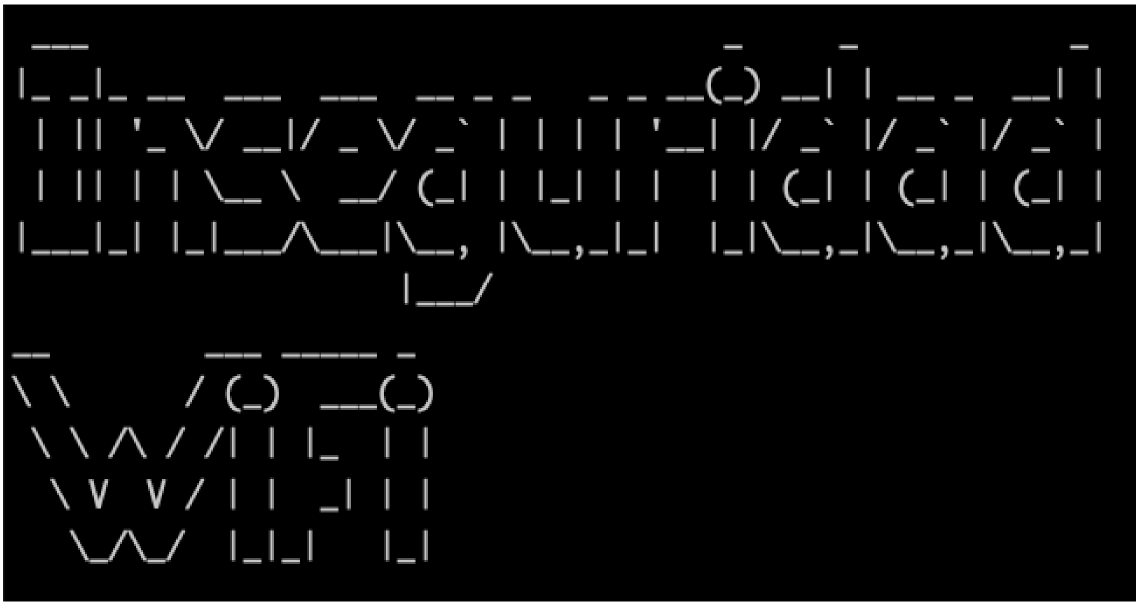


Inseguridad WiFi.

TFM-SO. Campus Internacional de Ciberseguridad.

Lucas Portolés de Val - 2021

INDICE

1- INTRODUCCIÓN.

1.1 Resumen.

Una red informática es la conexión entre diferentes dispositivos o redes que puedan operar de manera organizada. Desde la creación de la informática, el acceso autorizado a una red es una de las principales preocupaciones de la ciberseguridad. La mundialmente conocida tecnología WiFi, ha popularizado el acceso a redes a través del AP inalámbrico, pero curiosamente, es uno de los grandes olvidados en muchas estructuras domésticas y empresariales, a pesar de ser vector de acceso de una gran cantidad de vulnerabilidades conocidas y habitualmente bajo un pobre e insuficientemente gestionado, trabajo de actualización y configuración. Este trabajo investigará la situación actual en las redes con tecnología WiFi y los posibles vectores vulnerables, desde el prisma de la ciberseguridad, y ejemplificará una pequeña parte de lo que puede suceder y sucede, de manera práctica.

1.2 Abstract.

Network is a connection between different devices or networks that can operate in an organized way. Since the creation of computing, authorized access to a network has been one of the main concerns of cybersecurity. The well known, WiFi technology, has popularized access to networks through the wireless AP, but surprisingly, it is one of the great forgotten in many domestic and business structures, despite is an access vector of a large number of worldwide known vulnerabilities, and with an update work, usually insufficiently managed. This work will deep into the current situation of WiFi networks and the possible scenarios, from the prism of cybersecurity and will exemplify a small part of what can happen in a practical way.

1.3 Objetivos.

En este trabajo nos centraremos en tres macrobjetivos principales:

- Mostrar el panorama actual de las redes que utilizan la tecnología WiFi y las herramientas destinadas a auditarlas.
- Programar una herramienta pedagógica interactiva, que enseñe de manera práctica, cómo detectar contraseñas débiles, llevando a cabo una auditoría sobre conexiones WiFi reales.
- Y, por último, teorizar sobre la debilidad de la IP pública como prueba en un proceso judicial, mostrando cómo de manera no autorizada, una IP podría quedar incriminada en una acción ilegal, sin ser responsable de ella en absoluto.

1.4 Motivación.

Motivos que me impulsan a realizar este trabajo de fin de máster:
En primer lugar, como comentaba Chema Alonso en una entrevista dirigida por Juanjo Salvador, dentro del mundo de la ciberseguridad, aunque hay que saber un poco de todo, hay que tratar de especializarse en algún campo. Y dentro de esas especializaciones que deseo desarrollar, una de las que más me interesa es la auditoría Wireless, y más concretamente la auditoría WiFi.
Orientado a ello, y para complementar los conocimientos de seguridad ofensiva en redes, adquiridos en el presente máster de seguridad ofensiva, he llevado a término también, un pequeño curso de *Hacking WiFi* con S4vitar. Ambas vías me han aportado una excelente formación de seguridad en redes, aunque aún me quede mucho camino por recorrer, y mucha información de cara a este trabajo académico.

En segundo lugar, poner en práctica habilidades y conocimientos adquiridos en este máster de Ciberseguridad Ofensiva (Campus Internacional de Ciberseguridad).

Y, por último, devaluar el alcance judicial de la IP pública en los análisis forenses, valiéndome de sencillas técnicas de seguridad ofensiva. Ya que, a mi parecer, sí que debería tratarse como un indicio en un juicio pero nunca debería considerarse como una prueba, pues no es un elemento probatorio seguro. Aunque al momento actual es fácil encontrar bastante confusión y contradicción en estamentos judiciales a este respecto, encontrando sentencias que la enmarcan en ambos tipos.

1.5 Notas Previas.

(Nota) **-** Si bien en realidad, el término WiFi es únicamente una marca registrada que implementa el estándar 802.11, que es la forma más apropiada de llamar a esta tecnología inalámbrica, y no es exactamente un tipo de red ni un tipo de servicio, popularmente es conocida como red WiFi y por tanto en este trabajo en ocasiones nos tomaremos la licencia de referiremos a ella como tal.

(Nota) **–** Para esta investigación utilizaremos diversas utilidades de software, pero la más destacable es el sistema operativo Kali Linux desplegado en una virtualización de Virtual Box. Estuve dudando si utilizar Wifislax, porque si bien tiene muchas herramientas obsoletas y abandonadas, algunas de ellas sólo se encuentran allí, sin embargo, las más relevantes ya estaban en Kali y preferí prevenir posibles complicaciones.
(Nota) **–** A nivel hardware, hemos adquirido en Amazon por 9,66€, una tarjeta de red TP-Link TL-WN722N, con una velocidad de 150 Mbps.

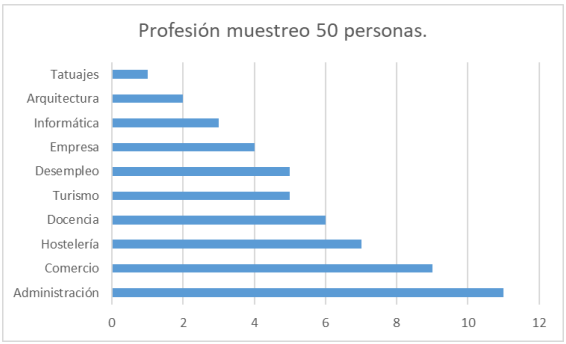
2 ESTADO DEL ARTE.

No es objetivo de este trabajo tratar todos los procesos que suceden en las redes inalámbricas con tecnología WiFi, ni en las herramientas destinadas a las auditorías inalámbricas, por tanto, trataremos de ceñirnos a los aspectos más útiles relacionados con el objeto de este estudio.

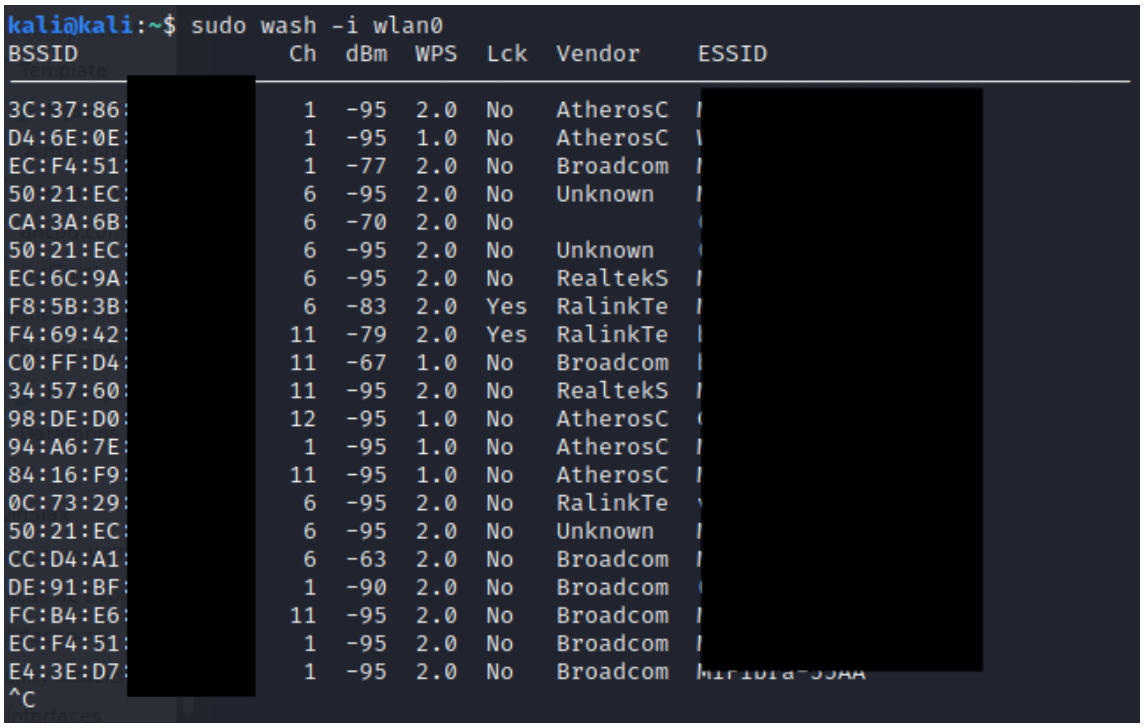
2.1 ¿Son vulnerables las Redes WiFi?

La fortaleza bajo el prisma de la seguridad en las redes WiFi, al momento de redactar este documento es bastante dispar, pero en líneas generales, a la vista está que suelen ser reseñablemente inseguras y no sólo en redes domésticas.

Tras un muestreo de 50 personas diferentes (vecinos, negocios con WiFi pública, profesionales, incluso profesionales de entidades financieras) 48 ignoraban que hay que actualizar los software de los router, como cualquier otro dispositivo, y los 2 restantes que sí lo sabían, no lo habían hecho nunca en los que estaban a su alcance. 46 de las personas a las que el autor de este muestreo ha preguntado dan poca o nula importancia a la seguridad en sus redes inalámbricas de estándar 802.11 y a veces simplemente ignoran los protocolos de seguridad más básicos y cómo se ha de actuar.

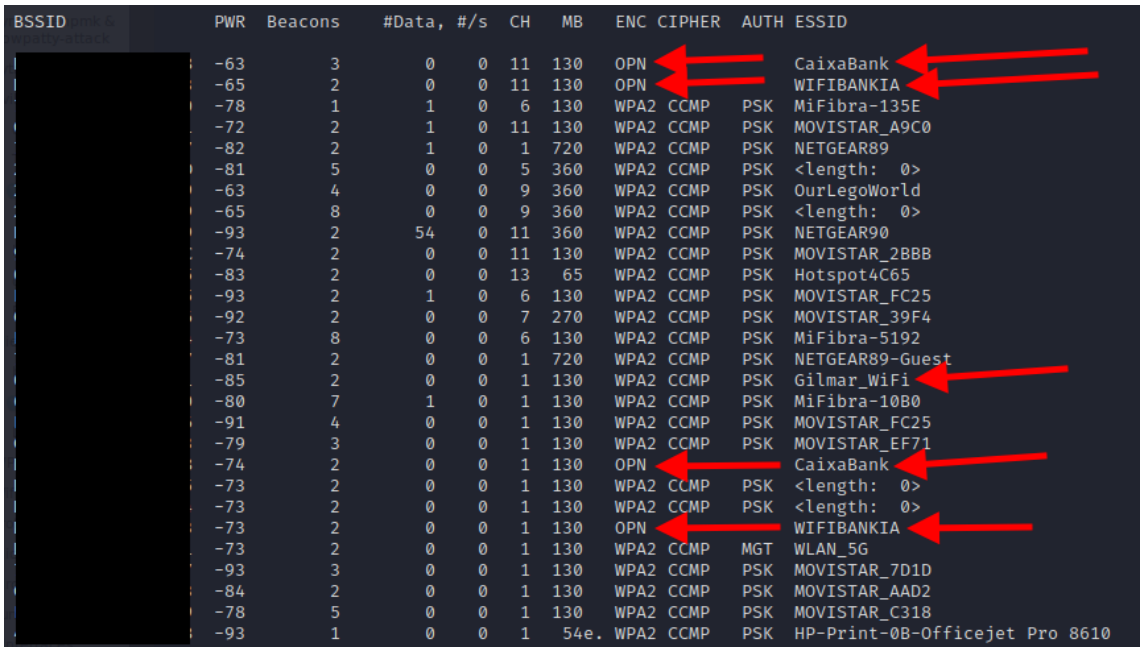


En la siguiente imagen podemos comprobar algunas debilidades en entornos domésticos en un área cercana a mi lugar de residencia. Aunque sobre estos términos hablaremos más tarde, adelantar que el PIN WPS está activo en muchas de ellas. Además, varios AP ni siquiera están actualizados a la versión 2.0 de WPS permitiendo probablemente un sencillo ataque Pixie Dust para obtener su contraseña de acceso. Y se permite identificar fácilmente por el nombre, routers de operadores como MOVISTAR u ORANGE, lo que acota los modelos y versiones a los que suelen utilizar estas compañías y al fabricante. La mayoría de estas marcas solían permitir peticiones de conexión ilimitadas durante años y seguramente podríamos probar con facilidad que muchos de estos dispositivos aún lo hacen, no obstante, no lo vamos a hacer porque sería ilegal.



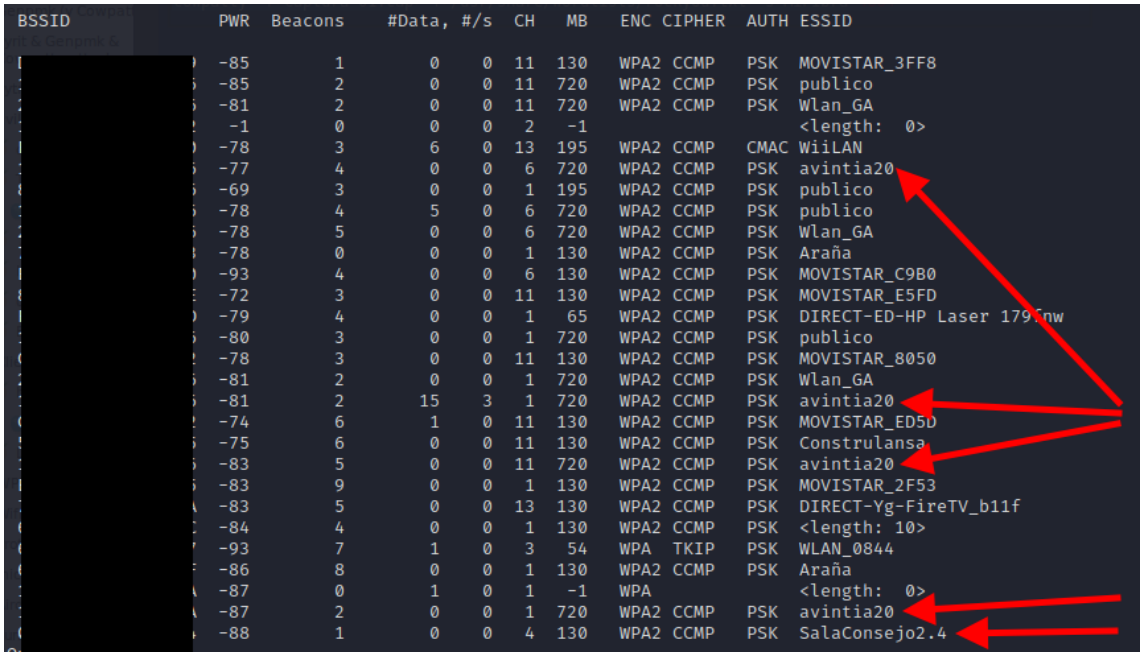
Todos estos usuarios, probablemente ignoran (aunque me consta que al menos dos de los que aparecen en estas listas son expertos programadores) que estar dentro de una red es saltar la que suele ser la principal protección de este tipo de arquitecturas, la puerta de enlace. Ni siquiera en muchas de las redes profesionales se acostumbra a tener firewalls internos y es muy habitual que sólo se cree un bastionado perimetral de seguridad. Y digamos que una vez accedido al interior, todas las medidas de seguridad habilitadas en las líneas externas, son inútiles y si existen equipos vulnerables, podría ser trivial comprometerlos.

En las siguientes imágenes, escaneadas en la calle (como se escanea habitualmente con un smartphone común en busca de redes) podemos encontrar cómo se ofrece una información desmesurada en el essid o nombre y cómo aún existen multitud de redes abiertas, con las consecuencias que pueden acarrear como está ampliamente demostrado a día de hoy.



