uc3m | Universidad Carlos III de Madrid

INGENIERÍA INFORMÁTICA - 4º CURSO

2024-2025

Ingeniería de la Ciberseguridad

Práctica 1 Estudio de la Fortaleza de Contraseñas

Grupo 21

AUTORES

Fernando Consiglieri Alcántara - 100472111 - 100472111@alumnos.uc3m.es

David Andrés Yáñez Martínez - 100451958 - 100451958@alumnos.uc3m.es

ÍNDICE

Explicaciones de los comandos de Fotomotos:

A continuación, se explicarán los comandos utilizados en John the Ripper para romper las contraseñas, justificando cada decisión a partir de las pistas dadas en el enunciado.

Se ha establecido la opción `--max-run-time` para todos los comandos, en caso de que el ordenador en el que se utilicen sea excesivamente lento. Sin embargo, los comandos están diseñados para ejecutarse en un tiempo considerablemente menor.

1.- Primer comando

`john --min-length=4 --wordlist=spanish.txt --format=Raw-MD5 --rule=jumbo --max-run-time=200 g21_foromotos_entrada.txt`

Justificación de uso:

Sabiendo que el mínimo de caracteres por contraseña es 4, la mayoría de los comandos incluirán el parámetro `--min-length=4`. También, se indicó que la mayoría de los usuarios hablaban español, esto nos indica que es probable que muchos usuarios utilicen en sus contraseñas palabras comunes en su idioma. Por ello, se utilizó un diccionario de contraseñas en español (`spanish.txt`).

Además, se añadió la regla `jumbo`, que permite a John probar variantes comunes de las contraseñas del diccionario, cómo agregar números o símbolos. Esto es importante porque muchos usuarios tienden a utilizar una contraseña simple, pero con ligeras modificaciones.

Resultados:

El comando rompió 40623 contraseñas pertenecientes a 43982 usuarios en 1 minuto y 20 segundos.

2.- Segundo comando

`john --min-length=4 --wordlist=spanish.txt --format=Raw-MD5 --rule=l33t --max-run-time=50 g21_foromotos_entrada.txt`

Justificación de uso:

El uso de este comando se debe a la pista que menciona que ForoMotos tiene un subforo de hacking, donde algunos usuarios usan la escritura leet (l33t), una jerga típica de los script kiddies que sustituye letras por números o símbolos (como usar "3" en lugar de "e", o "1" en lugar de "i"). Así que se utilizó la regla `l33t` para que John pudiera probar variaciones de este tipo en las contraseñas del diccionario en español.

Resultados:

El número de contraseñas rotas fue de 354 pertenecientes a 367 usuarios. Que el número de contraseñas rotas sea más bajo se debe a que el comando anterior con jumbo ya rompía contraseñas de la índole l33t.

3.- Tercer comando:

john --min-length=4 --wordlist=spanish.txt --format=Raw-MD5 --mask=?w?a?a --max-run-time=110 g21_foromotos_entrada.txt

Justificación de uso:

También es común que los usuarios utilicen como contraseña palabras seguidas de diferentes modificaciones como agregar números o símbolos al final. Se utilizó un ataque basado en máscaras (`?w?a?a`).

Resultados:

Este comando fue bastante efectivo, rompiendo 4115 contraseñas en solo 22 segundos estas contraseñas pertenecen a 4116 usuarios, lo que refuerza la idea de que muchos usuarios combinan palabras conocidas con pequeñas variaciones.

4.- Cuarto comando:

john --min-length=5 --max-length=5 --incremental=lowernum.chr --format=Raw-MD5 --max-run-time=40 g21_foromotos_entrada.txt

Justificación de uso:

Este comando está basado en la pista que menciona que en los primeros años de ForoMotos las contraseñas generadas automáticamente eran alfanuméricas en minúsculas de 5 caracteres. Muchos usuarios probablemente no cambiarían estas contraseñas generadas por el sistema, por lo que se probó con John todas las combinaciones posibles de letras minúsculas y números de exactamente 5 caracteres.

