

hACKING éTICO

Unidad 3. Actividad 1



13 de marzO de 2024

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

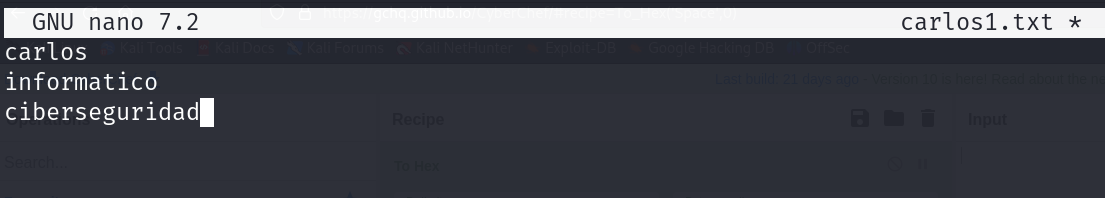
Índice

[Crea tus propios diccionarios 2](#_Toc161252143)

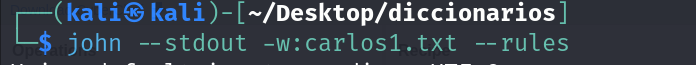
# Crea tus propios diccionarios

**Ejercicio 1: Crea tu primer diccionario**

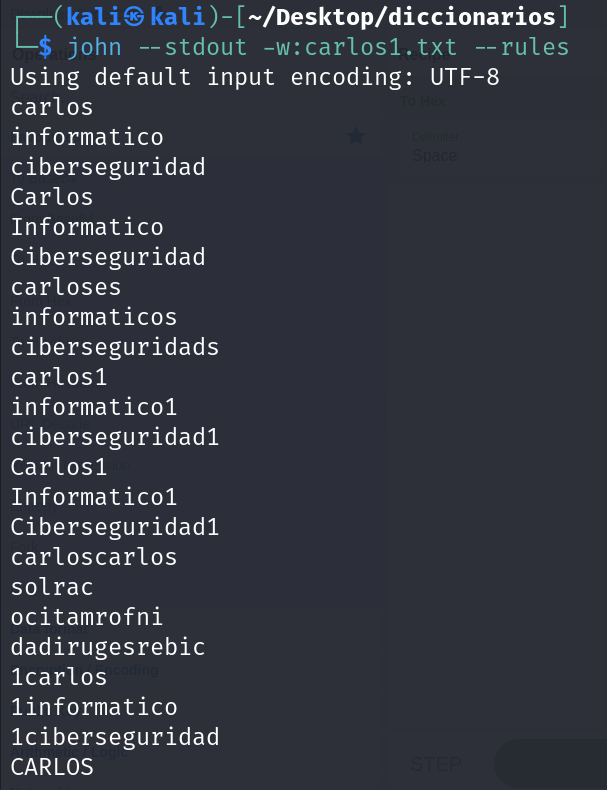
Primero me he creado el archivo carlos1.txt, y he introducido en el 3 reglas:



Ahora ejecutamos el comando:

