Universidad de Alcalá

Seguridad

Tema: Práctica 6 - Auditoría de Contraseñas

Participantes
Carlos Javier Hellín Asensio (carlos.hellin@edu.uah.es)
Darius Dumitras Tamas (darius.tamas@edu.uah.es)
Puesto: 9

Grado de Ingeniería Informática
Curso: 2021-2022

Datos técnicos

- Nombre de los ficheros analizados:
    - raw-md5.hashes9.txt
    - raw-md5.hashes2.txt

- Herramientas
    - Hashcat que viene instalado en los ordenadores de laboratorio
    - Hashcat 6.2.5 y 2.00 usando Kali en una máquina virtual

- Diccionarios usados y descargados de blackboard
    - 500_passwords.txt
    - passwords.txt
    - rockyou.txt

Resumen ejecutivo

El ataque por fuerza bruta ha resultado poco eficiente en cuanto al tiempo que tarda en encontrar contraseñas, aunque depende del tamaño de la máscara usada. Aun así, se han encontrado bastantes contraseñas. Con los diccionarios se ha visto que es más eficiente, aunque depende de emplear un diccionario apropiado, ya que se han encontrado menos contraseñas en algún caso cuando el diccionario era menos adecuado. Siguiendo con los diccionarios, al realizar una combinación de estos ha sido el logro más importante que se ha alcanzado, puesto que se han extraído más contraseñas que en cualquier ataque. El ataque híbrido también ha resultado útil, al permitir utilizar un diccionario apropiado y añadir más combinaciones posibles que puedan cubrir otras opciones que no tenga el propio diccionario. En cuanto a las permutaciones, han tenido un éxito medio de utilidad, puesto que también depende mucho del diccionario a permutar. Por último, en el ataque de reglas ha habido un caso donde se han encontrado bastantes contraseñas, pero se ve claramente que depende mucho de si las reglas tienen un buen fundamento y han sido bien creadas.

Fichero 1: raw-md5.hashes9.txt

Fuerza bruta

Se quiere conseguir un ataque generando palabras al vuelo siguiendo un patrón especificado, obteniendo un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat -m 0 -a 3 -o bruta1.txt  raw-md5.hashes9.txt --potfile-disable ?l?l?l?l?l?l?l?l
```

Ejemplo de las contraseñas que se generan son de 8 letras minúsculas: aaaaaaaa, mifbksco, awctgidl, pufsooth, sdbcisco, etc

```
Recovered........: 25128/3500000
```

```
Started: Sat May 14 10:45:47 2022
Stopped: Sat May 14 10:50:07 2022
```

Se han encontrado un total de 25.128 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 4 minutos, 20 segundos y el esfuerzo máximo es de 26^8 minúsculas = 208.827.064.576 hashes.

Straight

Se quiere conseguir un ataque usando el diccionario passwords.txt obteniendo un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat -m 0 -a 0 -o straight1.txt  raw-md5.hashes9.txt passwords.txt --potfile-disable
```

Ejemplo de las contraseñas del diccionario son:12345, dictum, biology, soccer1, etc.

```
Recovered........: 24/3500000 (0.00%)
```

```
Started: Sat May 14 10:54:07 2022
Stopped: Sat May 14 10:54:57 2022
```

Se han encontrado un total de 24 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 50 segundos y el esfuerzo máximo es de 2.293 hashes.

Combinator Attack

Se quiere conseguir un ataque que combina dos diccionarios para obtener un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat -m 0 -a 1 -o combinador1.txt raw-md5.hashes9.txt passwords.txt 500 passwords.txt --potfile-disable
```

Ejemplo de las contraseñas de combinar los dos diccionarios son: albertvenus, albertzeppelin, jimbo123456, dictumalbert, etc.