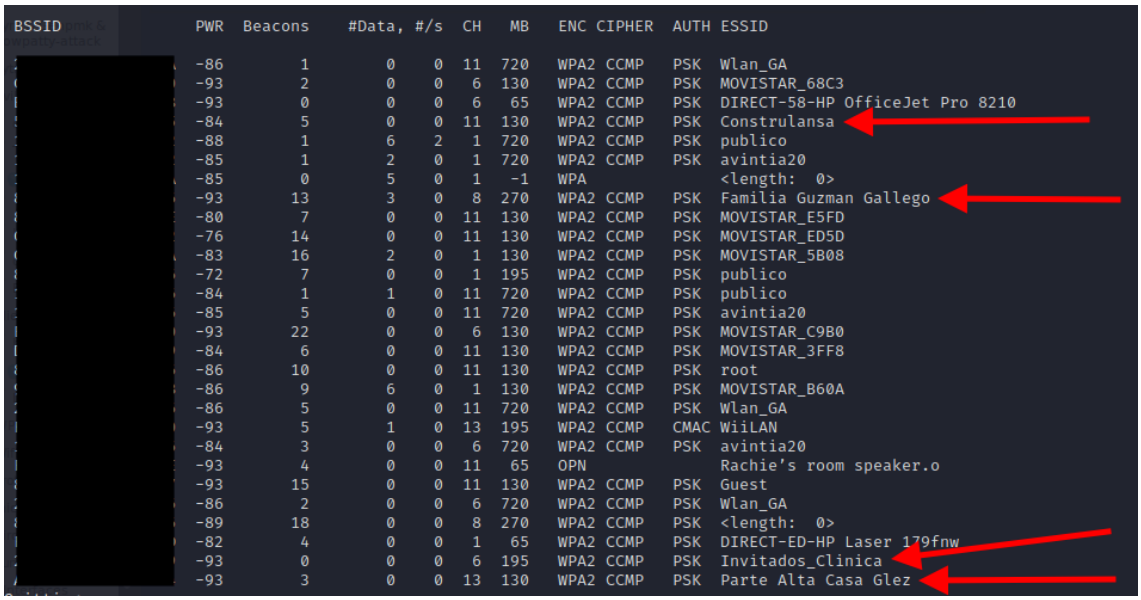
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[redacted]	-63	3	0	0	11	130	OPN			CaixaBank
[redacted]	-65	2	0	0	11	130	OPN			WIFIBANKIA
[redacted]	-78	1	1	0	6	130	WPA2	CCMP	PSK	MiFibra-135E
[redacted]	-72	2	1	0	11	130	WPA2	CCMP	PSK	MOVISTAR_A9C0
[redacted]	-82	2	1	0	1	720	WPA2	CCMP	PSK	NETGEAR89
[redacted]	-81	5	0	0	5	360	WPA2	CCMP	PSK	<length: 0>
[redacted]	-63	4	0	0	9	360	WPA2	CCMP	PSK	OurLegoWorld
[redacted]	-65	8	0	0	9	360	WPA2	CCMP	PSK	<length: 0>
[redacted]	-93	2	54	0	11	360	WPA2	CCMP	PSK	NETGEAR90
[redacted]	-74	2	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_2BBB
[redacted]	-83	2	0	0	13	65	WPA2	CCMP	PSK	Hotspot4C65
[redacted]	-93	2	1	0	6	130	WPA2	CCMP	PSK	MOVISTAR_FC25
[redacted]	-92	2	0	0	7	270	WPA2	CCMP	PSK	MOVISTAR_39F4
[redacted]	-73	8	0	0	6	130	WPA2	CCMP	PSK	MiFibra-5192
[redacted]	-81	2	0	0	1	720	WPA2	CCMP	PSK	NETGEAR89-Guest
[redacted]	-85	2	0	0	1	130	WPA2	CCMP	PSK	Gilmar_WiFi
[redacted]	-80	7	1	0	1	130	WPA2	CCMP	PSK	MiFibra-10B0
[redacted]	-91	4	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_FC25
[redacted]	-79	3	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_EF71
[redacted]	-74	2	0	0	1	130	OPN			CaixaBank
[redacted]	-73	2	0	0	1	130	WPA2	CCMP	PSK	<length: 0>
[redacted]	-73	2	0	0	1	130	WPA2	CCMP	PSK	<length: 0>
[redacted]	-73	2	0	0	1	130	OPN			WIFIBANKIA
[redacted]	-73	2	0	0	1	130	WPA2	CCMP	MGT	WLAN_5G
[redacted]	-93	3	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_7D1D
[redacted]	-84	2	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_AAD2
[redacted]	-78	5	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_C318
[redacted]	-93	1	0	0	1	54e.	WPA2	CCMP	PSK	HP-Print-0B-Officejet Pro 8610

Entidades financieras y AP que definen su operador.



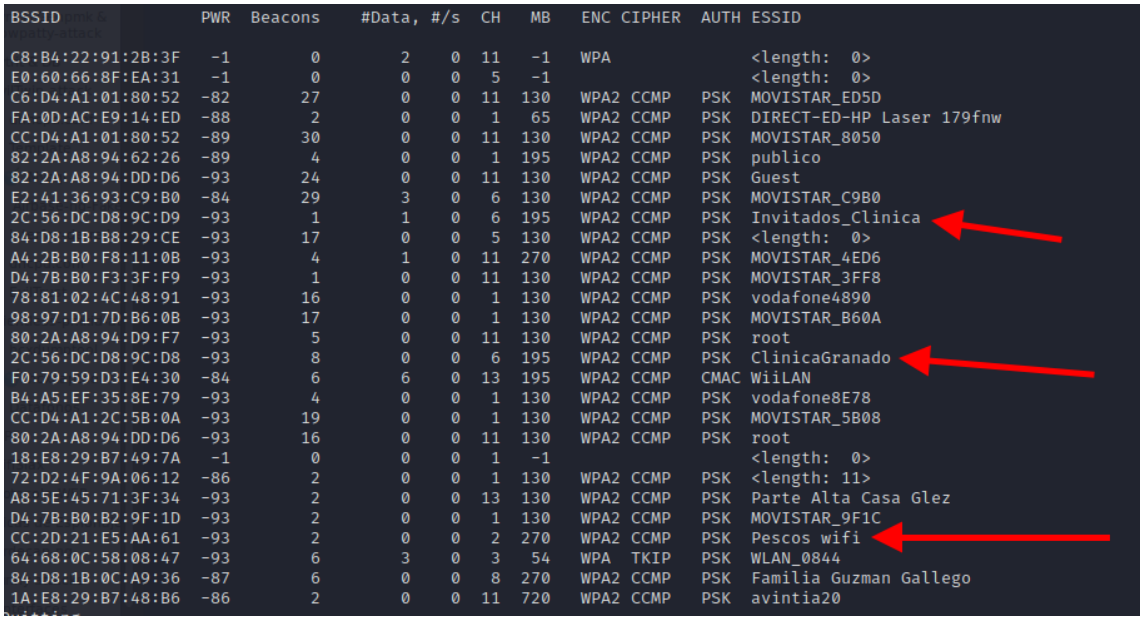
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[redacted]	-85	1	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_3FF8
[redacted]	-85	2	0	0	11	720	WPA2	CCMP	PSK	publico
[redacted]	-81	2	0	0	11	720	WPA2	CCMP	PSK	Wlan_GA
[redacted]	-1	0	0	0	2	-1				<length: 0>
[redacted]	-78	3	6	0	13	195	WPA2	CCMP	CMAC	WiiLAN
[redacted]	-77	4	0	0	6	720	WPA2	CCMP	PSK	avintia20
[redacted]	-69	3	0	0	1	195	WPA2	CCMP	PSK	publico
[redacted]	-78	4	5	0	6	720	WPA2	CCMP	PSK	publico
[redacted]	-78	5	0	0	6	720	WPA2	CCMP	PSK	Wlan_GA
[redacted]	-78	0	0	0	1	130	WPA2	CCMP	PSK	Araña
[redacted]	-93	4	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_C9B0
[redacted]	-72	3	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_E5FD
[redacted]	-79	4	0	0	1	65	WPA2	CCMP	PSK	DIRECT-ED-HP Laser 179[redacted]nw
[redacted]	-80	3	0	0	1	720	WPA2	CCMP	PSK	publico
[redacted]	-78	3	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_8050
[redacted]	-81	2	0	0	1	720	WPA2	CCMP	PSK	Wlan_GA
[redacted]	-81	2	15	3	1	720	WPA2	CCMP	PSK	avintia20
[redacted]	-74	6	1	0	11	130	WPA2	CCMP	PSK	MOVISTAR_ED5D
[redacted]	-75	6	0	0	11	130	WPA2	CCMP	PSK	Construlansa
[redacted]	-83	5	0	0	11	720	WPA2	CCMP	PSK	avintia20
[redacted]	-83	9	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_2F53
[redacted]	-83	5	0	0	13	130	WPA2	CCMP	PSK	DIRECT-Yg-FireTV_b11f
[redacted]	-84	4	0	0	1	130	WPA2	CCMP	PSK	<length: 10>
[redacted]	-93	7	1	0	3	54	WPA	TKIP	PSK	WLAN_0844
[redacted]	-86	8	0	0	1	130	WPA2	CCMP	PSK	Araña
[redacted]	-87	0	1	0	1	-1	WPA			<length: 0>
[redacted]	-87	2	0	0	1	720	WPA2	CCMP	PSK	avintia20
[redacted]	-88	1	0	0	4	130	WPA2	CCMP	PSK	SalaConsejo2.4

Conocida empresa que probablemente, incluso etiqueta su consejo de administración.



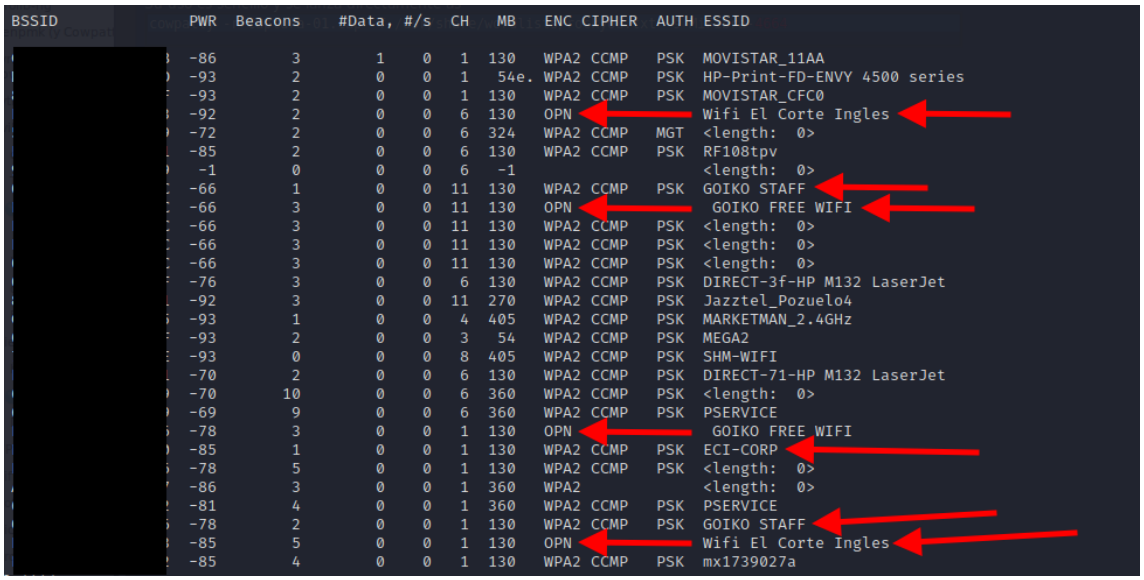
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[redacted]	-86	1	0	0	11	720	WPA2	CCMP	PSK	Wlan_GA
[redacted]	-93	2	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_68C3
[redacted]	-93	0	0	0	6	65	WPA2	CCMP	PSK	DIRECT-58-HP OfficeJet Pro 8210
[redacted]	-84	5	0	0	11	130	WPA2	CCMP	PSK	Construlansa
[redacted]	-88	1	6	2	1	720	WPA2	CCMP	PSK	publico
[redacted]	-85	1	2	0	1	720	WPA2	CCMP	PSK	avintia20
[redacted]	-85	0	5	0	1	-1	WPA			<length: 0>
[redacted]	-93	13	3	0	8	270	WPA2	CCMP	PSK	Familia Guzman Gallego
[redacted]	-80	7	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_E5FD
[redacted]	-76	14	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_ED5D
[redacted]	-83	16	2	0	1	130	WPA2	CCMP	PSK	MOVISTAR_5B08
[redacted]	-72	7	0	0	1	195	WPA2	CCMP	PSK	publico
[redacted]	-84	1	1	0	11	720	WPA2	CCMP	PSK	publico
[redacted]	-85	5	0	0	11	720	WPA2	CCMP	PSK	avintia20
[redacted]	-93	22	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_C9B0
[redacted]	-84	6	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_3FF8
[redacted]	-86	10	0	0	11	130	WPA2	CCMP	PSK	root
[redacted]	-86	9	6	0	1	130	WPA2	CCMP	PSK	MOVISTAR_B60A
[redacted]	-86	5	0	0	11	720	WPA2	CCMP	PSK	Wlan_GA
[redacted]	-93	5	1	0	13	195	WPA2	CCMP	CMAC	WiiLAN
[redacted]	-84	3	0	0	6	720	WPA2	CCMP	PSK	avintia20
[redacted]	-93	4	0	0	11	65	OPN			Rachie's room speaker.o
[redacted]	-93	15	0	0	11	130	WPA2	CCMP	PSK	Guest
[redacted]	-86	2	0	0	6	720	WPA2	CCMP	PSK	Wlan_GA
[redacted]	-89	18	0	0	8	270	WPA2	CCMP	PSK	<length: 0>
[redacted]	-82	4	0	0	1	65	WPA2	CCMP	PSK	DIRECT-ED-HP Laser 179fnw
[redacted]	-93	0	0	0	6	195	WPA2	CCMP	PSK	Invitados_Clinica
[redacted]	-93	3	0	0	13	130	WPA2	CCMP	PSK	Parte Alta Casa Glez

Promotora inmobiliaria, clínica y usuarios por nombre.



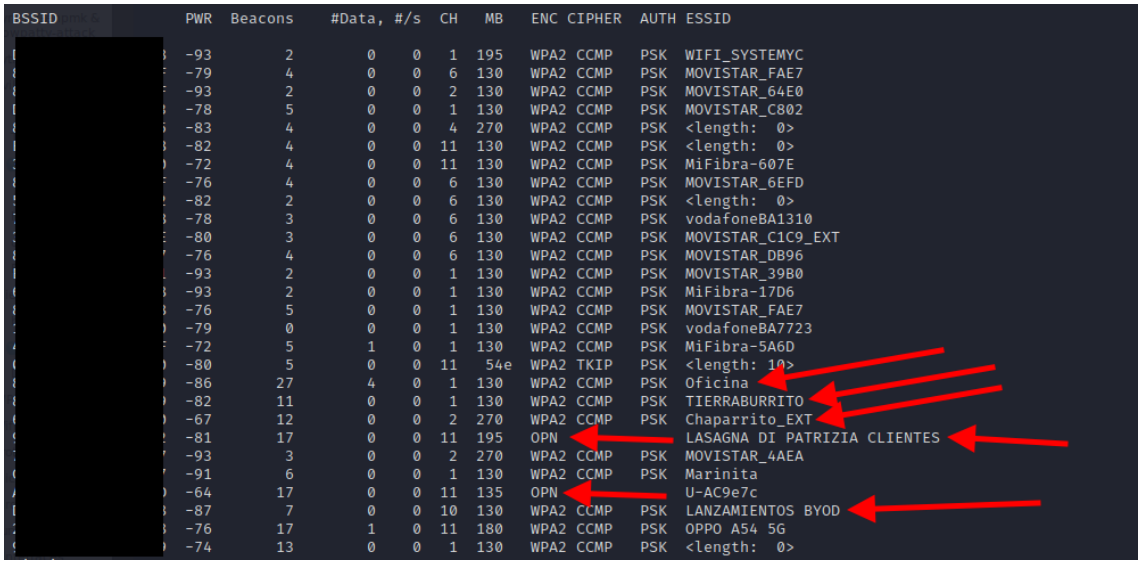
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C8:B4:22:91:2B:3F	-1	0	2	0	11	-1	WPA			<length: 0>
E0:60:66:8F:EA:31	-1	0	0	0	5	-1				<length: 0>
C6:D4:A1:01:80:52	-82	27	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_ED5D
FA:0D:AC:E9:14:ED	-88	2	0	0	1	65	WPA2	CCMP	PSK	DIRECT-ED-HP Laser 179fnw
CC:D4:A1:01:80:52	-89	30	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_8050
82:2A:A8:94:62:26	-89	4	0	0	1	195	WPA2	CCMP	PSK	publico
82:2A:A8:94:DD:D6	-93	24	0	0	11	130	WPA2	CCMP	PSK	Guest
E2:41:36:93:C9:B0	-84	29	3	0	6	130	WPA2	CCMP	PSK	MOVISTAR_C9B0
2C:56:DC:D8:9C:D9	-93	1	1	0	6	195	WPA2	CCMP	PSK	Invitados_Clinica
84:D8:1B:B8:29:CE	-93	17	0	0	5	130	WPA2	CCMP	PSK	<length: 0>
A4:2B:B0:F8:11:0B	-93	4	1	0	11	270	WPA2	CCMP	PSK	MOVISTAR_4ED6
D4:7B:B0:F3:3F:F9	-93	1	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_3FF8
78:81:02:4C:48:91	-93	16	0	0	1	130	WPA2	CCMP	PSK	vodafone4890
98:97:D1:7D:B6:0B	-93	17	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_B60A
80:2A:A8:94:D9:F7	-93	5	0	0	11	130	WPA2	CCMP	PSK	root
2C:56:DC:D8:9C:D8	-93	8	0	0	6	195	WPA2	CCMP	PSK	ClinicaGranado
F0:79:59:D3:E4:30	-84	6	6	0	13	195	WPA2	CCMP	CMAC	WiiLAN
B4:A5:EF:35:8E:79	-93	4	0	0	1	130	WPA2	CCMP	PSK	vodafone8E78
CC:D4:A1:2C:5B:0A	-93	19	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_5B08
80:2A:A8:94:DD:D6	-93	16	0	0	11	130	WPA2	CCMP	PSK	root
18:E8:29:B7:49:7A	-1	0	0	0	1	-1				<length: 0>
72:D2:4F:9A:06:12	-86	2	0	0	1	130	WPA2	CCMP	PSK	<length: 11>
A8:5E:45:71:3F:34	-93	2	0	0	13	130	WPA2	CCMP	PSK	Parte Alta Casa Glez
D4:7B:B0:B2:9F:1D	-93	2	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_9F1C
CC:2D:21:E5:AA:61	-93	2	0	0	2	270	WPA2	CCMP	PSK	Pescos wifi
64:68:0C:58:08:47	-93	6	3	0	3	54	WPA	TKIP	PSK	WLAN_0844
84:D8:1B:0C:A9:36	-87	6	0	0	8	270	WPA2	CCMP	PSK	Familia Guzman Gallego
1A:E8:29:B7:48:B6	-86	2	0	0	11	720	WPA2	CCMP	PSK	avintia20

Clínica y empresas.



