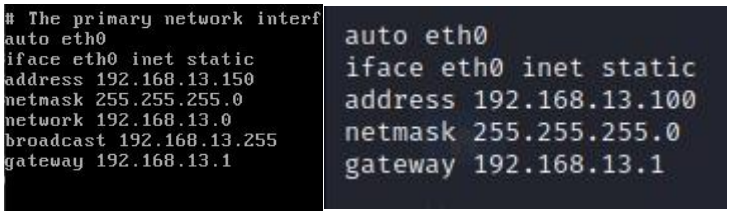
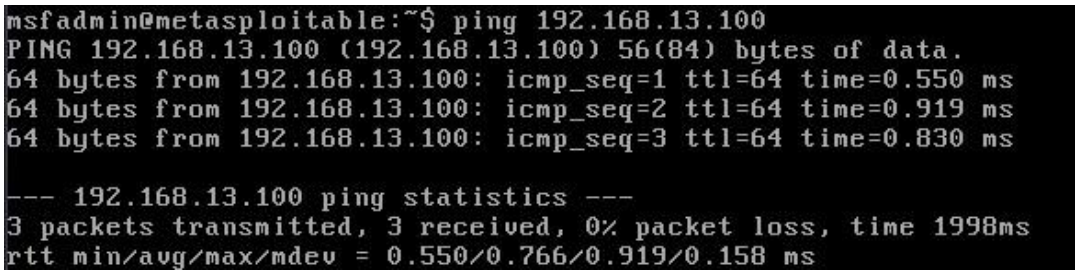
Simone Tartaglia

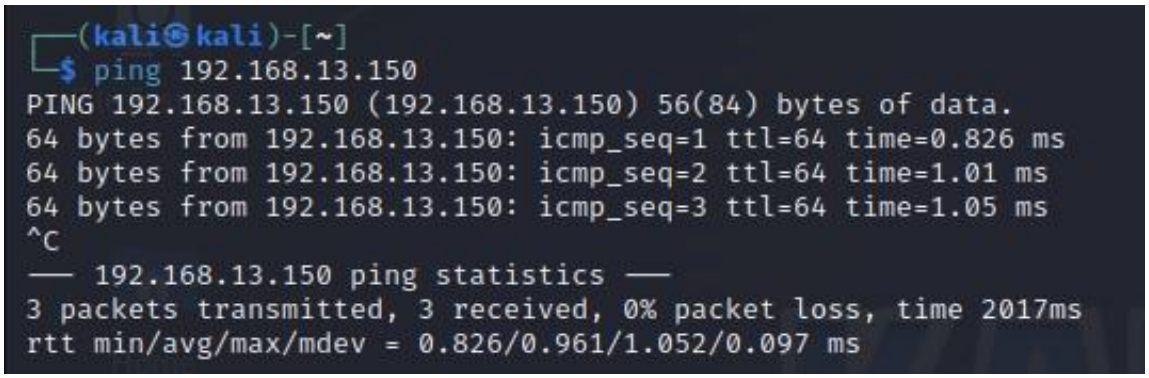
Progetto Modulo 4 Esercizio 1 SQL injection

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



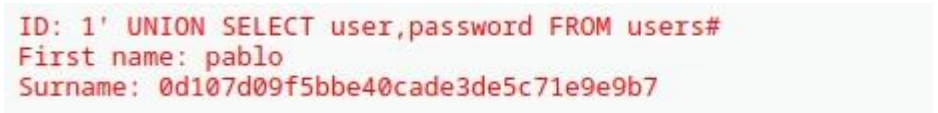
Dopo aver cambiato gli IP verifico che le due macchine comunichino con il comando "ping".





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

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



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 8×3])
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.
```