Come primo punto cambiamo gli IP delle 2 macchine come da traccia

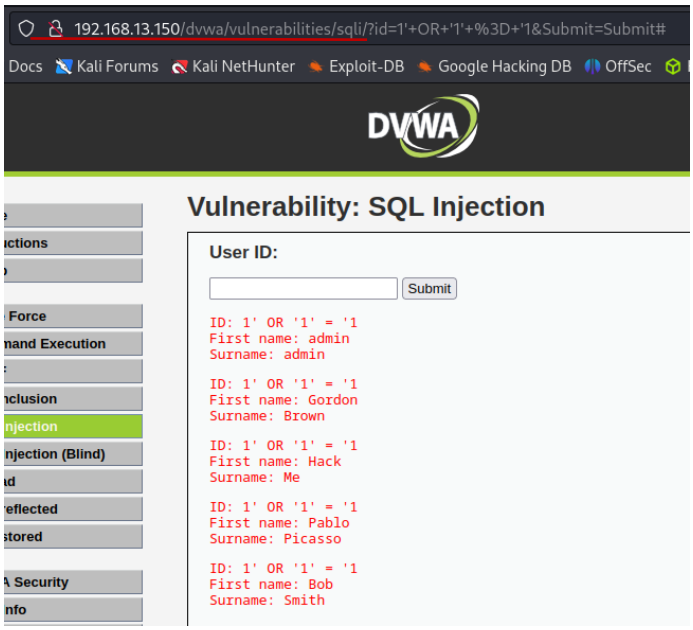
IP Kali:

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.13.100  netmask 255.255.255.0  broadcast 192.168.13.255
        inet6 fe80::a00:27ff:fec6:9a57  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c6:9a:57  txqueuelen 1000  (Ethernet)
        RX packets 29  bytes 4633 (4.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 3904 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