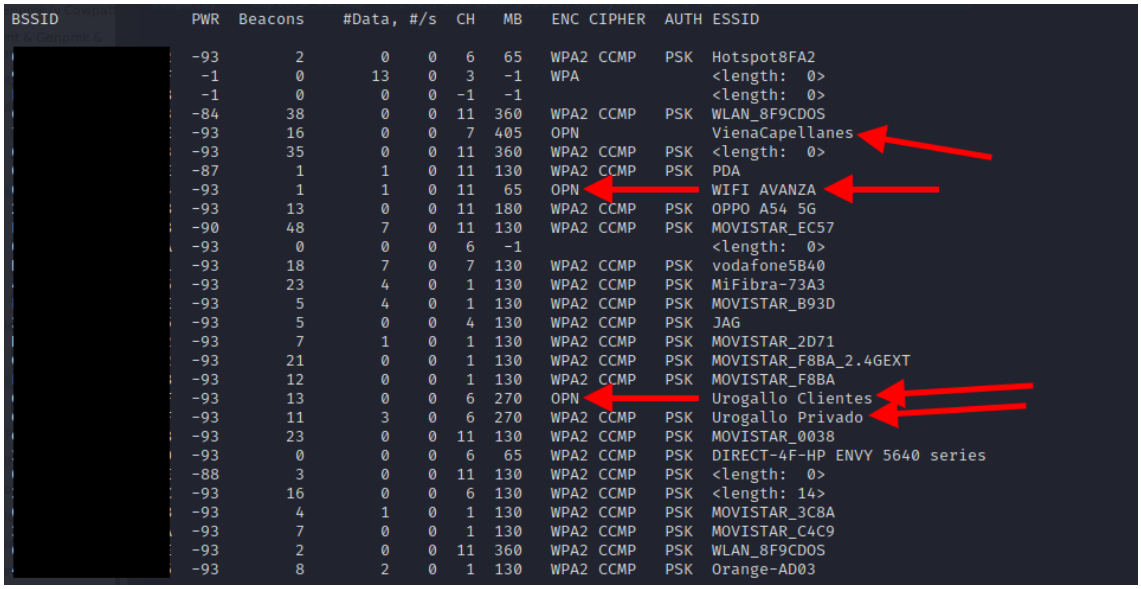
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[redacted]	-86	3	1	0	1	130	WPA2	CCMP	PSK	MOVISTAR_11AA
	-93	2	0	0	1	54e.	WPA2	CCMP	PSK	HP-Print-FD-ENVY 4500 series
	-93	2	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_CFC0
	-92	2	0	0	6	130	OPN			Wifi El Corte Ingles
	-72	2	0	0	6	324	WPA2	CCMP	MGT	<length: 0>
	-85	2	0	0	6	130	WPA2	CCMP	PSK	RF108tpv
	-1	0	0	0	6	-1				<length: 0>
	-66	1	0	0	11	130	WPA2	CCMP	PSK	GOIKO STAFF
	-66	3	0	0	11	130	OPN			GOIKO FREE WIFI
	-66	3	0	0	11	130	WPA2	CCMP	PSK	<length: 0>
	-66	3	0	0	11	130	WPA2	CCMP	PSK	<length: 0>
	-66	3	0	0	11	130	WPA2	CCMP	PSK	<length: 0>
	-76	3	0	0	6	130	WPA2	CCMP	PSK	DIRECT-3f-HP M132 LaserJet
	-92	3	0	0	11	270	WPA2	CCMP	PSK	Jazztel_Pozuelo4
	-93	1	0	0	4	405	WPA2	CCMP	PSK	MARKETMAN_2.4GHz
	-93	2	0	0	3	54	WPA2	CCMP	PSK	MEGA2
	-93	0	0	0	8	405	WPA2	CCMP	PSK	SHM-WIFI
	-70	2	0	0	6	130	WPA2	CCMP	PSK	DIRECT-71-HP M132 LaserJet
	-70	10	0	0	6	360	WPA2	CCMP	PSK	<length: 0>
	-69	9	0	0	6	360	WPA2	CCMP	PSK	PSERVICE
	-78	3	0	0	1	130	OPN			GOIKO FREE WIFI
	-85	1	0	0	1	130	WPA2	CCMP	PSK	ECI-CORP
	-78	5	0	0	1	130	WPA2	CCMP	PSK	<length: 0>
	-86	3	0	0	1	360	WPA2			<length: 0>
	-81	4	0	0	1	360	WPA2	CCMP	PSK	PSERVICE
	-78	2	0	0	1	130	WPA2	CCMP	PSK	GOIKO STAFF
	-85	5	0	0	1	130	OPN			Wifi El Corte Ingles
	-85	4	0	0	1	130	WPA2	CCMP	PSK	mx1739027a

Conocida empresa y restaurantes populares.



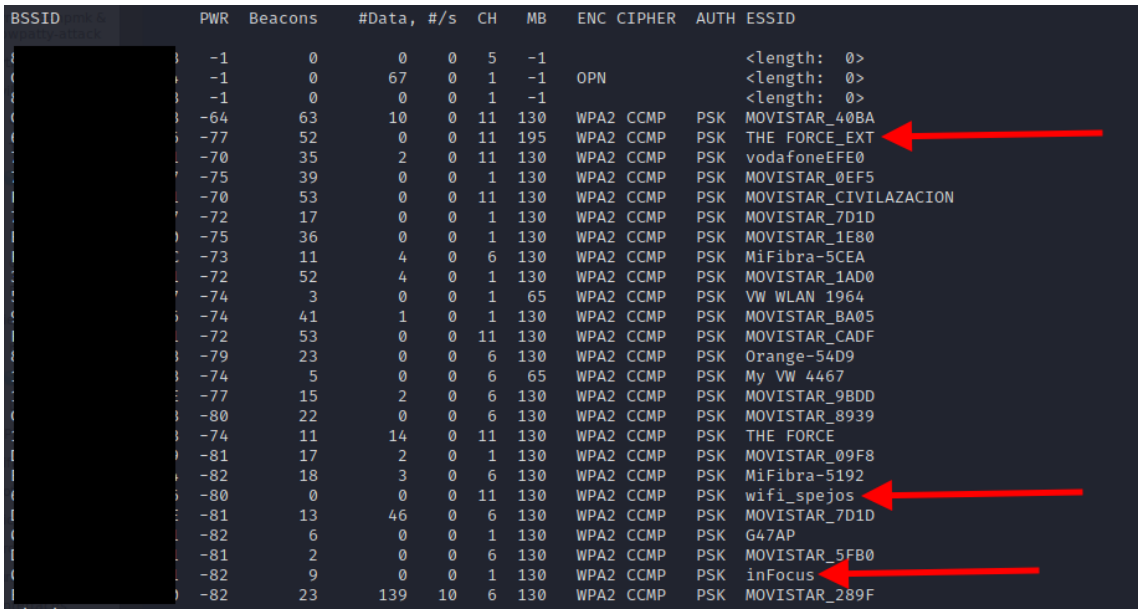
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[redacted]	-93	2	0	0	1	195	WPA2	CCMP	PSK	WIFI_SYSTEMYC
	-79	4	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_FAE7
	-93	2	0	0	2	130	WPA2	CCMP	PSK	MOVISTAR_64E0
	-78	5	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_C802
	-83	4	0	0	4	270	WPA2	CCMP	PSK	<length: 0>
	-82	4	0	0	11	130	WPA2	CCMP	PSK	<length: 0>
	-72	4	0	0	11	130	WPA2	CCMP	PSK	MiFibra-607E
	-76	4	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_6EFD
	-82	2	0	0	6	130	WPA2	CCMP	PSK	<length: 0>
	-78	3	0	0	6	130	WPA2	CCMP	PSK	vodafoneBA1310
	-80	3	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_C1C9_EXT
	-76	4	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_DB96
	-93	2	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_39B0
	-93	2	0	0	1	130	WPA2	CCMP	PSK	MiFibra-17D6
	-76	5	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_FAE7
	-79	0	0	0	1	130	WPA2	CCMP	PSK	vodafoneBA7723
	-72	5	1	0	1	130	WPA2	CCMP	PSK	MiFibra-5A6D
	-80	5	0	0	11	54e	WPA2	TKIP	PSK	<length: 10>
	-86	27	4	0	1	130	WPA2	CCMP	PSK	Oficina
	-82	11	0	0	1	130	WPA2	CCMP	PSK	TIERRABURRITO
	-67	12	0	0	2	270	WPA2	CCMP	PSK	Chaparrito_EXT
	-81	17	0	0	11	195	OPN			LASAGNA DI PATRIZIA CLIENTES
	-93	3	0	0	2	270	WPA2	CCMP	PSK	MOVISTAR_4AEA
	-91	6	0	0	1	130	WPA2	CCMP	PSK	Marinita
	-64	17	0	0	11	135	OPN			U-AC9e7c
	-87	7	0	0	10	130	WPA2	CCMP	PSK	LANZAMIENTOS BYOD
	-76	17	1	0	11	180	WPA2	CCMP	PSK	OPPO A54 5G
	-74	13	0	0	1	130	WPA2	CCMP	PSK	<length: 0>

Restaurantes y redes WiFi abiertas.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[redacted]	-93	2	0	0	6	65	WPA2	CCMP	PSK	Hotspot8FA2
	-1	0	13	0	3	-1	WPA			<length: 0>
	-1	0	0	0	-1	-1				<length: 0>
	-84	38	0	0	11	360	WPA2	CCMP	PSK	WLAN_8F9CDOS
	-93	16	0	0	7	405	OPN			VienaCapellanes
	-93	35	0	0	11	360	WPA2	CCMP	PSK	<length: 0>
	-87	1	1	0	11	130	WPA2	CCMP	PSK	PDA
	-93	1	1	0	11	65	OPN			WIFI AVANZA
	-93	13	0	0	11	180	WPA2	CCMP	PSK	OPPO A54 5G
	-90	48	7	0	11	130	WPA2	CCMP	PSK	MOVISTAR_EC57
	-93	0	0	0	6	-1				<length: 0>
	-93	18	7	0	7	130	WPA2	CCMP	PSK	vodafone5B40
	-93	23	4	0	1	130	WPA2	CCMP	PSK	MiFibra-73A3
	-93	5	4	0	1	130	WPA2	CCMP	PSK	MOVISTAR_B93D
	-93	5	0	0	4	130	WPA2	CCMP	PSK	JAG
	-93	7	1	0	1	130	WPA2	CCMP	PSK	MOVISTAR_2D71
	-93	21	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_F8BA_2.4GEXT
	-93	12	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_F8BA
	-93	13	0	0	6	270	OPN			Urogallo Clientes
	-93	11	3	0	6	270	WPA2	CCMP	PSK	Urogallo Privado
	-93	23	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_0038
	-93	0	0	0	6	65	WPA2	CCMP	PSK	DIRECT-4F-HP ENVY 5640 series
	-88	3	0	0	11	130	WPA2	CCMP	PSK	<length: 0>
	-93	16	0	0	6	130	WPA2	CCMP	PSK	<length: 14>
	-93	4	1	0	1	130	WPA2	CCMP	PSK	MOVISTAR_3C8A
	-93	7	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_C4C9
	-93	2	0	0	11	360	WPA2	CCMP	PSK	WLAN_8F9CDOS
	-93	8	2	0	1	130	WPA2	CCMP	PSK	Orange-AD03

Otros restaurantes y redes WiFi abiertas.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[redacted]	-1	0	0	0	5	-1				<length: 0>
	-1	0	67	0	1	-1	OPN			<length: 0>
	-1	0	0	0	1	-1				<length: 0>
	-64	63	10	0	11	130	WPA2	CCMP	PSK	MOVISTAR_40BA
	-77	52	0	0	11	195	WPA2	CCMP	PSK	THE FORCE_EXT
	-70	35	2	0	11	130	WPA2	CCMP	PSK	vodafoneEFE0
	-75	39	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_0EF5
	-70	53	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_CIVILAZACION
	-72	17	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_7D1D
	-75	36	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_1E80
	-73	11	4	0	6	130	WPA2	CCMP	PSK	MiFibra-5CEA
	-72	52	4	0	1	130	WPA2	CCMP	PSK	MOVISTAR_1AD0
	-74	3	0	0	1	65	WPA2	CCMP	PSK	VW WLAN 1964
	-74	41	1	0	1	130	WPA2	CCMP	PSK	MOVISTAR_BA05
	-72	53	0	0	11	130	WPA2	CCMP	PSK	MOVISTAR_CADF
	-79	23	0	0	6	130	WPA2	CCMP	PSK	Orange-54D9
	-74	5	0	0	6	65	WPA2	CCMP	PSK	My VW 4467
	-77	15	2	0	6	130	WPA2	CCMP	PSK	MOVISTAR_9BDD
	-80	22	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_8939
	-74	11	14	0	11	130	WPA2	CCMP	PSK	THE FORCE
	-81	17	2	0	1	130	WPA2	CCMP	PSK	MOVISTAR_09F8
	-82	18	3	0	6	130	WPA2	CCMP	PSK	MiFibra-5192
	-80	0	0	0	11	130	WPA2	CCMP	PSK	wifi_spejos
	-81	13	46	0	6	130	WPA2	CCMP	PSK	MOVISTAR_7D1D
	-82	6	0	0	1	130	WPA2	CCMP	PSK	G47AP
	-81	2	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_5FB0
	-82	9	0	0	1	130	WPA2	CCMP	PSK	inFocus
	-82	23	139	10	6	130	WPA2	CCMP	PSK	MOVISTAR_289F

Peluquerías y empresas.

2.2 Muy breve resumen de la historia de las redes WiFi.

Podríamos decir que la historia de lo que conocemos por WiFi se remonta a 1997. Un grupo de científicos del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) convinieron unos estándares que permitían el intercambio de información a través de redes inalámbricas dando lugar a la conocida familia de normas 802.11 (término más apropiado para referirse al WiFi), que después derivaría en múltiples actualizaciones.

Dos anécdotas no aportan mucho a este trabajo pero que son interesantes de mencionar rápidamente, son que la primera red WLAN es atribuida a 7 ordenadores que la universidad de Hawaii repartió en 1971 entre diferentes islas. Y que se asume a la actriz Hedy Lamarr como la precursora de esta tecnología.

2.3 Wi-Fi Alliance

Aunque una gran parte de los usuarios no lo sepan, WiiFi (Wireless Fidelity) es una marca registrada perteneciente a la WiFi Alliance.

Quién es la Alianza WiFi.

Esta organización es la impulsora de los estándares para redes inalámbricas más utilizados hoy en día. En 1999 las empresas 3Com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies se unieron y crearon su precursora, llamada Wireless Ethernet Compatibiity Alliance o WECA. En el año 2000, esta alianza registraba la conexión de redes inalámbricas según la norma IEEE 802.11b bajo el nombre comercial WiFi.

2.4 Ventajas y desventajas de las redes WiFi.

Es indudable que su principal ventaja es la conexión sin cables en la que múltiples dispositivos pueden conectarse simultáneamente a una misma red sin demasiada logística.

La velocidad de conexión en relación al cable es por el contrario una desventaja, pero sin lugar a dudas su principal desventaja es la seguridad. La exposición a cualquier dispositivo receptor sitúa estas redes al alcance de cualquiera, que permite, entre otras cosas, interceptar los paquetes transmitidos, situándose como un Man in the Middle. Además, es vulnerable a múltiples ataques a los que haremos alusión más adelante.

2.5 Breve resumen de los estándares WiFi 802.11.

802.11

Fue el origen de la tecnología inalámbrica tal como la conocemos hoy. Definida en 1997 lograba un máximo de 2 Mbit por segundo.

802.11a

Apenas 2 años más tarde se obtenía una ventaja y una desventaja. Se optó por un cambio de banda de 2.4 GHz a 5 GHz, espacio mucho más libre que permitía menor interferencia. Se lograron 54 Mbit por segundo pero por otro lado se perdió alcance.

802.11b

Este es el estándar que impulsó WiFi Alliance. A pesar de que contaba con una velocidad algo menor de 11 Mbit por segundo fue muy bien recibida ya que aumentaba el alcance hasta casi 500 metros.

802.11g

Combinaba los dos anteriores compatibilizándolos.

802.11n

Utilizan por primera vez varias antenas y por primera vez emiten en dos bandas, 2,4 GHz y 5 GHz.

802.11ac

Es el más extendido actualmente. Permite atravesar mejor los obstáculos físicos como muros.

2.6 Algoritmos y seguridad en redes WiFi.

Un algoritmo, como define la RAE realiza una serie finita de operaciones que permiten hallar la solución a un problema. En el caso del WiFi los algoritmos empleados en los protocolos de seguridad, realizan una serie de operaciones de cifrado que representan un elemento crucial de cara a la protección de nuestras comunicaciones inalámbricas.

WiFi abierto.

Sin duda, es el estado más peligroso de una red WiFi. No sólo no solicita contraseña para estar dentro de la red, sino que no cifra las comunicaciones y por tanto cualquiera podría interceptarlas de un modo trivial.
Es el escenario ideal para un atacante.

WEP.

Este protocolo de cifrado es el siguiente estado más inseguro posible de las redes WiFi actuales. Cuando se constituyó trataba de equipararse al sistema de cifrado por cable (wired equivalent privacy - privacidad equivalente a cableado), sin embargo, distaba mucho de conseguirlo. Se basa en el cifrado RC4 que es actualmente considerado inseguro, a pesar de que en algunos casos pueda estar justificado su uso. Es algo menos inseguro que la red WiFi abierta pero no deja de ser un escenario atractivo para los atacantes. No obstante, su uso es cada vez más testimonial, aunque asombrosamente, aún se puede encontrar.
La mayor debilidad de este modo de cifrado es que sus vectores de inicialización (IV) se repite demasiadas veces.

WEP2.

Este fue un intento infructuoso de resolver las deficiencias de WEP, sobre todo para entornos que aún no estaban preparados para implementar WPA. Se mejoró la longitud del vector de inicialización ampliándola a 128 bits, pero esto no fue suficiente y no resolvió otras vulnerabilidades que presentaba el cifrado RC4.

WEP Plus.

Si bien era más robusto, requería de ser usado en ambos extremos de la comunicación, lo que dificultaba su puesta en marcha. Tampoco resolvió las carencias de WEP.

WPA.

Como se puede suponer, el protocolo WPA (Wi-fi Proteceted Access) apareció para cubrir las debilidades del cifrado WEP, aportando mayor foco en la seguridad. Así que de tal modo se puede entender WPA como la evolución del protocolo WEP.
Realmente utiliza igualmente el RC4, sin embargo, modifica las claves temporales cada 10000 paquetes, mejorando la vulnerabilidad del protocolo WEP. Al compartir en esencia los elementos con WEP en principio es igualmente vulnerable a muchos ataques similares pero los combate con otros recursos como la rotación de claves de difusión, etc.

WPA personal.

En muchas ocasiones, para una red doméstica, la elección de WPA personal en lugar de WPA Enterprise, puede proporcionar una capa de seguridad suficiente, ya que todos los miembros que la utilizan suelen ser confiables, como en el caso de una familia. En este protocolo, todos los usuarios comparten un único el usuario y una única contraseña. Pero obviamente esto puede ser una vulnerabilidad en según qué contextos.

Imagen https://www.tp-link.com/ar/support/faq/500/

WPA Enterprise.

Se añade una capa de autenticación remota, por medio de un servidor RADIUS, en el que cada usuario tiene su propia clave de autenticación y su propia contraseña. Suele estar orientado para redes empresariales.

