# Metasploit Server Code Exploitation

Activities

[Server Code Exploitation 1](#_Toc90496903)

[How to Create Screenshots 1](#_Toc90496904)

[Find and Exploit the Vulnerability 1](#_Toc90496905)

[Assignment Submission 3](#_Toc90496906)

Time needed: 30 minutes

## How to Create Screenshots

Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

# Find and Exploit the Vulnerability

Time Required: 30 minutes

Objective: Find the vulnerability.

1. Start **Metasploitable 2**.
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 >> nmapscan**
5. Type: **less nmapscan**
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.

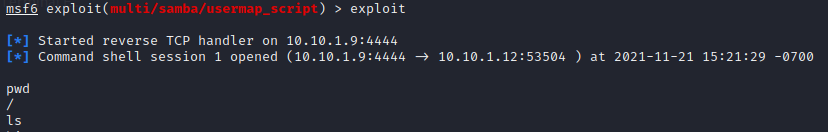


Payloads are small pieces of code that will run on the target computer once the vulnerability has been exploited.

1. To show the options that can be set, type: **show options**
2. The exploit is already set to port **139**.
3. Use the set RHOST command to set the IP address of the target.  
   **set RHOST IPADDRESS**
4. Type: **show options**
5. 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. 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 execute any command you wish on the exploited server.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.