Assignment: Metasploit & Msfcli Hands-on

Question 1: Metasploit Basics

Explain the difference between a **bind shell** and a **reverse shell** in Metasploit. Provide an example of when you would use each.

Question 2: Searching for Exploits

Use Metasploit to search for vulnerabilities related to **Ubuntu**. Write the command you used and list any two exploits you found.

Question 3: Exploit Module Configuration

You have identified `ms08_067_netapi` as an exploit for a Windows XP target. Write the Metasploit commands to:

1. Use the exploit
2. Show the available options
3. Set the target IP to `192.168.1.100`
4. Set the payload to `windows/shell_reverse_tcp`

Question 4: Msfcli Execution

Using **Msfcli**, write a single command to exploit a Windows XP machine at `192.168.1.100` using `ms08_067_netapi` with a **bind shell payload**.

Question 5: Understanding Exploit Execution

After executing an exploit in Metasploit, explain what happens step by step when a reverse shell is used. Include:

- What Metasploit does when you run `exploit`
- How the target machine responds
- How the attacker gains access