Password cracking

ERNESTO ROBLES

Dispotivi coinvolti

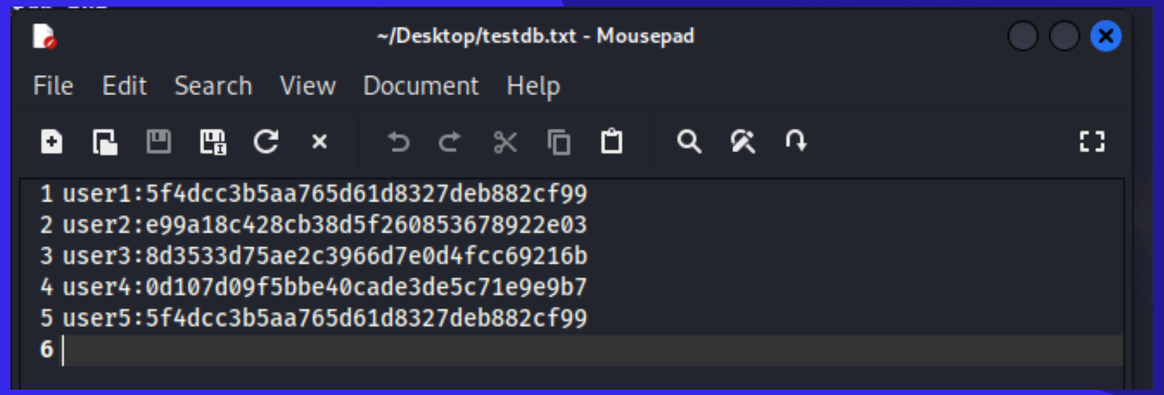
MACCHINA KALI: 192.168.1.60
MACCHINA METASPOITABLE: 192.168.1.67

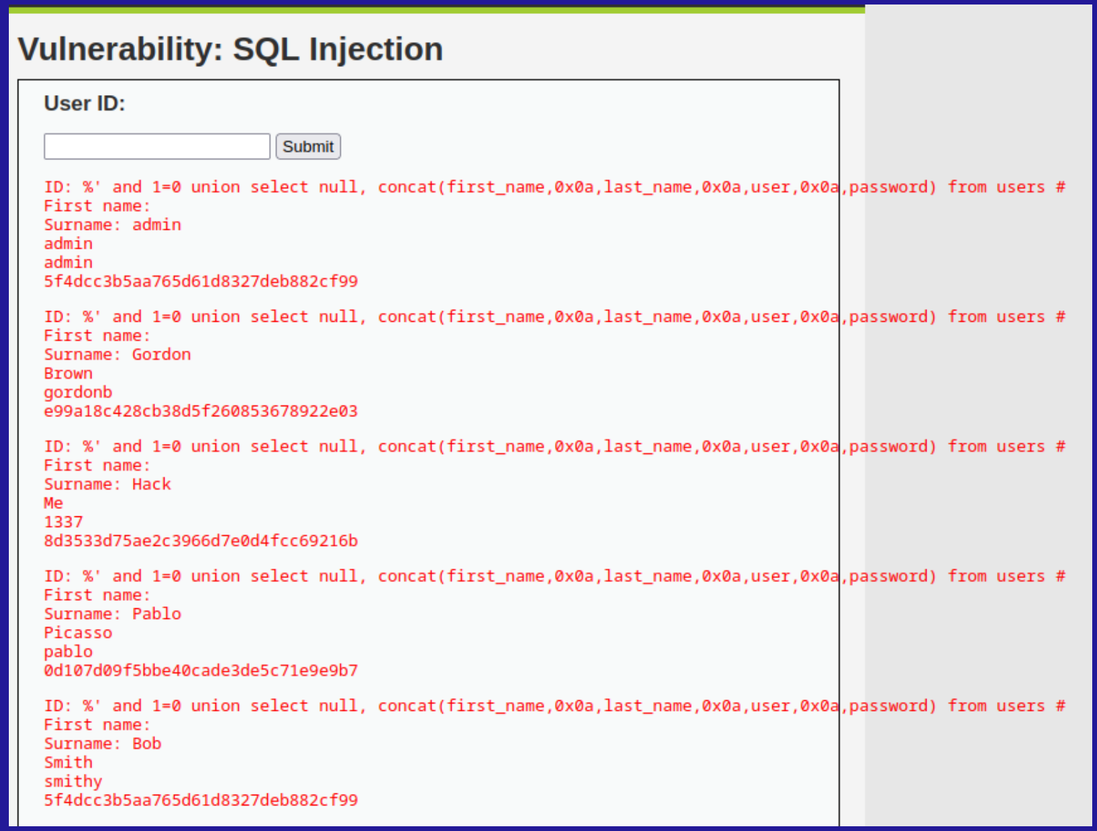
Strumenti utilizzati

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

PASSWORD HASH

Sfruttando le SQL Injection si estraggono dati dal databse 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.





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.

```
┌──(kali3㉿kali3)-[~/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.