uninformaticobajolinux.blogspot.com

Manual Crunch (Crear diccionarios o wordlists) en Kali linux (Parte 1)

4-5 minutos

COMO INSTALAR CRUNCH

En mi caso Kali Linux lo tiene instalado.

Pero si no es su caso y lo tienen que instalar seguir los pasos.

Para cualquier distrito Linux con ir a la terminal y escribir:

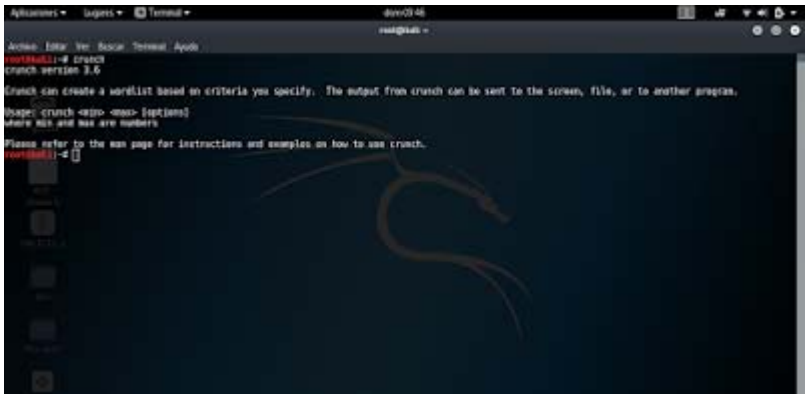
```
sudo apt-get install crunch
```

Y se instalará automaticamnte.

En el caso de que no se instalará por que no lo encuentra ver este post y después realizar de nuevo los pasos.
Con esto añadiremos nuevos repositorios para que logre encontrar el programa.

Manual crunch [Parte 1]

Bueno es aconsejable que lo hagáis a la misma vez que leeis para que lo recordéis mejor y no olvidéis practicar en cada parte del manual para que las siguientes partes sean mas sencillas.



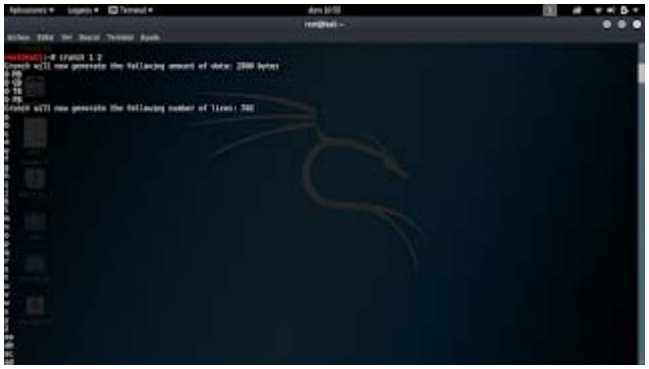
Bastaría con escribir "crunch" en una terminal para conseguir información:

Que nos explica que el comando es de la siguiente forma **crunch [MínimoCifras] [MáximoCifras] [parámetros]**

Ahora veremos unos ejemplos:

Es tan sencillo como decirle la cantidad de carácteres que estamos buscando seguido de alguna opción, Vamos a lanzarlo de una forma básica a ver que tal, probemos con generar todas las posibles combinaciones para una palabra de 2 caracteres:

Si no le ponemos ningún parámetro coge por default el abecedario de la a-z en minúscula y sin la "ñ"



Al principio empieza por 1 letra únicamente ya que le hemos dicho que empiece desde 1 carácter hasta dos.
Tras escribir el comando y dar enter nos muestra en pantalla esto:

```
Crunch will now generate the following amount
of data: 2080 bytes



0 MB
```

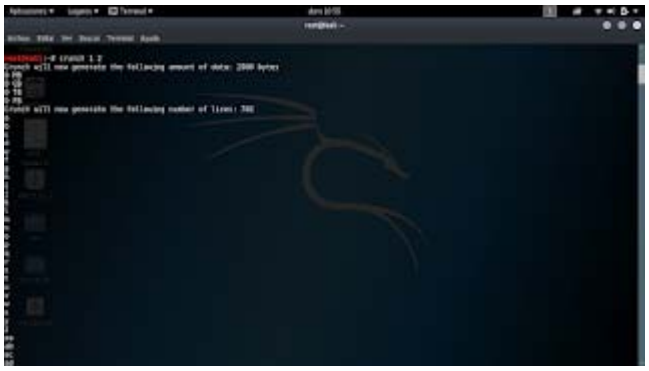
```
0 GB


0 TB


0 PB


Crunch will now generate the following number
of lines: 702
```

Crunch nos avisa de cuanto espacio ocupará y cuantas líneas imprimirá.
Comparto 30 líneas para que veais como lo hace.



