REDES WIFI:
¿REALMENTE SE PUEDEN PROTEGER?

-MISTIC- Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Autor: Juan Ricardo Vila Ríos

Director: Marco Antonio Lozano Merino

Realizado en colaboración con la empresa INCIBE

Diciembre de 2017

AGRADECIMIENTOS

A Marta, por haberme apoyado en la decisión de embarcarme en este Máster y no haberse quejado ni un solo día del tiempo dedicado al mismo.

A Martín, que sin entenderlo todavía ha tenido que compartir sus primeros meses de vida con la recta final del Máster, por lo cual pienso compensarle toda su vida.

RESUMEN DEL TRABAJO

El trabajo presentado a continuación tiene como objetivo analizar la seguridad en las redes WiFi. Al hablar de las redes WiFi nos referimos al termino popular del mismo, que abarca en concreto el protocolo WLAN (Wireless Local Área Network) y por tanto aquellas tecnologías definidas por el estándar 802.11x.

Este análisis se representará de una forma que pueda ser comprensible por todos los públicos y no solo por el personal con altos niveles de conocimientos técnicos. Con esto se busca concienciar al gran público que es el que debe tomar consciencia de la seguridad de las redes que usa.

Para ello se llevará a cabo un proceso de investigación que se plasmará en una parte inicial más teórica en la cual analizar la evolución de las redes WiFi y la seguridad de las mismas a lo largo de los años.

A continuación, se realizarán pruebas de concepto, que intentarán plasmarse de la forma mas sencilla posible con el fin de demostrar que hoy en día, para las redes menos protegidas ni tan siquiera es necesario un experto con altos conocimientos técnicos, aunque es el experto el que dada la facilidad de ataque existente hoy en día puede realizar más daño en caso de un ataque exitoso.

Por último, y a nivel personal, tenemos unas conclusiones y unas pequeñas recomendaciones para mejorar un poco nuestra seguridad en cuanto a redes WiFi se refiere.

SUMMARY

The aim of the work presented below is to analyze the WiFi networks security. For WiFi networks, we are referring to the popular term of it, which covers, in particular, the WLAN protocol (Wireless Local Area Network) and then those technologies defined by the 802.11x standard.

This analysis will be represented in a way that can be understood by all audiences and not only by people with high levels of technical knowledge. This way, we are trying to make the public aware of the insecurity of the networks they use every day.

For this purpose, a research process will be carried out that will be represented into the initial part of the work where we analyze the evolution of WiFi networks and their security over the years.

Later on, proofs of concept will be carried out, which will be represented in the simplest way possible in order to demonstrate that nowadays, less protected networks can be hacked by people with no technical knowledge, although an expert could be the one doing more damage in the event of a successful attack.

Finally, and on a personal level, we have some conclusions and some small recommendations to improve our security in terms of WiFi networks.

TABLA DE CONTENIDO

INTRODUCCIÓN

EXPLICACIÓN DETALLADA DEL PROBLEMA A RESOLVER

En este proyecto, Redes wifi: ¿Realmente se pueden proteger?, se busca analizar la seguridad de las propias redes wifi, tanto públicas como domésticas y corporativas. Dentro de este objetivo se busca también la facilidad o dificultad de acceder las mismas de acuerdo a las medidas de protección que estas ofrecen.

Para ello, además del uso de herramientas de auditoría se explorarán en concreto los ataques que más afectan al usuario de a pie hoy en día y que son más complicados de evitar como son “linset” o “wiphishing”.

ENUMERACIÓN DE LOS OBJETIVOS QUE SE QUIEREN ALCANZAR

Analizar la seguridad de las redes wifi: públicas, domésticas y empresariales.

Analizar si hay equipos no reconocidos conectados a dicha red.

Pruebas de ataques reales para explorar las opciones y los posibles mecanismos de protección.

Análisis de los posibles riesgos de una red comprometida, especialmente ante ataques “man-in-the-middle” y la captura del tráfico de dichas redes.

Investigar sobre la creciente oferta de dispositivos IoT y los riesgos que estas suponen.

DESCRIPCIÓN DE LA METODOLOGÍA QUE SE SEGUIRÁ DURANTE EL DESARROLLO DEL TFM

Para la realización de este TFM se tomará la vertiente del Estudio Explicativo mediante el Método Inductivo intentando que este pueda ser comprensible no solo por expertos en la materia si no por cualquier persona que tenga curiosidad o interés sobre el mismo. Esto viene significando que mediante el uso de casos prácticos se intentará explicar la problemática de las redes Wireless y los mecanismos de protección de que se disponen.

Se realizará pues una investigación aplicada para buscar la respuesta al título de este proyecto mediante la aplicación y la experimentación, para la posterior explicación de los mismos.

Debido a la limitación de medios el análisis para llevar dicha tarea a cabo será cualitativo, pero siempre orientado a decisiones, buscando soluciones a los problemas que nos podamos encontrar.

Si bien se realizara una labor de investigación bibliográfica, intentare darle un enfoque experimental para llevar a cabo una investigación, dentro de los posible, de forma empírica.

Por último, comentar que dicha investigación se realizara de forma experimental en laboratorios creados para ello para no entrar en problemas legales durante la realización del mismo.

LISTADO DE LAS TAREAS A REALIZAR PARA ALCANZAR LOS OBJETIVOS DESCRITOS

- Investigación bibliográfica previa sobre seguridad Wireless y nuevos tipos de ataques.
- Investigación más profunda sobre distintos tipos de ataques a redes WIFI.
- Creación de laboratorios para realización de pruebas.
- Experimentación de laboratorios probando diferentes ataques.
- Aplicar medidas de seguridad y experimentar de nuevo sobre dichas redes.
- Análisis de la información recopilada.
- Exposición de dicha información de forma comprensible para todos los públicos.

PLANIFICACIÓN TEMPORAL DETALLADA DE ESTAS TAREAS Y SUS DEPENDENCIAS.

Durante el primer periodo se realizará el proceso de investigación tanto de la seguridad Wireless y los respectivos ataques como la de los específicos “linset” y “wiphising” como de las posibles medidas que se puedan tomar para proteger o mitigar dichos ataques. En función a dicha información se prepararán los laboratorios y las herramientas necesarias para la fase de experimentación.

Durante el segundo periodo y ya con los laboratorios preparados se realizarán pruebas experimentales de ataques sobre los distintos tipos de redes (públicas, domésticas, empresariales) y se buscará también aplicar medidas de seguridad o mitigación para, con ellos activos, volver a comprobar la seguridad de dichas redes.

Por último, en una tercera fase, se realizará un análisis de la información recopilada en las anteriores dos fases y esta será plasmada en una memoria final intentando alcanzar un público lo más amplio posible.

UNA PEQUEÑA REVISIÓN DEL ESTADO DEL ARTE

Dado que la informática y tecnología asociada a la misma son siempre unos sectores muy cambiantes, durante el transcurso de la realización de este proyecto se realizará también un pequeño proceso de investigación sobre los últimos métodos de auditoría Wireless y de posibles nuevas vulnerabilidades que existan sobre estas redes.

Es preciso tener en cuenta que, aunque en la actualidad todos los protocolos tienen vulnerabilidades, no lo era cuando irrumpieron fuerte en el mercado funciones como el WPS, pensado para facilitar las conexiones, pero que al mismo tiempo debilita en gran manera la seguridad de las redes. A pesar de ello, es un servicio que siguen integrando gran parte de los puntos de acceso vendidos hoy en día.

