Day 20: Metasploitable & Nessus Scan Practical

Date: July 12, 2025

Objective:

Hands-on practice of scanning and detecting vulnerabilities using **Nessus** against the intentionally vulnerable virtual machine **Metasploitable 2**.

Nessus + Metasploitable Lab Setup

1. **Identify the Metasploitable IP Address:**

Boot Metasploitable in a virtual environment (such as VMware or VirtualBox), and note the internal IP address assigned to it.

2. **Launch Nessus:**

Open Nessus in a web browser and log in to the dashboard. Create a new scan using the **Advanced Scan** option, target the Metasploitable IP address, and initiate the scan.

3. **Analyze the Scan Report:**

Once completed, Nessus will generate a detailed report. This includes open ports, services running on those ports, and known vulnerabilities associated with them. Each issue is categorized by severity for prioritization.

Concept: Backdoor

A **backdoor** is an unauthorized or hidden entry point into a computer system, typically installed by attackers to retain access. Unlike legitimate access, it bypasses normal authentication mechanisms, often remaining undetected for extended periods.

Backdoors are commonly used for persistent access, remote control, or to deploy malware in a compromised system.

Concept: SSL (Secure Socket Layer)

SSL is a cryptographic protocol that provides secure communication between a client and server. Its primary goals include:

- Encrypting data in transit to ensure privacy.
- Authenticating server identity.
- Preventing eavesdropping and tampering.

Although **TLS (Transport Layer Security)** has officially replaced SSL in modern systems, the term SSL is still commonly used to describe secure HTTP connections (HTTPS).