**Network Scanning- Vulnerability Scanning- NMAP scanning tool-**

**Network Scanning-**

Network scanning is a procedure for identifying active devices on a network by employing a feature or features in the network protocol to signal devices and await a response.

Network scanning is the process of troubleshooting the active devices on your system for vulnerabilities. It identifies and examines the connected devices by deploying one or more features in the network protocol. These features pick up vulnerability signals and give you feedback on the security status of your network.

Network scanning facilitates system maintenance, monitoring, and security assessments. When implemented effectively, network scanning gives you insights into some of the best ways to protect your network against cyberattacks.

**Work-**

Network administrators scan your network to evaluate IP addresses and detect live hosts connected to it.

* Keep in mind that cybercriminals use the same technique to spot weaknesses in your network. The idea is to identify the loopholes before the bad guys discover them.
* For network administrators to identify how IP addresses are mapped in the network, they may need to use tools such as Nmap.
* Nmap is an effective network scanning tool that uses IP packets to detect devices attached to a network. It helps to simplify the mapping of IP addresses.
* You can use network scanners to inspect where the network is stronger or weaker in your workplace with the help of network administrators.
* A basic working rule of network scanning is to identify all devices on a network and map their IP addresses. To do this, you must use the network scanner to forward a packet to all available IP addresses connected to the network.
* After sending this ping, you need to wait for their response. Once the feedback arrives, the network scanner uses them to measure the status and inconsistencies of the host or application. During this process, the responding devices are active while the non-responding devices are inactive.

**Vulnerability Scanning-**

* Vulnerability scanning helps you to detect vulnerabilities that exist on your network. Running a check on your system exposes threats that were hidden away from you.
* In most organizations, vulnerability scanning is conducted by the IT department. But if you want to get thorough feedback, consider hiring a third-party security expert. Since they aren't familiar with your network, they'll conduct an objective analysis from an outsider's perspective.
* Vulnerability scanning can also be performed by cyberattackers intending to identify weak spots in your network. Beat them to it by identifying and closing the weak links.
* Besides identifying loopholes, vulnerability scanning also evaluates the security capacity of your network against cyberattacks. It uses a database to analyze possible attacks. This database provides the vulnerability scanner with packet construction anomalies, flaws, default configurations, paths to sensitive data, and coding bugs that can enable cyber attackers to exploit your network.

**NMAP scanning tool-**

Nmap is a network scanning tool—an open source Linux command-line tool—used for network exploration, host discovery, and security auditing. Gordon Lyon (pseudonym Fyodor Vaskovich) created it to help map an entire network easily and find its open ports and services.

Working of Nmap

Nmap is convenient during penetration testing of networked systems. Nmap provides the network details, and also helps to determine the security flaws present in the system. Nmap is platform-independent and runs on popular operating systems such as Linux, Windows and Mac.

Nmap is a useful tool for network scanning and auditing purposes.

* It can search for hosts connected to the Network.
* It can search for free ports on the target host.
* It detects all services running on the host with the help of operating system.
* It also detects any flaws or potential vulnerabilities in networked systems.

here are the following Nmap functions, as follows:

1. Ping Scanning

The ping scanning gives information about every active IP on your Network. We can perform a ping scan by using the below command:

#nmap-sn<target>

-PS/PA/PU/PY[portlist]: TCP SYN/ ACK, UDP or SCTP discovery to given ports.

2. Port Scanning

Port scanning is one of the most popular forms of reconnaissance ahead of a hack, helping attackers determine which ports are most susceptible.

There are many ways to execute port scanning using Nmap.

# sS TCP SYN scan

# sT TCP connect scan

# sU UDP scans

# sY SCTP INIT scan

# sN TCP NULL

3. Host scanning

Host scanning provides a detailed description of a particular host or IP address. As mentioned above, you can scan a host using the following command:

# Nmap -sp <target IP range>

4. OS Scanning

OS scanning is the most powerful feature of Nmap. It sends TCP and UDP packets to a port and analyzes the response when using this type of scan. It compares the response to a database of operating systems and returns information on a host's OS. To run the OS scan, use the command, given below:

Nmap -O <target IP>

5. Scan the Most Popular Ports

If you are running Nmap on a home server, this command is easy. It scans 'popular' ports for a host. You can use the command given below to scan the popular ports:

Nmap - Top-ports 20 192.168.1.106

Replace "20" with the number of ports you want to scan. It gives a brief output that details the most common ports status and allows you to see if you have any unnecessarily open ports.

6. Output to a file-If we want the output of results of Nmap scan of any file, you can add an extension to the command.Add:-oN output.txt The command is the output of results to a text file.