

Day 20: Metasploitable & Nessus Scan Practical

Objective:

Practice scanning for vulnerabilities with **Nessus** on **Metasploitable 2**, a machine made to be vulnerable.

Nessus + Metasploitable Lab Setup

1. **Find Metasploitable IP:** Start Metasploitable in a virtual machine (like VMware) and get its IP address.
2. **Start Nessus:** Open Nessus, log in, create an **Advanced Scan**, target the Metasploitable IP, and start.
3. **Check Report:** Nessus makes a report with open ports, services, and vulnerabilities, ranked by severity.

Concept: Backdoor

A hidden way into a computer system, usually put there by attackers to keep access. It skips normal login and is often undetected. Backdoors are used for long-term access, remote control, or to put malware on a system.

Concept: SSL (Secure Socket Layer)

A security protocol for safe communication between computers. It encrypts data, checks server identity, and stops spying or tampering. Even though TLS has replaced it, people still say SSL for secure web connections (HTTPS).