uninformaticobajolinux.blogspot.com

Manual Crunch (Crear diccionarios o wordlists) en Kali linux (Parte 3)

3-4 minutos

Manual crunch [Parte 3]

Pues llegados a este punto ya sabemos generar diccionarios con distintos charset, sabemos aplicar patrones en la generación, concatenar palabras, así como especificar con cuales caracteres queremos generar, así que considero que estamos avanzando en crunch.
Crunch puede mandar los resultados a la pantalla, puede crear un archivo ó pasarle la salida a otro programa (generalmente un crackeador como aircrack) pero hasta ahora solamente hemos sacado los resultados en pantalla, es decir no se han creado ningun archivo ni nada parecido, asi que vamos a ello.

Enviando el output de crunch a un archivo.txt o a un comprimido.

Pues la idea básica de crear un diccionario es poder usarse posteriormente para dar con el hash válido en una prueba de fuerza bruta, así que de alguna forma debemos poder generar un fichero a partir de la salida, esto es posible usando la **opción -o (output)** seguido del nombre del archivo, tomemos como ejemplo el ejercicio de Federico 12021992 Nieve y creemos un fichero, el comando sería:

```
crunch 1 1 -o NombreDiccionario.txt -p federico
12021992 nieve
```

Opcionalmente tambien podríamos especificar la ruta donde queremos volcar el diccionario, por ejemplo:

Vamos a avanzar un poco más profundo y hagamos que cada 5000 líneas crunch nos generó 1 fichero, pues para que, dependiendo el entorno en el que se vaya a auditar necesitamos seccionar el ataque, es decir dividir el diccionario en una cantidad específica, para lograr mejor acoplamiento con los temporizadores de los crackeadores, para lograr esa división de un diccionario en varios ficheros de menor tamaño usamos la opción -c (esta opción solo funciona si el -o START está presente en la linea) por ejemplo:

Y si me fuera a la carpeta documentos me encontraría con esto:

Esto inicia el proceso de crear múltiples ficheros con 5000 lineas cada uno, tal y como podemos ver en la imagen:

Aclaraciones

- **El START** funciona como nombre de archivo para el primer fichero a crear, a partir de ahí los ficheros tomarán el nombre de la última linea del archivo anterior + la primera linea del archivo posterior.
- Aunque debo aclarar que en algunos caso es posible llenar el disco duro al generar un diccionario, todo depende de lo que le digamos a crunch, por ejemplo, si yo dijese:

```
crunch 15 25 -o demasiado.txt
```

¿Se fijan en el tamaño del fichero?

¡ 2744 PB !

Eso sería demasiado.txt para cualquier disco duro.

Pero entre tanta generación que tal si creamos un fichero y lo comprimimos a bzip, de un solo golpe, suena complicado pero sería simplemente agregar la opción -z seguido del tipo de compresión deseado, por ejemplo:

De esta forma se iniciaría el mismo proceso anterior solo que en comprimidos gzip, en cualquier otro formato soportado por crunch (gzip, bzip2, lzma, and 7z)

Pues como podrán ver, no es tan complicado mandar la salida a un fichero txt, gzip, bzip2, lzma ó 7z.