

uninformaticobajolinux.blogspot.com

Manual Crunch (Crear diccionarios o wordlists) en Kali linux (Parte 4)

2-3 minutos

Y a esto se le podría sumar muchos mas parámetros como el de comprimir, o el de charset.lst, etc..

Bueno, para aprender el siguiente parámetro nos tenemos que poner en situación. Para ello haremos el siguiente ejercicio:

Tenemos que averiguar el email de una persona, para ello sabemos su usuario de twitter. Donde recuperando contraseña nos da *er9*@****.*** y sabemos que es *er9*@gmail.com .

Tenemos que crear un diccionario con las posibles combinaciones, suponiendo que la primera letra es minúscula y el carácter despues del 9 es un número. Tendremos que crear el diccionario.

Usaremos el parámetro aprendido anteriormente:

```
crunch 15 15 -t @er9%@gmail.com
```

¿Con esto tendría que valer, no?



Se aprecia a simple vista que la @ no la coje como un carácter, sino que la coje como si de una minúscula se tratase, como solucionar este bug o como lo queráis llamar. Pues con el parámetro que teníamos pendiente desde el principio.

Este parámetro solo se puede usar junto a -t ya que es para corregir el bug de poder poner la "@" como carácter.

```
crunch 15 15 -t @er9%@gmail.com -l
aaaaa@aaaaaaaaaa
```



¡Voila! Como veis, ya nos representa el carácter @ donde queremos.

Ahora pasaré a explicar como se usa -l

Después de escribir el parámetro, escribimos letras por carácter donde no va el carácter @. Ejemplo: Queremos que busque "hol@" para ello sería **crunch 4 4 -t @@@@ -l aaa@**

Último parámetro de esta parte del manual...

Seguro has pensado por qué tiene que empezar

aaaaaa,aaaaab,aaaaac... esto en 3 caracteres no se nota pero

en 6 o 7 ya si se nota asi que hasta que llegue a "baaaaa"

puede tardar 5^{27} posibilidades hasta llegar a esa combinación,

si sólo usamos el abecedario de minúsculas si usamos el

alfanumérico-mixto seria 5^{66} posibilidades.

Para poder hacer que vaya cambiando la letra desde la izquierda es:

[illegible]

Aqui terminamos el manual de crunch, quedan algunos parámetros mas pero no son de gran utilidad.