Práctica 1: Estudio de la Fortaleza de Contraseñas

Descripción

El objetivo de esta práctica es profundizar en el estudio de la fortaleza de contraseñas y el uso de herramientas de rotura de las mismas. Para ello, cada grupo de prácticas tendrá que generar varios conjuntos de contraseñas de distinta complejidad y estudiar empíricamente el esfuerzo necesario para romperlas usando distintas estrategias.

Pasos a seguir

1. *Generación de datasets de contraseñas de diferente complejidad*. Genere 25 datasets de 100 contraseñas cada uno. Cada dataset ha de contener contraseñas de una complejidad similar de acuerdo a una cierta combinación de métricas de complejidad. Incluya, al menos, los siguientes datasets:
    a. 5 datasets de contraseñas de longitud 3, …, 7 formadas únicamente por letras minúsculas.
    b. 5 datasets de contraseñas de longitud 3, …, 7 formadas únicamente por letras mayúsculas.
    c. 5 datasets de contraseñas de longitud 3, …, 7 formadas únicamente por números.
    d. 5 datasets de contraseñas de longitud 3, …, 7 formadas por caracteres alfanuméricos (tanto mayúsculas como minúsculas) y símbolos.
    e. Para los restantes 5 datasets, use estrategias que impliquen el uso de palabras tomadas de un diccionario.
    f. **Punto extra opcional**. Repita los pasos anteriores (es decir, genere otros 25 datasets) usando un algoritmo de hashing muy diferente en términos de complejidad del usado para los primeros 25. Por ejemplo, use md5crypt para el primer grupo y SHA-512 para el segundo.
2. Diseñe al menos 5 estrategias diferentes para romper contraseñas usando John the Ripper. Cada estrategia viene definida por un modo de rotura y, cuando proceda, los correspondientes parámetros, reglas o fichero de configuración.
3. Ejecute cada una de las estrategias diseñadas en el paso 2 contra cada uno de los datasets generados en el paso 1. De un tiempo limitado a John the Ripper y deténgalo tras ese tiempo, pues para algunos datasets podría necesitar un tiempo muy elevado en su equipo. Una vez finalizado el proceso para cada dataset, obtenga las siguientes métricas:
    a. Porcentaje de contraseñas rotas
    b. Media y mediana del tiempo requerido para romper una contraseña
4. Organice los resultados obtenidos tabularmente. Cada tabla debe contener una fila por cada dataset y una columna por cada una de las métricas descritas en el paso 3.

Inspecciónelos visual y analíticamente y describa las principales conclusiones que saca de este estudio.

Entregable

Cada grupo de prácticas ha de entregar un informe en el que se incluyan los siguientes apartados:

1. *Generación de los datasets*. Descripción de la estrategia seguida para generar los diferentes datasets de contraseñas de diferente complejidad. Añada como suplemento el código fuente empleado para generarlos.
2. *Metodología*. Descripción de las diferentes configuraciones usadas con John the Ripper para romper los datasets generados en el paso 1. Para cada estrategia, describa el propósito de la misma y el tipo de contraseñas que pretende romper.
3. *Resultados y análisis*. Descripción de los resultados obtenidos, específicamente el número de contraseñas rotas y el tiempo empleado para cada pareja dataset - estrategia. Discuta las principales conclusiones.

Fecha

El plazo para entregar la práctica es de 30 días a partir de la sesión donde se introduce la misma.