InSkill:-

1.Dheeraj is learning Reaver. As a beginner he wants to know the use of following commands in Reaver:- i) Wash ii) Reaver

a)**Wash:**
The `wash` command scans for nearby Wi-Fi networks with WPS enabled and displays information such as the network's SSID, BSSID, and WPS version. This helps Dheeraj identify vulnerable networks that can be targeted using Reaver.

Wash Command:

sudo wash -i <interface>

b)**Reaver:**
The `reaver` command launches a brute-force attack on the WPS PIN of a selected Wi-Fi network. It systematically guesses the PIN to crack it, allowing Dheeraj to obtain the WPA/WPA2 passphrase. Reaver also includes options to customize the attack, such as setting the timeout and delay between attempts to increase the chances of success.

Reaver Command:

sudo reaver -i <interface> -b <BSSID> -c <channel> -vv

2. Write down the wireless interface names, monitor mode, ESSID, Channel, BSSID of the target and paste the screen shots of execution and the outputs.

Steps to Perform Wi-Fi Hacking Using Reaver (Educational Purposes Only):

1. **Identify Your Wireless Interface:**
   - Open a terminal and type:

     ```
     iwconfig
     ```

   - This will list all wireless interfaces. Look for something like `wlan0` or `wlan1`.
2. **Enable Monitor Mode:**
   - To put your wireless interface into monitor mode, type:

     ```
     sudo airmon-ng start <interface>
     ```

   - Replace `<interface>` with your wireless interface name (e.g., `wlan0`).
   - After running the command, your interface name might change to something like `wlan0mon`.
3. **Scan for WPS-Enabled Networks:**
   - Use the `wash` command to find WPS-enabled networks:

     ```
     sudo wash -i <monitor_interface>
     ```

- Replace `<monitor_interface>` with the name of your interface in monitor mode (e.g., `wlan0mon`).
- This will display the ESSID, BSSID, Channel, and other details of the WPS-enabled networks.

4. **Note Down the Information:**
   - Identify the target network and note down the following:
     - **ESSID:** The network name (e.g., `MyWiFiNetwork`).
     - **BSSID:** The MAC address of the network (e.g., `00:11:22:33:44:55`).
     - **Channel:** The channel on which the network is operating (e.g., `6`).
     - **Monitor Interface:** The name of your interface in monitor mode (e.g., `wlan0mon`).
5. **Run Reaver:**
   - Now, initiate the Reaver attack with the following command:

     ```
     sudo reaver -i <monitor_interface> -b <BSSID> -c <Channel> -vv
     ```

   - Replace `<monitor_interface>`, `<BSSID>`, and `<Channel>` with the values you noted down.
6. **Output and Screenshots:**
   - The terminal will start displaying the progress of the Reaver attack. If successful, it will eventually display the WPS PIN and the WPA/WPA2 passphrase.
   - You can take a screenshot of the terminal window using your operating system's screenshot tool.