Crack

#Possible Hash - in Kali

hash-identifier

2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03

#with John

john --rules --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

#hash p/ whireless

aircrack-ng Net_Adao-01.cap -J john
hccap2john john.hccap > wap

Sintaxe usando crunch/Jhon/aircrack-ng:

Crunch 8 8 | john --session=session1 | aircrack-ng -b [bssi do alvo] -w - handshake-01.cap

crunch 8 8 | john --stdin --session=session1 --stdout | aircrack-ng -b [bssi do alvo] -w - handshake-01.cap

Outras sintaxes:

john pass.db

john --single pass.db

john --single '/home/morgan/Documentos/interceptor/Net_Adao/wpa'

john --wordlist=wordlist.txt pass.db

john --show senha.db

john --incremental [arquivo wpa]

#Ignorando Shells invalidas

O John vai passar por todas senhas e ignorar as apresentadas no comando.

john --shells=-/bin/false pass.db

#Especificando o numero de saltos - Neste caso o John vai tentar quebrar as senhas com os tamanhos pre definidos na sintaxe

john --salts 8 pass.db

(default)
john --wordlist=/home/morgan/Documentos/wordlist-02.mate/WiFi-WPA/probable-v2-wpa-top4800.txt /home/morgan/Documentos/wpa

#with Hashcat

hashcat -m 13100 -a 0 hash.txt /usr/share/wordlists/rockyou.txt --force

#with Online

https://crackstation.net/