```
Recovered........: 9929/3500000
```

```
Started: Sat May 14 10:58:09 2022
Stopped: Sat May 14 10:59:03 2022
```

Se han encontrado un total de 9.929 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 6 segundos y el esfuerzo máximo es de 2.293 + 502 = 2.795 hashes.

Hybrid Attack

Se quiere conseguir un ataque con diccionario y un patrón especificado para obtener un archivo con las contraseñas Se utiliza la siguiente orden:

```
└─$ hashcat --force -m 0 -a 6 -o hybrid1.txt raw-md5.hashes9.txt rockyou.txt ?l?l?l?l --potfile-disable
```

Ejemplo de las contraseñas que junto al diccionario se generan 4 letras minúsculas son: 123456adsg, loversinjkw, 654321wxyz, abcdefgxyz, etc.

```
Recovered........: 12936/3500000
Started: Sat May 14 11:06:39 2022
Stopped: Sat May 14 11:10:50 2022
```

Se han encontrado un total de 12.936 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 36 segundos y el esfuerzo máximo es de 26^4 * 14.344.392 = 6.555.042.878.592 hashes.

Permutation

Se quiere conseguir un ataque usando permutaciones de las letras pertenecientes a las palabras dentro del diccionario 500_passwords.txt obteniendo un archivo con las contraseñas. Se utiliza la siguiente orden:

```
─$ hashcat-cli64.bin -m 0 -a 4 -o permutation1.txt raw-md5.hashes9.txt 500_passwords.txt --potfile-disable
```

Ejemplo de las contraseñas que se generan permutaciones del diccionario son: password, wrodssap, ggiedo, ssecnirp, etc.

```
Recovered.: 360/3500000 hashes
Started: Sat May 14 12:24:24 2022
Stopped: Sat May 14 12:24:28 2022
```

Se han encontrado un total de 360 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 4 segundos y el esfuerzo máximo es una aproximación de 502 contraseñas del diccionario * 8! letras de media por palabra = 20.240.640 hashes.

Rule-based Attack

Se quiere conseguir un ataque utilizando un diccionario que se aplican reglas a cada palabra obteniendo un archivo con las contraseñas. Se utiliza la siguiente orden:

```
─$ hashcat -m 0 -a 0 -o reglas1.txt raw-md5.hashes9.txt 500_passwords.txt -r /usr/share/hashcat/rules/best64.rule --potfile-disable
```

Ejemplo de las contraseñas que se generan junto a las reglas son: 123456, atatat, rebecca00, 6666123, etc.

```
Recovered........: 324/3500000 (0.01%)
Started: Sat May 14 13:09:01 2022
Stopped: Sat May 14 13:09:15 2022
```

Se han encontrado un total de 324 contraseñas, de entre las 3.500.500 que tiene el fichero. Ha tardado 14 segundos y el esfuerzo máximo es de 502 contraseñas del diccionario * 77 reglas = 38.654 hashes.

Fichero 2: raw-md5.hashes2.txt

Fuerza bruta

Se quiere conseguir un ataque generando palabras al vuelo siguiendo un patrón especificado, obteniendo un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat -m 0 -a 3 -o bruta2.txt raw-md5.hashes2.txt --potfile-disable ?l?l?l?l?l?d?d
```

Ejemplo de las contraseñas que se generan con 5 letras minúsculas y 2 números son: fkxdq64, xqxqx57, raoul57, catou57, etc.

```
Recovered........: 14201/3500000
```

```
Started: Sat May 14 13:41:19 2022
Stopped: Sat May 14 13:42:06 2022
```

Se han encontrado un total de 14.201 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 47 segundos y el esfuerzo máximo es de 26^5 * 10^2 = 1.188.137.600 hashes.

Straight

Se quiere conseguir un ataque usando el diccionario 500_passwords.txt obteniendo un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat -m 0 -a 0 -o straight2.txt raw-md5.hashes2.txt 500_passwords.txt --potfile-disable
```

Ejemplo de las contraseñas del diccionario son: 12345, albert, donald, ladies, etc.

