MANUAL RÁPIDO DE USO DE JOHN THE RIPPER

1. Creamos tres usuarios para probar.

sudo adduser alumno-single
sudo adduser alumno-dic
sudo adduser alumno-brute

con sus respectivas contraseñas:

sudo passwd alumno-single -> alumno
sudo passwd alumno-dic -> estrella (o cualquier palabra a elegir)
sudo passwd alumno-brute -> 132

2. Instalamos John the ripper (en Kali ya está instalado)

sudo apt-get install john

3. Configuramos John con un diccionario

1. Bajarse un diccionario: english de Openwall (wordlists languages Spanish)
   - Se podría modificar el diccionario y agregar alguna contraseña

   Importamos la SAM

2. unshadow /etc/passwd
/etc/shadow

Verlo

3. unshadow /etc/passwd /etc/shadow >

mypasswd

4. Intentamos los tres tipos de ataques:

1) SINGLE

john -single -format=crypt -user=alumno-single mypasswd

2) DICCIONARIO (usamos el diccionario en español bajado de Openwall)

john -format=crypt -user=alumno-dic -wordlist=lower.lst mypasswd

(o -w=lower.lst)

3) INCREMENTAL (FUERZA BRUTA)

john -format=crypt -incremental:digits -user=alumno-brute mypasswd

NOTA: modificar antes el /etc/john/john.conf, la línea donde pone formas dígits

minlen=3 maxlen=3) Si no, tardaría mucho.

Opciones para el ataque por fuerza bruta:

-incremental=*alpha* – Letters only.
-incremental=*digits* – Numbers only.
-incremental=*lanman* – Letters, numbers, and some special characters.
-incremental=*all* – All possible characters.

INSERTAR PANTALLAZOS CON LAS TRES CONTRASEÑAS DESCIFRADAS (john --show mypasswd)