Resultados:

El resultado fue de 7265 contraseñas rotas en solo 7 segundos perteneciente a 7265 usuarios.

5.- Quinto comando:

john --min-length=6 --max-length=6 --incremental=lowernum.chr --format=Raw-MD5 --max-run-time=200 g21_foromotos_entrada.txt

Justificación de uso:

Luego, se aplicó una estrategia similar, pero esta vez basada en la pista de que en una etapa posterior ForoMotos comenzó a generar contraseñas alfanuméricas en minúsculas de 6

caracteres. De nuevo, John fue configurado para probar todas las combinaciones posibles de letras minúsculas y números, pero con una longitud de exactamente 6 caracteres.

Resultados:

Este ataque resultó aún más efectivo, rompiendo 11604 contraseñas en 1 minuto y 31 segundos.

6.- Sexto comando:

john --min-length=6 --max-length=6 –incremental=custom.chr --max-run-time=900 --fork=8 --format=Raw-MD5 g21_foromotos_entrada.txt

Justificación de uso:

Finalmente se realizó un ataque de fuerza bruta completo para las contraseñas de 6 caracteres, ya que, aunque se habían roto muchas contraseñas con los métodos anteriores, era necesario intentar cubrir todas las combinaciones posibles. Fue utilizado el modo incremental para que John probará todas las combinaciones posibles de caracteres, no sólo letras minúsculas y números. Además, del uso de 8 procesos paralelos (`--fork=8`) para acelerar el ataque.

Se utilizó un archivo de caracteres propio llamado custom.chr que contiene las letras minúsculas, mayúsculas, números y los símbolos: `“: ! @ # % &”`. Esto se hizo para reducir el número de combinaciones a probar eliminando los símbolos ASCII imprimibles que no habían sido utilizados en anteriores contraseñas.

Resultados:

Este comando rompió las contraseñas de 14322 usuarios adicionales en 15 minutos, lo cual indica que algunos usuarios utilizaban combinaciones más complejas o fuera de lo esperado en los intentos previos.

Conclusiones Foromotos:

En resumen, todos los comandos utilizados estuvieron basados en las pistas dadas sobre la longitud de las contraseñas, el idioma de los usuarios, las tendencias de uso y las reglas de generación de contraseñas en ForoMotos. Fue usado un diccionario en español, reglas de variación y ataques incrementales para maximizar el número de contraseñas rotas.

Al final, se rompieron un total de **81656 contraseñas**, lo que demuestra que los usuarios de ForoMotos siguen patrones bastante predecibles en sus contraseñas.

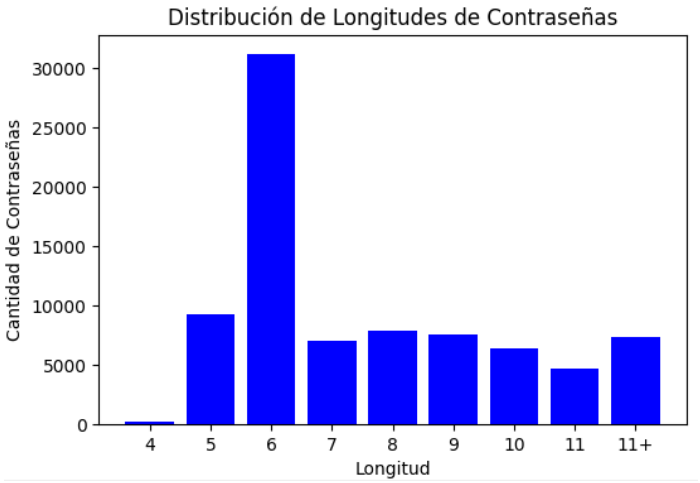
Análisis de Foromotos:

Se consideró oportuno llevar a cabo un análisis de los resultados obtenidos del dataset de Foromotos, ya que es el más interesante. Este análisis, realizado utilizando el archivo

