado mediante las pruebas se obtuvo que cada cifrado tiene diferentes niveles de vulnerabilidad, siendo el mas vulnerable el WEP y el menos vulnerable el WPA2-PSK .

PRUEBAS

Se realizaron pruebas en un moden de la compañía Claro El Salvador. Con seguridad estándar donde se penetro la red utilizando la herramienta Goyscript .

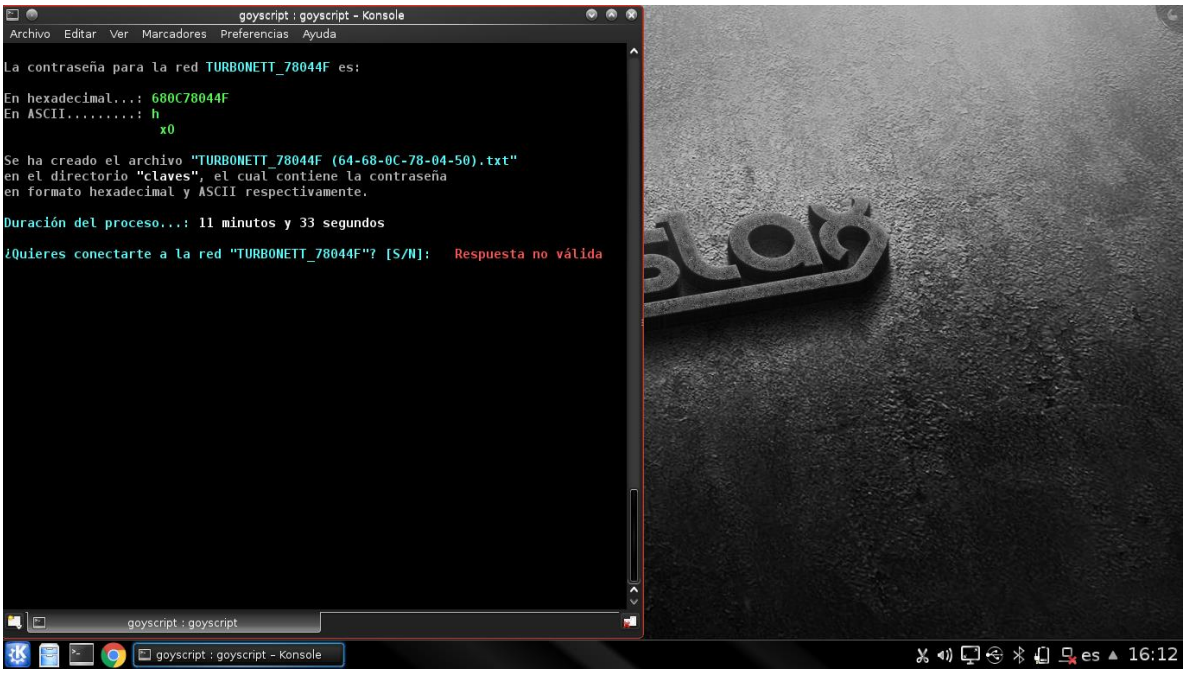

Figura 17 Prueba exitosa

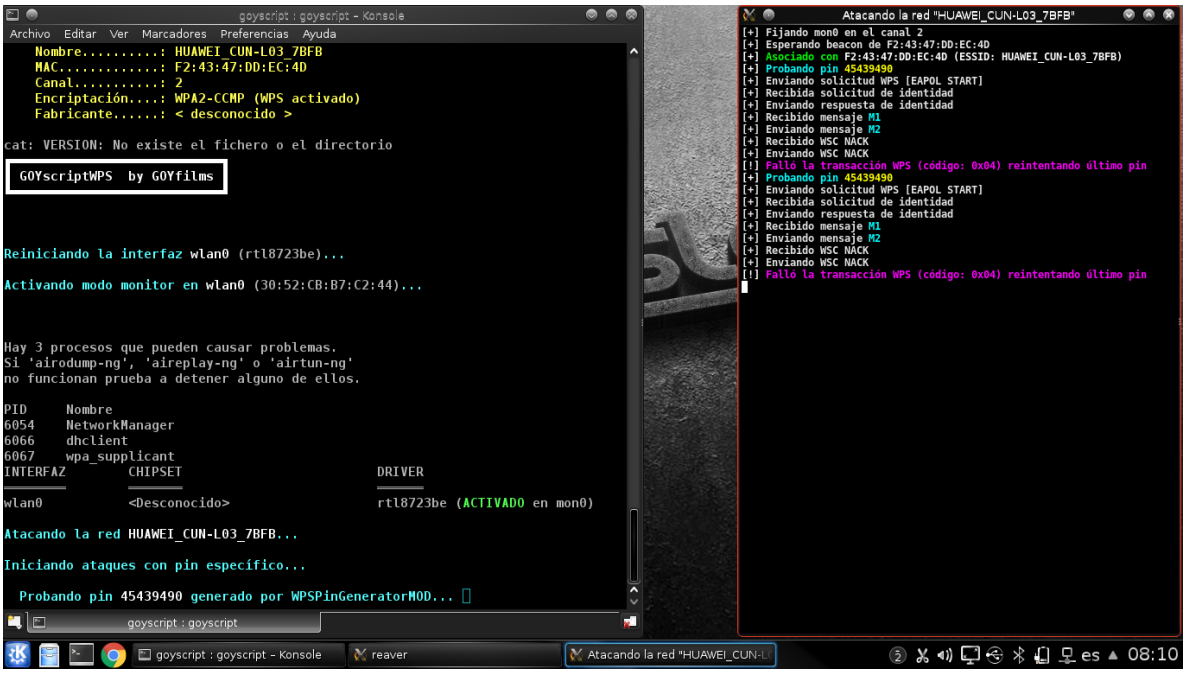

Figura 18 Proceso de prueba

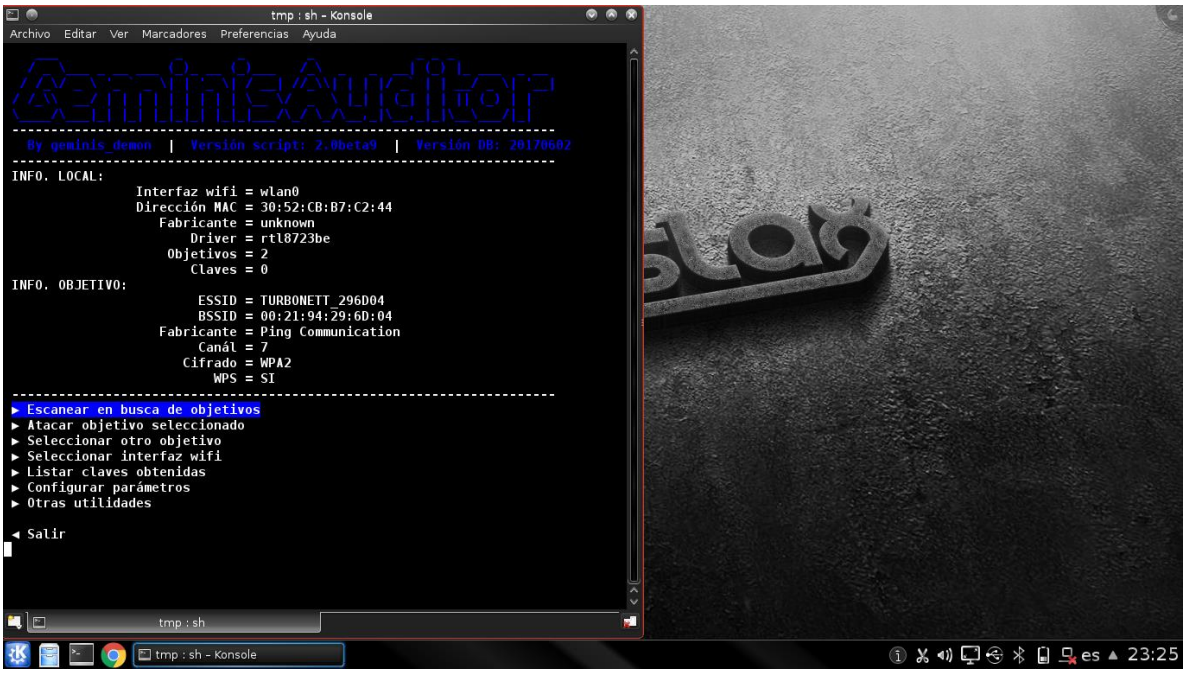

Figura 19 Prueba con la herramienta Geminis Auditor

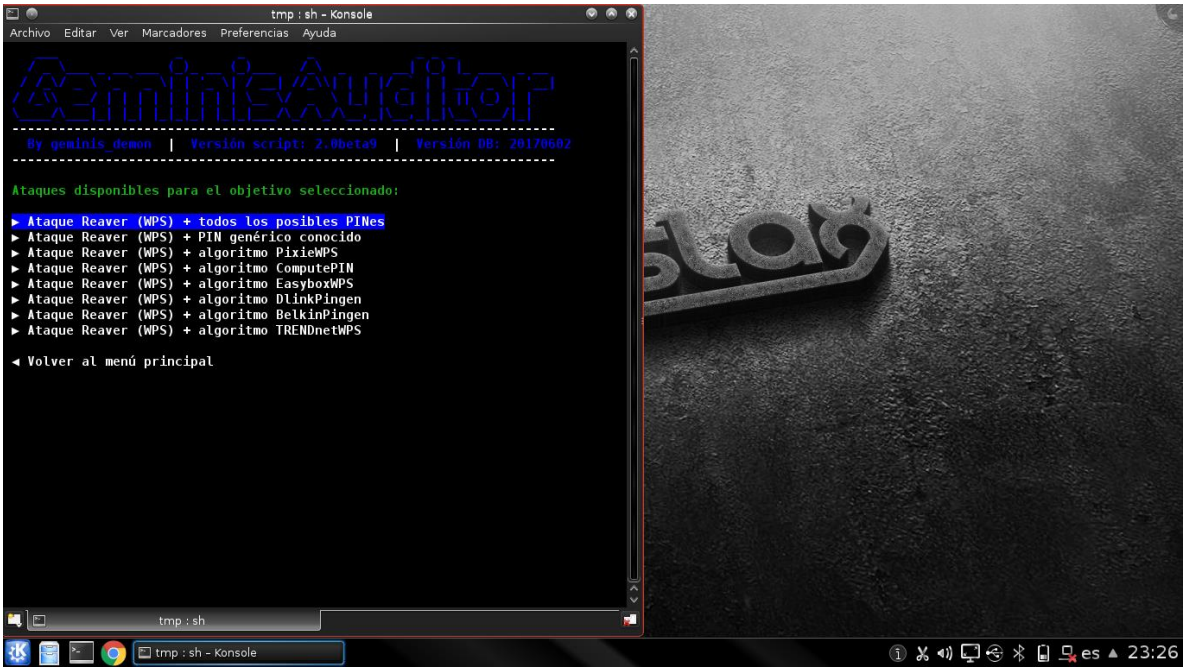

