Examen WIFI

Pasos para wifi no oculto:

1.$sudo ifconfig wlan0 down

2.$sudo macchanger –a wlan0

3.$sudo iwconfig wlan0 mode monitor

4.$sudo ifconfig wlan0 up

5.$sudo airodump-ng wlan0

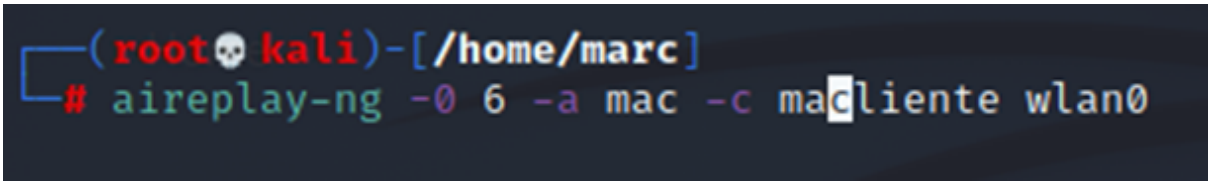
6. Fet això identificar la xarxa victima, apuntar-nos el seu BSSID, el canal que utilitza i identificar si el mètode de encriptació és vulnerable o no. (tots vulnerables menys WPA3).

El següent pas serà capturar el handshake.

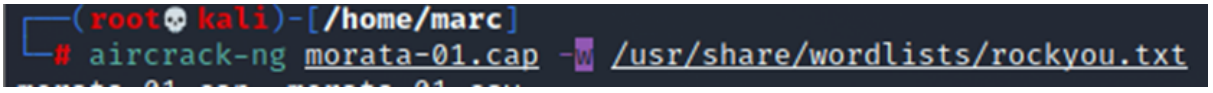
7.

-c(channel) –bssid (bssid) -w (arxiu on es guradarà el handshake)

8.Si li costa capturar el handshake haurem de tirar un client amb la següent comanda.



9.Una vegada capturat correctament el handshake.



Generación de diccionarios i cracking de hashes:

En aquest apartat del tema realitzarem atacs a hashes utilitzant principalment l'eina de crackeig de contrasenyes hashcat combinada amb eines de creació de diccionaris, regles i màscares.

-Passos a seguir:

1.Obtenció de Hashes

1)Capturar els valors de hash de l'objectiu

2)Identificar la funció de hash utilitzada

2.Formatejar Hashes

1)Adequar el format de hash a l'aplicació de cracking

3.Avaluar la complexitat del Hash

1)Revisar les taules disponibles de velocitat de cracking de hash per tal d'obtenir la mesura que determinarà la complexitat del hash a atacar

Caclcular la nostra capacitat de Cracking hashcat -b

5.Atac Personalitzat

1)Crear atacs personalitzats basant-nos en la informació del punt anterior.

2)Utilitzar atacs basats en màscares o en regles detectades amb la combinació de diccionaris.

7.Repetir Fase Atac

Pla d'atac

1) **Atac de Diccionari a Mida**

```
hashcat -a 0 -m 0 -w 4 hash.txt customlist.txt
```

-a → attack-mode (0=directe) -m → hash-type (0 = md5) -w → workload-profile (4 = Nightmare)

2) **Atac de Diccionari a Mida + Regles**

```
hashcat -a 0 -m 0 -w 4 hash.txt customlist.txt -r best64.rule --loopback
```

-r → rules --loopback → reutilitza passwords que ja han crackejat un hash

3) **Atac de Diccionari Clàssic**

```
hashcat -a 0 -m 0 -w 4 hash.txt wordlist.txt
```

4) **Atac de Diccionari Clàssic + Regles**

```
hashcat -a 0 -m 0 -w 4 hash.txt wordlist.txt -r best64.rule --loopback
```

5) **Atac de Diccionari a Mida + Regles (Round 2!)**

Afegim passwords descobertes al diccionari per atacar de nou amb permutes sobre el que hem trobat.

```
awk -F ":" '{print $2}' hashcat.potfile >> customlist.txt
hashcat -a 0 -m 0 -w 4 hash.txt customlist.txt -r best64.rule --loopback
```

Pla d'atac

6) Atac de Màscara

Ataquem per força bruta utilitzant patrons i longituds de contrasenya habituals basat en el rockyou.

```
hashcat -a 3 -m 0 -w 4 hash.txt rockyou-1-60.hcmask
```

-a → attack-mode (3=bruteforce) -m → hash-type (0 = md5) -w → workload-profile (4 = Nightmare)

7) Atac Híbrid de Màscara i Diccionari Clàssic

Utilitzant un diccionari clàssic, conduïm atacs híbrids buscant variacions de passwords comuns, emprant màscares que s'afegeixen pel principi o pel final.

```
hashcat -a 6 -m 0 -w 4 hash.txt wordlist.txt rockyou-1-60.hcmask
hashcat -a 7 -m 0 -w 4 hash.txt rockyou-1-60.hcmask wordlist.txt
```

-a → attack-mode (6=Hybrid Wordlist + Mask, 7=Hybrid Mask + Wordlist)

8) Atac de Diccionari a Mida + Regles (Round 3!)