`stadistics.py`, ha revelado varios aspectos relevantes sobre el conjunto de datos de contraseñas crackeadas:

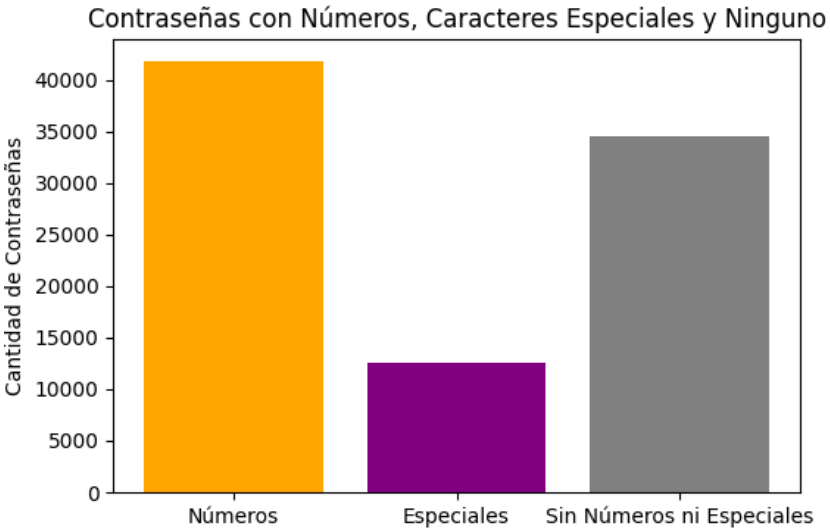
Eficiencia en el Cracking: Partiendo de un dataset de 187431 usuarios distintos. Se ha conseguido vulnerar la cuenta de 81656 usuarios. Se ha logrado crackear el 43,57% de las contraseñas del total, lo cual es un porcentaje significativo, considerando el tamaño del dataset original.

Longitud de contraseñas:



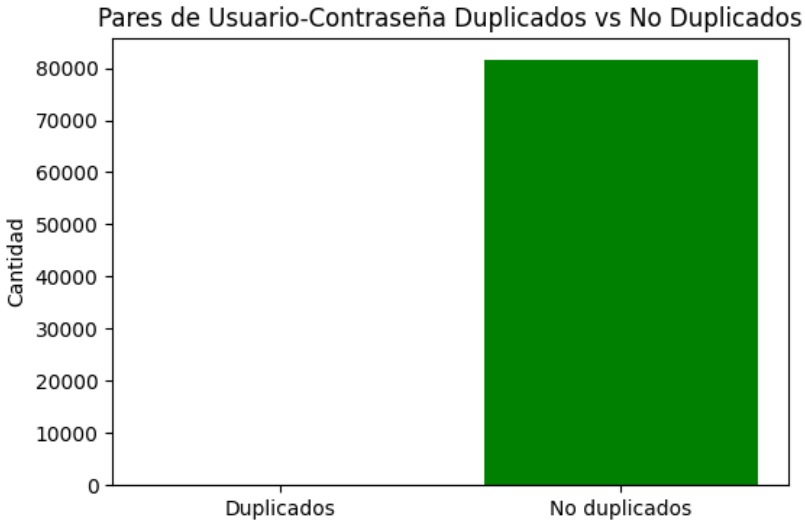
Al observar la gráfica, podemos notar que la mayoría de las contraseñas (31246) tienen una longitud de 6 caracteres, con una presencia significativa de contraseñas de longitud 5 (9302) y 8 (7927). Este patrón es lógico, ya que es más sencillo crackear contraseñas más cortas, lo que nos ha permitido obtener un mayor número de ellas. Además, esto se debe a la pista de que la web generaba contraseñas de longitud 5 y 6 de manera predeterminada. Esta tendencia también indica que muchas de las contraseñas recuperadas podrían considerarse débiles debido a su longitud reducida.

