PreSkill:-

1.**What is NMAP, and why is it used for network scanning?**
NMAP is a network scanning tool used to discover hosts and services on a network, identify open ports, and assess security. It helps in network inventory and vulnerability assessment.

2.**Describe the different types of scanning techniques supported by NMAP.**
NMAP supports techniques like TCP SYN scan (stealth scan), TCP connect scan (full open scan), UDP scan (for finding open UDP ports), and OS detection, among others.

3.**How can you perform a TCP SYN scan using NMAP? Explain the steps involved.**
Use the command `nmap -sS <target>`, where `<target>` is the IP address or hostname. This performs a stealth scan by sending SYN packets to determine open ports without completing the TCP handshake.

4.**What is the purpose of performing a UDP scan? How can you execute it using NMAP?**
A UDP scan identifies open UDP ports on a target system, as UDP services are often less monitored. Execute it with `nmap -sU <target>`, where `<target>` is the IP address or hostname.

5.**What is a comprehensive scan? How is it different from other scanning techniques?**
A comprehensive scan performs detailed checks including port scanning, service detection, and OS fingerprinting. It provides a thorough assessment compared to basic scans that may only check for open ports.

VIVA:-

1.**Explain the concept of stealth scanning and how it can be achieved with NMAP.**
Stealth scanning minimizes detection by avoiding a full TCP handshake. NMAP achieves this with the TCP SYN scan (`-sS`), which sends SYN packets to ports and waits for responses without completing the handshake.

2.**How does NMAP identify the operating system of a target host? Discuss the techniques used.**
NMAP uses OS fingerprinting to identify a target's OS by analyzing TCP/IP stack responses. It sends various probes and examines the responses to match patterns against a database of known OS signatures.

3.**What is banner grabbing, and why is it useful during a network scan? How can NMAP accomplish banner grabbing?**
Banner grabbing involves retrieving and analyzing service banners to gather information about software versions. NMAP accomplishes this with service detection (`-sV`), which queries services to identify and display their banners.

4.**What are some common options and flags used in NMAP? Provide examples and explain their significance.**

- `-sS`: TCP SYN scan, detects open ports stealthily.

- `-sU`: UDP scan, finds open UDP ports.
- `-p <port>`: Scans specific ports (e.g., `-p 22,80`).
- `-O`: OS detection, identifies the operating system.
- `-A`: Aggressive scan, includes OS detection, version detection, script scanning, and traceroute.

5.**How can NMAP be used for vulnerability scanning? Discuss the process and the benefits of integrating vulnerability scanning with network scanning.**
NMAP can be used for vulnerability scanning with the `--script` option, which runs various scripts to detect vulnerabilities. Integrating it with network scanning provides a comprehensive view of network security, identifying weaknesses along with open ports and services.