Penetration Testing Lab Environment

Secure lab design and initial reconnaissance

Overview

Designed an isolated virtual security-testing environment with separate attacker and deliberately vulnerable target systems. Confirmed safe connectivity and established a repeatable baseline for later web-security assessments.

Approach

- Configured an isolated virtual network for authorized testing.
- Verified connectivity and enumerated exposed services at a high level.
- Prepared standard reconnaissance tooling and documented the assessment boundary.

Key findings

- A controlled environment is essential before vulnerability validation begins.
- Early service discovery helps focus testing and establish a defensible evidence trail.

Defensive recommendations

- Keep vulnerable systems isolated from production networks.
- Document scope, network boundaries, and authorized assets before testing.

Publication note: This is a sanitized portfolio summary. All testing was performed in intentionally vulnerable, isolated training environments. Target identifiers, credentials, payloads, screenshots, and step-by-step exploitation instructions have been omitted.