uninformaticobajolinux.blogspot.com

Manual Crunch (Crear diccionarios o wordlists) en Kali linux (Parte 2)

4 minutos

[Empezar por la parte 1]

Manual crunch [Parte 2]

Hasta ahora hemos aprendido a usar crunch al nivel básico, es decir, sólo sabemos generar diccionarios especificandole el tamaño y el conjunto de caracteres a usarse, y muchos pensaran que esa es toda la magia de generar diccionarios y la verdad es que se queda corto, siganme y veremos qué otras cosas podemos hacer.

Imaginemos por un instante que logras ver la unos caracteres de la contraseña o que el final es su fecha de nacimiento, o el nombre de su mascota...

Para que necesitamos que nos haga un diccionario entero si ya conocemos carácteres, pues se soluciona de la siguiente forma:

```
crunch 5 5 -t inf@@
```

Y si nos fijamos crunch ha generado palabras sin modificar los 3 primeros caracteres, con lo cual si la palabra clave es "infor" eventualmente sera generada, pero que pasaría si el administrador del sitio ha querido complicarla y ha puesto "inf0r" como password? pues podemos hacerlo de dos formas, una sencilla y otra un poco mas compleja, para la forma compleja podríamos hacerlo al especificar un charset alfanumérico escribiendo:

```
crunch 5 5 -f /usr/share/crunch/charset.lst
lalpha-numeric -t inf@@
```

o bien podríamos especificar los caracteres que queremos usar:

```
crunch 5 5
abcdefghijklmnñopqrstuvwxyz1234567890 -t inf@@
```

Con ambos comandos tendríamos el mismo resultado, simplemente son dos formas de hacer lo mismo.

Ahora viene la forma sencilla que es simplemente cambiar el símbolo **"@"** por el tipo de carácter que queremos insertar en la generación del diccionario, recuerden que con la opción **-t**, podemos especificar un patrón de carácteres que serán los únicos en cambiar al generar el diccionario, así los carácteres que podemos especificar para el patrón son:

- @ insertará minúsculas

- , insertará mayúsculas
- % insertará números
- ^ insertará símbolos

Sabiendo esto, vamos a suponer que queremos generar un diccionario donde la primera letra sea en mayúscula, pero que a lo largo del mismo, tanto el 2º como el 3º carácter se queden fijos, pues para hacerlo agregamos una **","** que tal como expliqué anteriormente, insertará mayúsculas, pero recordemos que había un número en el password, así que también necesitamos insertar 1 solo número en el 4º carácter de nuestra palabra, pues sólo contamos hasta el lugar número 4 e insertamos un "%" que como también expliqué anteriormente, sólo inserta números, la clave sería "**Inf0r**" y el comando final quedaría como esto:

```
crunch 5 5 -t ,nf%@
```

Toda esta flexibilidad la hemos logrado con la opción -t, espero que la hayan entendido y les sea muy práctica en un futuro. Pero no piensen que hemos terminado, esto continúa y.. ¡Se pone mejor!

Imaginemos que a una persona, la estudias y sabes;

- Su nombre : Federico
- La fecha de nacimiento : 12021992

- El nombre de su mascota : Nieve

Veamos, vamos a generar un diccionario concatenando palabras, en este caso generar simplemente por carácteres sería casi imposible dada la longitud final **"federico12021992nieve"** así que en crunch existe una opción que nos permite concatenar palabras, veamos como:

```
crunch 1 1 -p Federico 12021992 Nieve
```

Obtendriamos algo como esto

Como se habran fijado, con la **opción -p** es posible lograr concatenar palabras, pero hay una particularidad, y es que fíjense que en la parte donde se especifican la longitud menor y la mayor yo he colocado **"1 1"** y pues la verdad es que cuando se usa la **opción -p** los números no son procesados, pero son necesarios para el argumento, es decir que podremos colocar cualquier cosa y sera irrelevante para la salida.