## **Question 1: BACKDOOR AND PRIVILEGE ESCALATION (20 MARKS)**

**For each step, screen shot and explain the result.**

**Objective**: Exploit the backdoor in vsftpd 2.3.4 to gain shell access on the vulnerable target machine using Metasploit, then use *local\_exploit\_suggester* for privilege escalation.

**Requirements**:

* Kali Linux (or any Metasploit-installed machine)
* A vulnerable target machine (e.g., Metasploitable 2)
* Both machines are on the same network

**Scenario**:

You have discovered a server (IP: 192.168.56.101) running an FTP service. A vulnerability scan shows it is running vsftpd 2.3.4, which is known to have a backdoor. Your task is to exploit this vulnerability and gain access to the target and do privilege escalation.

**Step 1**: Run Metasploit. **(1 mark)**

**Step 2**: Search for the exploit. **(2 marks)**

**Step 3**: Use the exploit with the backdoor. **(3 marks)**

**Step 4**: Set the target IP. **(3 marks)**

**Step 5**: Exploit the target. **(3 marks)**

**Step 6**: Interact with the shell. Show the session created. **(3 marks)**

**Step 7**: Use and run Metasploit's post/multi/recon/local\_exploit\_suggestor. **(5 marks)**

## **QUESTION 2: REVERSE SHELL (30 MARKS)**

**For each step, screen shot and explain the result.**

**Objective**: Gaining a reverse shell via PHP Web Shell

**Requirements**:

* Kali Linux (or any Metasploit-installed machine)
* Target: Metasploitable 2 or a VM running vulnerable Apache Tomcat
* Apache Tomcat with default credentials (id: tomcat password:tomcat)

**Scenario**:

You have discovered that a host at 192.168.56.103 is running **Apache Tomcat 7.0.XX** with default credentials.

Your task is to:

1. Exploit Apache Tomcat Manager using Metasploit
2. Use a **reverse shell payload**
3. Gain access to the target machine

**Step 1**: Run metasploit. **(1 mark)**

**Step 2**: Search for Tomcat Manager exploit. **(2 marks)**

**Step 3**: Use the exploit. **(3 marks)**

**Step 4**: Set the RHOSTS, RPORT (use default Tomcat port), HTTPUSERNAME, HTTPPASSWORD and TARGETURI. **(10 marks)**

**Step 5**: Set a reverse shell payload (*java/meterpreter/reverse\_tcp*), LHOST and LPORT. **(5 mark)**

**Step 6**: Launch the exploit. **(3 marks)**

**Step 7**: Interact with the shell by using command *sessions*. Use *getuid* and *sysinfo*. **(3 marks)**

**Step 8**: Drop to a regular shell. The screen should return result as follows:

shell

whoami

uname -a

Show the similar result with a similar screen shot. **(3 marks)**

**END OF QUESTION**