4602161254205122361 8.pdf

Manual Crackeo Apuntes TAI

3º Tecnologías Avanzadas de la Información

Grado en Ingeniería Informática - Tecnologías Informáticas

Escuela Técnica Superior de Ingeniería Informática
Universidad de Sevilla

MANUAL:

CÓMO DESBLOQUEAR LOS APUNTES DE LA ASIGNATURA

TECNOLOGÍAS AVANZADAS DE LA INFORMACIÓN

BASADO EN MI EXPERIENCIA PERSONAL

Antonio Javier Palma Guerrero

Tecnologías Avanzadas de la Información

3º de GII-TI. Grupo 1.

Curso 2019/2020

Introducción

Tras mucho darle vueltas, hago este pequeño manual para que todo aquel que lo desee pueda intentar obtener la contraseña de estos apuntes que se suben cifrados a la web de la asignatura.

Para el curso 2019/2020 yo mismo me he encargado de subirlos para quien no quiera dedicarle tiempo, pero habrá alumnos que lo intenten y no sabrán en un principio cómo hacerlo. Así, con este manual, me gustaría poner mi granito de arena para orientar un poco a quien desee intentarlo.

Elección de la herramienta

El primer paso que debemos realizar es buscar una herramienta que pueda servirnos para intentar crackear el correspondiente PDF cifrado. Para ello, debemos tener en cuenta, entre otras cuestiones, el sistema operativo.

Hay herramientas muy famosas como John The Ripper, Caín y Abel, etc. En mi caso, he usado el software pdfcrack, que va a través de la Terminal de Linux, instalándolo a través de la Terminal.

Si quieres usar pdfcrack:

```
sudo apt-get install pdfcrack
```

En caso de tener que usar una herramienta distinta a ésta, no podrás seguir paso a paso este pequeño manual, pero puedes quedarte con los conceptos para saber cómo seguir.

Primeras pruebas. ¿Funciona?

Una vez tenemos la herramienta, lo primero que debemos hacer es probarla. En el caso de pdfcrack, esta herramienta permite probar por fuerza bruta para que el mismo programa genere contraseñas de forma aleatoria.

```
pdfcrack nombreDelArchivo.pdf
```

Es recomendable probarlo para comprobar que funciona, pero así no va a encontrar la contraseña. Normalmente, las contraseñas que va generando así son cortas, cuando en el curso 2019/2020 la contraseña era de 14 caracteres.

Habrá herramientas que no permitan hacer estos ataques de fuerza bruta así, si no que pedirán algo más, y que es el siguiente paso para lograr acercarnos a las contraseñas: los diccionarios.

Diccionarios

Los diccionarios, como su propio nombre indica, son archivos llenos de palabras. Por lo general, por cada línea en el archivo hay una palabra, pudiendo ser los diccionarios de un tamaño muy variable.

Al usar un diccionario para buscar la posible contraseña de un archivo, el programa recorre el diccionario línea a línea, probando si la palabra de la línea n consigue abrir el archivo cifrado. En el caso de conseguir abrir el archivo, el programa parará y notificará cuál es la palabra que ha funcionado. Si no lo consigue, llegará hasta el final, indicando que no ha encontrado ninguna contraseña valida.

```
a
a-
aarónico
aaronita
aba
ababa
ababillarse
ababol
abacá
abacal
abacalero
abacería
abacero
abachar
abacial
ábaco
...
```

Ejemplo de estructura de un diccionario

Muchos de los programas que podemos usar piden diccionarios desde un primer momento. Por suerte, son fáciles de encontrar, googleando un poco aparecen muchos diccionarios distintos.

Pruebas definitivas

Una vez que sabemos qué son los diccionarios y tenemos clara la herramienta a usar, podemos usar los diccionarios que vayamos encontrando.

A partir de aquí, ya es cuestión de suerte que aparezca la contraseña, ya que puede que probemos muchos diccionarios distintos hasta encontrar la contraseña del archivo que estamos intentando crackear. Por suerte, estos diccionarios se recorren en cuestión de segundos, o minutos en los casos en los que los diccionarios sean muy extensos o pesados.

Mi recomendación es buscar los diccionarios en GitHub, ya que en esta web es donde he conseguido encontrar un diccionario que pudiera abrir el archivo del desafío del curso 2019/2020.

En el caso de probar con la herramienta pdfcrack, usada por mí, la forma de hacerlo es la siguiente:

```
pdfcrack nombreDelArchivo.pdf --wordlist=diccionarioDescargado
```

Como podemos ver, el primer parámetro que se pasa es el nombre del archivo cifrado que queremos abrir. Después, encontramos la opción --wordlist, a la que se le pasa el diccionario que se desee probar.

De esa forma, en la Terminal devuelve cada x tiempo la palabra que está probando en ese instante, hasta que indica finalmente si ha encontrado o no la contraseña.

En caso de encontrar la contraseña y querer quitarle la contraseña de manera definitiva, en Internet hay muchas webs que permiten hacerlo, para no estar metiendo una contraseña bastante compleja cada vez que se quiera abrir el archivo.

Conclusiones

Como se ha podido ver en las páginas de este manual, realmente el proceso es bastante sencillo una vez que se sabe qué hacer para intentar desbloquearlo. Sin embargo, intentándolo desde cero, probando una y otra vez sin saber cómo seguir para conseguir algo, puede ser bastante duro y agotador.

Este documento se lee en solo unos minutos. Sin embargo, yo fui haciendo pruebas (posibles herramientas, diccionarios…) durante semanas, por no tener una base de la que partir.

Espero que te haya servido de ayuda, para saber cómo meterle mano, y puedas desbloquear por ti mismo el archivo cifrado de los apuntes.