**Experiment No. 12**

# Title: Metasploit Part I - Exploiting VSFTPD

**Roll No.: 16010420075 Experiments No.: 12**

# Aim: Exploit VSFTPD by performing an attack and transfer a file.

\

**Resources:** virtual box

**Theory**

Metasploitable is a Linux virtual machine that is designed to be vulnerable. This virtual machine can be used for security teaching, tool testing, and typical penetration testing approaches.

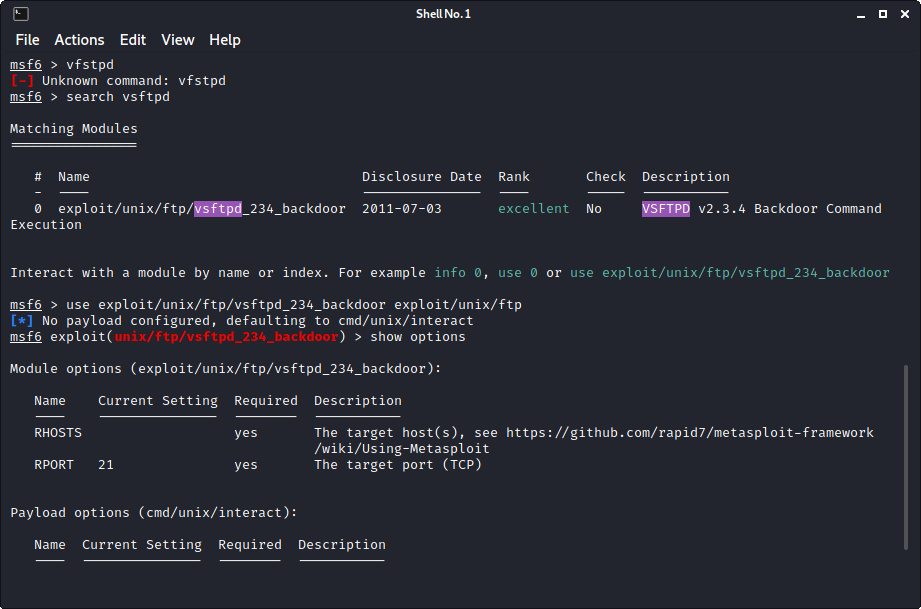
The attack on VSFTPD 2.3.4 is based on transmitting a series of specified bytes on port 21 to activate the malicious vsf sysutil extra(); function, which, if executed successfully, opens the system's backdoor on port 6200.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**IMPLEMENTATION AND RESULTS:**

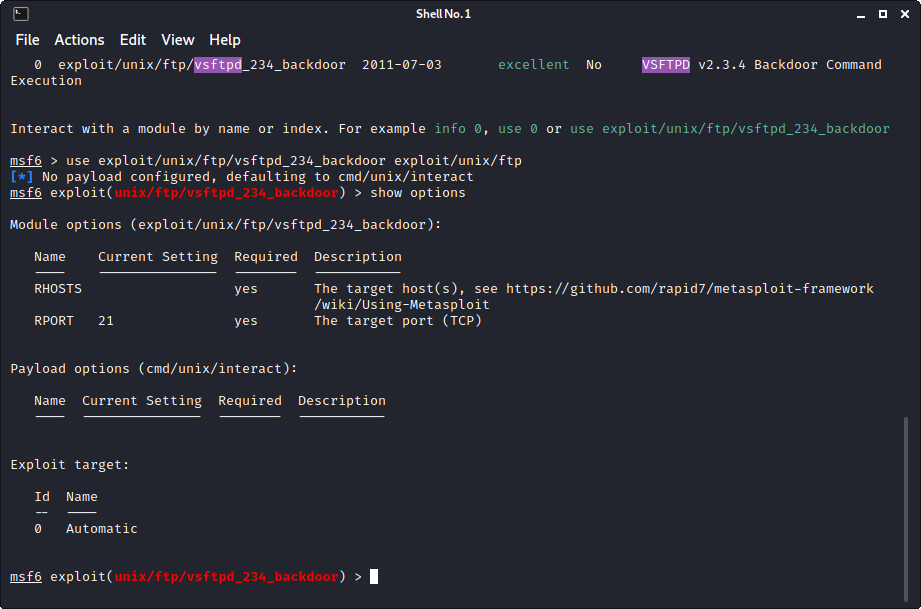
**Step 1:** Open Metasploitable machine and login.