No podemos dejar de lado la creciente oferta de dispositivos IoT. A pesar de que todavía hay una guerra de estándares abierta, la verdad es que WiFi está empezando a escalar posiciones en cuota de mercado y se prevé que lo haga en mayor medida según se vaya implantando el último standard WiFi HaLoW 802.11ah (Low power, long range).

OTRA INFORMACIÓN DE INTERÉS

A fin de aclarar puntos sueltos decir que el siguiente trabajo, que se podría realizar en un ambiente real, se realizará en laboratorio para evitar los problemas legales de hacerlo en un ambiente real, y para evitar retrasos que supondría el obtener los permisos necesarios para su realización en un ambiente real dentro de la legalidad.

El presupuesto para este será bajo, ya que con casi cualquier router se podría empezar a experimentar, aunque intentaré que este tenga el mayor número de funcionalidades o sea compatible con OpenWrt.

Para realizar las pruebas usaremos una máquina virtual con Wifislax y equipada con una tarjeta inalámbrica ALFA AWUS036H que nos permita trabajar con ella en modo monitor e inyectar código.

EVOLUCIÓN DE LA SEGURIDAD EN LAS REDES WIFI

OSA

Open System Authentication (OSA) o Autenticación Abierta fue el primer sistema que había para la conexión de redes WIFI. En este sistema el cliente envía un mensaje de autenticación y el receptor le responde con uno de aprobación.

Por aquel entonces el sistema de Autenticación Abierta solo requería saber cuál era el SSID al que se quería conectar y la seguridad venia de únicamente 2 puntos. El primero, la distancia, escasa en los inicios. El segundo, el filtrado MAC, con el cual se podía limitar los dispositivos aquellos que eran especificados dentro de ese filtrado.

La seguridad por tanto es mínima dado que la suplantación de las MAC (o MAC Spoofing) es algo relativamente sencillo.

WEP Y SKA

HISTORIA

Wired Equivalent Privacy (WEP) corresponde al sistema de cifrado incluido en la norma 802.11 y fue el primer protocolo de seguridad implementado en las redes WIFI. Se consideraría un Standard de seguridad en 1999. Como el nombre indica, se suponía que iba a ser equivalente a la seguridad en las redes cableadas, pero pronto se descubrieron fallos de seguridad que provocan que la seguridad WEP sea muy fácil de romper. Ya en 2001 se podían encontrar exploits para la misma y el FBI demostraría en 2005 como dicha seguridad se podía romper en tan solo minutos usando herramientas disponibles de forma pública.

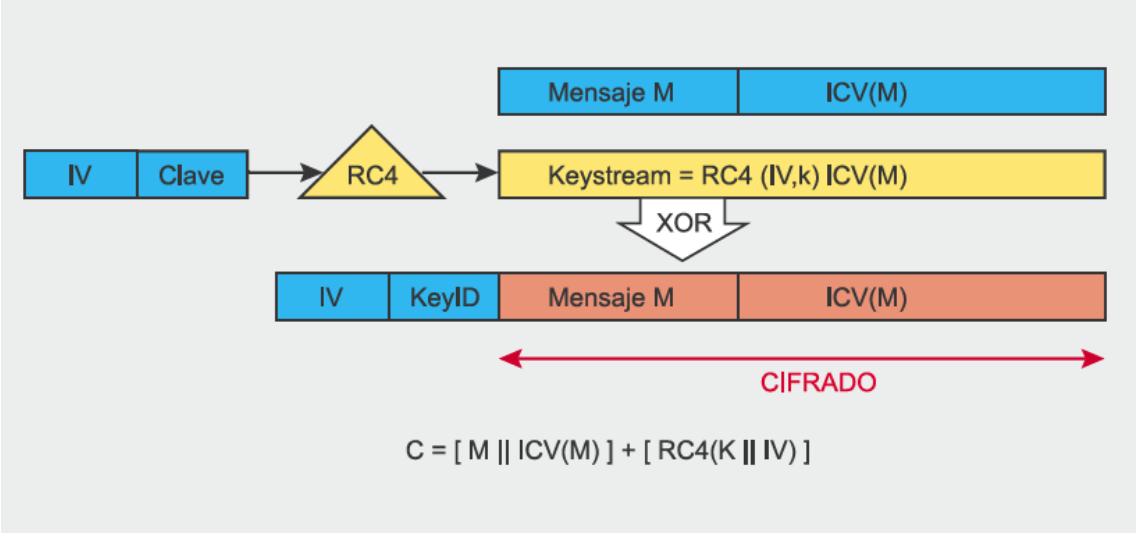
FUNCIONAMIENTO Y SEGURIDAD

Al sistema de cifrado usado por WEP se le llamaba Shared Key Authentication (SKA). Se basaba en configurar de 1 a 4 claves pre-compartidas que eran usadas por todos los clientes que se conectaban a la red WIFI.

La encriptación en WEP funciona mediante un algoritmo de seguridad RC4 con claves de 64 bits de los cuales 24 son fijos correspondientes al Vector de Inicialización (IV) y los restantes 40 corresponden a la clave. Con el fin de intentar que la clave no se repita, el IV se genera en un extremo de forma dinámica para cada trama y se envía dentro de la misma al otro extremo.

La forma de trabajar del algoritmo WEP es la siguiente; Primero se calcula un Cyclic Redundancy Code (CRC) de 32 bits de los datos (CRC-32) para garantizar la integridad de los mensajes (ICV). Por otro lado, se coge el IV y se le añade la clave creando el *seed*. El PRNG de RC4 genera una secuencia de caracteres pseudoaleatorios de 32 bits a partir del *seed.* Se calcula la O exclusiva (XOR) de ambos mensajes de 32

bits, obteniendo así el mensaje cifrado. Por último, Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos de la trama.



1 Algoritmo de cifrado WEP [1]

VULNERABILIDADES Y ATAQUES

Por un lado, se encuentra la falta de una especificación a la hora de implementar el IV, lo cual lleva a que muchos fabricantes hagan un simple valor incremental en la misma hasta cubrir las 2^{24} combinaciones (16 millones apróx.) y vuelvan a empezar.

Por otro lado, aunque el CRC-32 viaje cifrado, este puede ser modificado por el camino sin necesidad de conocer el resto, de ahí que en vez de CRC se recomiende como ICV el algoritmo SHA1-HMAC [2].

También se encuentra como debilidad la forma de negociar nuevas conexiones, en la que el mismo mensaje es enviado sin cifrar, y luego cifrado con la clave WEP, facilitando el trabajo para romper dicha clave.

Por último, está la ausencia de protección contra mensajes repetidos (replay), lo cual puede ser utilizado también para realizar ataques contra la seguridad WEP.

INYECCIÓN DE TRAMAS

El protocolo WEP no dispone de ningún sistema para detectar tramas duplicadas, es por ello que esto se considera una vulnerabilidad.

Un atacante puede capturar una trama WEP y retransmitirla tantas veces como quiera, donde el receptor la dará por válida en caso de existir una asociación. De no existir se pueden modificar las direcciones del emisor y/o receptor por otra que si se encuentre asociada y de nuevo el receptor dará por válida la trama.

Se permite pues repetir el IV, ya que esto no es un problema para el receptor, que no lo controla, como cambiar la cabecera MAC, pues esta no se incluye dentro del código de integridad ICV.