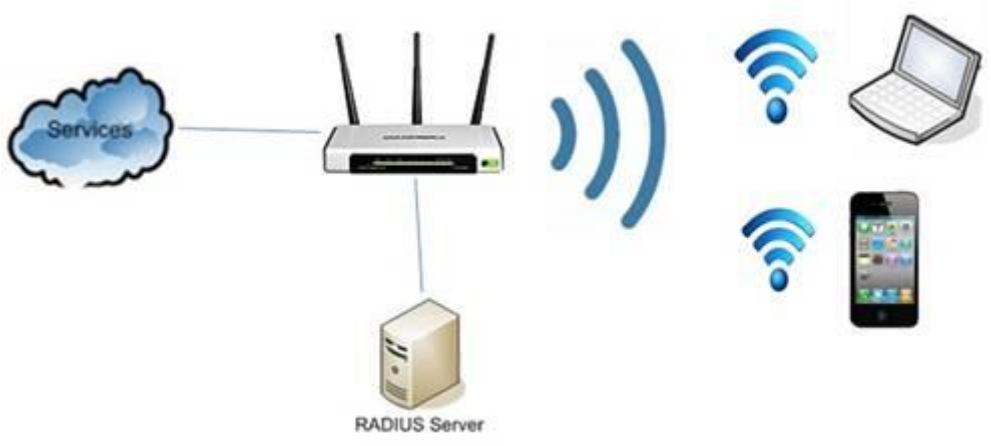


Imagen https://www.tp-link.com/ar/support/faq/500/

WPA2.

El WPA2 es una evolución del cifrado WPA y su característica más destacada en relación al anterior, es que implementa el cifrado AES 128 (Advanced Encryption Standard). Este algoritmo de cifrado es considerado uno de los más seguros al momento actual.

WPA2 personal.

La variación principal respecto del WPA personal está en la mejora de los métodos de cifrado.

WPA2 Enterprise.

Como en el caso anterior su mejora principal respecto del WPA Enterprise radica en el método de cifrado.

WPA3.

De un recorrido reciente, fue presentado por primera vez por la WiFi Alliance en 2018. La característica más determinante es que pasa del cifrado de 128 bits al de 192 bits. Está aún poco popularizado, probablemente porque los métodos de cifrado WPA2 son considerados aún seguros. En cualquier caso, es lanzado antes de que el método WPA2 quede obsoleto.

Una novedad interesante es el **Wi-Fi Easy Connect**, que permite a dispositivos que no cuentan con unas interfaces de acceso directo por medio de otro. De este modo es posible configurar por ejemplo un dispositivo IoT por medio de un código QR en un teléfono móvil.

WPA3 personal.

La variación principal respecto del WPA2 personal está en la mejora de los métodos de cifrado.

WPA3 Enterprise.

Como en el caso anterior su mejora principal respecto del WPA2 Enterprise radica en el método de cifrado.

Autenticación remota por medio de un servidor RADIUS.

Ahora mismo se utiliza en un gran espectro de contextos en los que se requiere autenticación. El proceso está sustentado entre la arquitectura cliente-servidor, en el que RADIUS es el servidor y Firebox es el cliente. El proceso de autenticación será bien a través de una petición HTTPS en principio por el puerto 4100 o bien por VPN. Los usuarios no tratan con los códigos de cifrado. Serán manejados desde un segundo plano tras presentar sus credenciales ocultando a posibles atacantes, mucha información del proceso.

La autenticación puede ser únicamente por medio de credenciales o además se puede añadir una capa extra de seguridad, exigiendo un certificado digital tras aportar dichas credenciales.

Dentro de este método de autenticación también es posible encontrar vulnerabilidades, sin embargo, incorpora dificultades añadidas a un posible atacante que trate de introducirse en la red de manera ilegítima.

Imagen https://www.redeszone.net/tutoriales/servidores/servidor-radius-cloud-autenticacion-clientes/

2.7 Algunas herramientas para auditorías WiFi.

No es objetivo de este trabajo tratar todos los procesos que suceden en las redes inalámbricas con tecnología WiFi, ni todas las herramientas destinadas a las auditorías

inalámbricas, por tanto, trataremos de ceñirnos a algunos aspectos que ilustren el objeto de este estudio.

Comenzaremos conociendo algunas de las herramientas comunes utilizadas en auditorías WiFi.

Suite Aircrack-ng.

Imagen https://www.aircrack-ng.org/

Quizás la suite de herramientas más popular actualmente. Viene integrada en Kali Linux y consta de las siguientes herramientas:

airbase-ng, aircrack-ng, airdecap-ng, airdecloak-ng, airdriver-ng, aireplay-ng, airmon-ng, airodump-ng, airolib-ng, airserv-ng, airtun-ng, easside-ng, packetforge-ng, tkiptun-ng, wesside-ng, airdecloak-ng.

De las que son más utilizadas para auditorías encontraremos:

Airmon-ng - Activa la tarjeta inalámbrica en modo monitor para la intercepción de los paquetes entre extremos.

Airodump-ng - Scanner de redes en busca de los AP disponibles y de sus clientes asociados (o no) y de sus direcciones MAC (BSSID - STATION) o de su nombre otorgado (ESSID)

Epígrafes que mostrará del AP:

BBSSID es la dirección MAC del AP.

PWR nos comenta la proximidad a la señal. Cuanto más alto el valor más cercano.

Si encontramos a veces un -1 significa que el controlador no acepta informes de niveles de señal. O que el cliente está fuera del alcance y está escuchando la mitad de la comunicación.

BEACONS Número de paquetes enviados.

DATA Número de paquetes capturados.

#/s Número de paquetes de datos medidos por segundo durante los últimos 10 segundos.

CH Canal en el que operan (que se pueden repetir).

MB Velocidad máxima permitida por el AP.

ENC el cifrado detectado. En domésticas lo más común es WPA y WPA2

CIPHER es el cifrado empleado. Hay diversos. Lo común en WPA2 es CCMP.
AUTH El protocolo de autenticación.
ESSID Nombre asignado al AP.

Epígrafes del cliente:
BSSID Dirección MAC de los AP.
STATION Dirección MAC de dispositivos que están conectados a los AP.
Rate Da dos valores. La tasa de recepción seguida de la tasa de retransmisión.
Si el valor tiene una e es que tiene el QOS habilitado.
Lost Muestra el número de paquetes perdidos durante los últimos 10 segundos.
Frames Número de paquetes enviados del cliente al AP.
Notes Alguna información adicional en función de lo que se capture.
Probes Aquí se definen las preguntas a las que trata de conectarse constantemente los dispositivos.
Probe request. Busca constantemente las estaciones anteriores a las que se ha conectado alguna vez. El dispositivo opera en todos los canales que tiene habilitados para transmitir. Y hace peticiones constantes broadcast destiny en busca de AP.
Probe response. El AP sin embargo sólo opera en un canal y responde al dispositivo ofreciéndole su disponibilidad e iniciando el proceso de handshake.

Aireplay-ng - Inyector de tramas de red con distintos fines. Listado de las inyecciones y sus flags necesarios:

--deauth count : deauthenticate 1 or all stations (-0)
--fakeauth delay : fake authentication with AP (-1)
--interactive : interactive frame selection (-2)
--arpreplay : standard ARP-request replay (-3)
-chopchop : decrypt/chopchop WEP packet (-4)
--fragment : generates valid keystream (-5)
--caffe-latte : query a client for new IVs (-6)
--cfrag : fragments against a client (-7)
--migmode : attacks WPA migration mode (-8)
--test : tests injection and quality (-9)

Aircrack-ng **-** Herramienta destinada a recuperar las claves WEP y WPA - PSK a partir de tramas de redes inalámbricas capturadas. Tiene diferentes funcionalidades, pero la principal es el uso de la fuerza bruta contra capturas.

Wash.

Wash, también integrada en Kali Linux, es una herramienta para escanear e identificar puntos de acceso activos, proporcionándonos varios datos importantes:

- Su dirección MAC (BSSID).
- El canal en el que opera.
- La intensidad con la que recibimos su señal.
- La versión de su WPS en caso de estar activo.
- Si el WPS está bloqueado o no.
- El fabricante.
- El nombre que se le ha otorgado (ESSID).

Reaver-WPS.

Realizará un ataque de fuerza bruta (Pixie Dust) sobre el PIN WPS de un AP y una vez obtenido, recupera los datos de conexión de dicho AP.

Kismet.

Kismet es una aplicación open source destinada a interceptar tramas de redes 802.11 o como son más conocidas redes WiFi. Kismet es un sistema pasivo al contrario de la mayoría de los sniffer y no genera inyecciones. Kismet tiene funciones incluidas de detección de intrusos y de otras aplicaciones de rastreo de redes inalámbricas. Funciona con cualquier red inalámbrica y corre en varias distribuciones de Linux y en MacOS.

NetStumbler.

Programa para Windows que permite monitorizar redes inalámbricas 802.11 a través de tarjetas de red en modo monitor. Nos mostrará los AP, sus direcciones MAC, fabricantes y sus SSID, como otros detalles sobre intensidad, cobertura, orientación óptima, AP no autorizados (Rogue AP), verificar configuraciones adecuadas o inadecuadas, etc. Se utiliza con interfaz gráfica al contrario de la mayoría de las que hay disponibles y eso la pone más al alcance de cualquier usuario que se inicia.
Algunos valores que muestra la interfaz: MAC, SSID, Name, Chan, Speed, Vendor.

Caín y Abel.

Habitualmente simplificado como Caín, es una herramienta para sistemas Windows de “recuperación de contraseñas”. Utiliza métodos como la intercepción de tramas

inalámbricas, cracking de hashes por fuerza bruta, e incluso utilización de Rainbow Tables para la aceleración del proceso.
No es código abierto y algunos antivirus lo reconocen como malware. Montoro, fundador y propietario de oxid.it y creador de la herramienta, asegura que no contiene ningún tipo de malware no obstante se recomienda ejecutarlo con precauciones.

CoWPAtty.

Cowpatty es otra herramienta de crack de claves WPA y WPA2 para auditorías de redes inalámbricas que suele venir con Kali Linux. Realiza ataques de diccionario offline contra cifrados WPA y WPA2 basados en PSK. Se incluyó inicialmente en **BackTrack** precursora de la actual Kali. CowPAtty puede acelerar el ataque si utiliza un fichero con claves precalculadas para el AP objetivo.

2.8 Algunos entornos vulnerables y ataques conocidos.

(Apunte previo) - Falsificación previa de la dirección MAC.

La direcciónn MAC de cada dispositivo es, a priori, un código unívoco e irrepetible. Una medida que dificultará el rastreo posterior de cualquier acción que se lleve a cabo en el ataque, es la falsificación de la dirección MAC de nuestra tarjeta de red. Para ello, aunque hay múltiples vías, podemos utilizar la sencilla herramienta Macchanger con la que será fácil disfrazar la MAC legítima.

Ejemplo, mi MAC TP-Link (oculto las direcciones MAC que no son pertinentes con esta única: 00:00:00:00:00:00):

```
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:00:00:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Le pedimos la MAC aunque en este caso se puede ver en ifconfig:

```
kali@kali:~$ macchanger -s wlan0
Current MAC:   00:00:00:00:00:00 (unknown)
```

Permanent MAC: 00:00:00:00:00:00 (unknown)

Utilizamos macchanger
macchanger ofrece multiples propiedades con las direcciones MAC de las tarjetas de red:
kali@kali:~$ macchanger -s tun0
Current MAC: 00:00:00:00:00:00 (XEROX CORPORATION)
Permanent MAC: 00:00:00:00:00:00 (unknown)

Muestra dos MAC. La current MAC y la permanent MAC.
¿Y por qué hace esto?
Porque en realidad la MAC se puede falsificar.

kali@kali:~$ macchanger -s eth0
Current MAC: 00:00:00:00:00:00 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 00:00:00:00:00:00 (CADMUS COMPUTER SYSTEMS)

De tal manera cuando se audita o cuando se hace hacking a una red, se debe comenzar falsificando la MAC aunque se dé un OUI (identificador único de organización) válido para que parezca real.
No olvidemos que en cualquier caso siempre se puede hacer un restore.

Entornos vulnerables.

WiFi abierto.

No nos adentraremos en las posibilidades en este entorno ya que en este caso el ataque es de una complejidad muy baja al poder capturar las comunicaciones que circulan y en especial, las que viajan sin cifrar. Sin ir más lejos, resultaría trivial ejecutar un Man in The Middle con un sniffer al alcance de cualquiera como ***Wireshark*** **o Tshark,** que viene a ser lo mismo, capturando todas las tramas transmitidas. Ya en 2010, ***Firefox*** lanzó un Add-on llamado ***Firesheep*** que buscaba precisamente demostrar lo sencillo que era y es, el secuestro de sesiones HTTP.

Entorno basado en WEP.

Sin duda, un atacante se alegra cuando encuentra que la seguridad de un sistema WiFi está basada en WEP. A estas alturas se encuentra ampliamente comprometido.

Hay múltiples caminos para vulnerar WEP y su cifrado RC4 pero por citar uno sencillo, lo podemos hacer por medio de la suite Aircrack-ng.
El proceso inicial para capturar el HandShake es el mismo que en otros protocolos, pero con la diferencia que una vez capturado, es menos dificultoso de descifrar.
Con multitud de herramientas como Aircrack-ng sería trivial.

Imagen https://mundo-hackers.weebly.com/ataques-wep.html

Algunos ataques conocidos.

Evil Twin.

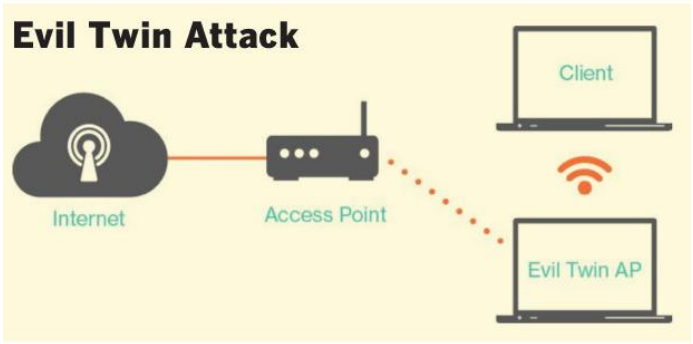


Imagen https://sliitcs2.medium.com/wi-fi-hacking-using-evil-twin-attacks-and-captive-portals-part-1-e1006ff2c723

El famoso Evil Twin todavía sigue siendo un ataque con mucha probabilidad de éxito. El eje central de este ataque, también llamado “Rogue Access Point”, consiste en hacerse pasar por un punto de acceso legítimo e interceptar el tráfico de clientes que no descubran el engaño.
Un ejemplo sería un establecimiento público en donde simular un WiFi existente. En el caso de copiar el mismo nombre, habría quien se conectaría creyendo estar en la red legítima.
Las posibilidades una vez que estos han caído en la trampa, son múltiples.

Hay herramientas tremendamente sencillas como WIFIPHISHER que nos permiten simular un AP con muy poca dificultad.

Algunas herramientas para montar un Evil Twin.

WIFIPHISER:
https://github.com/wifiphisher/wifiphisher

Evil Twin Framework (con enlaces a tutoriales en YouTube):
https://github.com/Esser50K/EvilTwinFramework

Si nos vemos obligados a conectarnos a una red pública, debemos tomar todas las medidas posibles para cerciorarnos de que es la red legítima. Por ejemplo observa que sólo haya una red o que si nos redirige a un portal cautivo, al menos todo e tráfico vaya cifrado por https o por cualquier otro método.

Hay algunas herramientas como **Linset**, **Fluxion**, **wifimosys** que trabajan con .cap previos en los que ya se tiene un handshake y cuando el usuario trata de poner la contraseña, utilizando Aircrack-ng, si ve que no es válida, le redirige a una página de error hasta que la escribe bien. Cuando lo hace correctamente, entonces le dice que será reconectado en breve y ya lo libera y el usuario se vuelve a concetar, habiendo facilitado sus credenciales válidas.

Pixie Dust.

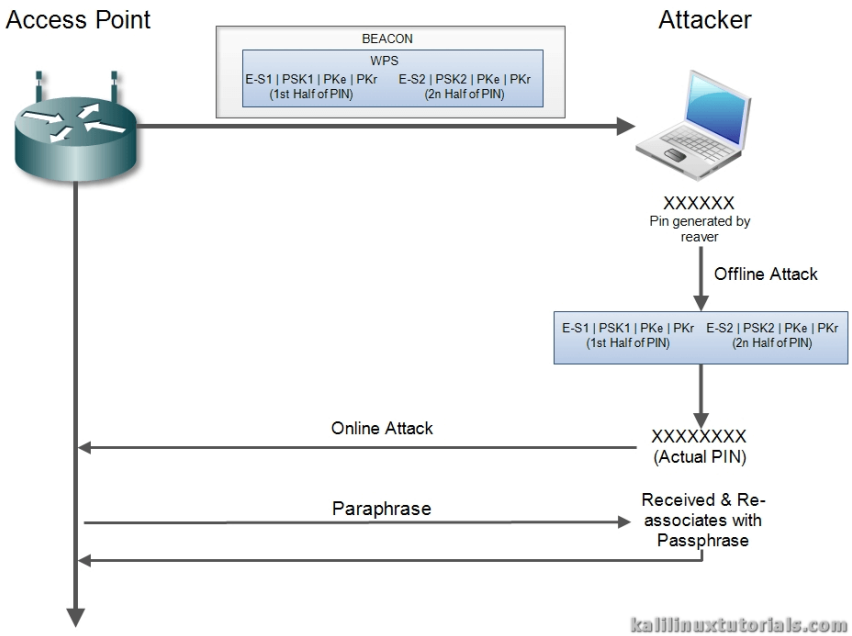


Imagen https://kalilinuxtutorials.com/reaver-pixewps/

Un viejo conocido también pero no por ello menos peligroso. Si bien los router actuales suelen tener medidas preventivas contra este tipo de ataque, todavía se pueden encontrar routers que permiten este ataque de manera exitosa e incluso maneras de evadir las protecciones que dificultan pero no resuelven el vector de ataque.

Todo proviene de uno de los métodos del Wi-Fi Protected Setup o como es más conocido, WPS. En concreto el método PIN WPS. Está presente en la mayoría de los router actuales aunque en WPA3 (aún poco extendido), el PIN WPS es eliminado y sustituido por otro método más seguro a priori, llamado Easy Connect.

El PIN WPS se utiliza para simplificar la conexión de dispositivos a WiFi. El cliente envía un PIN al AP y este a cambio le devuelve los datos para la conexión. Lo que sucede es que son siempre ocho números que además internamente aún se simplifican más pues se dividen en dos parejas de cuatro números, y además el último de la segunda pareja es calculable porque es checksum. Así su predictibilidad es cuestión de tiempo con una reducción de cien millones de combinaciones a sólo once mil. Posteriormente se han añadido funciones como limitar el número de intentos por minuto, aunque esto también se puede evadir.

Herramienta como pixiewps simplifican el ataque fuera de línea, aprovechando la baja o inexistente aleatoriedad que ofrece este método de conexión fácil.

Aunque el método de WPS por botón es ligeramente mejor que el de el WPS PIN escrito en la parte baja del Router, sigue siendo vulnerable por el tiempo en el que se pulsa y que no necesita credenciales para sincronizarse.

Algunas herramientas para lanzar un Pixie Dust:

Existen herramientas que simplifican mucho el ataque como **Reaver**, presente en Kali Linux, que implementa un ataque de fuerza bruta que puede recuperar las credenciales en un promedio de unas 4 a 10 horas.

https://github.com/t6x/reaver-wps-fork-t6x

Existe también **Bully** WPS que es una buena alternativa a Reaver, también presente en Kali y que funciona contra algunos chips que Reaver falla y que implementa algunas mejoras en relación a la primera.

https://github.com/bdpurcell/bully/

DoS - Denegación de servicio.

Este método de ataque bien conocido en otros escenarios además de en el ámbito WiFi puede parecer de los menos frecuentes en las redes inalámbricas. Sin embargo es más común de lo que parece para lograr accesos indebidos e intrusiones en redes no autorizadas. En particular el método de deautenticación WiFi, que es uno de los tipos de DoS, es utilizado para forzar la reconexión y la captura de handshakes.

Heramienta **para lanzar un ataque DoS:**

Aireplay-ng

Es utilizada para inyectar paquetes tramas en la red y en uno de sus ataques deautentica a los usuarios. En concreto la opción número 0.

Ettercap.

A través de su plugin dns_spoof se redirige el tráfico de cualquier cliente que desee autenticarse a una dirección que el atacante configure y que no dé servicio, sin dejar resolver ninguna otra.

KRACK (Key Reinstallation Attack).

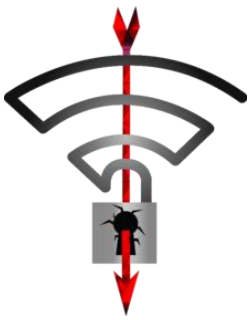


Imagen https://es.wikipedia.org/wiki/KRACK

Este es un ataque conocido por lo interesante de su metodología pero que no es fácil de reproducir en un ambiente doméstico por los conocimientos necesarios para llevarlo a cabo y por los medios necesarios. A pesar de que en un primer momento se creó cierta alarma, esto se diluyó rápidamente cuando diversos estudios fácilmente localizables, definían las dificultades de llevarlo a cabo. No obstante la vulnerabilidad existe y es viable fuera del entorno de laboratorio teniendo en cuenta que hay objetivos más interesantes que un acceso WiFi doméstico como dispositivos IoT, y otros targets conectados a redes locales.

Esta vulnerabilidad ocurre en el tercer paso del handshake de cuatro vías cuando el router envía la llave de cifrado. Estas cuatro vías están orientadas a ponerse de acuerdo entre AP y cliente de cuál va a ser el cifrado que van a utilizar para comunicarse. El

factor más relevante es que entre cliente y AP existen pequeños cortes pero para mantener la conexión se mantiene enviando la clave de cifrado una y otra vez. Esto hace que un atacante pueda capturar y reproducir esa clave de cifrado para interceptar comunicaciones como emails, etc. Teniendo en cuenta que WPA2 no verifica que la clave no haya sido utilizada antes, el atacante puede lograr que el cliente utilice una llave anterior y a partir de aquí interceptar sus comunicaciones.

KR00K.

Se parece a la anterior en la búsqueda de la interceptación de las comunicaciones pero la diferencia más sustancial es que esta no se basa en el cifrado sino en un bug en los dispositivos con chips Broadcom y Cypress, marcas muy extendidas en el mundo.
Esta vulnerabilidad ocurre en dispositivos cuando se comunican por WiFi y existe una señal baja. Si bien existe una clave de cifrado, cuando hay una disociación los valores se resetean y en ese momento, que los atacantes pueden forzar, son vulnerables de perder la confidencialidad en sus comunicaciones.

Michael-Shutdown-exploitation.

Ataque que podría apagar un router remoto.
En los routers más actuales no funciona normalmente aunque en algunos dispositivos algo más antiguos sí que funciona. Se ejecuta con mdk3 y es sencillo.
mdk3 wlan0 (o la tarjeta que corresponda) m (tipo de ataque) -t (MAC del AP) <MAC>
Y tras lanzar el ataque si tiene éxito logra apagarlo.

Beacon flood attack.

El ataque beacon flood attack consiste en anunciar muchos AP en un mismo canal y colapsar a los dispositivos disponibles. Bien por colapsar la red o por confusión, los clientes no podrían conectarse al AP legítimo.

Heramienta para lanzar un ataque Beacon flood mode**:**

Con la herramienta **mkd3**, por ejemplo podríamos crear un archivo txt con un texto como por ejemplo MiRed1, MiRed2, MiRed3, etc. Esto ofrecerá diferentes AP y llegaría a colapsar.
Después lanzaríamos:
mkd3 <tarjeta de red por ejemplo: wlan0> b (beacon flood mode) -f (fichero) -a (authentication Dos mode) -s (speed) 1000 (velocidad recomendable) -c <channel>

Clientless atack WPA/WPA2.

Esta es una vulnerabilidad que no afecta a todos los fabricantes, pero les sucede a un buen número de ellos. No siempre es necesario obtener el handshake de 4 vías para lograr los datos de acceso. De hecho sin que haya clientes conectados se pueden obtener por medio del PMKID que ofrecen muchos de ellos en el primer paquete de las 4 vías. Esto se diseñó así para facilitar el roaming de los clientes. En este caso se puede extraer el WPA PSK (Pre-Shared Key o clave pre-compartida) del PMKID y por tanto todo lo necesario para descifrar la contraseña de conexión al AP.

Herramienta para lanzar un Clientless attack.

Hcxdumptool nos permitirá hacer una captura con esa primera trama de todos los APs disponibles. Después con **hcxpcaptool** podremos convertirlo al formato que hashcat puede interpretar para poder realizar a todos los hashes obtenidos un ataque de fuerza bruta. En caso de que se haya obtenido y que la contraseña esté en el diccionario, será descifrada sin necesidad de ningún cliente conectado.

PMKID = HMAC-SHA1-128 (PMK, "Nombre PMK" | MAC_AP | MAC_STA)

3 Auditor00

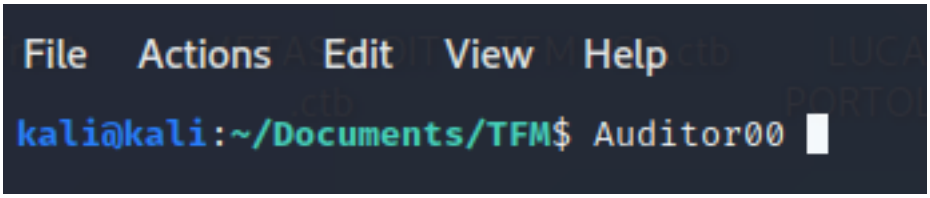
Auditor00 es una herramienta programada por el autor de este trabajo, que más que una herramienta, podría definirse como un tutorial interactivo que enseña el uso de algunas herramientas ya existentes, con el fin de realizar una auditoría de contraseñas débiles en una red WiFi.
Esta herramienta lleva de la mano, paso por paso, haciendo ingresar los comandos necesarios para realizar dicha auditoría en el propio entorno. En un entorno real.

El repositorio está disponible en GitHub:
https://github.com/Lucas73/Auditor00

Una vez terminada la demostración de la auditoría, con las credenciales obtenidas haremos una petición desde esa IP pública vulnerada, a un servidor externo, evidenciando lo frágil que es la IP pública como prueba incriminatoria en un delito. Unas credenciales robadas podrían utilizarse para cometer ciberdelitos e incriminar a una dirección IP pública, completamente ignorante e inocente.

Lanzamos la App.

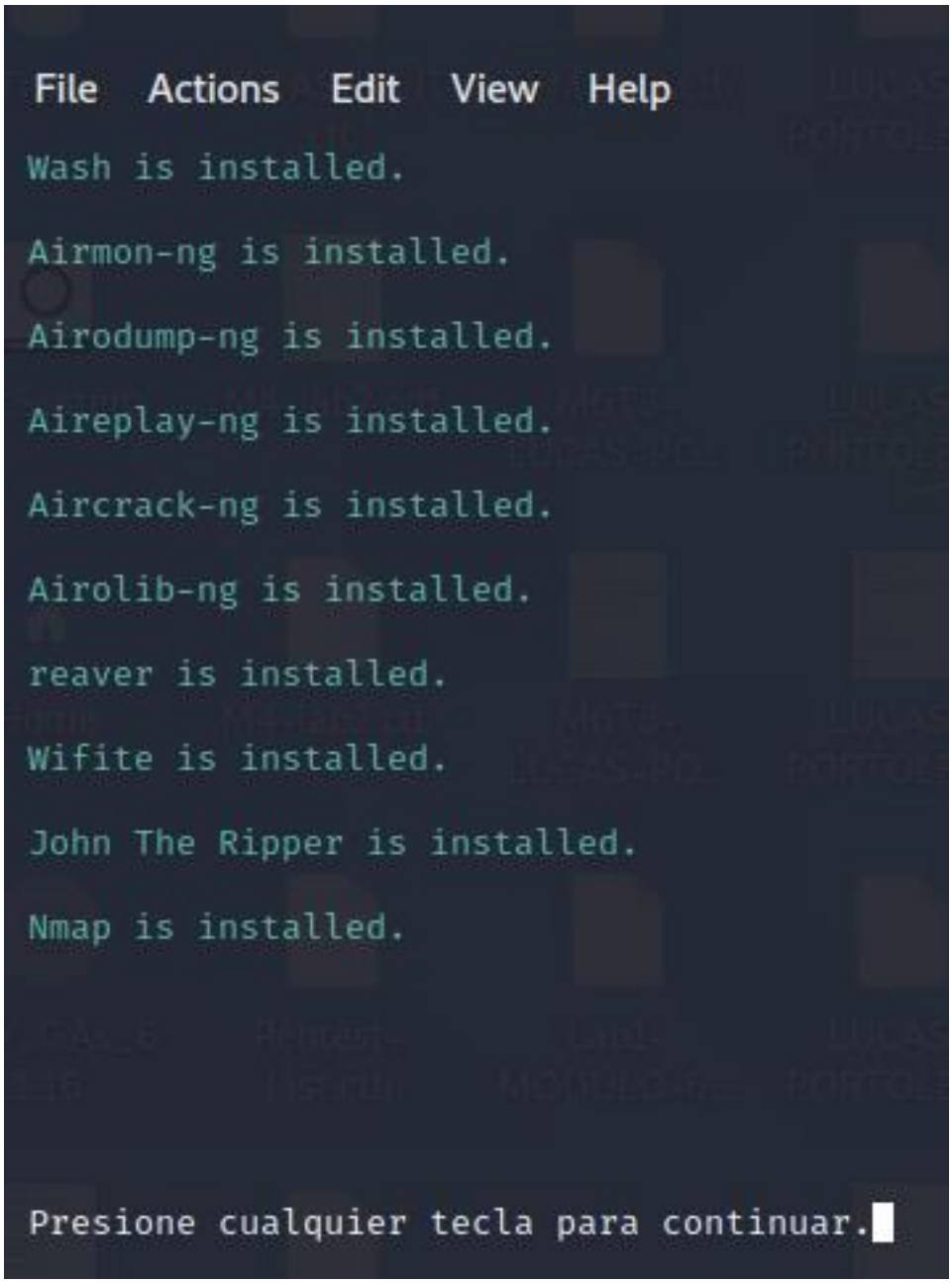
Para lanzar la App, en este caso sencillamente hemos creado un alias y no nos adentraremos en la metodología de hacer la utilidad ejecutable.




File Actions Edit View Help
MENU DE OPCIONES
(IMPORTANTE: seguir el orden numérico)
1) Opción 1 - Revisar dependencias
2) Opción 2 - Falsificación de dirección MAC
3) Opción 3 - Tarjeta en Modo Monitor
4) Opción 4 - Ataque por deautenticación
5) Opción 5 - Ataque por Fuerza Bruta
6) Salir
Elija una opción.
1: Revisar dependencias
2: Falsificación de dirección MAC
3: Tarjeta en Modo Monitor
4: Ataque por deautenticación
5: Ataque por Fuerza Bruta
6: SALIR

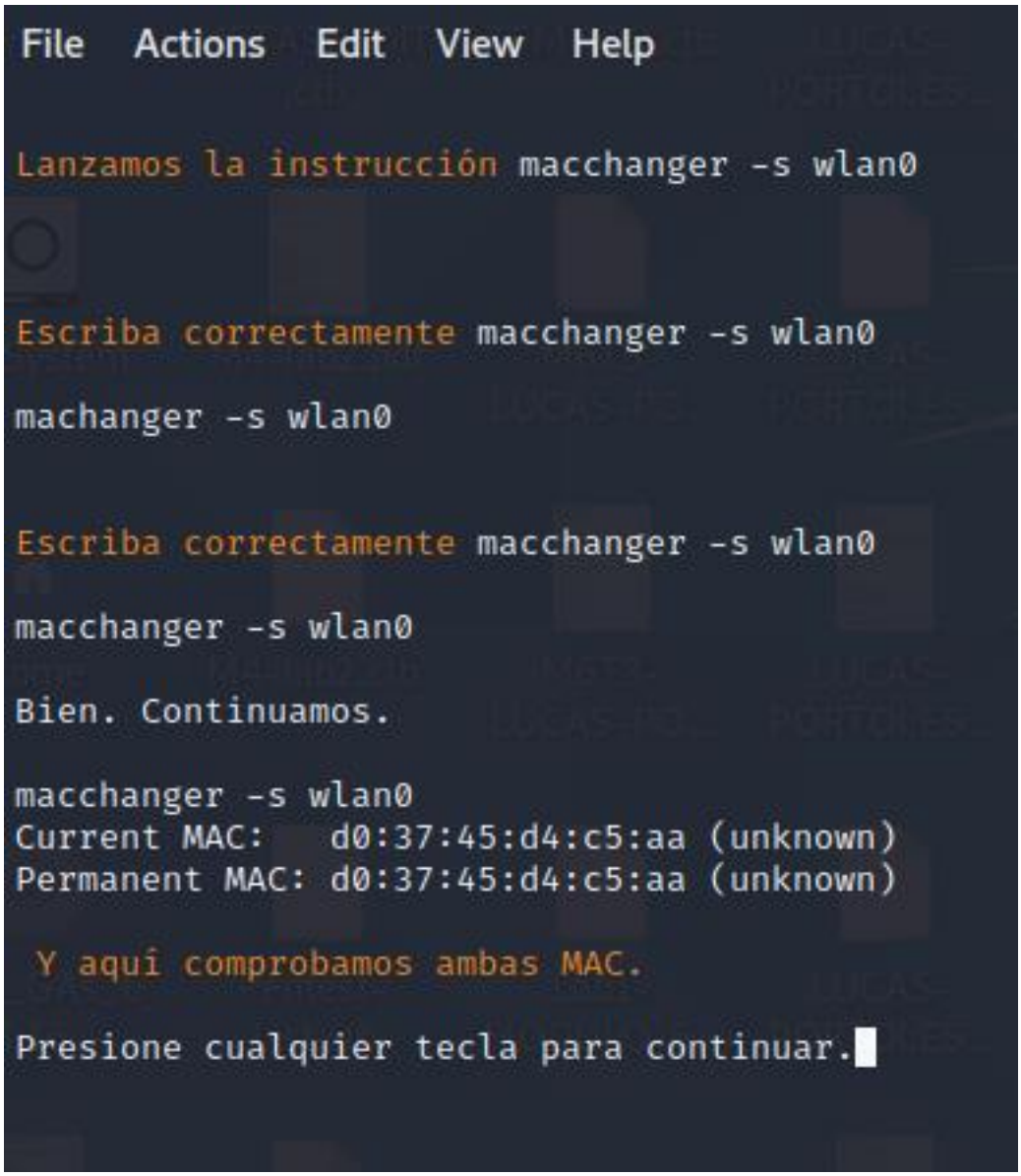
1 Revisar dependencias.

El primer paso que mostramos al usuario es a comprobar la revisión de las dependencias.
Seleccionamos la opción 1 y el sistema comprueba que tengamos lo necesario.
Dentro de esta comprobación hay herramientas de más, porque en un futuro está contemplado como mejoras futuras, incorporar otros ataques como Pixie Dust, etc.



2- Falsificación de dirección MAC.

El siguiente paso es falsificar la dirección MAC para dificultar el rastreo de nuestra auditoría. Utilizaremos una herramienta llamada MacChanger.
Aunque en realidad los comandos los lanzamos desde atrás para evitar errores imprevistos, forzamos al usuario a escribir los comandos necesarios para que aprenda en la práctica cómo hacerlo. Y si se equivoca debe repetirlo correctamente.



Una vez que el usuario ha comprobado su dirección MAC llega el momento de falsificarla.

```
El paso siguiente será elegir una nueva dirección MAC.
Escoja una palabra clave o una parte de ella.
Ejemplo: Apple, App, Tp-Link, Tp-, Ubiquiti, Ubi, Cisco, Cis, etc.

Ubiquiti
```

Primero es necesario buscar un fabricante real para que sea más auténtica.

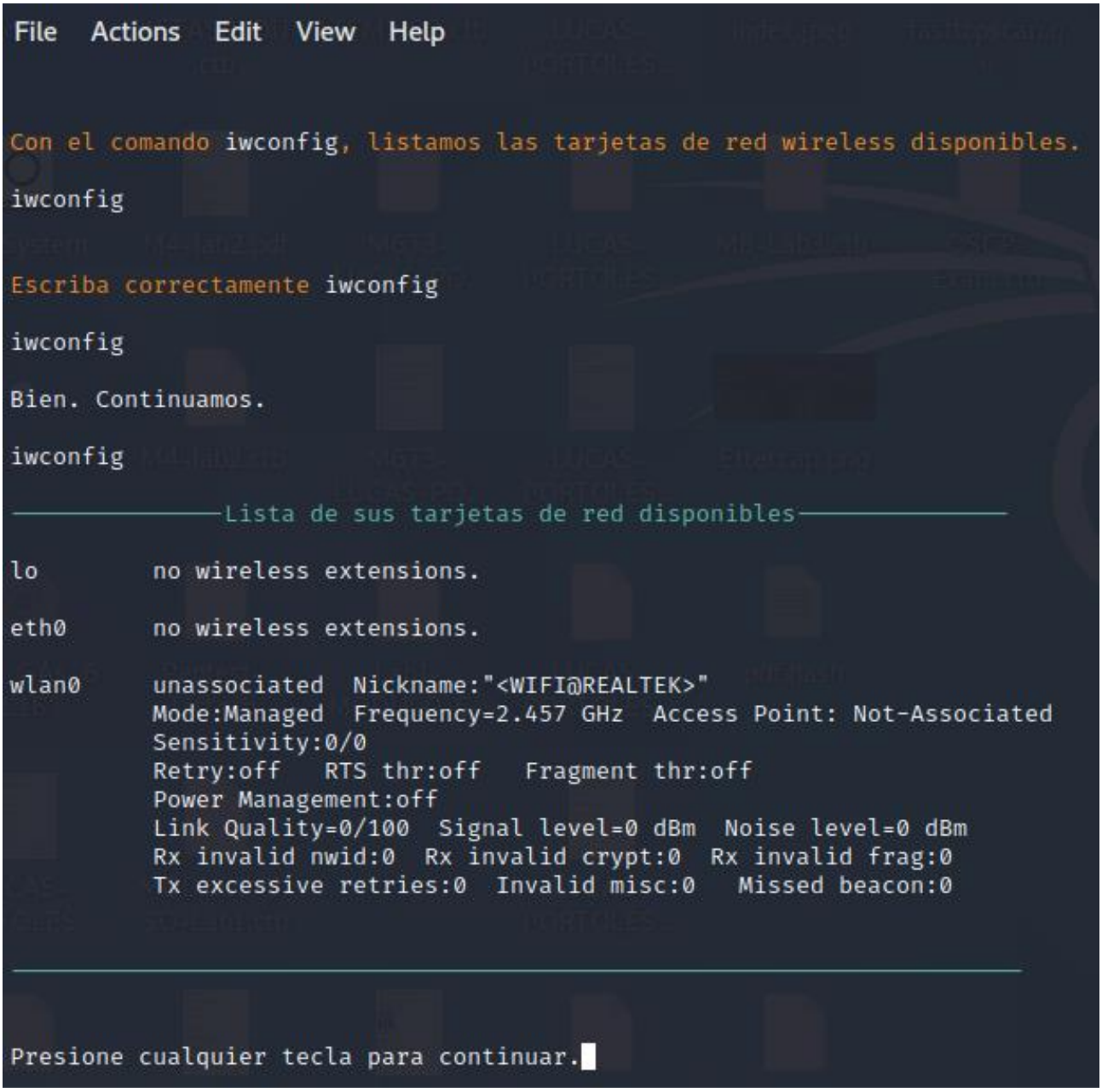
```
El paso siguiente será elegir una nueva dirección MAC.
Escoja una palabra clave o una parte de ella.
Ejemplo: Apple, App, Tp-Link, Tp-, Ubiquiti, Ubi, Cisco, Cis, etc.