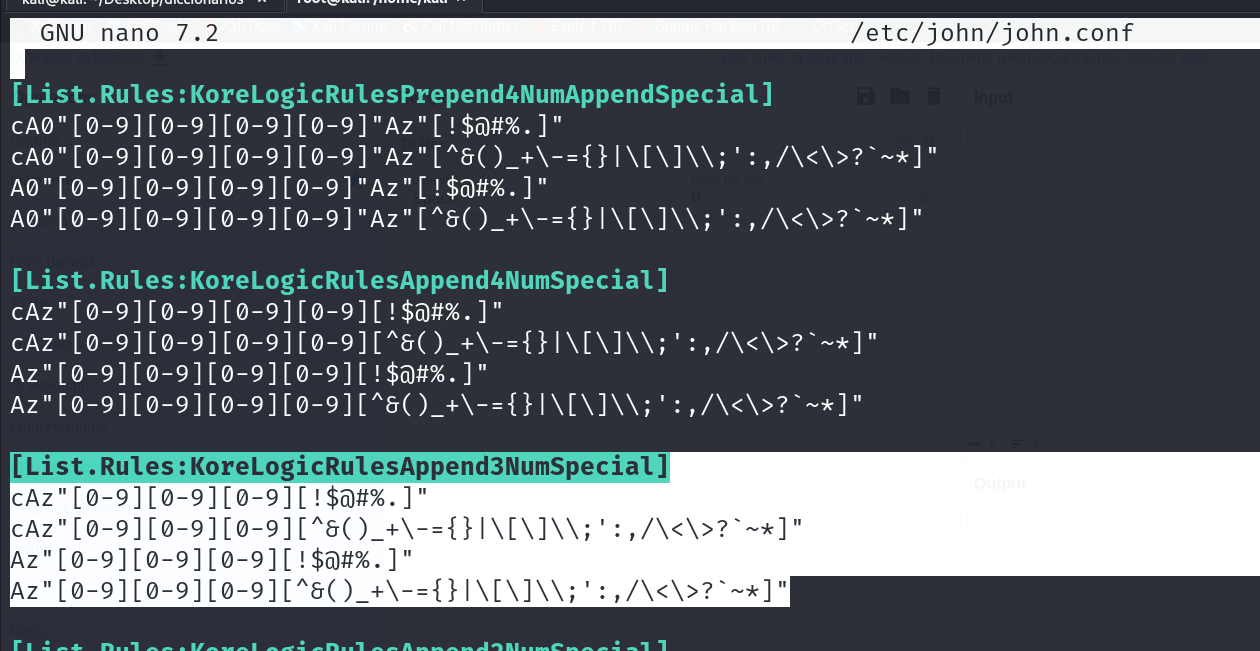


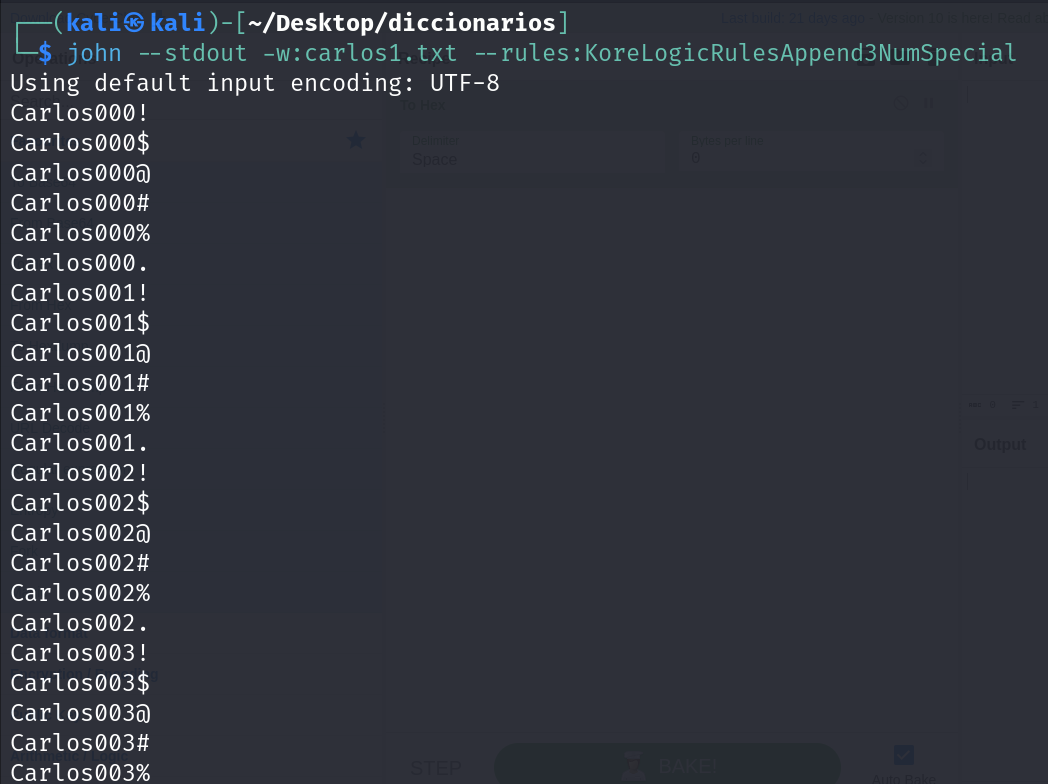
El resultado:



**Ejercicio 2: Busca una regla concreta …**

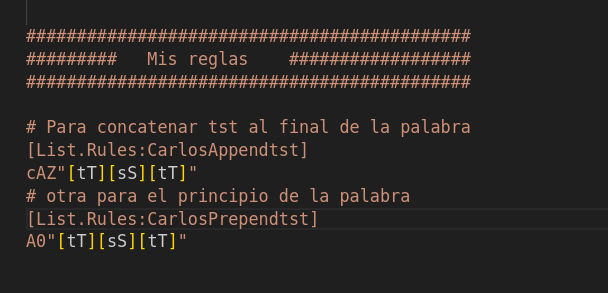
La regla es :



