Muhammad Tayab’s report of 1st of 3rd week

Network Scanning Fundamentals

Network scanning is a fundamental process in network security and administration, used to discover devices, services, and potential vulnerabilities within a network. It involves the systematic examination of a network to gather information about the devices connected to it, the services running on those devices, and any security issues that might be present. Here’s an overview of network scanning fundamentals, techniques, and tools:

Fundamentals of Network Scanning

1. **Purpose**:
    - **Discovery**: Identify active devices and nodes in the network.
    - **Mapping**: Create a map of the network topology.
    - **Vulnerability Assessment**: Identify potential security weaknesses.
    - **Compliance**: Ensure the network adheres to security policies and regulations.
2. **Types of Scans**:
    - **Host Discovery (Ping Sweep)**: Identifies live hosts on a network.
    - **Port Scanning**: Determines which ports are open on a host and what services are running.
    - **Service Scanning**: Identifies the software and version running on open ports.
    - **Vulnerability Scanning**: Looks for known vulnerabilities in the network.
3. **Scanning Phases**:
    - **Pre-Scanning**: Planning and defining the scope and objectives of the scan.
    - **Scanning**: Executing the scan using various techniques and tools.
    - **Post-Scanning**: Analyzing results, reporting findings, and remediation.

Techniques of Network Scanning

1. **Ping Sweep**:
    - **Purpose**: Identify which IP addresses are active.
    - **Technique**: Sends ICMP (Internet Control Message Protocol) echo requests to a range of IP addresses and waits for responses.
2. **Port Scanning**:
    - **Purpose**: Discover open ports and services on a host.
    - **Types**:
        - **TCP Connect Scan**: Establishes a full TCP connection to the target port.
        - **SYN Scan**: Sends TCP SYN packets to check for open ports without completing the handshake.
        - **FIN Scan**: Sends TCP FIN packets to detect open ports based on responses.
        - **Xmas Scan**: Sends packets with the FIN, PSH, and URG flags set to probe for open ports.
3. **Service Scanning**:
    - **Purpose**: Identify the services running on open ports and their versions.

   - **Technique**: Connects to open ports and queries the services for banner information or responses that reveal their type and version.

4. **OS Fingerprinting**:
   - **Purpose**: Determine the operating system running on a host.
   - **Technique**: Analyzes responses to specific probes to infer the OS type and version.
5. **Vulnerability Scanning**:
   - **Purpose**: Identify known vulnerabilities in the network.
   - **Technique**: Uses databases of known vulnerabilities and tests hosts for their presence.

Tools for Network Scanning

1. **Nmap (Network Mapper)**:
   - **Purpose**: Comprehensive network discovery and security auditing.
   - **Features**: Host discovery, port scanning, service detection, OS fingerprinting, and scripting.
   - **Example**:

   ```
   nmap -sS -p 1-65535 -T4 192.168.1.1
   ```

2. **Angry IP Scanner**:
   - **Purpose**: Simple and fast IP address and port scanner.
   - **Features**: Scans IP addresses and ports, provides information about each host.
   - **Example**:

   ```
   ipscan 192.168.1.0/24
   ```

3. **OpenVAS (Open Vulnerability Assessment System)**:
   - **Purpose**: Comprehensive vulnerability scanning and management.
   - **Features**: Detects vulnerabilities and provides detailed reports.
   - **Example**:

   ```
   openvas-start
   ```

4. **Nessus**:
   - **Purpose**: Vulnerability scanning and assessment.
   - **Features**: Scans for a wide range of vulnerabilities and provides remediation suggestions.
   - **Example**:

   ```
   nessuscli scan run --target 192.168.1.0/24
   ```

5. **Masscan**:
   - **Purpose**: High-speed port scanning.
   - **Features**: Can scan the entire Internet in minutes.
   - **Example**:

     ```
     masscan -p1-65535 192.168.1.0/24
     ```

6. **Hping**:
   - **Purpose**: Packet crafting and network analysis.
   - **Features**: Ping scanning, TCP/IP packet generation, and traceroute-like functionality.
   - **Example**:

     ```
     hping3 -S 192.168.1.1 -p 80
     ```

Types of Network Scans

Network scans can be broadly classified into several types based on their objectives and techniques:

1. **Host Discovery Scans**:
   - **Purpose**: Identify live hosts within a network.
   - **Techniques**: Ping sweep, ARP scan, ICMP echo request.
2. **Port Scanning**:
   - **Purpose**: Determine which ports are open and which services are running on those ports.
   - **Techniques**: TCP connect scan, SYN scan, UDP scan, FIN scan, Xmas scan.
3. **Service Scanning**:
   - **Purpose**: Identify the type and version of services running on open ports.
   - **Techniques**: Banner grabbing, application-layer protocol queries.
4. **OS Fingerprinting**:
   - **Purpose**: Determine the operating system running on a host.
   - **Techniques**: Active and passive fingerprinting methods.
5. **Vulnerability Scanning**:
   - **Purpose**: Identify known vulnerabilities in hosts and services.
   - **Techniques**: Database-driven checks against known vulnerabilities.

TCP Connect Scanning

- **Definition**: TCP Connect scanning is a type of port scan that involves establishing a full TCP connection with the target port.
- **Process**:
  1. The scanner sends a TCP SYN packet to the target port.
  2. If the port is open, the target responds with a SYN-ACK packet.
  3. The scanner completes the connection by sending an ACK packet.

4. Once the connection is established, the scanner can close it using a FIN packet.

- **Usage**: This method is reliable and straightforward but can be easily detected and logged by the target system since it establishes a full connection.
- **Example with Nmap**:

```
nmap -sT 192.168.1.1
```

UDP Scanning

- **Definition**: UDP scanning is used to determine which UDP ports are open on a target host.
- **Process**:
  1. The scanner sends a UDP packet to the target port.
  2. If the port is open, the target may respond with a UDP packet (though many services may not respond).
  3. If the port is closed, the target usually responds with an ICMP Port Unreachable message.
- **Usage**: UDP scanning can be slow and less reliable due to the stateless nature of UDP and the common practice of blocking or rate-limiting ICMP responses.
- **Example with Nmap**:

```
nmap -sU 192.168.1.1
```

Banner Grabbing

- **Definition**: Banner grabbing is the process of capturing and analyzing the banners returned by network services to identify the software and its version.
- **Purpose**: Determine the type and version of services running on a target, which can help in identifying potential vulnerabilities.
- **Process**:
  1. Connect to the target service on the open port.
  2. Capture the banner information that the service sends back.
- **Tools**: Telnet, Netcat, Nmap, and specialized banner grabbing tools.
- **Example with Netcat**:

```
nc 192.168.1.1 80
```

Network Enumeration Methods

Network enumeration involves discovering and mapping the structure of a network. It includes the following methods:

1. **Ping Sweeps**:
   - **Purpose**: Identify live hosts in a network range.
   - **Tools**: Nmap, fping.
   - **Example**:

```
nmap -sn 192.168.1.0/24
```

2. **SNMP Enumeration**:
   - **Purpose**: Retrieve information about network devices using the Simple Network Management Protocol.
   - **Tools**: snmpwalk, snmpenum.
   - **Example**:

   ```
   snmpwalk -v 2c -c public 192.168.1.1
   ```

3. **NetBIOS Enumeration**:
   - **Purpose**: Discover Windows network shares and resources using NetBIOS.
   - **Tools**: nbtscan, Nmap.
   - **Example**:

   ```
   nbtscan 192.168.1.0/24
   ```

4. **LDAP Enumeration**:
   - **Purpose**: Query the Lightweight Directory Access Protocol to gather information about directory services.
   - **Tools**: ldapsearch, Nmap.
   - **Example**:

   ```
   ldapsearch -x -h 192.168.1.1 -b "dc=example,dc=com"
   ```

5. **DNS Enumeration**:
   - **Purpose**: Gather DNS records to understand the domain's structure.
   - **Tools**: dig, dnsenum, Nmap.
   - **Example**:

   ```
   dnsenum example.com
   ```

Scanning Tools and Utilities

Network scanning tools and utilities are essential for identifying hosts, services, and vulnerabilities within a network. They help security professionals and network administrators ensure the security and proper configuration of network assets. Some common tools and utilities include:

- **Nmap**: Used for network discovery and security auditing.
- **Wireshark**: A network protocol analyzer that captures and displays packet data.
- **Angry IP Scanner**: A fast and user-friendly IP address and port scanner.
- **Nessus**: A vulnerability scanner that identifies vulnerabilities in systems and applications.
- **OpenVAS**: An open-source vulnerability scanner.
- **Metasploit**: A penetration testing framework that includes various tools for scanning and exploiting vulnerabilities.