Figura 20 Tipos de Ataques que nos permite ejecutar Geminis Auditor

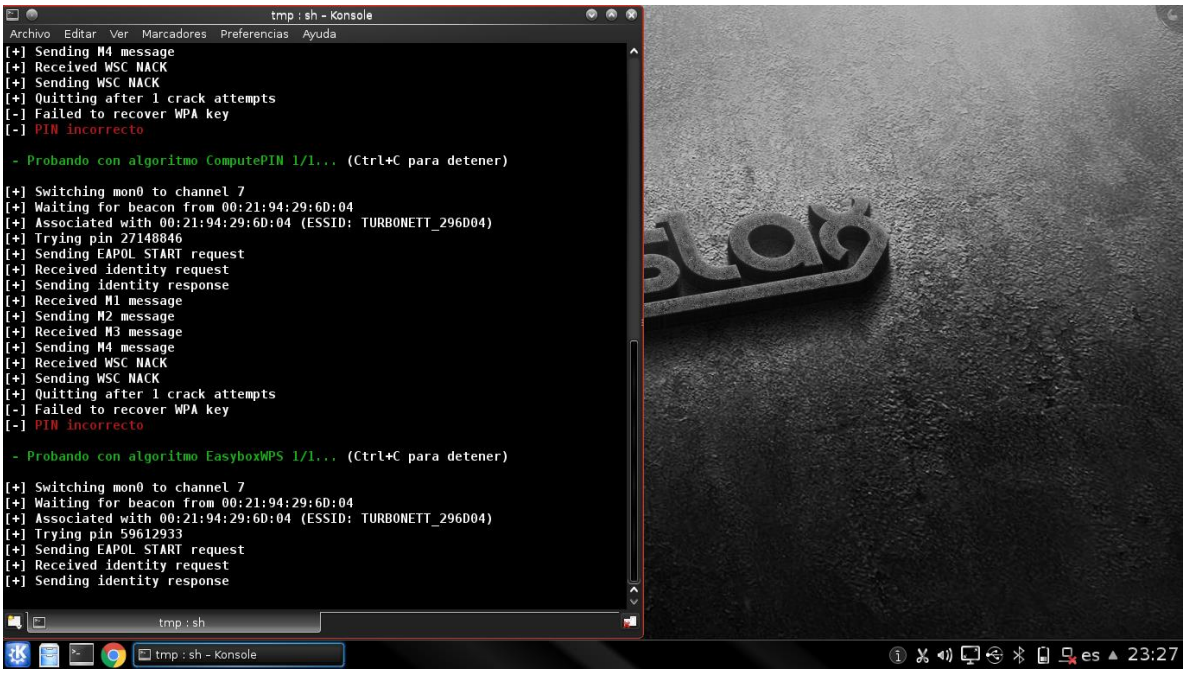

Figura 21 Intento de Penetracion en un moden Huawei con la herramienta Geminis Auditor

Conclusiones

La seguridad de las redes informáticas depende mucho de su cifrado ya que existen diferentes tipos de cifrado los cuales hacen más difícil que otra persona pueda acceder a nuestras redes de forma maliciosa. Además, esto depende de que tan fuerte sea nuestra contraseña lo mas recomendable es incluir en estas letras, números y signos la cual sería la forma más efectiva de proteger nuestras redes ya que si solo usamos letras o números fácilmente pueden irrumpir en ellas.

Debemos tomar en cuenta que día con día surgen nuevas herramientas las cuales permiten a terceras personas tener acceso fácil a nuestras redes, sino tomamos a bien de cambiar las contraseñas en ciertos periodos de tiempo y monitorear quien hace uso de nuestra red.

Bibliografía

www.xataka.com

www.norfipc.com

www.informaticamoderna.com

Andy Rathbone. Windows vista para dummies

June Jamrichoja Parsons, Carl McDaniel Conceptos de Computación: Nuevas Perspectivas.

Red Inalámbrica – Wikipedia, la enciclopedia libre es.wikipedia.org