Nmap (Network Mapper)

Nmap (Network Mapper) is **a powerful open-source tool used for network discovery and security auditing**. It is widely used by network administrators, penetration testers, and security professionals to **scan and map networks, identify active hosts, discover services, detect vulnerabilities, and assess network security**.

Key Functions of Nmap

1. **Host Discovery**

- Nmap can detect live hosts on a network. This is useful for identifying which devices are currently active and reachable on a network, often referred to as ping scanning.

2. **Port Scanning**

- One of Nmap's core features is port scanning, which identifies the open, closed, or filtered ports on a host. This helps determine what services or applications are running on a system.
- Commonly scanned ports include well-known ports for services like HTTP (80), HTTPS (443), FTP (21), and SSH (22).

3. **Service and Version Detection**

- Nmap can identify the specific services running on a host, including the version of the software (e.g., Apache HTTP Server version 2.4). This helps assess the security of the services running on a machine.

4. **Operating System Detection**

- Nmap can analyze the network responses from a target to guess the operating system and version being used. This is known as OS fingerprinting, which can provide insight into the vulnerabilities or misconfigurations of the target system.

5. **Vulnerability Scanning**

- With the **Nmap Scripting Engine (NSE)**, Nmap can be extended to run custom scripts for tasks such as vulnerability detection, malware detection, and even performing brute-force password guessing attacks.
- NSE includes scripts that detect specific vulnerabilities (e.g., Heartbleed or SMB vulnerabilities).

6. **Network Mapping**

- Nmap can create a detailed network topology by discovering all devices on a network and the connections between them. This is often used for creating an overview of the network infrastructure.

How Nmap Works

Nmap sends specially crafted packets to the target systems and analyzes their responses to gather information. The most common methods include:

1. **TCP SYN Scan (also called half-open scan)**

- Nmap sends a SYN packet (used to initiate a TCP connection) and waits for a response. If the port is open, the target replies with a SYN/ACK packet. If the port is closed, the target responds with a RST (reset) packet.
- This method is **fast and stealthy**, as it doesn't complete the full TCP handshake, which might help avoid detection by firewalls.

2. **UDP Scan**

- Nmap can scan UDP ports by sending empty UDP packets to the target. If the target port is closed, an ICMP "port unreachable" message is usually returned. UDP scanning is slower than TCP scanning because there is no formal handshake like in TCP.

3. **TCP Connect Scan**

- This method completes the **full TCP handshake**, establishing a connection with the target host. While accurate, it is slower and more easily detected by security systems like intrusion detection systems (IDS).

4. **ACK Scan**

- Used to **determine the firewall rules on a network**, Nmap sends TCP ACK packets to the target to identify whether the port is filtered or unfiltered.

Common Nmap Commands

- Basic Host Discovery:

```
nmap 192.168.1.1
```

This command performs a basic scan of the target IP address (192.168.1.1), checking the status of common ports.

- Scan a Range of IP Addresses:

```
nmap 192.168.1.1-100
```

This command scans a range of IP addresses from 192.168.1.1 to 192.168.1.100.

- Service Version Detection:

```
nmap -sV 192.168.1.1
```

This command detects the version of services running on the target.

- Operating System Detection:

```
nmap -O 192.168.1.1
```

This command attempts to detect the operating system of the target host.

- Stealth Scan (SYN Scan):

```
nmap -sS 192.168.1.1
```

This command performs a stealthy SYN scan on the target.

- Scan Specific Ports:

```
nmap -p 80,443 192.168.1.1
```

This command scans only ports 80 (HTTP) and 443 (HTTPS) on the target host.

- Run Nmap Scripts:

```
nmap --script vuln 192.168.1.1
```

This command runs the vulnerability detection script against the target host.

Benefits of Nmap

- **Comprehensive Scanning**: Nmap can perform a wide range of scans, from simple port checks to complex service and OS detection.
- **Customizable with Scripts**: The **NSE(Nmap Scripting Engine)** allows users to extend Nmap's functionality for specific tasks, such as detecting vulnerabilities or running custom scripts.
- **Free and Open Source**: Nmap is freely available and continuously updated by a large community of users and developers.

Limitations of Nmap

- Active **Detection**: Nmap is an active scanner, meaning it sends packets to the target, which may trigger security alerts or logs in IDS/IPS systems.
- **False Positives/Negatives**: **Firewalls, IDS, and load balancers can affect Nmap's results**, causing ports or services to appear open, closed, or filtered incorrectly.
- **Time-Consuming**: Scanning large networks with many hosts can be time-consuming, especially when using slower scan techniques like UDP scanning.

Summary

Nmap is a versatile and powerful tool for network discovery, scanning, and security auditing. It is essential for tasks like identifying open ports, discovering network services, detecting vulnerabilities, and mapping network infrastructures.