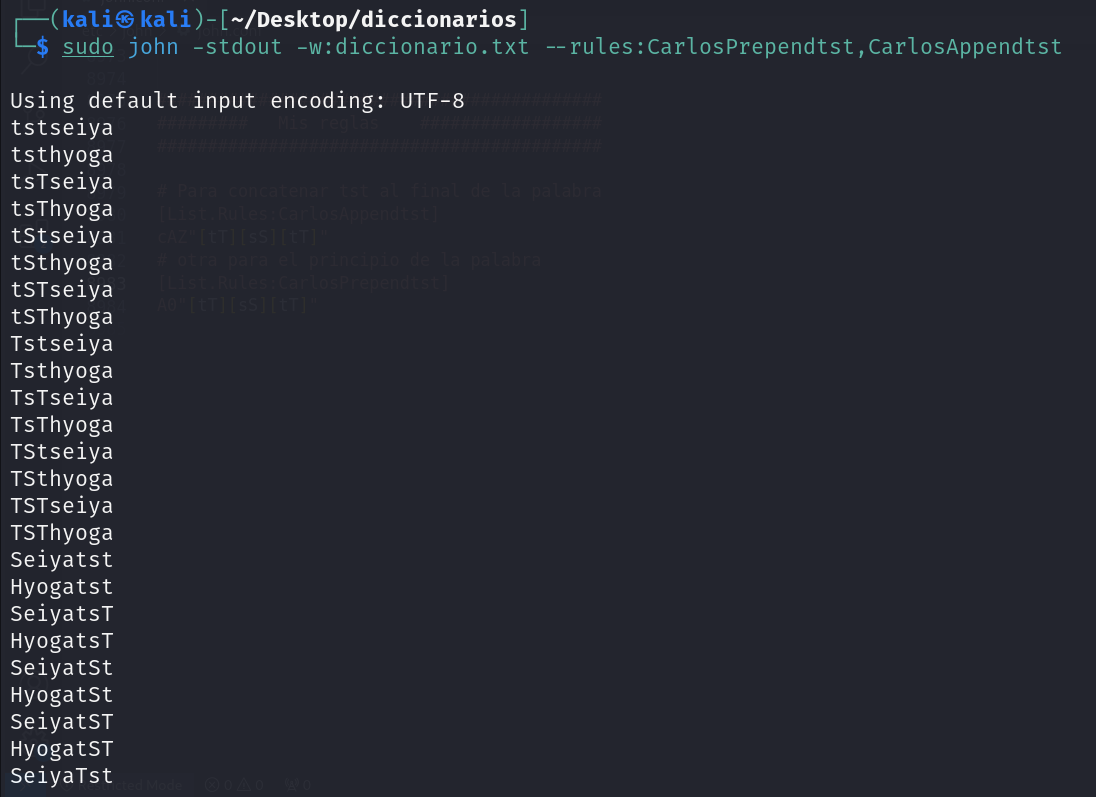
El comando usado es(solo he puesto mi nombre pq sino iba a salir demasiado texto):  


**Ejercicio 3: Regla personalizada …**

Nos creamos las reglas:

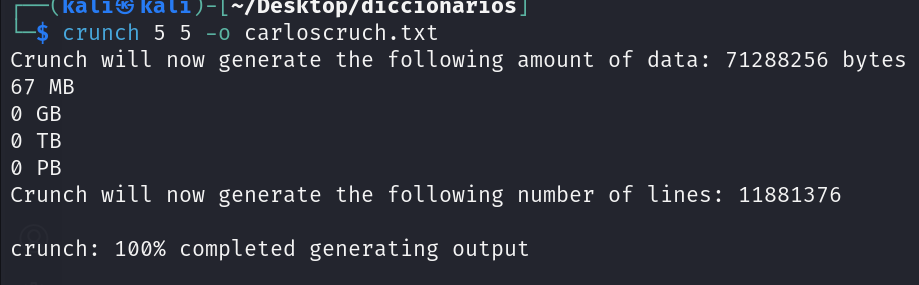


La ejecutamos y comprobamos que funciona:



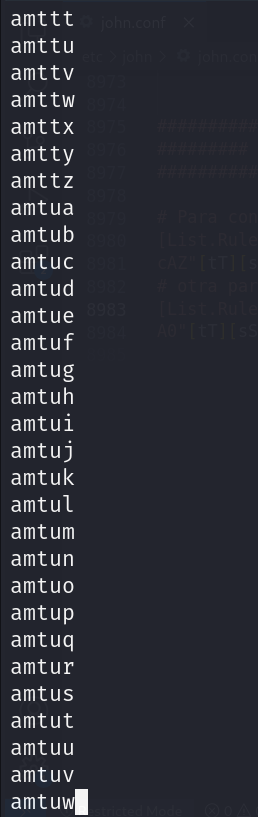
**Ejercicio 4: Crunch – palabras de 5 dígitos**

El comando usado:



Me ha generado 11881376 contraseñas.

