Introduction to Nmap

Nmap (Network Mapper):

- Open-source network analysis and security auditing tool.
- Written in C, C++, Python, and Lua.
- Designed to scan networks, identify hosts, services, and applications.
- Determines operating systems and versions of hosts.
- Capable of detecting packet filters, firewalls, and intrusion detection systems (IDS).

Use Cases

- **Security Auditing:** Assess network security.
- **Penetration Testing:** Simulate attacks to find vulnerabilities.
- **Firewall and IDS Checking:** Verify configurations.
- **Network Mapping:** Identify network topology.
- **Response Analysis:** Analyze network responses.
- **Open Port Identification:** Find open ports.
- **Vulnerability Assessment:** Identify security weaknesses.

Nmap Architecture

Nmap supports various scanning techniques:

1. **Host Discovery:** Identify active hosts on a network.
2. **Port Scanning:** Identify open ports.
3. **Service Enumeration and Detection:** Determine running services and versions.
4. **OS Detection:** Identify operating systems.
5. **Nmap Scripting Engine:** Script interactions with target services.

Syntax

Basic syntax:

php
Copy code

```
nmap <scan types> <options> <target>
```

Scan Techniques

Nmap provides several scanning techniques, including:

- **TCP SYN Scan (-sS):** Default and popular, sends SYN packet without completing the TCP handshake.
- **TCP Connect Scan (-sT):** Completes the TCP handshake.
- **TCP ACK Scan (-sA):** Determines if ports are filtered.
- **Window Scan (-sW):** Similar to ACK scan with window size examination.
- **Maimon Scan (-sM):** Bypasses some firewalls and packet filters.
- **UDP Scan (-sU):** Scans for open UDP ports.
- **TCP Null, FIN, Xmas Scans (-sN, -sF, -sX):** Bypass some firewalls and packet filters.
- **Custom TCP Scan (--scanflags <flags>):** Customizes TCP flags.
- **Idle Scan (-sI <zombie host[ ]>):** Uses a third-party host to send packets.
- **SCTP INIT/COOKIE-ECHO Scans (-sY, -sZ):** Scans for SCTP protocol.
- **IP Protocol Scan (-sO):** Scans for open IP protocols.
- **FTP Bounce Scan (-b <FTP relay host>):** Uses FTP server to relay scans.

Example Command

TCP-SYN scan example:

Copy code

```
sudo nmap -sS localhost
```

Output:
bash
Copy code

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-11 22:50 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000010s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5432/tcp open  postgresql
5901/tcp open  vnc-1

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

- Shows four open TCP ports: SSH, HTTP, PostgreSQL, and VNC-1.
- Indicates port numbers, state, and service type.