FALSIFICACIÓN DE LA AUTENTICACIÓN

Este sistema ataca el uso del intercambio de 4 tramas como proceso de autenticación. Estas son: petición de autenticación, reto, respuesta y resultado.

Es por ello que un atacante que capture las tramas de un usuario autenticado en un AP, podría autenticarse en dicho AP sin necesidad de conocer la clave WEP.

ATAQUE DE FRAGMENTACIÓN

Este ataque cuyo objetivo es generar un archivo XOR requiere la captura de al menos un paquete de datos para ser iniciado. Se basa en extraer poco a poco información de dichos paquetes acerca del PRGA para luego validarlo reenviando al AP un paquete ARP y/o paquetes LLC. Si la respuesta es válida añadimos algo más de información y seguimos con el ataque. Esto se repite hasta alcanzar los 1500 bits del PRGA. Para ello se utiliza la herramienta aireplay-ng con una llamada de la siguiente forma:

aireplay-ng -5 -b MAC-AP -h MAC-Origen-Paquetes mon0

ATAQUE FMS/KOREK

Un ataque muy exitoso contra las redes WEP es el FMS por estadística de IV que ataca el cifrado RC4, en concreto la débil implementación de los vectores de inicialización. Esto se hace por análisis de los paquetes capturados, con mayor éxito cuanto mayor sea el número de paquetes capturados.

Para ello se usa tanto airodump para capturar los paquetes WEP como aircrack para crackear la clave.

Posteriormente Korek mejoraría el proceso estableciendo relaciones entre diferentes bytes de la clave RC4 lo que reduciría el número de paquetes capturados necesarios para crackear la clave de los 4-6millones en el ataque FMS a solo 700 mil para el de Korek para que la probabilidad de acierto sea superior al 50%.

ATAQUE PTW

Este ataque es una mejora más del ataque FMS/Korek añadiendo dos nuevos conceptos para mejorar el análisis de los paquetes y el ataque al algoritmo RC4. Tras esta mejora los paquetes necesarios para un ataque exitoso por encima del 50% se reducen a solo 35-40 mil paquetes.

ATAQUE CHOP-CHOP

El objetivo del ataque Chop-Chop es generar un archivo XOR. En este caso en vez de múltiples paquetes solo necesita uno, lo más pequeño posible. También requiere una señal fuerte y estar asociado al AP, lo que implica estar cerca del mismo.

El ataque se basa en eliminar el último byte de datos cifrados y generar un nuevo paquete (más pequeño) con e ICV parcheado. A partir de aquí se intenta averiguar cuál es ese byte eliminado probando todas las combinaciones posibles y forjando dichos paquetes parcheados. Estos se envían al AP y se espera por una respuesta positiva. Una vez localizado se podría ir repitiendo el proceso sobre el resto de bytes hasta obtenerlos todos.

En este caso nos apoyaremos tanto en la herramienta aireplay-ng como en packetforge-ng para forjar los paquetes.

ATAQUE CAFFE LATTE

Este ataque a diferencia del resto tiene como objetivo el cliente en vez del AP y se puede llevar a cabo en aproximadamente 5 minutos bajo condiciones óptimas. Para ello se abusa de que los AP, a diferencia de los clientes, no necesitan autenticación en el caso de WEP.

Para llevarlo a cabo se crea un Fake AP con ESSID igual a alguno al que la víctima se haya conectado antes. A pesar de tener diferentes claves el proceso llegaría hasta la asociación de cliente y AP.

Al reto de autenticación nuestro Fake AP responderá siempre que es válido para que el cliente intente obtener una IP. Al no conseguirlo (no se la damos) este se asigna una automáticamente y nos envía paquetes ARP para anunciarla. Dada la información obtenida de esos ARP de nuevo entra en acción nuestro Fake AP. Ahora es este el que introduce peticiones ARP de una IP cualquiera y como destino la IP del cliente. Este responderá a dichas peticiones generando el tráfico que necesitaremos para capturar los paquetes con IVs que nos llevaran a crackear la clave correspondiente.

HERRAMIENTAS

AIRMON-NG

Script para activar el modo monitor de las tarjetas inalámbricas.

AIREPLAY-NG

Herramienta para inyectar paquetes en la red. Entre los diferentes ataques que se suelen realizar con esta herramienta nos encontramos con la desautenticación de clientes, falsas autenticaciones, inyección de ARP y diversos de los ataques citados en este trabajo.

AIRODUMP-NG

Se usa para capturar paquetes de la red como pueden ser las IVs en el caso de redes con seguridad WEP.

AIRCRACK-NG

Este es el programa principal de la Suite, que se encarga de crackear la clave de la red wifi para los diferentes métodos de seguridad y dadas unas determinadas condiciones.

PACKETFORGE-NG

Esta herramienta tiene como objetivo ayudarnos a forjar paquetes encriptados que luego podamos inyectar en la red, como en el caso de las peticiones ARP.

WPA

HISTORIA

Wi-Fi Protected Access (WPA) corresponde a la norma 802.11i, pero solo a una parte de ella pues dicha norma todavía estaba en desarrollo cuando se propuso WPA en el año 2003. La razón de adelantarse a la publicación de la norma se encontraba en la falta de seguridad en el protocolo WEP y la demanda de mayor seguridad por parte de los usuarios.

FUNCIONAMIENTO Y SEGURIDAD

Para mejorar la seguridad de WEP se integra el Protocolo de Integridad de Clave Temporal (TKIP) con el uso de llaves dinámicas y mejorando por tanto el cifrado RC4 de WEP.

WPA viene a solucionar la debilidad del IV incluyendo vectores de 48bits y asignando unas reglas para la secuenciación de los mismos, para evitar los problemas existidos en WEP.

PSK

Es un modo menos seguro dentro de las redes inalámbricas en el que se usan las Pre-Shared Keys (PSK). Este está diseñado para pequeñas redes domésticas o de oficina donde varios usuarios comparten la misma contraseña.

WPA+TKIP/AES

Esto vienen dado así dado con el uso de las PSK, se consideran las redes WPA como WPA Personal, dentro de las cuales se puede configurar como TKIP o como AES. Dentro de las TKIP (Temporal Key Integrity Protocol) se usa una única llave que se mezcla con los mensajes.

WPA+AES

Después llegará WPA-AES, que es la codificación más segura (refiriéndose a AES), especialmente en su aplicación en WPA2, y que se basa también en el uso de una clave precompartida de entre 8 y 63 caracteres.

EAP

Extensible Authentication Protocol (EAP) es un protocolo de autenticación usado mayoritariamente en redes inalámbricas. Es compatible tanto con WPA como con WPA2. Hay diferentes métodos que operan dicho protocolo: EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP y EAP-TTLS.

RADIUS

Este protocolo de autenticación será implementado tanto en WPA como en WPA2, permitiendo una capa mayor de seguridad. Además, a partir del 2003 será compatible con el esquema de autenticación EAP.

VULNERABILIDADES Y ATAQUES

El método más habitual para atacar este tipo de redes es el uso de fuerza bruta mediante el uso de herramientas como Aircrack. El éxito se basa en tener la clave dentro del diccionario a usar, o en caso de los modernos sistemas con ayuda de GPU esperar el tiempo adecuado hasta dar con la combinación correcta.

Para descubrir usuarios dentro del protocolo EAP también existe una herramienta llamada WeaPe.