**Step 2:** Search for VSFTPF 2.3.4 vulnerability in Metasploit framework using ‘search vsftpd’

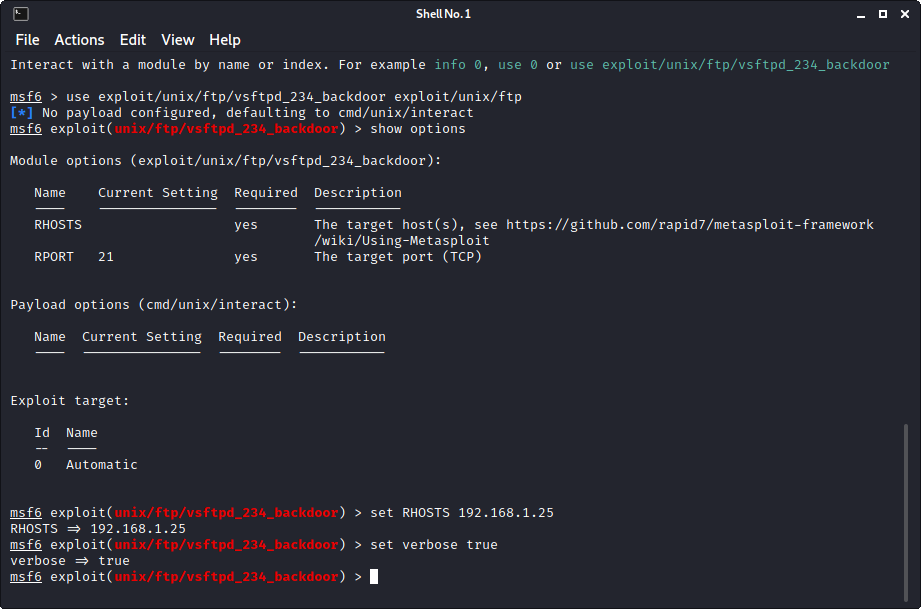


**Step 3:** Copy the exploit name and enter it in the command ‘use <enter exploit> exploit/unix/ftp’

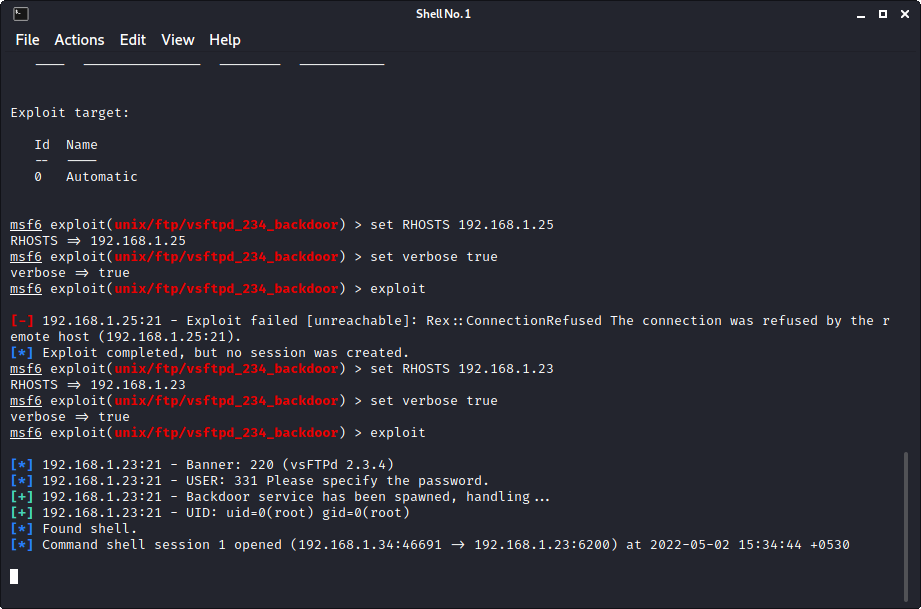
**Step 4:** Look for options of attack using ‘show options’, here we see the types of attack that can be performed.



