MANUAL RÁPIDO DE USO DE JOHN THE RIPPER

1. Creamos tres usuarios para probar.

sudo useradd alumno-single
sudo useradd alumno-dic
sudo useradd alumno-brute

con sus respectivas contraseñas:

sudo passwd alumno-single -> alumno
sudo passwd alumno-dic -> always
sudo passwd alumno-brute -> 132

2. Instalamos John the ripper (se puede bajar de openwall.com y compilarlo, o a través de apt en Ubuntu)

sudo apt-get install john

Configuramos John con un diccionario

2. Bajarse un diccionario: english de Openwall (wordlists languages English tiny)
    - Se podría modificar el diccionario y agregar alguna pass

Importamos la SAM

3. unshadow /etc/passwd /etc/shadow
verlo
4. unshadow /etc/passwd /etc/shadow > mypasswd

Intentamos los tres tipos de ataques:

1) SINGLE

john -single -user=alumno-single mypasswd

2) DICCIONARIO

john -user=alumno-dic -wordlist="lower.lst" mypasswd (o -w=lower.lst)

3) INCREMENTAL (FUERZA BRUTA)

john -incremental:digits -format=crypt -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.