Lo que me genera:



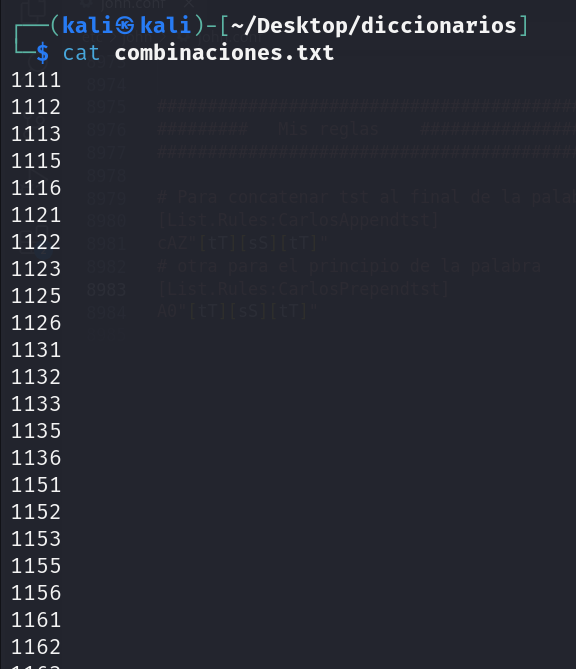
**Ejercicio 5: Crunch – conjunto de caracteres**

En este tengo una duda y no sabia si el pin que tiene es de 4 digitos o de 6 digitos. Como no estaba seguro he puesto este comando:



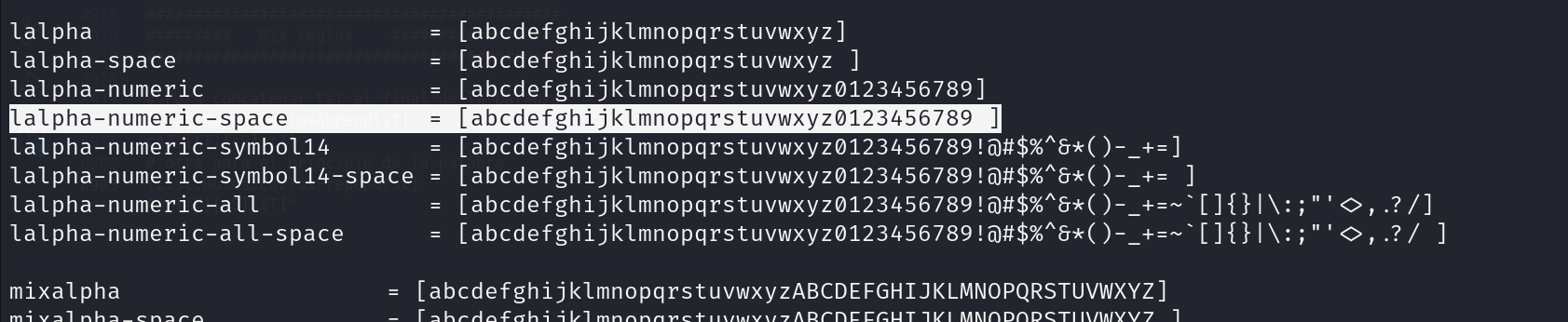
Este te crea combinaciones con esos numero de hasta 4 caracteres como mínimo y máximo como 6, en caso de ser solo de 4 caracteres cambias el 6 por un 4.

El resultado de las combinaciones:

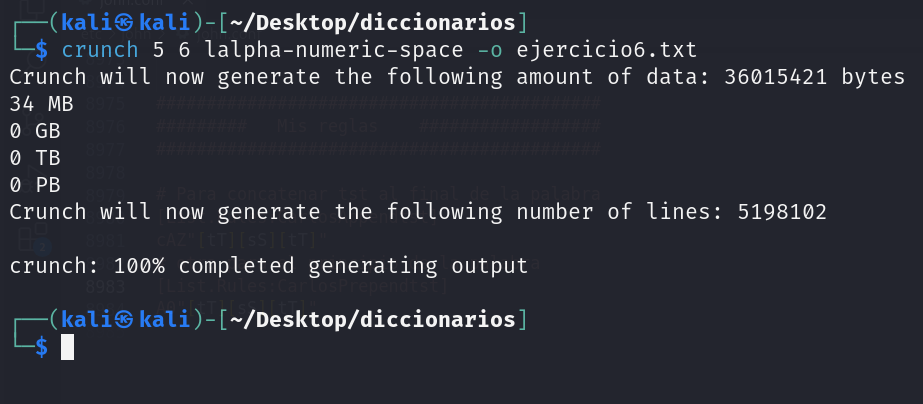


**Ejercicio 6: Crunch – Usando charsets**

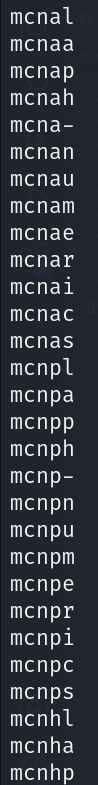
Investigando en /usr/share/crunch/charset.lst he visto que hay una forma de poner minúsculas, números y espacios en blanco:



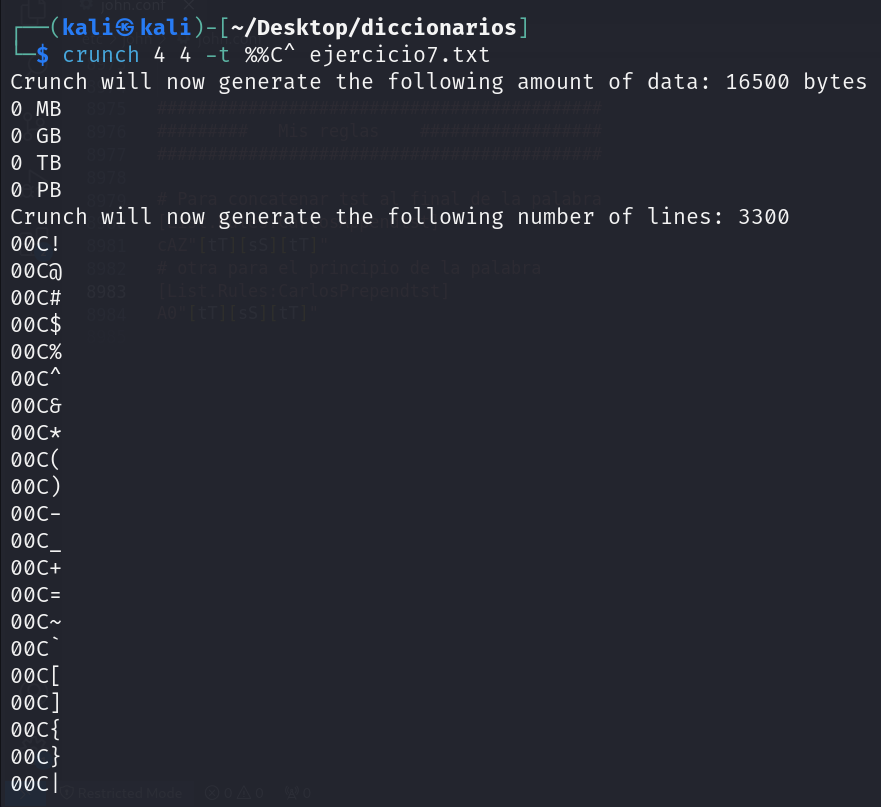
El comando usado es:



Como resultado tenemos:

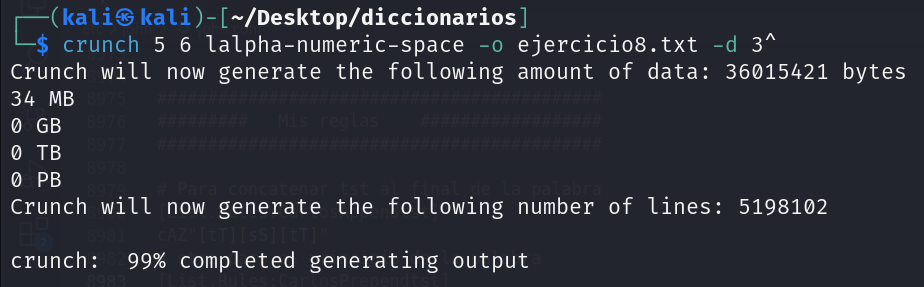


**Ejercicio 7: Crunch – Uso de un patrón**



**Ejercicio 8: Crunch – Repeticiones de caracteres**

El comando usado:



El resultado:



**Ejercicio 9: Crunch – Combinaciones de palabras**