HERRAMIENTAS

- Suite Aircrack-ng
- Pyrit
- Reaver
- Goyscript

WPA 2

HISTORIA

Wi-Fi Protected Access 2 (WPA2), publicado en 2006, viene para mejorar el existente WPA corrigiendo sus deficiencias incluyendo esta vez todas las opciones de 802.11i.

FUNCIONAMIENTO Y SEGURIDAD

Esta introduce el Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) para sustituir al TKIP, basándose esta vez en un cifrado por bloques AES con longitud variable de clave de 128, 192 o 256 bits, el cual se considera muy seguro. También introducirá el hanshake de 4 vías que esta tan de moda hoy en día al ser el que da entrada a WPA2 por las últimas vulnerabilidades encontradas.

RSN

Robust Security Network es la nueva arquitectura usada para las redes inalámbricas, que viene a dejar de lado el uso de WEP. Es la que se conoce como WPA2 y que trae cambios especialmente interesantes en cuanto a cuestiones de seguridad.

EAP/TLS O PEAP

Protected Extensible Authentication Protocol (PEAP) es un protocolo que encapsula a EAP con una capa de seguridad extra, Transport Layer Security (TLS), para corregir las deficiencias de EAP. Aunque no se especifica en la norma que métodos usar, los más habituales son EAP-MSCHAPv2 y EAP-GTC.

VULNERABILIDADES Y ATAQUES

El método hasta ahora más habitual para atacar este tipo de redes es el uso de fuerza bruta mediante el uso de herramientas como Aircrack (con escaso éxito salvo suerte con el diccionario al ser un proceso muy lento) o recorriendo a otras posibilidades como los ataques WPS.

KRACK

Más recientemente y a pesar de dicha “seguridad” se ha publicado un estudio en el que se demuestra que las redes WPA2 también se encuentran comprometidas. El sistema se llama Key Reinstallation Attacks (KRACK) y dadas las condiciones adecuadas permite analizar el tráfico cifrado de cualquier red WIFI hasta la fecha. Por tráfico cifrado se refieren al cifrado por la propia red, no al que va dentro de los protocolos HTTPS o sobre una VPN.

HERRAMIENTAS

- Las mismas que en el caso de WPA
- KRACK

MEDIDAS DE SEGURIDAD ADICIONALES

OCULTACIÓN DE SSID

Ocultar el SSID no es tanto una medida efectiva para aquellos que realmente tengan nuestra red como objetivo, sino más bien una medida para el ámbito doméstico donde el hecho de que no se vea públicamente tu WIFI puede llegar para que el "vecino" no intente hacer uso de ella. Otra buena idea para dificultarle un poco el trabajo es tanto cambiarle el nombre SSID como la contraseña por defecto.

Esto son los básicos de los básicos, pero dado que esta pequeña guía tiene como fin orientar un poco a gente de cualquier nivel, no está de más comentar también estas nociones básicas.

FILTRADO MAC

El filtrado MAC es de nuevo un sistema que añade una pequeña capa de seguridad, que es más bien una pequeña traba adicional, pues como veremos también más adelante es relativamente sencillo hacer un bypass de este filtrado.

Este se basa en que el Router/AP tenga una lista blanca de MAC's reconocidas impidiendo el acceso de cualquier otra que no esté en dicha lista.

USO DE IP'S ESTÁTICAS

El uso de IP's estáticas es otra medida que puede dificultar un poco más un ataque a nuestra red, pero que al igual que las anteriores es una medida extra de tipo ligero.

Dentro de esta sección se podría incluir también la restricción de número de IP's permitidas, pero esto no es permitido por cualquier Router, y es una medida que también se puede hacer bypass por medio de la desautenticación.

DESHABILITAR WPS

Wi-Fi Protected Setup (WPS) es una funcionalidad WIFI que como veremos más adelante trae consigo más problemas que ayudas. Es por ello que la recomendación es la de deshabilitar dicho servicio a fin de evitar posibles ataques por este lado.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Se basa en el uso de un servidor de autenticación adicional que comprueba la información mediante esquemas de autenticación como PAP, CHAP o EAP. Se usa para gestionar usuarios que obtiene de diferentes medios como puede ser archivos de texto, bases de datos, servidores LDAP, etc…

Ésta si se puede considerar una medida adicional de seguridad pues añade una capa extra de seguridad.

VPN

Virtual private network (VPN) se puede considerar una medida de seguridad adicional, aunque está más bien orientada al ámbito profesional. De esta forma toda la información viaja cifrada y aunque la WIFI se viera vulnerada nuestra información no lo estaría.

ATAQUES COMUNES A REDES WIFI

MAC SPOOFING

MAC Spoofing es una técnica mediante la cual se "engaña" al sistema operativo para que este deje de usar la dirección MAC que posee el dispositivo de red (la cual supuestamente no se puede cambiar), y use la que el usuario le asigna. Esta técnica ya venía heredada de las redes cableadas, y es la que permite tanto saltarse el filtrado MAC, como hacerse pasar por un cliente que ya esté conectado a la red, o simplemente como método adicional para anonimizar la conexión.

Realmente existen 2 direcciones MAC para la tarjeta, la que viene asignada por el fabricante, y una segunda lógica asignada por el sistema operativo. Esta segunda por defecto tendrá la misma dirección que trae por defecto la dirección física que asigna el fabricante.

En el Mac Spoofing se aprovecha que esta dirección es lógica para modificar la misma, aunque se mantenga la original guardada en la tarjeta.

