Network Scanning

1/ Network Scanning Basics

Network scanning is part of reconnaissance. It actively probes targets to identify live hosts, open ports, services, and weaknesses, giving detailed technical insights into the network.

Types of Scanning

- **Active Scanning**: Involves direct communication with the target by sending packets. Examples include **Nmap port scans**. This is more accurate but also easier to detect.

- **Passive Scanning**: Collects information without directly interacting with the target, usually by **sniffing traffic** on the network. It is stealthy but provides less detailed results.

Objectives of Scanning

- **Live Host Discovery**: Identify which IP addresses are currently active.

- **OS Discovery**: Detect the operating system and version.

- **Open Ports & Services**: Find accessible ports (e.g., 22/SSH, 80/HTTP) and determine what services are running.

- **Network Mapping**: Understand how devices are connected (routers, firewalls, servers).

2/ TCP Reset (RST) in Network Scanning

When performing **network scanning** (e.g., with Nmap), the **TCP Reset (RST) flag** is very important to understand the state of a port.

What Happens

- If a **TCP packet is sent to a closed port**, the target responds with a **RST flag**.
- This tells the scanner that the port is **not open and not listening for connections**.

Example in Scanning

- **SYN Scan (Half-Open Scan):**
    - If the port is **open** → Target replies with **SYN-ACK**.
    - If the port is **closed** → Target replies with **RST**.
- **Connect Scan:** Similar behavior, but it completes the handshake before detecting the port status.

3/ ICMP (Internet Control Message Protocol)

ICMP is a network protocol used by devices to **send error messages and operational information** about network communications. It is part of the IP protocol suite.

Key Uses

- **Host/Network Reachability:** Check if a host is alive (e.g., using `ping`).
- **Error Reporting:** Notify issues like “Destination Unreachable” or “Time Exceeded.

ICMP Header Structure

- **Type (1 byte):** Indicates the kind of ICMP message (e.g., Echo Request, Destination Unreachable).
- **Code (1 byte):** Provides more detail about the Type (e.g., why a destination is unreachable).
- **Checksum (2 bytes):** Error-checking of the ICMP message.

- **Optional Data:** Some ICMP messages include additional fields, like the original IP header or payload.

ICMP Type	Code	Description
0	0	eco reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	7	destination host unknown
8	0	eco request
10	0	router discovery
11	0	TTL expired

Table 1-3 ICMP Message Types

Key Points for Network Scanning

- **Echo Request (Type 8)** → Used by `ping` to test if host is alive.
- **Echo Reply (Type 0)** → Confirms host is reachable.
- **Destination Unreachable (Type 3)** → Shows closed ports or unreachable networks.

4/ Network Scanning Techniques

1. Host Discovery Techniques

These techniques help determine which hosts are **alive** on the network.

1. ICMP Echo (Ping)

- Sends an **ICMP Echo Request** to a target IP.
- If the host responds with **Echo Reply**, it is alive.
- **No reply** may indicate the host is down or ICMP is blocked by a firewall.
- Commonly used in **ping sweeps** to quickly discover multiple hosts.

2. ARP Ping (Local Networks)

- Sends an **ARP request** to detect hosts in the same subnet.
- Works even if ICMP is blocked.
- Very efficient for **LAN discovery**.

2. Open Port Scanning Techniques

These techniques determine which ports on a host are **open, closed, or filtered**, indicating what services are available.

1. TCP Connect Scan

- Fully completes the TCP 3-way handshake: **SYN** → **SYN-ACK** → **ACK**.
- **Port States:**
  - **Open:** Handshake completes successfully; a service is listening.
  - **Closed:** Host responds with **RST**; no service is listening.
  - **Filtered:** No response or ICMP unreachable; a firewall or filter is blocking access.
- Simple to use but **easily detected** by intrusion detection systems.

2. SYN Scan (Half-Open Scan)

- Sends **SYN** packets but does **not complete the handshake**.
- **Port States:**
  - **Open:** Target responds with **SYN-ACK**.
  - **Closed:** Target responds with **RST**.
  - **Filtered:** No response or ICMP unreachable.
- Faster and **stealthier** than TCP Connect Scan.

3. Idle Scan (Idle Connection Scan)

Definition

Idle Scan is a **stealth scanning technique** used in network reconnaissance to discover **open ports on a target** without sending packets directly from the attacker's machine. Instead, it uses a third-party **"zombie" host** with a predictable IP ID sequence.

This way, the attacker remains hidden, and the target sees the zombie as the source of the scan.

How It Works

1. **Attacker finds a zombie** (an idle machine with low traffic and predictable IP ID increments).
2. **Attacker spoofs packets** so they appear to come from the zombie.
3. Depending on how the target responds, the zombie's IP ID field changes, and the attacker measures that difference to infer whether the target's port is:
   - **Open**: The zombie's IP ID increases differently.
   - **Closed/Filtered**: No unusual IP ID change.

Advantages

- Very stealthy: The target never sees the attacker's real IP.
- Bypasses firewalls/IDS that track attacker IPs.

Limitations

- Needs a "quiet" zombie host with predictable IP ID behavior.
- Slower than direct scanning.
- Many modern OSes randomize IP ID fields, making idle scans harder.

3. OS Detection Techniques

OS detection, also known as fingerprinting, is the process of identifying the operating system running on a target machine. This information is crucial in network reconnaissance because it helps determine potential vulnerabilities and how to interact with the system. The most common techniques include:

1. Ping with TTL Analysis

- When a device sends an ICMP Echo Reply (ping response), the **Time-To-Live (TTL)** field in the IP header reveals information about its OS.
- Every operating system starts with a **default TTL value**:
    - **Windows**: typically 128
    - **Linux/Unix**: typically 64
    - **Cisco devices**: often 255
- By measuring the TTL value received and considering the number of hops, one can estimate the OS family.

2. Banner Grabbing

- Many services return a “banner” when a connection is made, which may include OS or software details.
- Examples:
    - **Web servers**: A response header might show `Apache/2.4.41 (Ubuntu)` or `Microsoft-IIS/10.0`.
      .
- Can be performed using tools such as nmap and netcat, or automated scanners.

3. Active Fingerprinting with Nmap (-O)

- **Nmap’s `-O` option** sends crafted TCP, UDP, and ICMP packets to the target.
- It analyzes differences in response behavior:
    - TCP sequence number generation
    - Window sizes
    - TCP options (MSS, timestamps, SACK)
    - ICMP error messages
- Based on this, Nmap compares results against its large fingerprint database and provides an OS guess with an accuracy percentage.
- **Advantages**: Very powerful, can even identify OS versions.
- **Limitations**: Generates noticeable traffic and can be blocked or logged by firewalls/IDS.