Vamos a analizar esto unos segundos...

Tenemos que crunch ha generado todas las posibles combinaciones para una palabra de 2 caracteres, pero notan alguna particularidad?

No se han usado numeros, simbolos, mayúsculas ni espacios en blanco. La razón se explica a continuación:

Crunch utiliza una variable llamada **charset (character setting)**

y es como el conjunto de carácteres que serán usados para la generación del **diccionario/wordlist,** por defecto el chardset es **lalpha (El abecedario en minúscula sin "ñ")** pero que tal si probamos a configurar otro chardset.

Antes de nada tendremos que localizar el archivo **charset.lst** en mi caso está en /usr/share/crunch/charset.lst

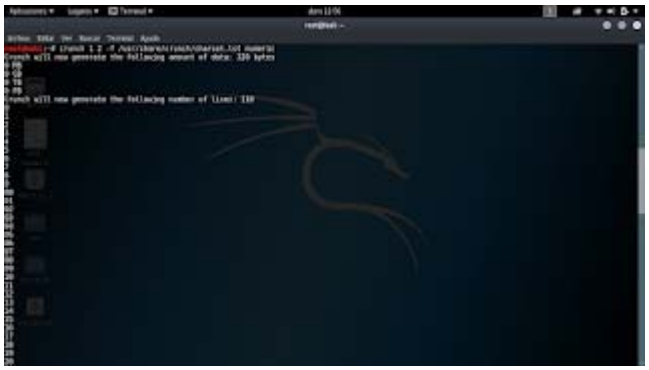
No tengo que dicer que si estais en el mismo directorio que este el archivo no hara falta poner la ruta, solo con el nombre charset.lst será suficiente.

```
crunch 1 2 -f /usr/share/crunch/charset.lst numeric
```

Analizemos el comando:

- **crunch** Para llamar al programa.
- **1** Mínimo de carácteres.
- **2** Máximo carácteres.
- **-f /usr/share/crunch/charset.lst numeric** Le dice a crunch que tiene que cojer el archivo charset.lst y el tipo de carácter.

Como siempre, al presionar enter crunch nos indicara cuantas lineas y cuanto espacio sera usado, analicemos las primeras líneas:



Todo ha ido bien, pero ahora notamos una pequeña diferencia, y es que solo ha generado numeros, pero eso es justo lo que

queríamos no? Y como lo hemos logrado pues con la **opción -f** y listo!!
Esta opción le indica dónde buscar el fichero de variables, es decir, donde están preestablecidas todos los charset, es decir que debemos especificar la ruta al archivo así como nuestra selección dentro del mismo, en mi caso tengo el charset.lst en mi directorio **/usr/share/crunch/charset.lst**

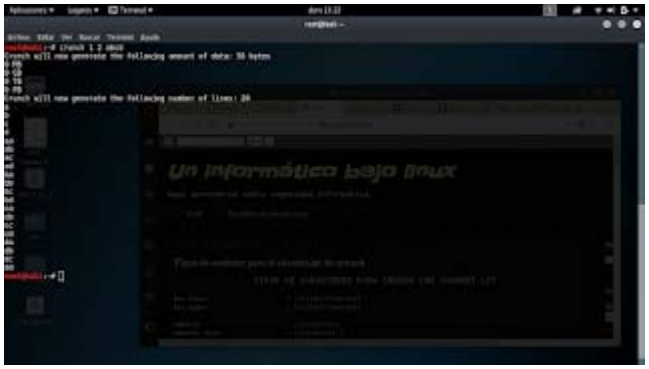
Cuantos charset podemos elegir además de lalpha y de numeric?
Miren por ustedes mismo

Para saber sobre los tipos de carácter visite este enlance.

Si no quieren especificar ningun charset pueden simplemente pasarle a crunch cuales caracteres desean usar en la generación, por ejemplo:

```
crunch 1 2 abcd
```

Esto sacará en pantalla todas las combinaciones de un carácter y dos carácteres con las letras "abcd".



Empiezan a entender el sentido de la palabra "**Flexibilidad**" para referirse a crunch.

Si desea seguir aprendiendo sobre esta herramienta vease las siguientes partes.