Afegim passwords descobertes al diccionari a mida per atacar de nou amb permutes sobre el que hem trobat.

```
awk –F ":" '{print $2}' hashcat.potfile >> customlist.txt
hashcat -a 0 -m 0 -w 4 hash.txt customlist.txt –r dive.rule --loopback
```

9) Atac de Combo

Atac de diccionari basat en combinacions de les paraules incloses en el propi diccionari

```
hashcat -a 1 -m 0 -w 4 hash.txt wordlist.txt wordlist.txt
```

-a → attack-mode (1=Combination)

Pla d'atac

10) Atac Híbrid a Mida

Afegim passwords descobertes al diccionari per atacar de nou amb un atac híbrid amb diccionari a mida

```
awk –F ":" '{print $2}' hashcat.potfile >> customlist.txt
hashcat -a 6 -m 0 -w 4 hash.txt customlist.txt rockyou-1-60.hcmask
hashcat -a 7 -m 0 -w 4 hash.txt rockyou-1-60.hcmask customlist.txt
```

11) Atac de Màscara a Mida

Arribats a aquest punt, totes les contrasenyes dèbils haurien d'haver caigut, però en poden quedar encara algunes. Prenent com a punt de partida les passwords descobertes, identifica patrons i genera un conjunt de màscares a mida per atacar de nou. Descarta aquelles màscares ja incloses en el rockyou-1-60.hcmask.

```
hashcat -a 3 -m 0 -w 4 hash.txt customs_masks.hcmask
```

12) Atac de Força Bruta

Si tot lo anterior ha fallat, sols queda una cosa: la força bruta. Aquí cal que siguis conscient de la potència de càlcul de la que disposes i de la mida de l'espai de claus, ja que altrament l'atac pot resultar totalment inviable. Com a regla general, per longituds per sobre dels 8 caràcters qualsevol atac per força bruta resulta estèril.

```
hashcat -a 3 -m 0 -w 4 hash.txt –i ?a?a?a?a?a?a?a?a
```

-Eines per la creació de diccionaris:

A.Crunch (https://tools.kali.org/password-attacks/crunch)

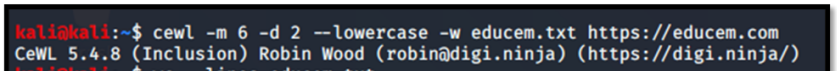
1.Permet generar diccionaris per atacs de força bruta.

2.Permet definir alfabets, màscares i longituds, així com combinar amb cadenes fixes.

B.**CeWL** (https://tools.kali.org/password-attacks/cewl)

1.Permet generar diccionaris a partir de paraules obtingudes de la web.

2.Permet indicar profunditat de cerca, longitud mínima de paraula, transf. a mínúsc…



C.**Mentalist** (https://github.com/sc0tfree/mentalist)

1.Permet generar diccionaris basats en permutacions i combinacions freqüents.

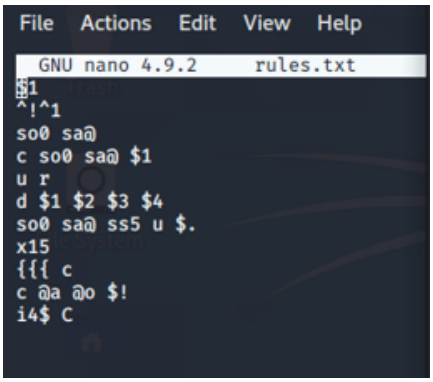
2.Permet configurar les regles desitjades i combinar-les com calgui.

-Creació de regles:

Nom	Funció	Descripció
Nothing	:	No fer res
Lowercase	l	Passa a minúscules totes les lletres de la paraula.
Uppercase	u	Passa a majúscules totes les lletres de la paraula.
Capitalize	c	Passa a majúscula la primera lletra de la paraula i la resta a minúscules.
Invert Capitalize	C	Passa a minúscula la primera lletra de la paraula i la resta a majúscules.
Toggle Case	t	Passa a majúscules les lletres en minúscules de la paraula i viceversa.
AppendChar	$X	Afegeix al final de la paraula el carácter X.
PrependChar	^X	Afegeix al principi de la paraula el carácter X.
Replace	sXY	Substitueix totes les aparicions del caràcter X a la paraula pel caràcter Y.
Reverse	r	Capgira la paraula sencera.
Duplicate	d	Duplica la paraula sencera.

Nom	Funció	Descripció
Truncate left	[	Elimina el primer caràcter
Truncate right	]	Elimina el darrer caràcter
Rotate left	{	Rota els caràcters de la paraula a l'esquerra
Rotate right	}	Rota els caràcters de la paraula a la dreta
Extract range	xNM	Extreu M caràcters a partir de la posició N a la paraula.
Sobreescriu @ N	oNX	Sobreescriu el caràcter a la posició N de la paraula per X.
Truncate @ N	'N	Trunca la paraula a la posició N
Insert @ N	iNX	Insereix el caràcter X a la posició N de la paraula.
Esborra @ N	DN	Esborra el caràcter existent a la posició N de la paraula
Toggle @	TN	Inverteix majúscules/minúscules al caràcter a la posició N de la paraula.
Purge	@X	Elimina totes les aparicions del caràcter X a la paraula.

Paraula	Regla	Sortida
password	$1	password1
password	^!^1	1!password
password	so0 sa@	p@ssw0rd
password	c so0 sa@ $1	P@ssw0rd1
password	u r	DROWSSAP
password	d $1 $2 $3 $4	passwordpassword1234
password	so0 sa@ ss5 u $.	P@55W0RD.
password	x15	asswo
password	{{{ c	Swordpas
password	c @a @o $!	Psswrd!
password	i4$ C	pASS$WORD



-Creació de màscares:

Símbol	Long. Alfabet	Alfabet
?l = lowercase	26 chars	abcdefghijklmnopqrstuvwxyz
?u = uppercase	26 chars	ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d = digits	10 chars	0123456789
?s = special	33 chars	<<space>>!"#$%&'()*+,-./:;<=>?@[\]^_`{\}~
?a = all	95 chars	lowercase+uppercase+digits+special
?h = hex	16 chars	0123456789abcdef
?H = HEX	16 chars	0123456789ABCDEF
?b = byte	256 byte	0x00 – 0xff