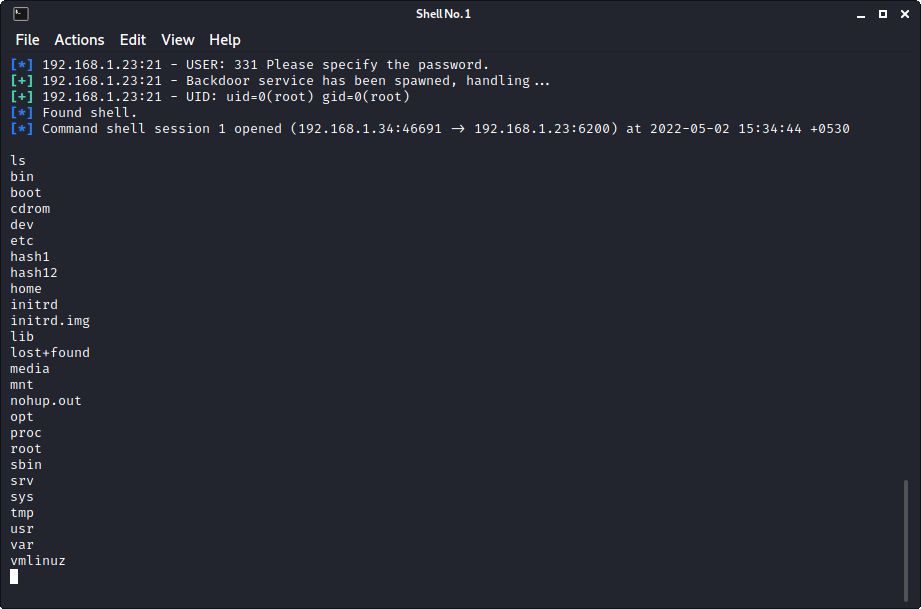
**Step 5:** Set RHOSTS to the victim IP using ‘set RHOSTS <victim’s IP>’



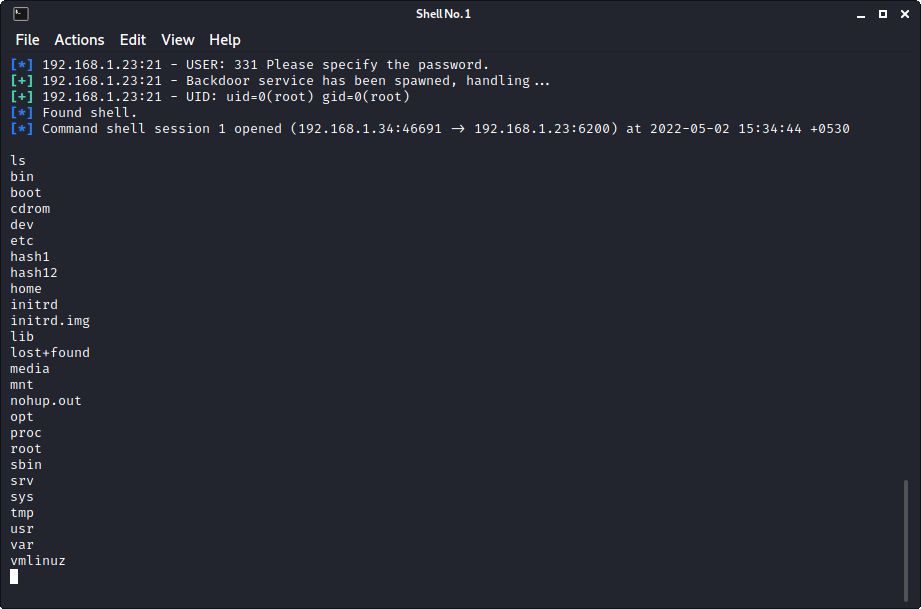
**Step 6:** Next, use the command to set verbose using ‘set verbose true’



**Step 7:** Exploit. Enter ‘exploit’.

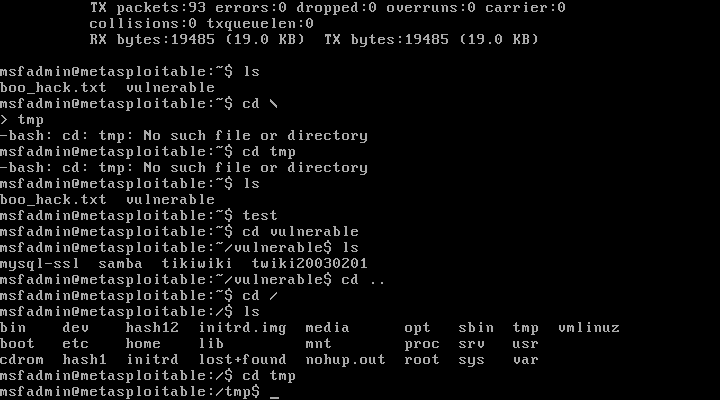


**Step 8:** List the files. Use ‘ls’.



**Step 9:** We’re in.Use ‘cd tmp’ to go to the temp folder in the exploited machine. Then create a test folder using ‘mkdir test’ and create a file ‘echo adfsf test.txt’



**Step 10:** Check the folders inside to see if the file is present. If found, attack is successful!

**Outcomes:**

**CO-3:** Understand attack methodology

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion: (Conclusion to be based on the objectives and outcomes achieved)**

Metasploitable 2 was used as an attack machine to exploit vsftpd 2.3.4 using Metasploit framework.

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**REFERENCES:**

* [www.kali.org](http://www.kali.org)