Ubiquiti

Lanzamos macchanger -l | grep -i Ubiquiti



Escriba correctamente macchanger -l | grep -i Ubiquiti

macchanger -l | grep -i Ubiquiti

Bien. Continuamos.

macchanger -l | grep -i Ubiquiti
5458 - 00:15:6d - Ubiquiti Networks Inc.
9983 - 00:27:22 - Ubiquiti Networks
12713 - 04:18:d6 - Ubiquiti Networks
13694 - 24:a4:3c - Ubiquiti Networks, INC
15289 - 68:72:51 - Ubiquiti Networks
18207 - dc:9f:db - Ubiquiti Networks, Inc.

Hemos lanzado macchanger -l | grep -i Ubiquiti
Y esta de arriba es la lista con los resultados.

El fabricante es identificado por las 3 primeras parejas y son las que respetaremos.
Las segundas 3 parejas las pondremos al azar.

Presione cualquier tecla para continuar.
```

```
Escriba correctamente sudo macchanger -s wlan0

sudo macchanger -s wlan0

Bien. Continuamos.

sudo macchanger -s wlan0
Current MAC:   dc:9f:db:a6:c8:d4 (Ubiquiti Networks, Inc.)
Permanent MAC: d0:37:45:d4:c5:aa (unknown)

Y podemos seguir con la intrusión algo menos rastreables.

Volvemos a levantar sudo ifconfig wlan0 up


Escriba correctamente sudo ifconfig wlan0 up

sudo ifconfig wlan0 up

Bien. Continuamos.

sudo ifconfig wlan0 up
Presione cualquier tecla para continuar.
```

```
Escriba correctamente sudo macchanger -m dc:9f:db:a6:c8:d4 wlan0

sudo machanger -m dc:9f:db:a6:c8:d4 wlan0


Escriba correctamente sudo macchanger -m dc:9f:db:a6:c8:d4 wlan0

sudo macchanger -m dc:9f:db:a6:c8:d4 wlan0

Bien. Continuamos.

sudo macchanger -m dc:9f:db:a6:c8:d4 wlan0
Current MAC:   d0:37:45:d4:c5:aa (unknown)
Permanent MAC: d0:37:45:d4:c5:aa (unknown)
New MAC:       dc:9f:db:a6:c8:d4 (Ubiquiti Networks, Inc.)


Ahora comprobamos que tiene la nueva MAC del fabricante escogido.


