InSkill:-

1)a. **Ping Sweep:**

- **Command:** `nmap -sn <target-range>`
- **Example:** `nmap -sn 192.168.1.0/24`
- **Description:** Identifies live hosts in a network without scanning ports.

b. **Port Scan:**

- **Command:** `nmap -p <port-range> <target>`
- **Example:** `nmap -p 22,80 192.168.1.1`
- **Description:** Scans specified ports on a target host to check which ones are open.

c. **TCP Full Open Scan:**

- **Command:** `nmap -sT <target>`
- **Example:** `nmap -sT 192.168.1.1`
- **Description:** Completes the TCP handshake with the target, identifying open ports.

d. **TCP SYN Scan:**

- **Command:** `nmap -sS <target>`
- **Example:** `nmap -sS 192.168.1.1`
- **Description:** Sends SYN packets and detects open ports without completing the handshake.

e. **UDP Scan:**

- **Command:** `nmap -sU <target>`
- **Example:** `nmap -sU 192.168.1.1`
- **Description:** Scans UDP ports to identify which ones are open.

f. **Version Detection Scan:**

- **Command:** `nmap -sV <target>`
- **Example:** `nmap -sV 192.168.1.1`
- **Description:** Detects the version of services running on open ports.

g. **OS Detection Scan:**

- **Command:** `nmap -O <target>`
- **Example:** `nmap -O 192.168.1.1`
- **Description:** Identifies the operating system of the target host based on TCP/IP stack responses.

h. **Aggressive Scan:**

- **Command:** `nmap -A <target>`

- **Example:** `nmap -A 192.168.1.1`
- **Description:** Performs an extensive scan including OS detection, version detection, script scanning, and traceroute.