PRUEBA DE CONCEPTO

Como ejemplo vamos a ver como se podría realizar este cambio dentro de Wifislax.

```
wifislax64 ~ # ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:87:24:9a:0a:99
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wifislax64 ~ # ifconfig wlan0 down
Terminado
wifislax64 ~ # macchanger -m 00:11:22:33:44:55 wlan0
Current MAC:   00:87:24:9a:0a:99 (unknown)
Permanent MAC: 00:87:24:9a:0a:99 (unknown)
New MAC:       00:11:22:33:44:55 (CIMSYS Inc)
wifislax64 ~ # ifconfig wlan0 up
Terminado
wifislax64 ~ # ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:11:22:33:44:55
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Aquí observamos cómo tras usar la aplicación macchanger sobre nuestra tarjeta inalámbrica conseguimos cambiar esa dirección lógica por otra asignada por nosotros. En el caso de recuperar el valor por defecto basta con repetir el proceso usando el valor de la Permanent MAC.

FAKE AP'S

Fake AP's es la base de muchos de los ataques sobre redes WIFI. Se basa en crear un AP con las condiciones que a nosotros nos interese. Estas serán habitualmente similares a aquella red que se quiere atacar. Dentro de esta categoría se pueden incluir gran parte de los ataques modernos y los más peligrosos hoy en día. Entre ellos vamos a citar varios ejemplos:

AP SPOOFING / SSID SPOOFING

En caso de ser una red abierta seria por ejemplo un simple SSID/AP Spoofing. Al imitar las condiciones de este cualquier cliente puede conectarse al Fake AP en vez de al que se quiere conectar.

ROGUE AP

Este caso se trata de aquellos AP que son instalados de forma ilegal en redes ajenas (estos se suelen dar más en redes empresariales) con el fin de realizar luego ataques desde otra ubicación como capturas de tráfico, robo de credenciales u otro tipo de intrusiones.

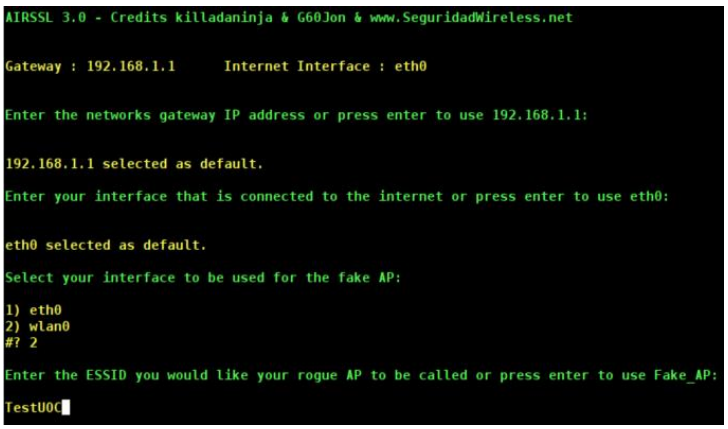
EVIL TWIN - LINSET

Evil Twin se basa en la técnica de crear un AP que parezca legítimo para incitar a los usuarios a conectarse al mismo. La idea es esperar a que el cliente se conecte al AP original. Una vez esto sucede se replica dicho AP y se sube la potencia del nuevo para que el cliente cree que este está más cerca. Después se desautentica al cliente del AP original y se espera a que este se conecte al Evil Twin. A partir de aquí de nuevo se vuelven a abrir nuevas puertas.

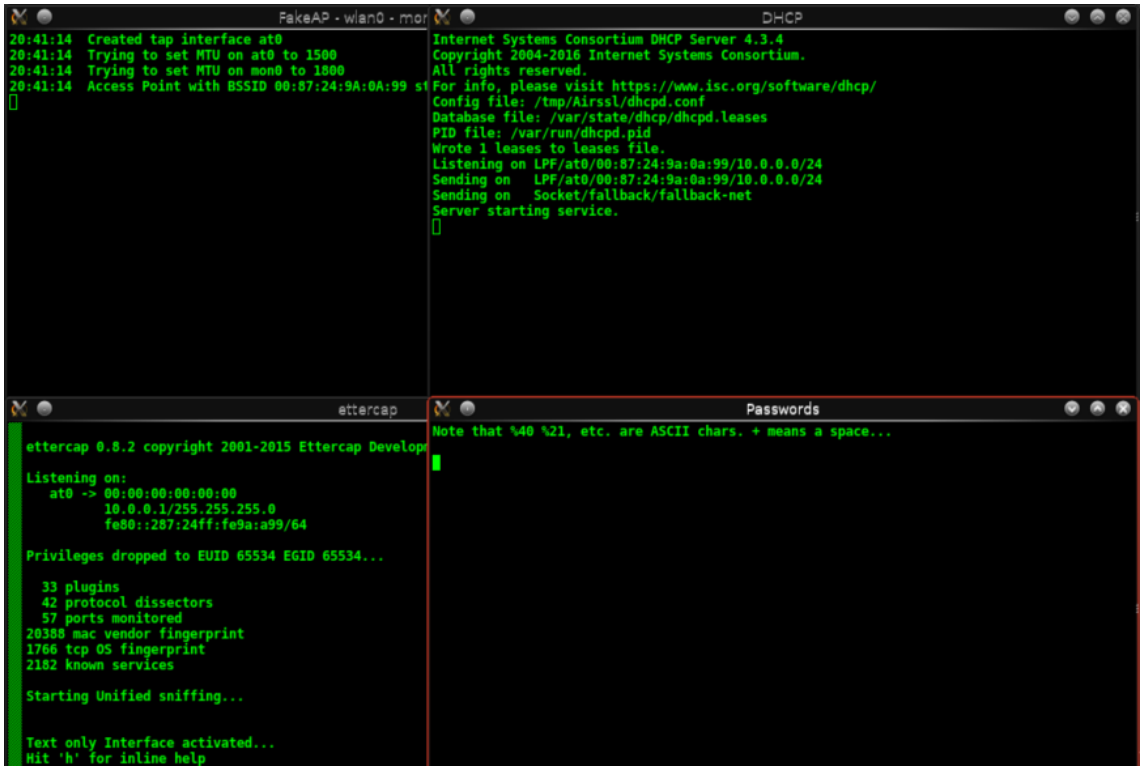
PRUEBA DE CONCEPTO

El uso de Fake AP's suele estar relacionado con ataques MitM. Como prueba de concepto montaremos un Fake AP como el que un atacante podría montar en un lugar público con la intención de captar a aquellos aficionados a las redes Wifi gratuitas.

Para llevar a cabo este ataque usamos la siguiente configuración. Conectamos nuestra maquina a la red y la máquina virtual se conecta a esta. Dentro de la máquina virtual con Wifislax usamos AirSSL para crear nuestro fake AP.



Despues de esto comprobamos que nuestro Fake AP está disponible. AirSSL nos daría directamente las siguientes opciones:



En la parte superior tenemos la información del Fake AP y del servidor DHCP. En ellos observaremos la actividad de los clientes que se conecten a nuestro FakeAP.

En la parte inferior tenemos otras 2 ventanas, ettercap y Passwords.

Ettercap es una aplicación orientada a los ataques MitM que nos permite capturar el tráfico de los clientes conectados a nuestro Fake AP.

La segunda ventana nos da un resumen de las contraseñas que es capaz de identificar automáticamente dentro del tráfico de los clientes.

En el caso de querer realizar un ataque Evil Twin - Linset deberíamos realizar además algunos pasos extra:

- Crear una web que simule una página de login y la base de datos correspondiente donde almacenar los intentos realizados y las credenciales.
- Clonar la MAC y el nombre del AP objetivo y usar esos datos para crear el Fake AP.
- Modificar iptables para que todas las conexiones pasen primero por nuestra web.
- Desautenticar los clientes conectados al AP con la ayuda de aireplay.
- Esperar que estos tengan activa la opción de conectarse a redes abiertas a su alcance.
- Usar los datos introducidos por los clientes en el AP original para confirmar que son válidos.
- Una vez validada la contraseña se desactiva el ataque.

MAN-IN-THE-MIDDLE

MitM, conocido como ataque de intermediario es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. Este tipo de ataques son especialmente sencillos de realizar por medio de un FakeAP simulando una red Wifi Pública Abierta. Es por ello que las redes abiertas son especialmente peligrosas si sobre ellas se tratan datos privados.

Con el último ataque sobre WPA2, KRACK, esto se vuelve posible de nuevo.