Escriba correctamente sudo macchanger -s wlan0
```

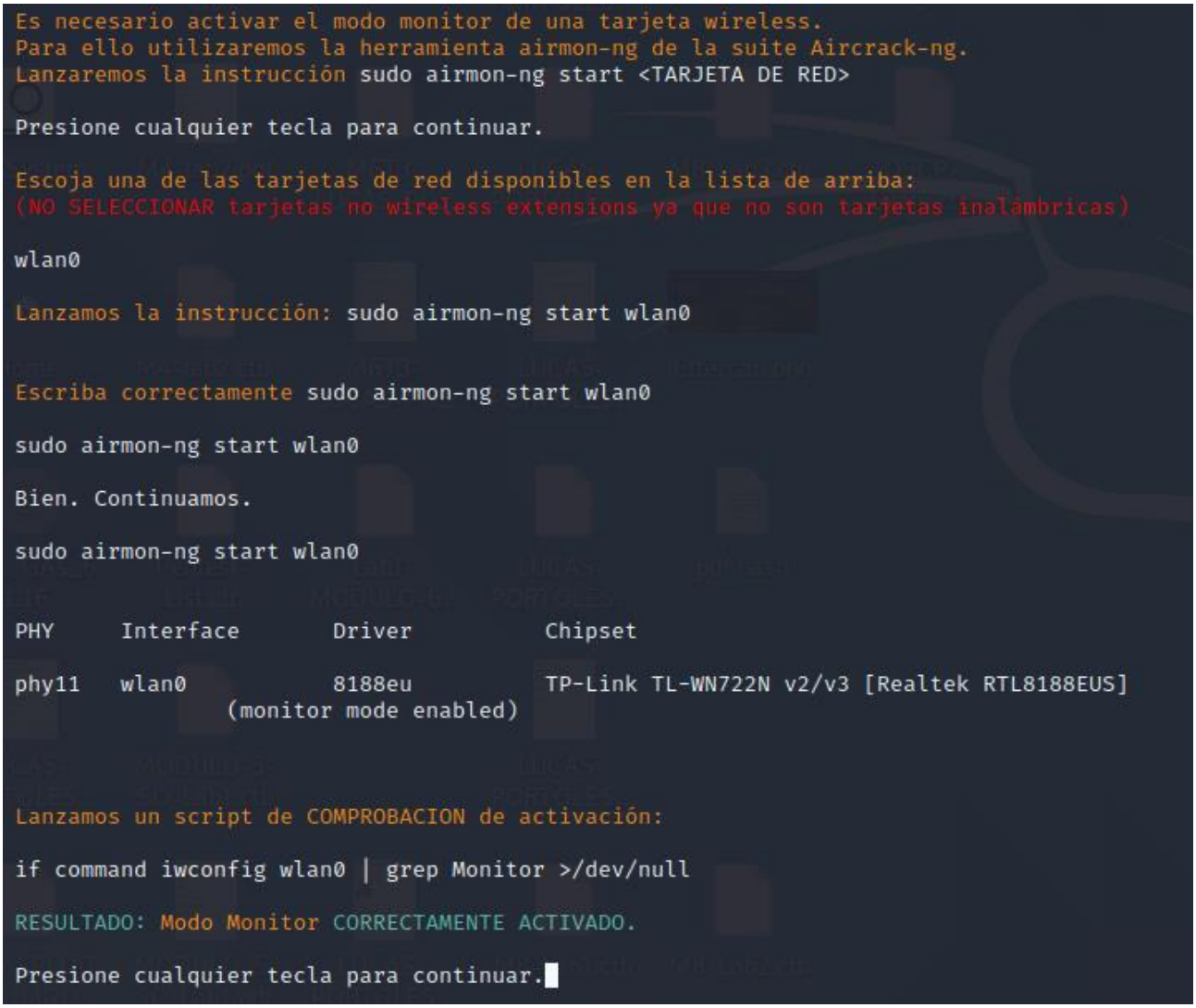
3- Tarjeta en Modo Monitor.

Para poder realizar una auditoría de red es necesario contar con una tarjeta de red inalámbrica y activarla en modo monitor para que capture las tramas que se transmitan.

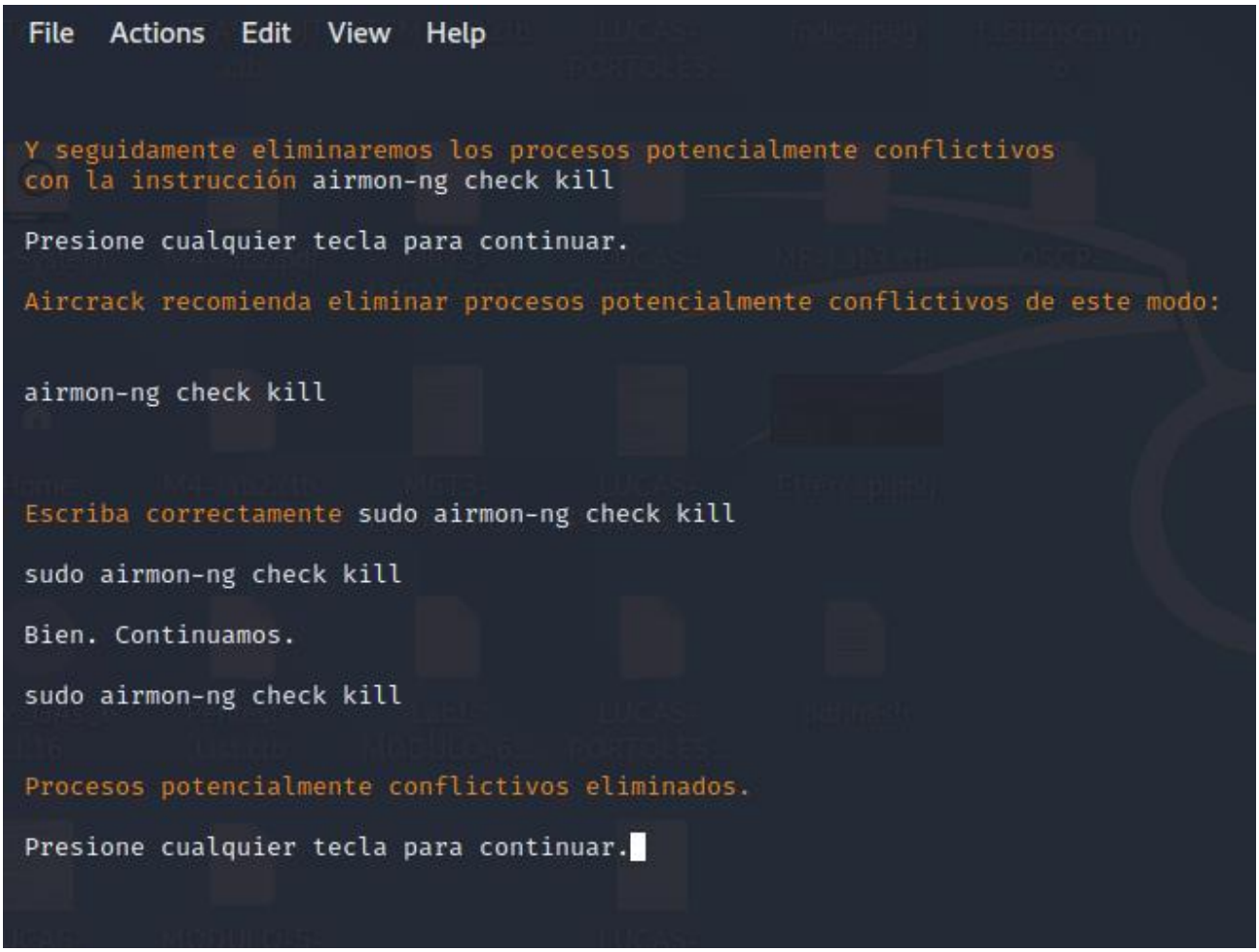


Como podemos ver, la tarjeta wlan0 está en Mode:Managed. Será necesario que cambie a Mode:Monitor.

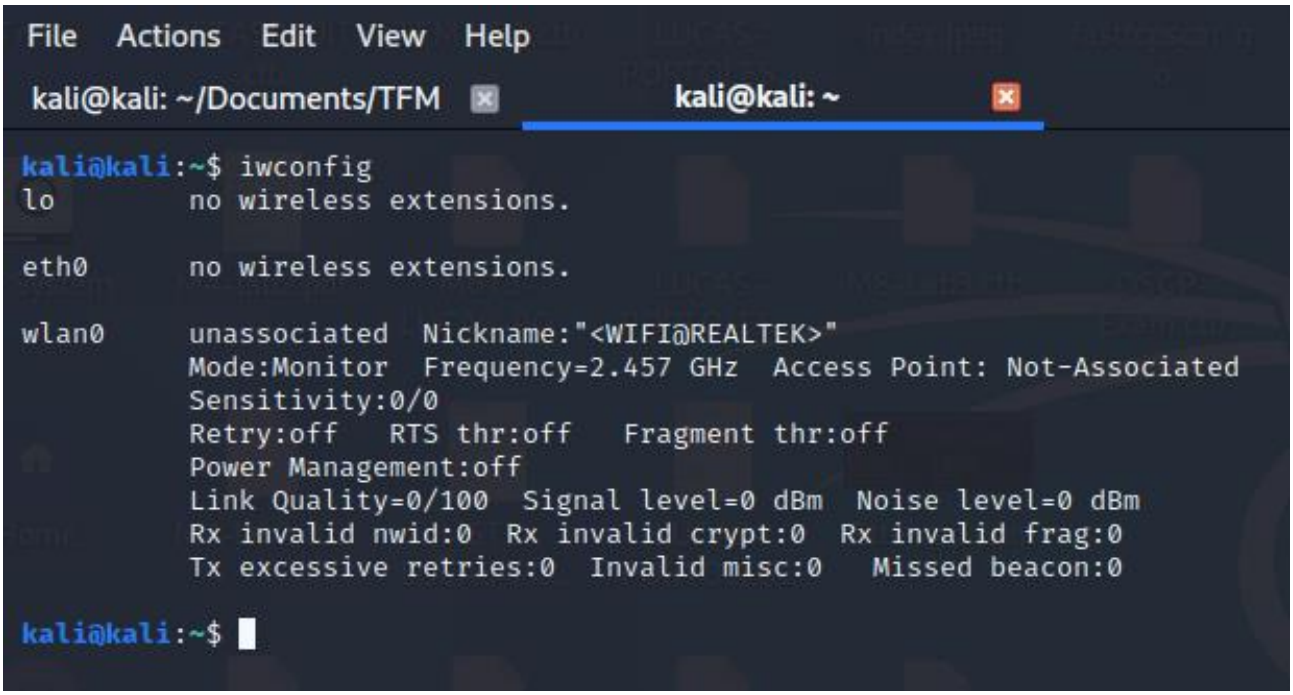
Auditor00 lo modificará aunque mientras lo hace guiará al usuario por los comandos necesarios para lograrlo.



Seguidamente eliminamos los procesos potencialmente conflictivos como nos recomienda la herramienta airmon-ng.



Y el modo monitor estará activado.



Si en otra terminal lo revisamos lo comprobaremos.

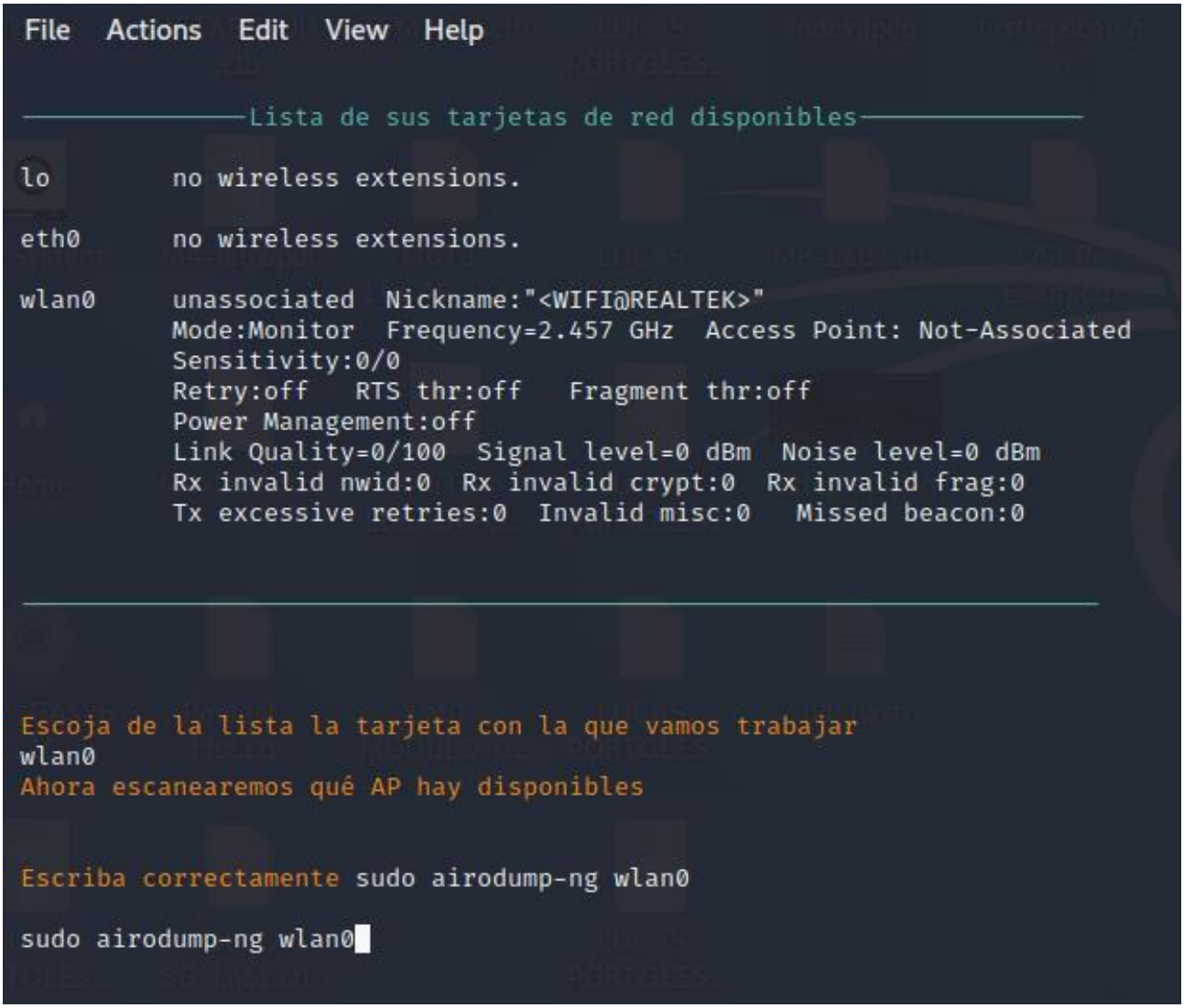
4- Ataque por deautenticación.

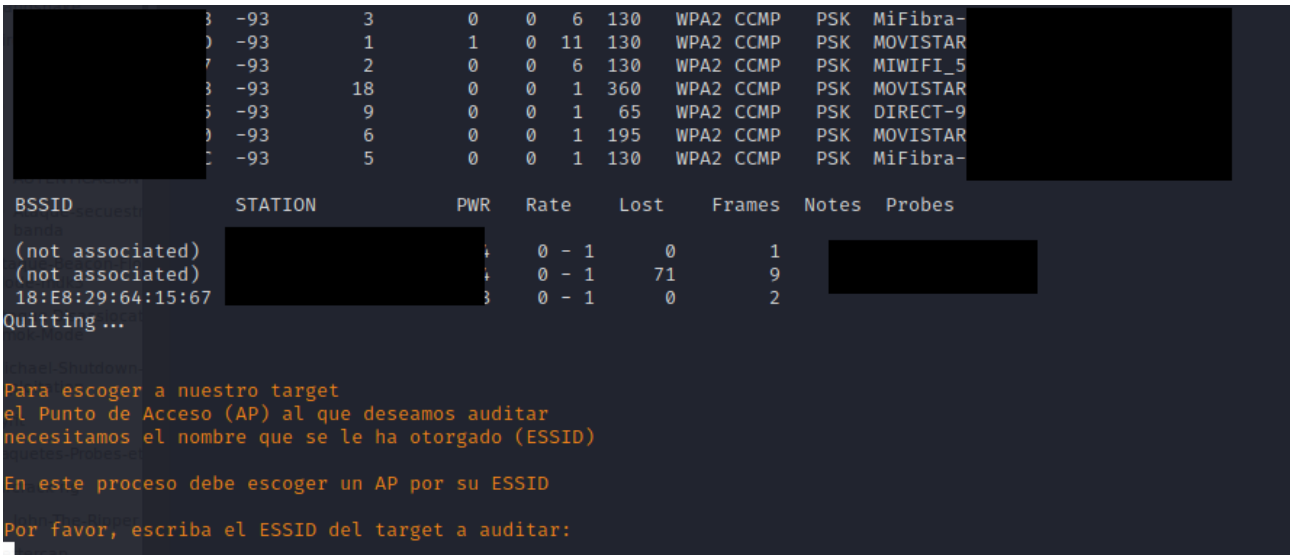
Este ataque envía paquetes de desasociación que se llevan a cabo a través de la herramienta aireplay-ng, con diversas intenciones:

- Localizar AP ocultos que se muestren al volver a asociarse.
- Generar peticiones ARP.
- Capturar handshakes WPA/WPA2 al reasociarse los clientes, para después trabajar con ellos offline.

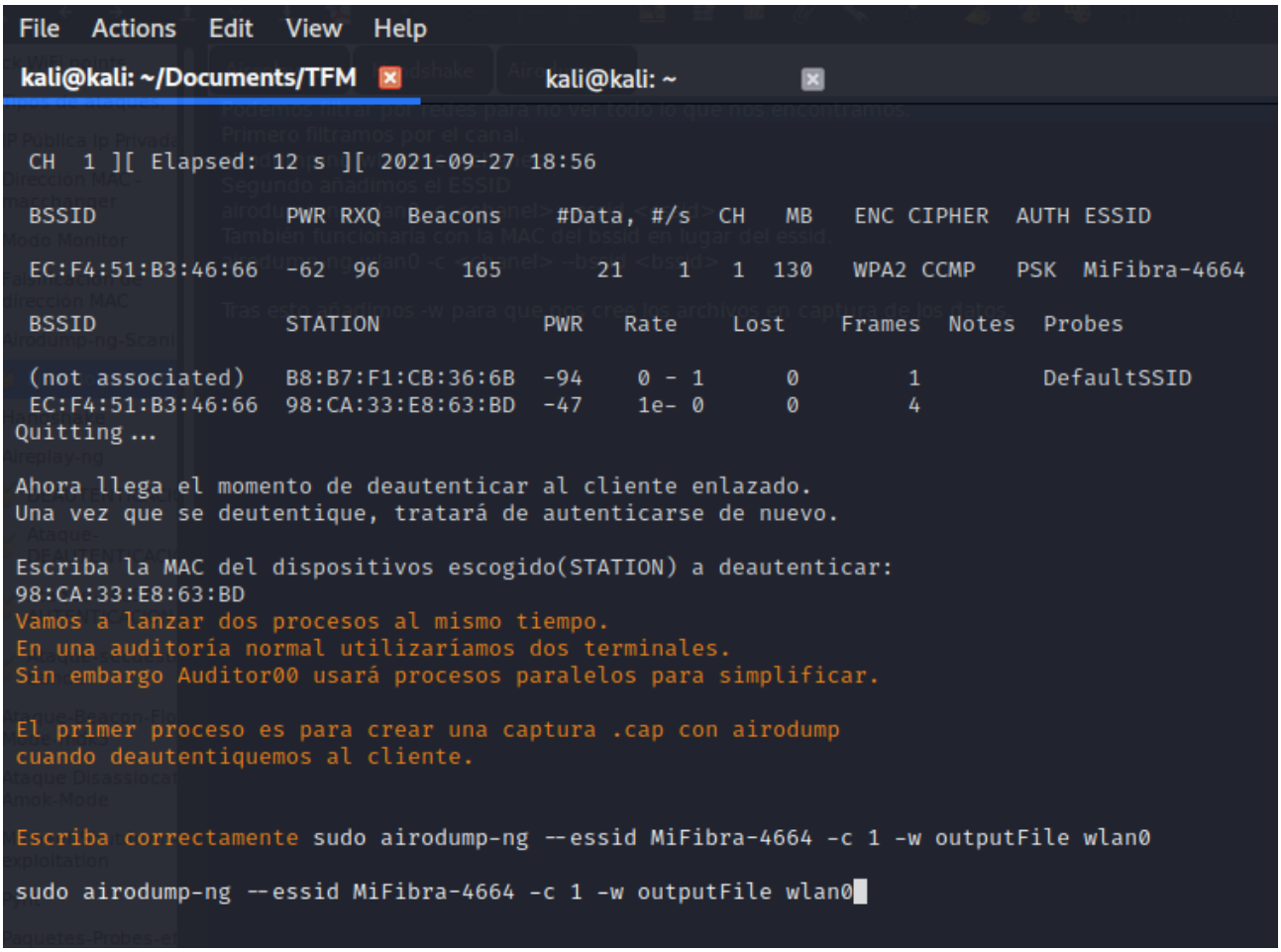
En concreto nosotros lo haremos por este último punto.

Primero escaneamos la red en busca del ESSID del AP que nos interesa.

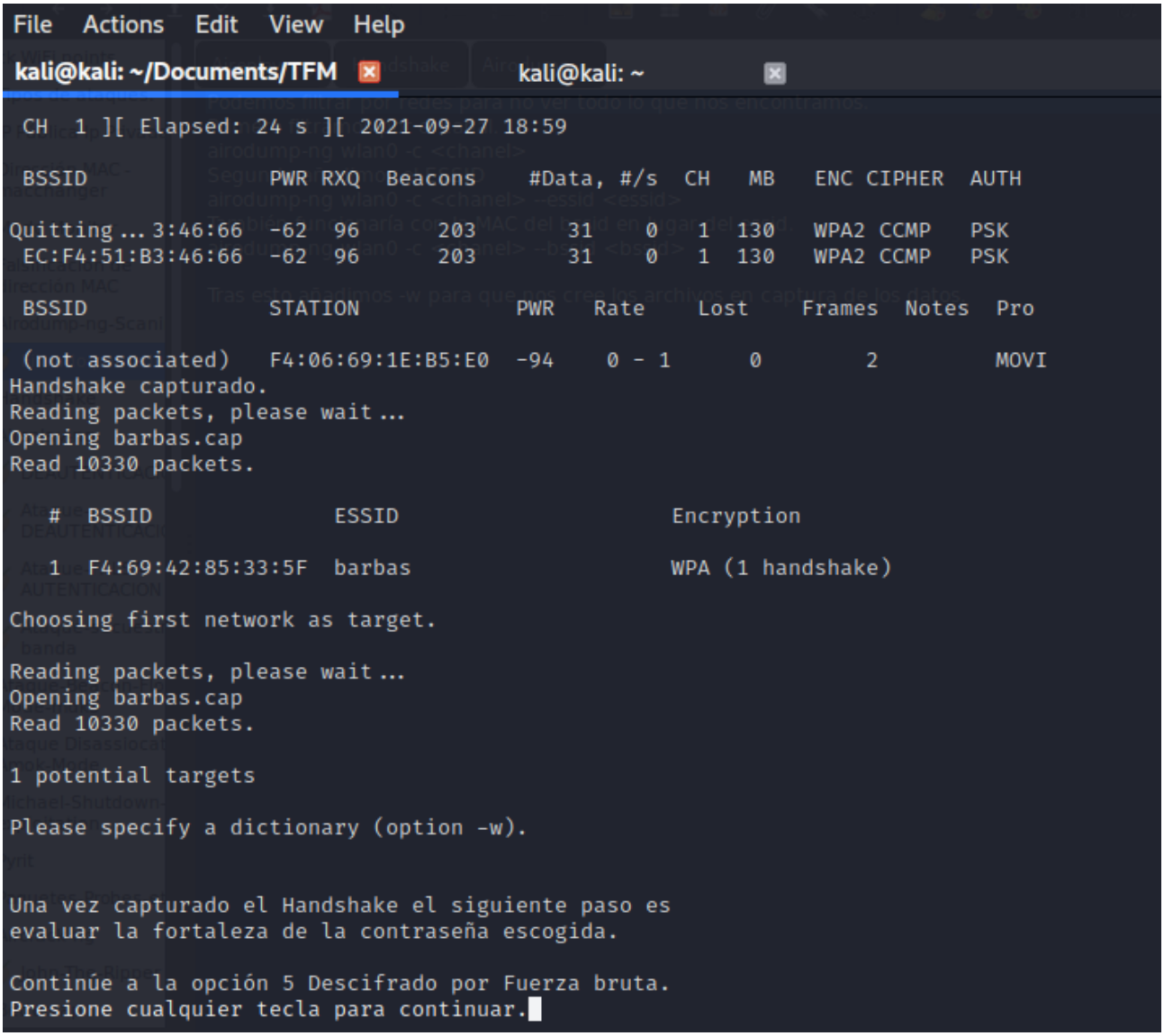




Escogemos un essid para desasociarlo.



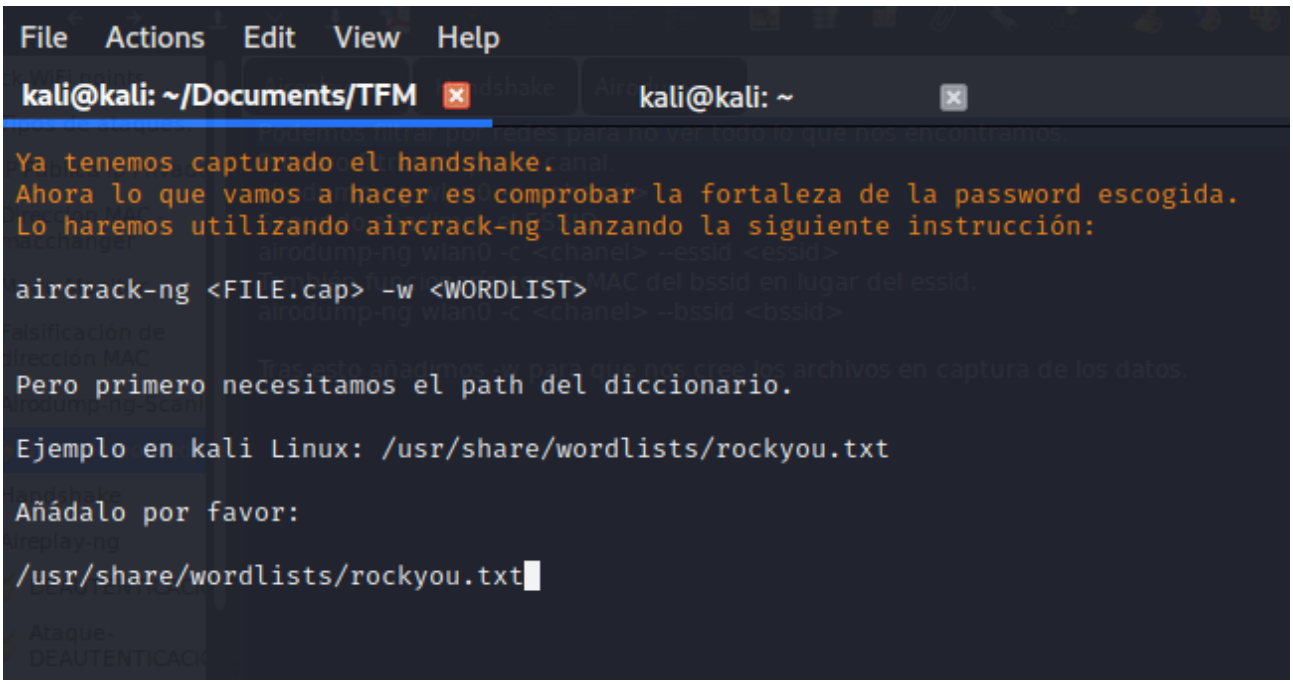
Lanzamos primero airodump-ng para lograr una captura y después airoplay-ng para desasociar al cliente y que luego se reconecte.

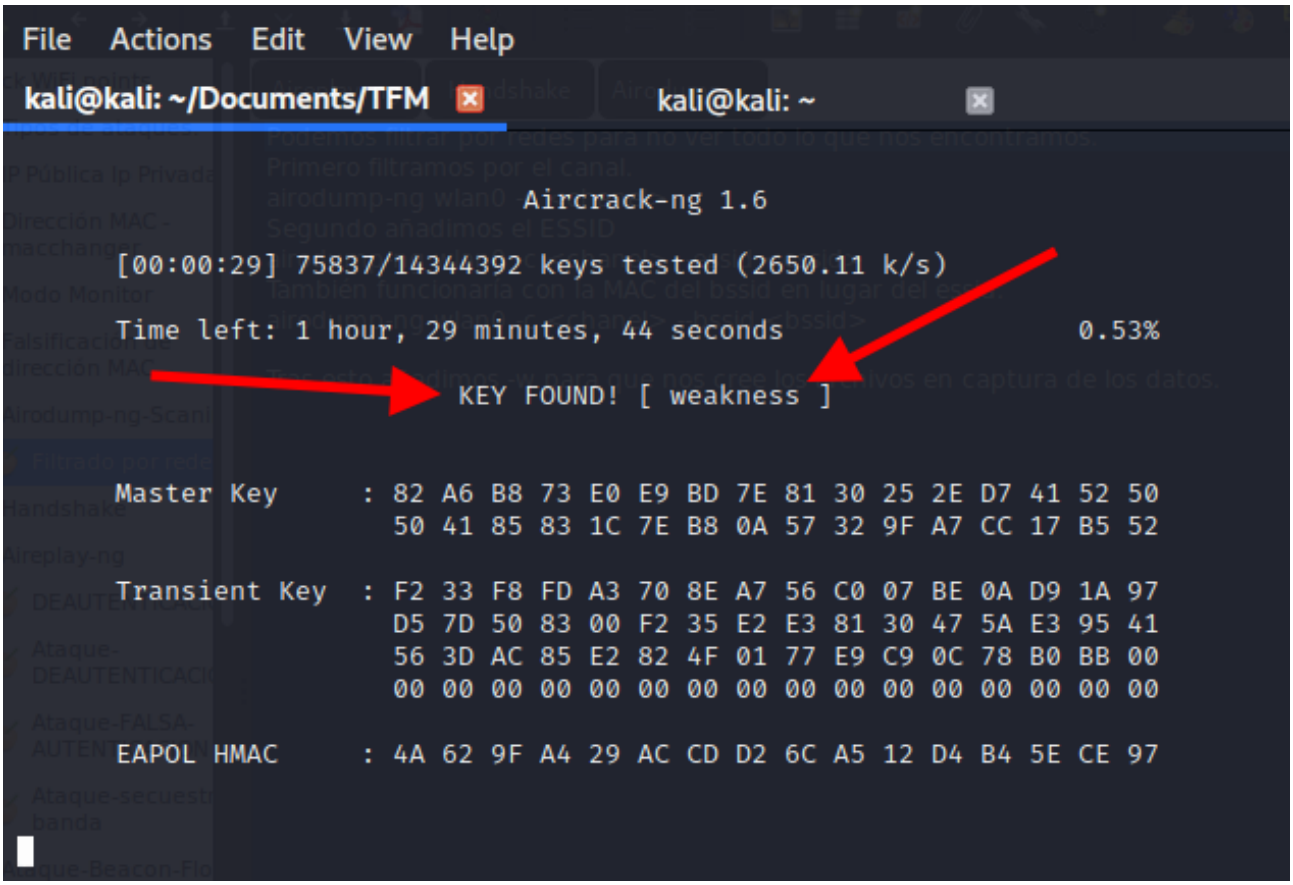


Lo hemos logrado. Al reconectarse hemos capturado el handshake.

5- Ataque por fuerza bruta.

Ahora utilizamos la herramienta Aircrack-ng para hacer una ataque de diccionario por fuerza bruta, offline, al handshake capturado en el apartado anterior.
Le pasaremos el diccionario más conocido dentro de Kali, rockyou.txt, para evaluar si la contraseña escogida es débil.





Tras 29 segundos tenemos éxito. La contraseña del WiFi es **weakness**.

Además, se ha creado un archivo <essid>.txt con la password capturada.

Incidencia con Auditor00.

Es posible encontrar alguna diferencia entre estas capturas y los vídeos de la demostración de la herramienta y esto se debe a que, terminando el trabajo, por algún error en la programación, se borró completamente el fichero y tuve que restaurar a partir de Git Hub una versión anterior que no era exactamente igual.

5 DEBILIDAD DE LA IP COMO PRUEBA.

No me adentraré mucho en este tema, pero como decía al principio de esta investigación, aún existen algunas sentencias y estamentos que consideran la IP pública una prueba incriminatoria, a pesar de que la sentencia número 987/2012 del Tribunal Supremo a 3 de diciembre de 2012, determinó que no era prueba suficiente para ello.

Europa defiende que se persiga e identifique a los piratas por su dirección IP

ACTUALIZADO 17/06/2021 12:14

El Tribunal de Justicia de la Unión Europea (TJUE) ha firmado una sentencia que concluye que se permite conocer el domicilio de una persona a través de su dirección IP (la que determina qué dispositivo está conectado a Internet).

Identificar clientes desde la dirección IP

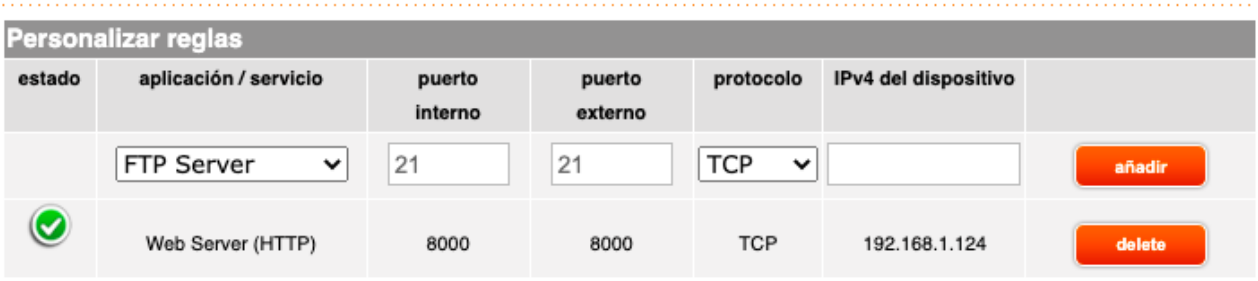
La demanda tenía por objeto o**btener una resolución que obligara a Telenet a proporcionar los datos de identificación de sus clientes** basándose en las direcciones IP recopiladas.

Las conexiones a Internet de ciertos clientes de Telenet se habían utilizado para compartir, a través de una red entre pares (peer-to-peer) y por medio del protocolo BitTorrent, películas incluidas en el catálogo de Mircom. Telenet se opuso a las pretensiones de Mircom.

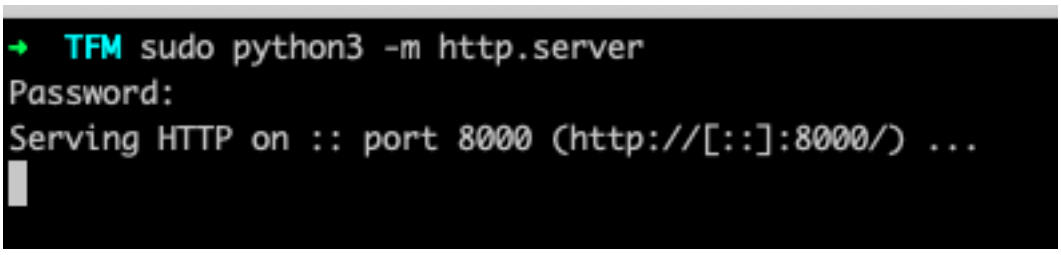
5.1 Utilización de la IP pública en la red WiFi vulnerada.

Una vez obtenidas las credenciales en la auditoría realizada con Auditor00, la IP de la red WiFi que hemos vulnerado, es ahora nuestra IP pública para salir a internet. Y cualquier acción ilegítima e ilegal que podamos llevar a cabo, quedará asociada a ella. Por tanto, una IP pública, que es muchas veces vulnerable, no debería tomarse como una prueba en un procedimiento judicial y únicamente debería tomarse como una evidencia.

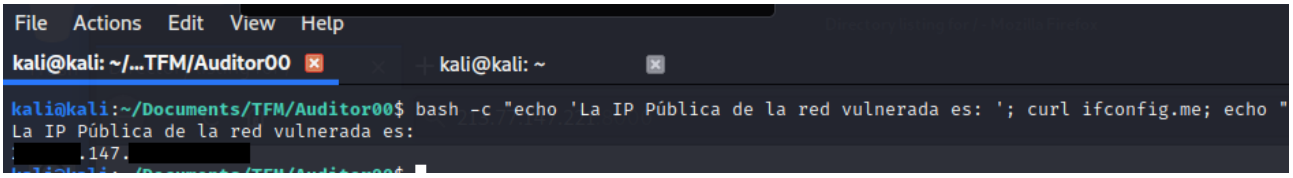
Como pequeña representación de esto, abrimos el puerto 8000 de una red doméstica:

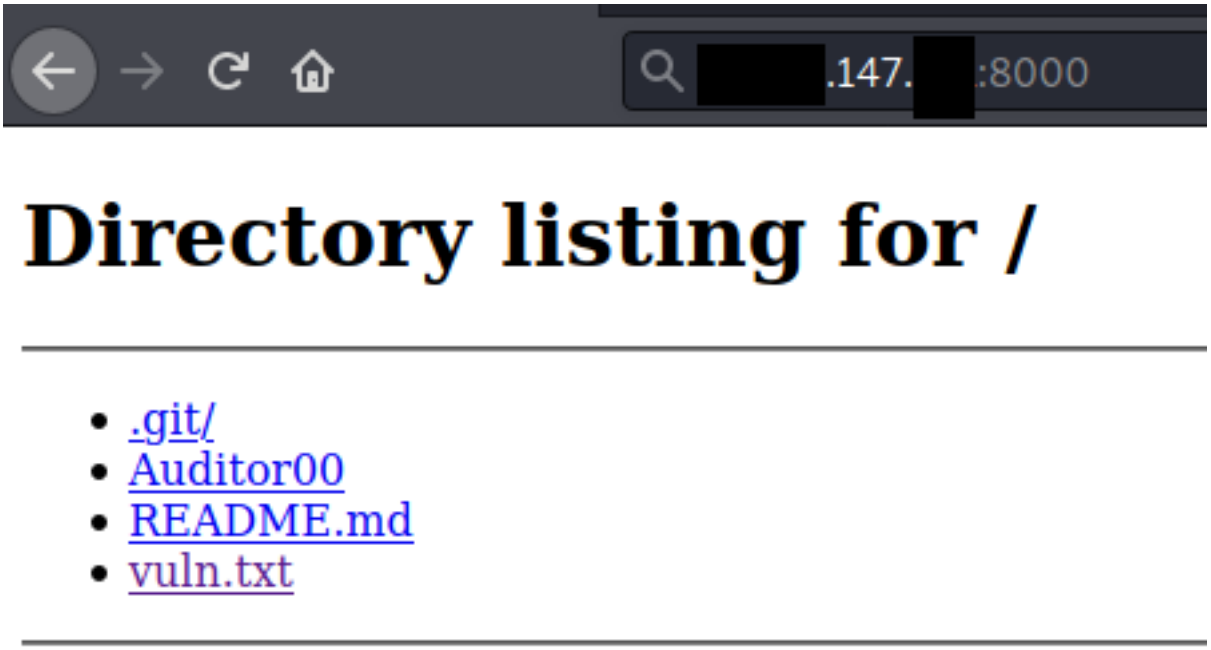


Y seguidamente levantamos un servidor http básico.

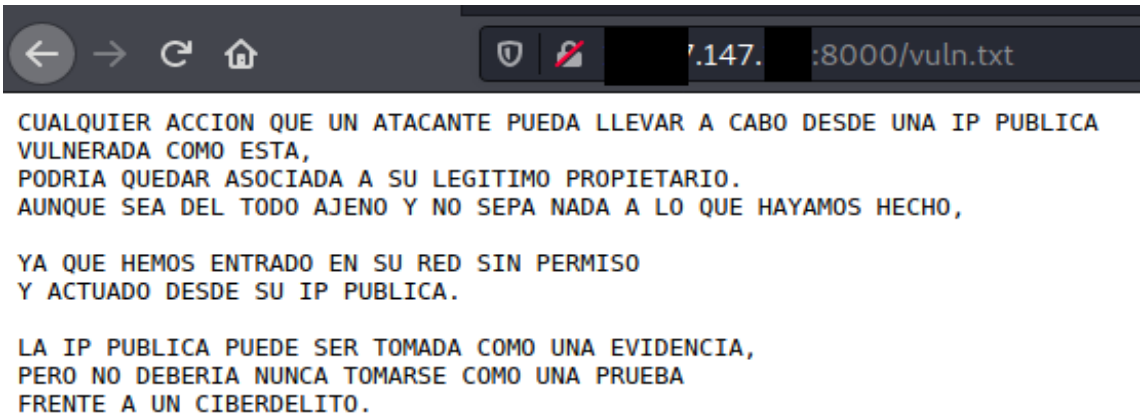


Ahora, accedemos con la contraseña **weekness** a la red vulnerada y comprobamos la IP (sólo muestro un bloque para que nadie me doxee).





Hacemos peticiones GET sencillas:



Y como vemos queda una muestra del rastro de logs:

6 LÍNEAS FUTURAS.

Como desarrollo de esta herramienta pedagógica, tengo intención cuando reúna un poco de tiempo de escalar Auditor00, añadiendo otro tipo de ataques.
Por ejemplo, para auditar el WPS a través de reaver.
También para levantar un Evil Twin y auditar por ejemplo a empleados despistados.
Para pasar un scanner de vulnerabilidades de router, como por ejemplo routersploit.
Para utilizar nmap por las redes vulneradas.
Creo que puede ser muy útil para estudiantes de ciberseguridad wireless que por ejemplo se preparen para la OSWP.

7 CONCLUSIONES.

Tras mi investigación, parece evidentemente probado lo que adelantaba al principio. Las redes WiFi suelen ser inseguras, principalmente por una descuidada configuración aunque no sólo por ello. No son necesarios complejos conocimientos para adentrarse en algunas redes y una vez en ellas, comprometer máquinas, enrutadores, etc. Como muestro con Auditor00, puede ser sencillo aprender a comprometer una red por vulnerabilidades como la configuración de contraseñas débiles y en mi propia experiencia (siempre en entornos en los que se me ha autorizado) he tenido éxito intentándolo en numerosas ocasiones.
Tras el presente trabajo, adquirí un router neutro HUAWEI para proteger un área sensible de mi empresa creando una subred y como no era viable deshabilitar el WiFi por cuestiones operativas, tomé algunas medidas como deshabilitar el WPS, configurar contraseñas robustas y otras medidas de mitigación, como la creación de un registro de logs, del que generalmente los router domésticos y los que proporcionan las operadoras, no disponen, y una revisión periódica del registro de los dispositivos que se han conectado a la subred y de alertas por email de enlace de nuevos dispositivos. Además creé alertas con avisos de revisión del firmware, para revisar las actualizaciones. Y mi intención es crear un firewall interno que controle los movimientos dentro de la red, para prevenir movimientos laterales.
Tanto las empresas, como los particulares, deberíamos concienciarnos de lo vulnerables y peligrosas que están siendo nuestras redes WiFi y que el hecho de que no sea un vector de entrada habitual, no debería llevar a pensar que los ataques sólo pueden perpetrarse de manera remota.

