Ethical Hacking

Lecture -3 (Theory)

Scanning

M.Sc. Halo Khalil Sharif

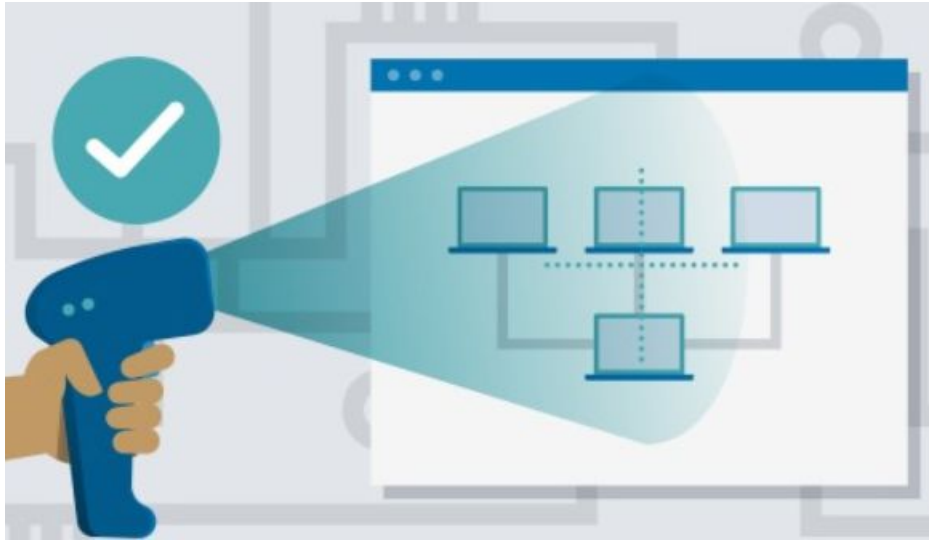
2025 – 2026

Outlines

- What is Scanning?
- Purpose of Scanning
- Types of Scanning
- Steps in the Scanning Process
- Scanning Techniques
- Common Scanning Tools

What is Scanning?

Scanning is the process of systematically investigative a network, system, or application to gather detailed information about its structure, vulnerabilities, and potential entry points.



Purpose of Scanning

- To identify open ports, services, and protocols.
- To detect vulnerabilities and misconfigurations.
- To map the network and understand its architecture.
- To prepare for potential exploitation or penetration testing.

Types of Scanning

1. Port Scanning
2. Network Scanning
3. Vulnerability Scanning

Types of Scanning

There are three primary types of scanning in ethical hacking:

1. Port Scanning

Objective : Identify open ports on a target system and determine what services are running.

Tools: Nmap, Netcat, Masscan.

Common Techniques:

- TCP Connect Scan: Establishes a full TCP connection to test each port.
- SYN Scan: also known as a "stealth" or "half-open" scan, used to determine if ports on a target system are open, closed or filtered. It sends a SYN packet to the target and waits for a response.
- UDP Scan: Checks open UDP ports.

Types of Scanning

2. Network Scanning

Objective: Discover active hosts, IP addresses, and network topology.

Tools: Nmap, Angry IP Scanner, Advanced IP Scanner.

Activities:

- Identifying live hosts using ICMP (ping) or ARP scans.
- Mapping devices on a network.
- Detecting devices' operating systems (OS fingerprinting).

ICMP

- **ICMP** stands for **Internet Control Message Protocol**.
- It is used for **sending error messages, control information, and diagnostics** between network devices.
- Network Layer (Layer 3 of the OSI model)

Main Purposes:

- **Error Reporting** – when something goes wrong, ICMP notifies the sender.
  Example: “Destination Unreachable” if a router can’t forward your packet.
- **Network Diagnostics** – tools like ping and traceroute use ICMP to test reachability and path performance.

ICMP in Ethical Hacking

ICMP is often used for:

- **Host Discovery** – find which IPs are alive (e.g., nmap -sn 192.168.1.0/24)
- **Network Mapping** – traceroute reveals hop-by-hop paths.
- **Detecting Firewalls or Filters** – dropped or modified ICMP responses can reveal network defenses.

ARP

- **ARP (Address Resolution Protocol)** is a **network protocol** used to map or translate an **IP address** (logical address) into a **MAC address** (physical address) within a local area network (LAN).
- It operates at the **link layer (Layer 2)** of the **OSI model.**

Why ARP is Needed?

Every device on a network has:

- an **IP address** (used for logical communication), and
- a **MAC address** (used for actual data transmission on Ethernet).

When a computer wants to send data to another IP address on the same LAN, it must know the **MAC address** of the destination. ARP helps discover that.

How ARP Works ?(Step-by-Step)

- **Host A** wants to send a packet to **Host B** (same subnet).
- **Host A** checks its ARP cache (a table of known IP–MAC pairs, temporarily stores IP ↔ MAC mappings.).

  If B's MAC address is found → it sends the frame directly.

  If not found → it broadcasts an **ARP Request**.

ARP Request:

"Who has IP 192.168.1.5? "

Sent as a broadcast frame to **FF:FF:FF:FF:FF:FF** (all devices see it).

- **Host B** (which owns 192.168.1.5) replies with an **ARP Reply**:

  "192.168.1.5 is at MAC 00:1A:2B:3C:4D:5E."

- **Host A** stores this mapping in its ARP cache for future use and send the frames.

Types of Scanning

3. Vulnerability Scanning

Objective: Identify known vulnerabilities in systems, applications, and services.

Tools: Nessus, OpenVAS, Qualys, Nikto.

Steps in the Scanning Process

1. **Defining the Scope:**

   Determine what systems, networks, or applications are in scope for scanning.

2. **Selecting Tools and Techniques:**

   Choose tools and methods based on the target environment.

3. **Performing Scans:**

   Run network, port, or vulnerability scans.

Steps in the Scanning Process

4. **Analyzing Results:**

- Review scan outputs to identify open ports, active services, and vulnerabilities.
- Prioritize findings based on severity.

5. **Documenting Findings:**

- Record all vulnerabilities and risks discovered.
- Include remediation recommendations for each issue.

Scanning Techniques

1. Active Scanning: Involves direct interaction with the target, such as sending packets to analyze responses (e.g., Nmap scans).

2.Passive Scanning: Detect network traffic and gathers information without direct interaction (e.g., using Wireshark).

Common Scanning Tools

Tool	Functionality
Nmap	Port scanning, OS detection, service discovery.
Nessus	Vulnerability scanning.
Nikto	Web server scanning for vulnerabilities.
OpenVAS	Comprehensive vulnerability management.
Wireshark	Passive traffic analysis.