PRUEBA DE CONCEPTO

Para el caso de los ataques MitM basta con crear un Fake AP para después capturar el tráfico que corre a través del mismo, en este caso podemos replicar el ataque que ya propusimos aquí. Una vez en este punto tanto ettercap como Wireshark pueden ser nuestros aliados.

WIPHISHING

Este, a modo de opinión personal, es uno de los más peligrosos cuando es enfocado a los usuarios con menos pericia. Su nombre viene derivado de WIFI y Phishing (suplantación de identidad). Es especialmente efectivo cuando es realizado en redes abiertas como la de los aeropuertos o centros comerciales. La idea es montar un simple AP que puede estar redirigido a la red original o cualquier otra, pero que sirve como punto de ataque MitM. Una vez dentro se puede esnifar el tráfico de los clientes, o incluso para acelerar el proceso, crear sitios de Phishing simulados como de cuentas de correo y bancos y redirigir los clientes a estas de forma que estos te entreguen las credenciales directamente.

PRUEBA DE CONCEPTO

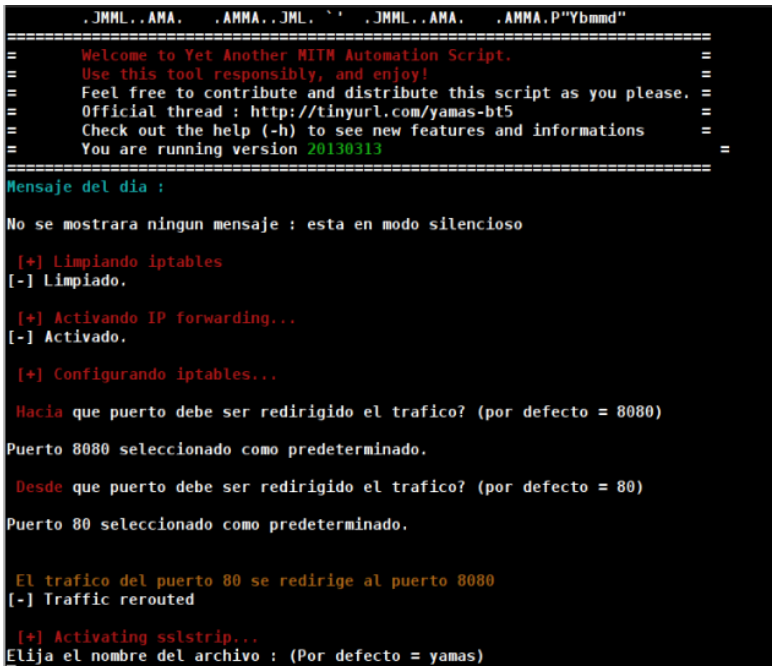
Para el caso del Wiphising basta con crear un Fake AP que incite a los usuarios a conectarse a ti, como los usados para ofrecer internet de forma gratuita en lugares públicos, para después capturar el tráfico que corre a través del mismo, en este caso podemos replicar el ataque que ya propusimos aquí.

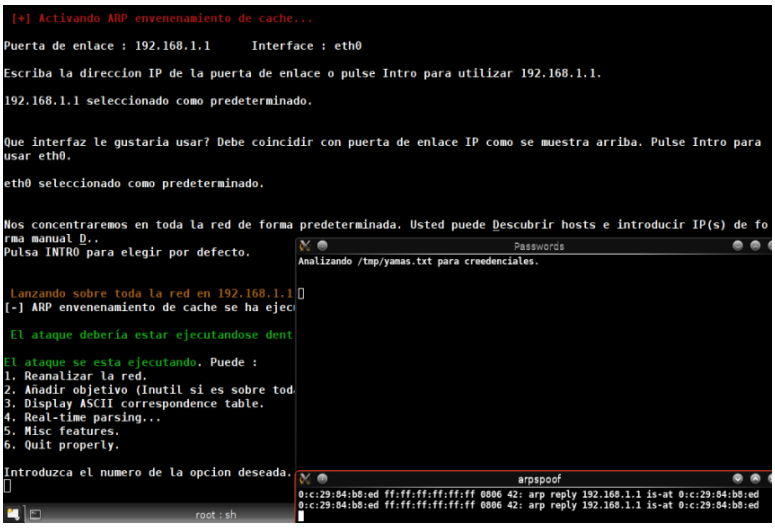
ARP SPOOFING

ARP Spoofing es un ataque basado en enviar mensajes ARP falsificados con la intención de asociar la MAC atacante a una IP de otro nodo de la red. Si se hace con éxito por ejemplo sobre la puerta de enlace predeterminada eso provocaría que el tráfico orientado a esta pasara por el equipo del atacante. A partir de aquí se pueden optar por distintos ataques, como ataques DoS, inyección de tráfico o simplemente redirigirlo al tiempo que se mantiene a la escucha (MitM). La pega en este caso es que para llevarlo a cabo es necesario estar previamente conectados a dicha red por medio del propio equipo o por otro equipo infectado previamente.

PRUEBA DE CONCEPTO

Para este tipo de ataque nos apoyamos en el script Yamas incluido dentro de Wifislax que ya automatiza el proceso del envenenamiento ARP.





SESSION HIJACKING

En este caso nos encontramos ante una mezcla de ataques que busca acceder a las cuentas de la víctima sin la necesidad de tener las credenciales de la misma. Para ello se empieza por un ataque de envenenamiento de ARP para hacer que el tráfico del objetivo pase por nuestro equipo. Una vez en este punto se empieza a Snifar el mismo con el fin de capturar las Cookies de sesión. Por último, solo queda abrir un navegador que te permita editar las cookies como puede ser el Firefox, acceder al sitio del que hemos capturado la cookie y editar la nuestra para pegar la cookie robada. Una vez que se vuelve a la página pasamos a estar logeados con la cuenta del objetivo.

PRUEBA DE CONCEPTO

La idea sería aprovechar el anterior ataque ARP Spoofing para secuestrar cookies de sesión de los clientes que pasan por nuestro "AP" y rehusarlas en un navegador que te permita editar Coolies. Se puede también acelerar este proceso mediante herramientas como "Fern Wifi Cracker" que ayuda en el proceso de secuestro de cookies de sesión.

FUERZA BRUTA

Estos ataques son realizados especialmente contra redes WEP y WPA en los que las claves son de menor tamaño y la operación es asumible. Se realizan probando por fuerza bruta con diccionarios ya predefinidos o por fuerza bruta probando todas las combinaciones posibles. Lo único necesario es capturar un Handshake de un cliente para poder llevar a cabo el ataque.

Las aplicaciones más modernas hacen uso incluso de las GPU para no hacer uso de ningún diccionario y multiplicar el número de claves que se pueden probar por segundo.

PRUEBA DE CONCEPTO

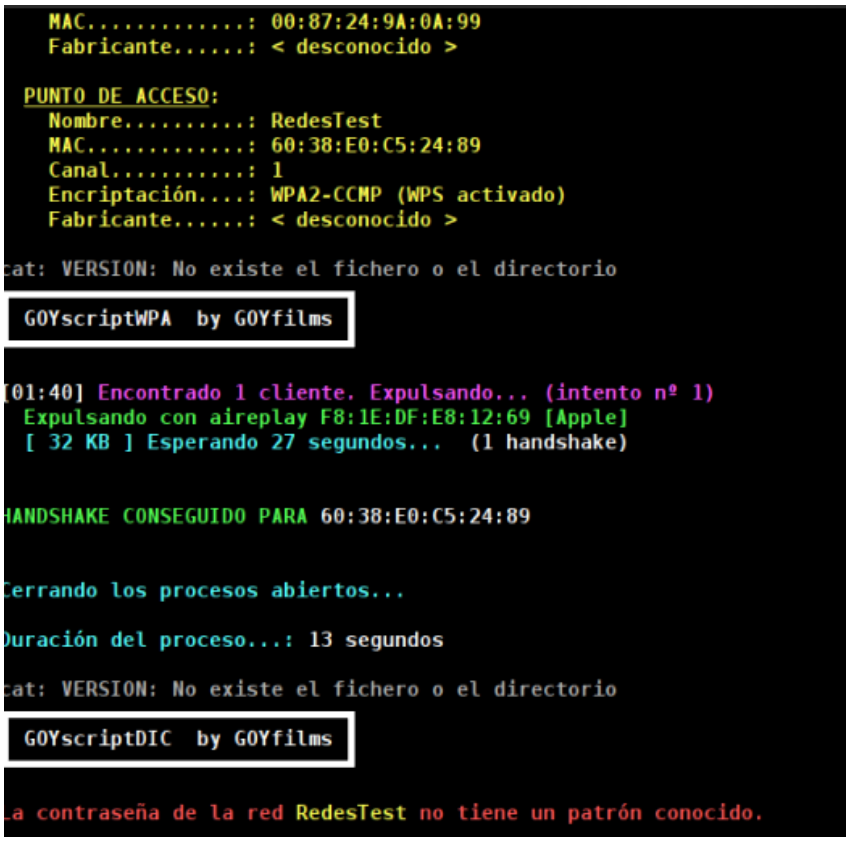
Este proceso se suele usar de forma un poco más manual y la idea es la de probar combinaciones mediante el uso de diccionarios, o incluso probando todas las combinaciones posibles (si por la vía de los diccionarios no se obtiene éxito). El objetivo inicial es capturar el handshake entre el cliente y el AP, para lo cual es necesario tener al menos 1 cliente conectado. En nuestro caso nos apoyamos en Goyscript para automatizar el proceso.

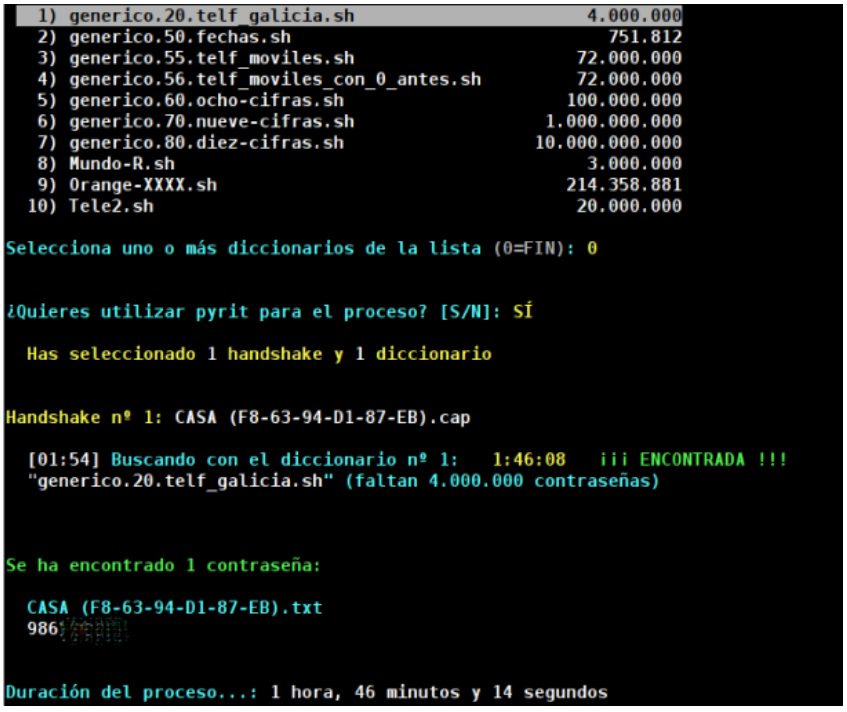
Despues usamos la herramienta aircrack-ng de la siguiente forma:

aircrack-ng ruta-handshake –w ruta-diccionario

