

Write-up: HackTheBox - Misc - Old is gold

SEBASTIÁN SEPÚLVEDA @PIBLACK

18 de mayo de 2019

Información: Categoría Misc, 10 points.

Descripción: Old algorithms are not a waste, but are really precious...

WRITEUP

Para comenzar con el desafío descargamos el fichero con el comando ya conocido

```
wget https://www.hackthebox.eu/storage/challenges/misc/0ld_is_g0ld.zip
```

Vemos que tiene un pdf! pero que nos depara el destino... Tenemos la opcion que mas nos llama a usar fuerza bruta con rockyou.txt.

Como realizamos fuerza bruta a un archivo pdf?:

Para resolver el problema, buscamos en google y nos aparece un programa que se llama **PDFCRACK**. En Kali lo descargamos con `apt-get install pdfcrack`

Pdftcrack lo que hace es fuerza bruta sobre el documento pdf, con algún diccionario que le demos como parámetro. En Kali hay que ingresar el siguiente comando:

```
pdfcrack -f "documento pdf que vamos a atacar" -w "diccionario que usaremos"
```

En este caso debemos ocupar:

```
pdfcrack -f Old_is_gOld.pdf command -w /usr/share/wordlist/rockyou.txt
```

La clave que encontramos es jumanji69

Abrimos el documento y nos encontramos con una imagen y nada de texto. Sin embargo, al presionar `ctrl+A`, Eureka!, encontramos algo que no sabemos que es, lo pegamos en un archivo de texto y se muestra puntos y guiones

Abstract

para decodificar el codigo morse ocupamos **Morse code**

finalmente encontramos la flag.

Flag: HTB{ripsamu3lmors3}