```
Recovered........: 5/3500000
```

```
Started: Sat May 14 13:47:30 2022
Stopped: Sat May 14 13:47:43 2022
```

Se han encontrado un total de 5 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 13 segundos y el esfuerzo máximo es de 502 hashes.

Combinator Attack

Se quiere conseguir un ataque que combina dos diccionarios para obtener un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat -m 0 -a 1 -o combinator2.txt raw-md5.hashes2.txt 500_passwords.txt rockyou.txt --potfile-disable
```

Ejemplo de las contraseñas de combinar los dos diccionarios son: 123456princessere, albertprincess-xx,12345angel, baseballfootball, etc.

```
Recovered........: 34078/3500000
```

```
Started: Sat May 14 14:01:56 2022
Stopped: Sat May 14 14:04:31 2022
```

Se han encontrado un total de 34.078 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 215 segundos y el esfuerzo máximo es de 502 + 14.344.392 = 14.344.894 hashes.

Hybrid Attack

Se quiere conseguir un ataque con diccionario y un patrón especificado para obtener un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat -m 0 -a 6 -o hybrid2.txt raw-md5.hashes2.txt passwords.txt ?l?l?d?d --potfile-disable
```

Ejemplo de las contraseñas que junto al diccionario se generan 2 letras minúsculas y 2 números son: researchrq83, dictumxq83, 1234qwerhg00, Pigletbu39, etc.

```
Recovered........: 1878/3500000
```

```
Started: Sat May 14 14:10:05 2022
Stopped: Sat May 14 14:10:48 2022
```

Se han encontrado un total de 1.878 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 43 segundos y el esfuerzo máximo es de 2.293 * 26^2 * 10^2 = 155.006.800 hashes.

Permutation

Se quiere conseguir un ataque usando permutaciones de las letras pertenecientes a las palabras dentro del diccionario passwords.txt obteniendo un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat-cli64.bin -m 0 -a 4 -o permutation2.txt raw-md5.hashes2.txt passwords.txt --potfile-disable
```

Ejemplo de las contraseñas que se generan permutaciones del diccionario: researchrq83, dictumxq83, ixamen, servil, etc.

```
Recovered.: 965/3500000 hashes
```

```
Started: Sat May 14 14:17:14 2022
Stopped: Sat May 14 14:17:19 2022
```

Se han encontrado un total de 965 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 5 segundos y el esfuerzo máximo es una aproximación de 2.293 contraseñas del diccionario * 7! letras de media por palabra = 11.556.720 hashes.

Rule-based Attack

Se quiere conseguir un ataque utilizando un diccionario que se aplican reglas a cada palabra obteniendo un archivo con las contraseñas. Se utiliza la siguiente orden:

```
└─$ hashcat -m 0 -a 0 -o reglas2.txt raw-md5.hashes2.txt passwords.txt -r /usr/share/hashcat/rules/generated.rule
```

Ejemplo de las contraseñas que se generan junto a las reglas son: ijimbo, ticdum, Elwood6, happy!!!, etc.

```
Recovered........: 16527/3500000
```

```
Started: Sat May 14 14:36:56 2022
Stopped: Sat May 14 14:37:19 2022
```

Se han encontrado un total de 16.527 contraseñas, de entre las 3.500.000 que tiene el fichero. Ha tardado 23 segundos y el esfuerzo máximo es de 2.293 contraseñas del diccionario * 14.734 reglas = 33.785.062 hashes.

Bibliografía

How I became a password cracker
https://arstechnica.com/information-technology/2013/03/how-i-became-a-password-cracker/

Getting Hashcat 2.00 - HASHCAT con VM Linux
https://samsclass.info/123/proj10/p12-hashcat.htm

Hashcat Wiki https://hashcat.net/wiki/

Hashcat doesn't write to output file
https://security.stackexchange.com/questions/193621/hashcat-doesn-t-write-to-output-file