Con esto aircrack probara todas las contraseñas del diccionario con la información del handshake. Para optimizar el proceso se podría apoyar uno en la herramienta hashcat mediante el uso de GPU, pero ante contraseñas de gran tamaño sigue siendo un proceso que requiere de mucho tiempo. Una GPU actual es capaz de probar del orden de 180.000 claves por segundo.

En nuestra máquina virtual la experiencia es que es capaz de probar 1000 claves por segundo lo que nos deja en una hora para una clave de 9 numeros que usamos como Test, y probando un diccionario con solo 4 millones de claves con la herramienta Pyrit bajo el script Goyscript DIC.





DENIAL OF SERVICE (DOS)

Cuando el atacante más allá de robar información lo que quiere es “anular” una red es cuando se suelen llevar acabo los ataques DoS. Para ello se conectan a la res y se realizan cientos de ataques de desautenticación por segundo, lo que acaba por dejar la red WIFI inaccesible y, en muchos casos, también la cableada (depende de la configuración de estas).

PRUEBA DE CONCEPTO

El ataque como se ha explicado se basa en desautenticar a 1 o todos los clientes de forma infinita. Para ello usamos la herramienta aireplay-ng con una llamada como la siguiente:

aireplay-ng -0 0 -a MAC-AP mon0

Otra opción sería desautenticar a un cliente especifico mediante:

aireplay-ng -0 0 -a MAC-AP -c MAC-CLIENT mon0

ATAQUE POR WPS

Este tipo de ataques no se centran en la seguridad propia de la red WIFI, sino más bien en una funcionalidad más moderna que incluyen algunos fabricantes que es el Wi-Fi Protected Setup (WPS), la cual está pensada para facilitar la configuración de red a los usuarios.

El ataque no es otro que usar la fuerza bruta para romper dicha funcionalidad, la cual se basa en una única clave numérica o PIN de 8 dígitos, bastante más fácil de romper que una clave WPA2 que además de ser de longitud variable permite una mayor longitud y un mayor juego de caracteres.

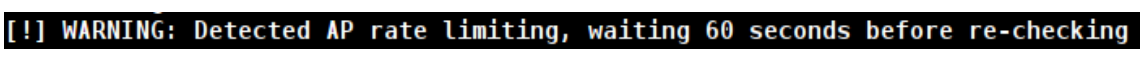
El objetivo final no es otro que el de obtener la clave pre-compartida de la red WPA/WPA2.

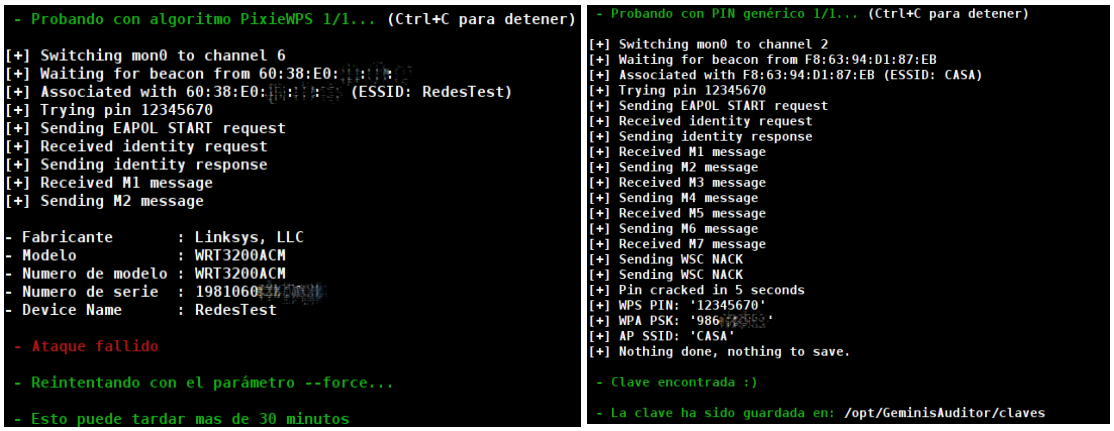
Aunque algunos Routers equipan medidas de protección contra este tipo de ataque lo ideal es desactivar dicha funcionalidad del mismo.

PRUEBA DE CONCEPTO

En este caso nos podemos apoyar en diversas herramientas como son Reaver, GoyScript WPS o Geminis Auditor. Como ejemplo diversos casos de ataques a WPS:

En el caso del Router utilizado en el laboratorio de pruebas, debido a ser de última generación ya viene con cierta protección contra ataques WPS. Como podemos ver en las capturas rápidamente nos encontramos con un problema con el número de intentos.





A la izquierda la prueba con el Router del laboratorio que ya nos deja prever que la espera va a ser muy larga para conseguir un ataque de éxito. A la derecha el que nos ofrece el proveedor, que demuestra como en los inicios del protocolo WPS este estaba implementado de una forma muy básica y con claves PIN por defecto que hace que este caiga en cuestión de 5 segundos.

Como último ejemplo tenemos un Router también de un proveedor de servicios, pero en este caso de una generación posterior. Este no viene con un pin establecido por defecto, pero tampoco implementa ninguna medida de seguridad adicional. Esto implica que en menos de 15 horas y a pesar de trabajar desde una Máquina Virtual con pocos recursos el ataque sea un éxito.

Es por ello que la recomendación pasa por tener desactivado siempre el WPS, pues en el peor de los casos es cuestión de tiempo tener éxito y en menor tiempo que atacando el propio protocolo WPA2.

KRACK

Key Reinstallation Attacks (KRACK), es el último ataque conocido sobre WPA2.

El ataque permite leer información de cualquier red WIFI moderna y, depende de la configuración de esta, puede permitir también inyectar y manipula la información que por esta circula. Lo que abre puertas a la inyección de malware o ramsonware por medio de esta técnica.

El ataque está basado en una serie de vulnerabilidades existentes en el estándar WIFI localizadas por el mismo grupo de investigación. Casi cualquier dispositivo con WIFI está afectado, y se recomienda actualizarlos lo antes posible (si estos disponen de alguna actualización, lo cual es más difícil con equipos más antiguos). Especialmente afectados se ven los equipos Linux y Android 6.0 o superior.

El principal ataque de KRACK es contra el handshake de 4 vías usado en el protocolo WPA2 para autenticar un cliente la primera vez que se conecta. Al mismo tiempo se negocia también la clave de encriptación que se usara de ahí en adelante.