Uso de Caracteres Especiales y Números:



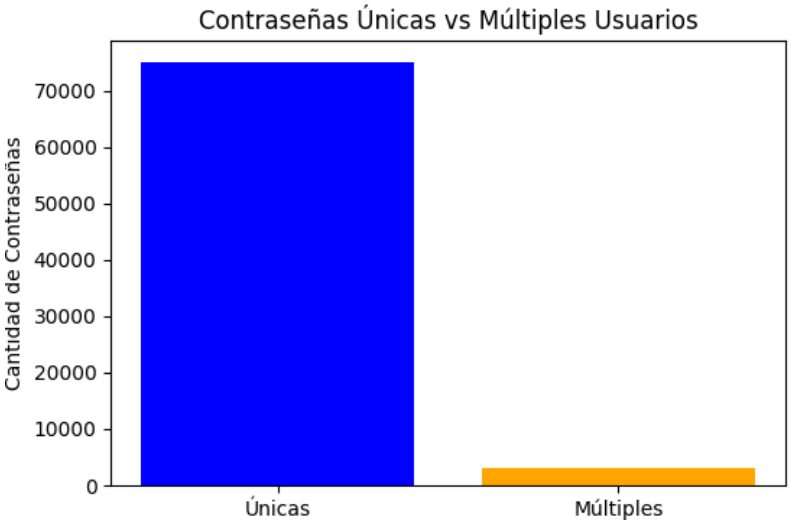
En la gráfica, se observa que un porcentaje considerable de las contraseñas incluye números (41881), lo que indica que los usuarios han intentado fortalecer sus contraseñas. Sin embargo, el número de contraseñas que contienen caracteres especiales es relativamente bajo (12565), lo que sugiere que es más complicado crackear contraseñas que incorporan estos elementos. Esta tendencia refleja el desafío que presentan las contraseñas con caracteres especiales, lo que resalta la necesidad de enfatizar su uso para mejorar la seguridad general de las contraseñas.

Duplicados:



Observando la gráfica, la falta de pares de usuario-contraseña duplicados indica que no se incluyen contraseñas crackeadas repetidas, cumpliendo así con el requisito de la práctica.

Diversidad en la Selección de Contraseñas:



Se observa una buena cantidad de contraseñas únicas (75209), lo que indica que, aunque hay múltiples combinaciones, la mayoría de los usuarios han elegido contraseñas diferentes.

Explicación de los scripts de Meneate:

A continuación, se explicará el script utilizado denominado `crack_meneate.py` para crackear las contraseñas de Meneate mediante Python.

La pista clave es que algunos usuarios suelen reutilizar las contraseñas en varios sitios, lo que significa que muchas de las contraseñas rotas en ForoMotos podrían ser reutilizadas en Meneate. Esto dio idea de aprovechar esa información para intentar romper las contraseñas bcrypt de Meneate de manera más eficiente. Como John the Ripper es muy lento para bcrypt debido a su naturaleza de alta complejidad, se utiliza Python para acelerar el proceso.

El script comienza cargando las contraseñas previamente crackeadas de ForoMotos en un diccionario. Luego, se importan los usuarios y sus correspondientes hashes bcrypt desde Meneate. A continuación, el script verifica si hay coincidencias entre los nombres de usuario presentes en el diccionario de contraseñas de ForoMotos y aquellos de Meneate.

Si se encuentra una coincidencia, el script compara la contraseña crackeada de ForoMotos con el hash bcrypt correspondiente. Si la contraseña coincide, significa que ambas contraseñas son idénticas.

Para acelerar el proceso, ya que bcrypt es lento, fueron utilizados hilos (multithreading), lo que permite probar varias contraseñas en paralelo, haciendo que el crackeo sea mucho más rápido. Finalmente, las contraseñas encontradas se guardan en el archivo `g21_meneate.txt`.

Resultados:

Este script rompió las contraseñas de 15021 usuarios de meneate en 2 minutos y 10 segundos.