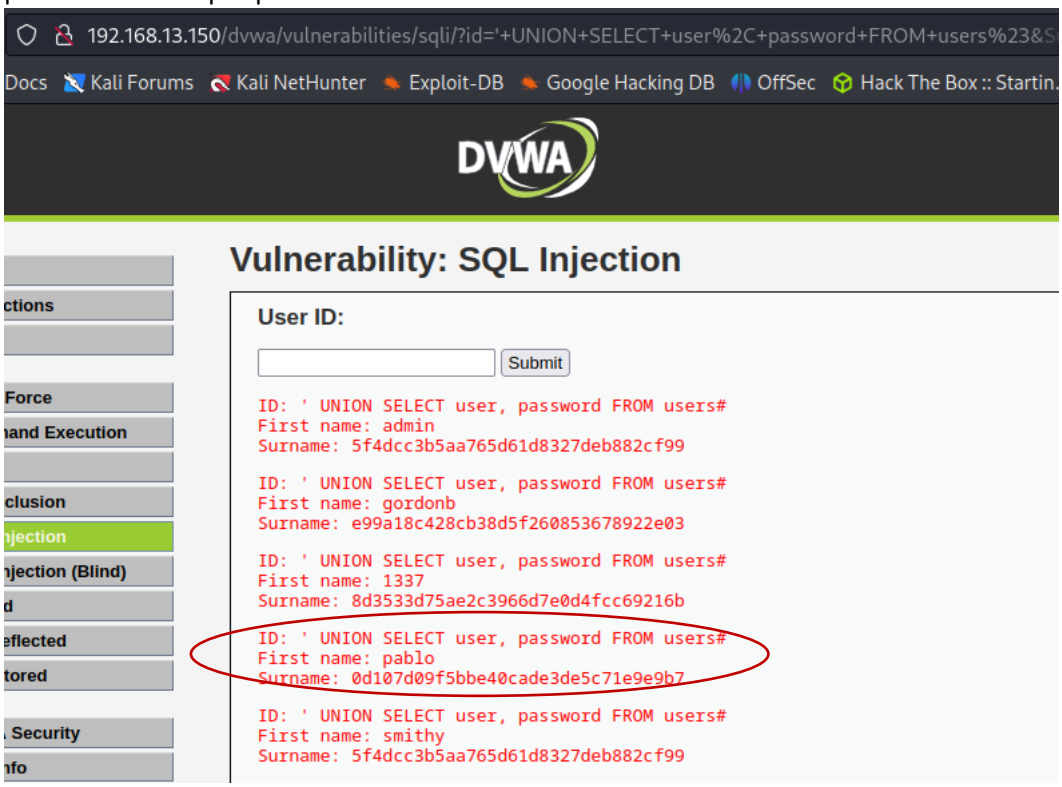
IP Metasploitable:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5c:ef:24
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5c:ef24/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3240 (3.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)
```

Dopo aver settato gli IP raggiungiamo la DVWA della macchina Kali via browser e settiamo la sicurezza LOW, successivamente ci spostiamo sulla scheda SQL Injection e inseriamo il primo comando per recuperare i nomi utenti (1’ or ‘1’ = ‘1). Otteniamo così l’user Pablo Picasso.



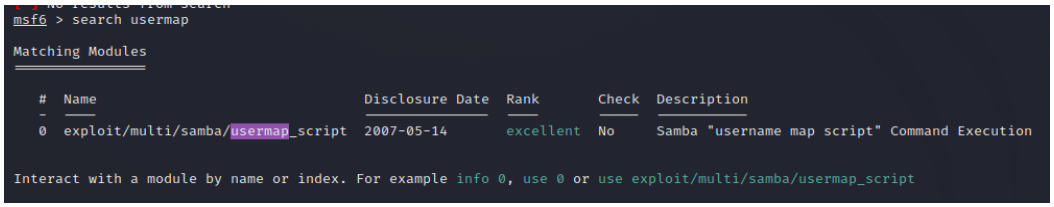
Successivamente tramite l'unione di più comandi cerchiamo di ottenere la password dell'utente (' UNION SELECT user, password FROM users#), otteniamo quindi la password cifrata che dovremo successivamente portare in chiaro per poterla usare.



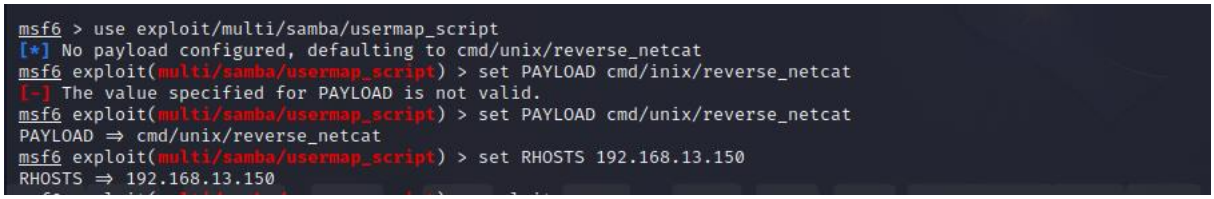
Dopo averla quindi decifrata con crackstation otteniamo quindi l'account **Pablo Picasso** con password **letmein**.

Hash	Type	Result
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

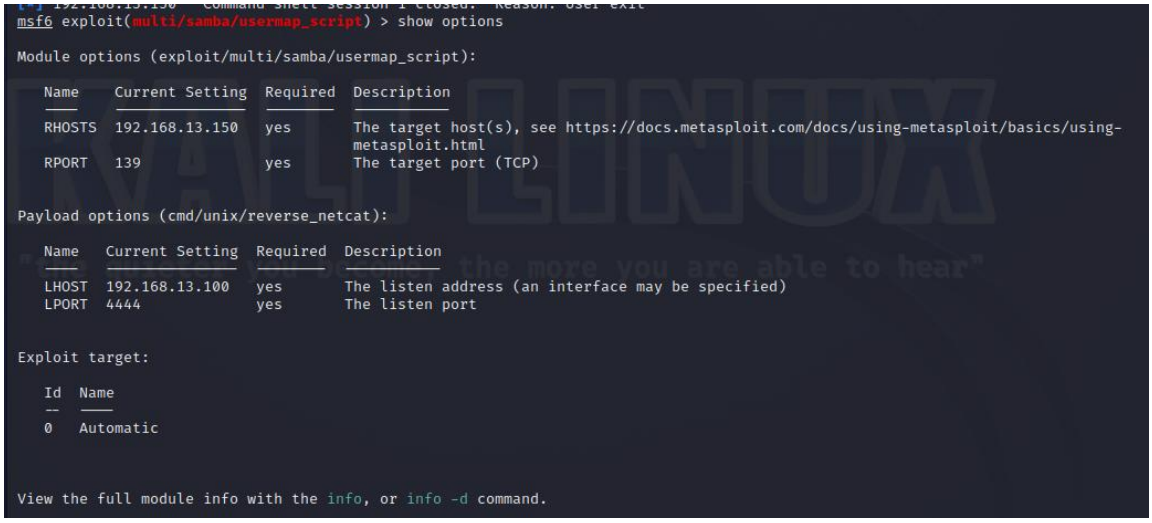
La seconda parte dell'esercizio riguarda l'utilizzo di una vulnerabilità attiva sulla porta 445 TCP usando msfconsole. Dopo aver avviato msfconsole facciamo una ricerca dell'exploit suggerito:



Successivamente settiamo tutti i vari parametri tra cui il PAYLOAD e l'RHOSTS



ed eseguiamo il comando show options per controllare di aver fatto tutto correttamente



Infine possiamo lanciare l'exploit tramite comando exploit, vediamo che otteniamo una sessione aperta da 192.168.13.100 verso 192.168.13.150, eseguiamo poi il comando ifconfig per conferma.