Cuando no hay confirmación de que se recibe la clave de encriptación el AP envía de nuevo la clave y se reseta el contador de paquetes. Esto es lo que usa KRACK, forzando este reset a base de enviar repetidamente el mensaje 3 del handshake de 4 vías, el cual contiene la clave de encriptación. De esta forma es como ataca el protocolo de encriptación pudiendo repetir paquetes, desencriptarlos o inyectar nuevos a medida.

PRUEBA DE CONCEPTO

Debido a la reciente aparición de las vulnerabilidades que ataca KRACK no ha sido posible reproducirlo en tan poco tiempo en nuestro laboratorio. A pesar de esto el propio Mathy Vanhoef, autor de dicho ataque, ha subido una demostración a youtube sobre el ataque basado en su propio paper. Esta puede encontrarse aquí: https://www.youtube.com/watch?v=Oh4WURZoR98

CONCLUSIONES

Tras la investigación realizada y tras las últimas vulnerabilidades detectadas se podría llegar a la conclusión de que la red WiFi más segura es aquella que esta desactivada, con ciertas excepciones, pero vamos a comentar las diferencias.

Tener una red con seguridad WEP es casi como tenerla sin seguridad, ya que la dificultad para saltarse dicha seguridad es casi nula hoy en día.

En cuanto a las redes WPA y WPA2, aplicando las mayores medidas de seguridad, hay diferencias entre el antes y el después de las nuevas vulnerabilidades encontradas con KRACK. Antes de dichas vulnerabilidades, y si la red aplicaba las medidas correctas de seguridad, la dificultad en cuanto a computación era tal que compensaba atacar al usuario antes que al AP. Esto se realizaba con ataques de ingeniera social mediante el uso de Fake AP's o mediante el peligroso Wiphishing.

También cabe destacar la importancia de desactivar el WPS, especialmente en los routers que entregan los proveedores de servicios, pues es un vector de ataque que puede volverse extremadamente efectivo.

Actualmente, y a falta de desarrollar un poco más las nuevas vulnerabilidades de KRACK, la seguridad tanto de WPA como de WPA2 se reduce de forma notable hasta el punto de dejar de ser seguras. Esto es debido a que una vez el ataque sea exitoso el tráfico dentro de la misma es vulnerable.

De esto deducimos que la forma más segura actualmente de usar redes inalámbricas seria mediante el uso de redes VPN para minimizar el impacto de KRACK haciendo que todo el tráfico dentro de la misma vaya cifrado.

La solución ante KRACK pasa por actualizar AP's y dispositivos, si estos disponen de actualización de software para corregir las citadas vulnerabilidades o, de no ser así, cambiar dichos AP's por unos que si dispongan de parche de seguridad.

El mayor problema nos lo encontramos en los dispositivos IoT. Gran parte de los dispositivos hoy en día usan credenciales por defecto que no te obligan ni te aconsejan cambiar. Además, no cifran las comunicaciones ni suelen incluir opciones de seguridad. Por último, tanto las webs de control como de configuración no suelen ser las más seguras por lo que estos equipos son especialmente vulnerables ante diferentes tipos de ataques, entre los que destaca la infección por malware que acaba usando dichos dispositivos como botnets para otros ataques o como mineros de criptomonedas.

GLOSARIO

- AES: Advanced Encryption Standard
- AP: Access Point
- ARP: Address Resolution Protocol
- CRC: Cyclic Redundancy Code
- DoS: Denial of Service
- EAP: Extensible Authentication Protocol
- FMS: Fluhrer, Mantin and Shamir
- GPU: Graphics Processing Unit
- ICV: Integrity Check Value
- IoT: Internet of Things
- IP: Internet Protocol
- IV: Vector de Inicialización
- KRACK: Key Reinstallation Attacks
- MAC: Media Access Control
- MIC: Message Integrity Code
- MitM: Man-in-the-Middle
- OSA: Open System Authentication
- PEAP: Protected Extensible Authentication Protocol
- PRGA: Pseudo Random Generation Algorithm
- RADIUS: Remote Authentication Dial-In User Service
- RC4: Ron's Cipher 4
- RSN: Robust Security Network
- SKA: Shared Key Authentication
- SSID: Service Set Identifier
- TFM: Trabajo Fin de Master
- TKIP: Temporal Key Integrity Protocol
- VPN: Virtual Private Network
- WEP: Wired Equivalent Privacy
- WIFI: Sustantivo procedente de la marca Wi-Fi
- WLAN: Wireless Local Area Network
- WPA: Wi-Fi Protected Access
- WPS: Wi-Fi Protected Setup

BIBLIOGRAFÍA

ARTÍCULOS

[1] G. Lehembre, “Seguridad Wi-Fi – WEP, WPA y WPA2”. Revista hakin9, enero de 2006.

[2] H. Krawczyk, M. Bellare, R. Canetti, “HMAC: Keyed-hashing for message authentication”, febrero de 1997.

[3] Mathy Vanhoef and Frank Piessens. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS). ACM.

PÁGINAS WEB

[4] https://www.krackattacks.com/

[5] https://blog.mojonetworks.com/wpa2-vulnerability

[6] https://www.aircrack-ng.org/doku.php