Penetration Test Workshop (CSE3157)

metasploit

Dr. Rourab Paul

Computer Science Department, SOA University

Digital Forensic

Introdcution

Metasploit is one of the most popular frameworks for penetration testing, vulnerability assessment, and exploitation. It provides security professionals and ethical hackers with tools to identify, exploit, and validate vulnerabilities in systems. Developed by Rapid7, the framework is open-source and widely used for ethical hacking and cybersecurity.

Key Features

1. **Exploitation**: Provides a library of pre-built exploits for vulnerabilities in various systems and software.
2. **Payloads**: Offers a variety of payloads to establish communication between the target and the attacker (e.g., reverse shells, Meterpreter).
3. **Post-Exploitation**: Enables further exploitation of a compromised system, such as privilege escalation, gathering sensitive data, or pivoting to other systems.
4. **Auxiliary Modules**: Includes scanners, fuzzers, and other tools to gather information or exploit non-vulnerable weaknesses.
5. **Custom Scripts**: Allows users to create custom exploits and payloads to target specific vulnerabilities.
6. **Multi-Platform Support**: Compatible with Windows, Linux, macOS, and mobile platforms.

Components

Exploits:

- Code designed to take advantage of specific vulnerabilities in software or systems.

Payloads:

- Code executed on the target after exploitation (e.g., shells, Meterpreter sessions).
- Examples include:
  - **Reverse shell:** The target connects back to the attacker.
  - **Bind shell:** The attacker connects to a shell on the target.
  - **Meterpreter:** An advanced, multi-functional payload.

Encoders:

- Used to obfuscate payloads and bypass antivirus systems.

Auxiliary Modules:

- Tools for scanning, fingerprinting, or brute-forcing services.

Post-Exploitation Modules:

- Tools to gather further information or perform actions after successful exploitation.

Types of Payloads

- **Single Payloads**:
  - Self-contained and perform an action without needing additional stages.
  - Example: Creating a new user.
- **Staged Payloads**:
  - Delivered in parts (stages) to bypass size limitations or detection.
  - Example: Initial shell followed by a Meterpreter session.

Work flow

Information Gathering:

- Use auxiliary modules like port scanners or vulnerability scanners to enumerate the target.
- Example: auxiliary/scanner/portscan/tcp.

Vulnerability Analysis:

- Identify known vulnerabilities in the target.
- Use tools like Nmap, Nessus, or Metasploit's vulnerability scanner.

Exploitation:

- Choose an appropriate exploit module for the identified vulnerability.
- Set the required parameters (e.g., target IP, port).
- Execute the exploit to gain access.

Post-Exploitation:

- Use post-exploitation modules for privilege escalation, lateral movement, or data exfiltration.

Cover Tracks:

- Use stealth techniques to remove logs or artifacts left on the target.

Thank You