Workshop: Comandos y Retos - Mifare Classic 1K

Comandos Útiles

- hf search # Buscar tarjeta en el lector
- hf mf autopwn # Ataques automáticos para descubrir claves
- hf mf dump # Descargar todos los sectores
- hf mf chk # Mostrar claves A y B conocidas
- hf mf wrbl -b <bloque> -k <clave> -d <hex> # Escribir en un bloque
- hf mf rdbl -b <bloque> -k <clave> # Leer un bloque específico
- hf mf csetuid <nuevo_uid> # Cambiar UID (solo tarjetas chinas)
- hf mf restore # Restaurar volcado en tarjeta virgen
- hf mf info # Mostrar detalles y claves de la tarjeta
- hf mf nested / hf mf hardnested # Ataques para obtener claves de sectores

Retos del Workshop

- Challenge 1: Leer el UID de tu tarjeta y anotarlo.
- Challenge 2: Escribir 'HackCon2025' en el bloque 8.
  - Comando: hf mf wrbl -b 8 -k ffffffffffff -d 4861636b436f6e32303235
- Challenge 3: Leer el bloque 8 y verificar que se escribió correctamente.
  - Comando: hf mf rdbl -b 8 -k ffffffffffff
- Challenge 4: Clonar una tarjeta facilitada por el instructor.
- Challenge 5: Cambiar el UID de una tarjeta china a uno que termine en '42'.
- Challenge 6: Hacer un dump completo y restaurarlo en otra tarjeta.
- Challenge 7: Recuperar la clave de un sector usando hardnested.

Hoja de Respuestas

- Challenge 1: UID leído: _____
- Challenge 2: Comando usado: _____
- Challenge 3: Salida esperada del bloque: _____
- Challenge 4: UID clonado: _____
- Challenge 5: Nuevo UID: _____
- Challenge 6: Archivo dump usado: _____
- Challenge 7: Sector atacado: ____ Clave recuperada: ____