Muhammad Tayab's report of 1st of 3rd week

What is Nmap?

Nmap (Network Mapper) is a free, open-source tool used for network discovery and security auditing. It is one of the most popular tools in the cybersecurity field for network scanning and mapping. Nmap uses raw IP packets to determine:

- What hosts are available on the network?
- What services (application name and version) those hosts are offering.
- What operating systems (and OS versions) they are running.
- What type of packet filters/firewalls are in use?

Basic Nmap Syntax and Options:

- **Host Discovery**:

  ```
  nmap -sn 192.168.1.0/24
  ```

- **Port Scanning**:

  ```
  nmap -sT 192.168.1.1
  ```

- **Service Version Detection**:

  ```
  nmap -sV 192.168.1.1
  ```

- **Operating System Detection**:

  ```
  nmap -O 192.168.1.1
  ```

- **Full Scan**:

  ```
  nmap -A 192.168.1.1
  ```

What is Ping Sweep and Sweep Detection?

Ping Sweep:

- **Definition**: A ping sweep is a network scanning technique used to identify which IP addresses in a range of IPs map to live hosts (computers).
- **Process**: The scanner sends ICMP Echo Requests (ping) to multiple IP addresses. If a host responds with an ICMP Echo Reply, it is considered live.
- **Tools**: Nmap, fping, hping.
- **Example with Nmap**:

  ```
  nmap -sn 192.168.1.0/24
  ```

Sweep Detection:

- **Definition**: Sweep detection involves identifying unauthorized or suspicious ping sweeps on the network, which could indicate a reconnaissance attempt by an attacker.
- **Techniques**: Analyzing network traffic for patterns of ICMP Echo Requests targeting multiple IP addresses within a short timeframe.
- **Tools**: Intrusion detection systems (IDS) like Snort, network traffic analyzers like Wireshark.

What is Network Mapping and Topology Discovery?

Network Mapping:

- **Definition**: Network mapping is the process of discovering and visualizing the physical and logical layout of a network, including all devices and their interconnections.
- **Purpose**: Helps in understanding the network structure, identifying unauthorized devices, and planning network expansion.
- **Tools**: Nmap, SolarWinds Network Topology Mapper, Microsoft Visio.

Topology Discovery:

- **Definition**: Topology discovery involves identifying the layout and configuration of network devices and their connections.
- **Purpose**: Essential for network management, troubleshooting, and security assessment.
- **Techniques**:
    - **SNMP**: Uses the Simple Network Management Protocol to gather information from network devices.
    - **CDP/LLDP**: Cisco Discovery Protocol and Link Layer Discovery Protocol provide information about directly connected devices.
    - **Traceroute**: Maps the route packets take from source to destination.

What is Vulnerability Scanning?

Definition: Vulnerability scanning is the automated process of identifying security weaknesses in a network, system, or application. It involves using tools to scan and detect known vulnerabilities, misconfigurations, and other security issues.

Purpose: Helps organizations identify and address security gaps before they can be exploited by attackers.

Process:

1. **Discovery**: Identifying all assets within the scope of the scan.
2. **Assessment**: Scanning the assets for known vulnerabilities using a database of known issues.
3. **Reporting**: Generating a report detailing the discovered vulnerabilities, their severity, and recommended remediation steps.

Tools:

- **Nessus**: One of the most widely used vulnerability scanners.
- **OpenVAS**: An open-source vulnerability scanning suite.
- **QualysGuard**: A cloud-based vulnerability management tool.
- **Rapid7 Nexpose**: A comprehensive vulnerability scanner that integrates with the Metasploit framework.

Example with OpenVAS:

```
openvas-start
```

Conclusion

Network scanning is a fundamental aspect of cybersecurity and network management. Tools like Nmap, Wireshark, and vulnerability scanners help in identifying potential security issues, ensuring network integrity, and protecting against attacks. Understanding and effectively using these tools are crucial for network administrators and security professionals.