8 BIBLIOGRAFÍA:

https://concepto.de/red-2/

https://es.wikipedia.org/wiki/Wifi

Seguro no lo sabías, WiFi es una marca y no un servicio.

https://www.excelsior.com.mx/hacker/seguro-no-lo-sabias-wifi-es-una-marca-y-no-un-servicio/1252709

Aircrack-ng

https://es.wikipedia.org/wiki/Aircrack-ng

Aircrack-ng

https://studylib.es/doc/783596/%C2%BFqu%C3%A9-es-aircrack-ng%3F

Wash

https://en.kali.tools/?p=341

HACKEAR LA CONTRASEÑA DE WPA WIFI / WPA2 USANDO REAVER SIN LISTA DE PALABRAS

https://noticiasseguridad.com/importantes/hackear-la-contrasena-de-wpa-wifi-wpa2-usando-reaver-sin-lista-de-palabras/

Netstumbler

https://www.seguridadwireless.net/netstumbler/#

Análisis NetStumbler

https://www.usitility.com/es/netstumbler/

NetStumbler

https://es.wikipedia.org/wiki/NetStumbler

Kismet

https://www.kismetwireless.net/#plugins

Kismet

https://es.wikipedia.org/wiki/Kismet

Pentesting WiFi: Usando Kismet para ver la actividad de un usuario de Wi-Fi a través de las paredes

https://securityhacklabs.net/articulo/usando-kismet-para-ver-la-actividad-de-un-usuario-de-wi-fi-a-traves-de-las-paredes

KISMET

https://www.seguridadwireless.net/kismet/

coWPAtty Download – Audit Pre-shared WPA Keys

https://www.darknet.org.uk/2017/12/cowpatty-audit-pre-shared-wpa-keys/

Como hackear redes wifi con Cowpatty

https://enablehack.wordpress.com/2017/06/24/como-hackear-redes-wifi-con-cowpatty/
coWPAtty Package Description
https://tools.kali.org/wireless-attacks/cowpatty
CoWPAtty, para usar desde un terminal Linux
https://www.softzone.es/programas/utilidades/mejores-herramientas-hacking-etico-wi-fi/
Caín y Abel (software)
https://es.wikipedia.org/wiki/Ca%C3%ADn_y_Abel_(software)
IEEE 802.11
https://es.wikipedia.org/wiki/IEEE_802.11
La historia del WiFi
https://purple.ai/es/blogs/la-historia-del-wifi/
Hedy Lamarr, la actriz que inventó el wifi.
https://historia.nationalgeographic.com.es/a/hedy-lamarr-actriz-que-invento-wifi_14882
¿Conoces la evolución del WIFI?
https://www.optical.pe/blog/conoces-la-evolucion-del-wifi/
Orígenes, ventajas y desventajas del Wi-Fi
https://guiauniversitaria.mx/origenes-ventajas-y-desventajas-del-wi-fi/
20 años de conexiones inalámbricas
https://www.computerworld.es/tecnologia/20-anos-de-conexiones-inalambricas
Protégete al usar WiFi públicas.
https://www.osi.es/es/wifi-publica
Algoritmos de cifrado en redes wifi.
http://agrega.juntadeandalucia.es/repositorio/02122016/90/es-an_2016120212_9110913/31_algoritmos_de_cifrado_en_redes_wifi.html
Protocolos de seguridad inalámbrica.
https://www.netspotapp.com/es/wifi-encryption-and-security.html
RC4.
https://es.wikipedia.org/wiki/RC4
Caos en la seguridad WiFi: un repaso a las vulnerabilidades de WEP, WPA, y WPA2
https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2
Seguridad WEP.
https://wikis.fdi.ucm.es/ELP/Trabajo:Seguridad_WEP
Temporal Key Integrity Protocol.
https://es.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol
Las diferencias entre WPA-Personal y WPA-Enterprise.

https://www.tp-link.com/ar/support/faq/500/
What Does Wi-Fi Protected Access-Enterprise (WPA Enterprise) Mean?
https://www.techopedia.com/definition/29074/wi-fi-protected-access-enterprise-wpa-enterprise
Cómo Funciona la Autenticación del servidor RADIUS
https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/authentication/radius_how_works_c.html
Problemas de seguridad en múltiples implementaciones RADIUS
https://unaaldia.hispasec.com/2002/03/problemas-de-seguridad-en-multiples-implementaciones-radius.html
WPA2
https://es.wikipedia.org/wiki/WPA2
Advanced Encryption Standard
https://es.wikipedia.org/wiki/Advanced_Encryption_Standard#Seguridad
Encriptación: ¿qué tan seguro es AES?
http://www.dataqubo.com/encriptacion-que-tan-seguro-es-aes/
Cifrado AES-256
https://www.boxcryptor.com/es/encryption/
WPA2 – Enterprise seguridad en las redes inalámbricas de tu empresa
https://grupogaratu.com/wpa2-enterprise-seguridad-en-las-redes-inalambricas-de-tu-empresa/
WPA3
https://es.wikipedia.org/wiki/WPA3
¿En qué se diferencia la seguridad WiFi WPA3 de WPA2?
https://www.xataka.com/basics/que-se-diferencia-seguridad-wifi-wpa3-wpa2
Wireshark
https://es.wikipedia.org/wiki/Wireshark
Firesheep: Add-on the Firefox que permite el hijacking de sessiones HTTP
https://www.welivesecurity.com/la-es/2010/10/27/firesheep-add-on-the-firefox-que-permite-el-hijacking-de-sessiones-http/
Riesgos asociados a las redes Wi-Fi públicas: cuáles son y cómo prevenirlos
https://www.welivesecurity.com/la-es/2019/02/05/riesgos-asociados-redes-wi-fi-publicas/
Paso a paso de cómo crackear WEP
https://medium.com/hacking-info-sec/paso-a-paso-de-c%C3%B3mo-crackear-wep-en-3-minutos-aec9e1d0d0b1
ETIQUETA: PROBE RESPONSE

https://notasinalambricas.wordpress.com/tag/probe-response
El malvado Evil Twin.
https://www.ventasdeseguridad.com/20080417951/articulos/analisis-tecnologico/el-malvado-evil-twin.html
REALIZAR UN ATAQUE EVIL TWIN PARA CAPTURAR CLAVES WI-FI CON WIFIPHISHER
https://origendata.com/2018/01/11/realizar-un-ataque-evil-twin-para-capturar-claves-wi-fi-con-wifiphisher/
¿En qué se diferencia la seguridad WiFi WPA3 de WPA2?
https://www.xataka.com/basics/que-se-diferencia-seguridad-wifi-wpa3-wpa2
¿Qué es el WPS y cómo funciona?
https://www.redeszone.net/tutoriales/redes-wifi/wps-que-es-como-funciona/
Qué es WPS Pin y por qué debes desactivarlo
https://www.osi.es/es/actualidad/blog/2014/11/07/que-es-wps-pin-y-por-que-debes-desactivarlo
Wi-Fi Protected Setup
https://es.wikipedia.org/wiki/Wi-Fi_Protected_Setup
Entendiendo cómo funciona el ataque Pixie-Dust
https://securityhacklabs.net/articulo/hackeando-redes-wifi-wpa-y-wpa2-protegidas-con-contrasena
PixieWPS
https://en.kali.tools/?p=334
Reaver Package Description
https://tools.kali.org/wireless-attacks/reaver
Bully Package Description
https://tools.kali.org/wireless-attacks/bully
Aireplay-ng
https://www.aircrack-ng.org/doku.php?id=aireplay-ng
Krack Wpa2 no hackea la contraseña WiFi
https://www.siliceo.es/krack-wpa2-contrasena-wifi-password/
¿Qué es el KRACK?
https://www.kaspersky.es/resource-center/definitions/krack
Aclarando KRACK Attack, la vulnerabilidad descubierta en WPA2
https://www.welivesecurity.com/la-es/2017/10/27/aclarando-krack-attack-wpa2/
Kr00k: así actúa la nueva vulnerabilidad crítica en chips WiFi que compromete millones de dispositivos

https://www.xataka.com/seguridad/kr00k-asi-actua-nueva-vulnerabilidad-critica-chips-wifi-que-compromete-millones-dispositivos

ATAQUE BEACON FLOOD

https://mundo-hackers.weebly.com/beacon-flood.html

Beacon Flooding Attack

https://medium.com/infosec-adventures/beacon-flooding-attack-a4baadc2242b

Nuevo ataque permite hackear WPA2 en pocos pasos

https://mejor-antivirus.es/noticias/nuevo-ataque-permite-hackear-wpa2-en-pocos-pasos.html

Ataque clientless a WPA/WPA2 usando PMKID

https://medium.com/hacking-info-sec/ataque-clientless-a-wpa-wpa2-usando-pmkid-1147d72f464d

Aircrack-ng - Deautenticación

https://www.aircrack-ng.org/doku.php?id=es:deauthentication