Web Server & DVWA Vulnerability Lab

# Overview

This lab focused on deploying a web server (Apache) and configuring the Damn Vulnerable Web Application (DVWA) on a target machine. A Nikto scan was performed from Kali Linux to identify vulnerabilities and misconfigurations.

# Lab Environment

- Attacking Machine: Kali Linux (DHCP-assigned IP)  
- Target Machine: DVWA hosted on Apache (Static IP: 192.168.1.10)  
- Network Configuration: Internal VirtualBox network  
- Tools Used: Nikto, Apache2, DVWA

# Key Findings from Nikto Scan

- Apache Version: 2.4.52 (outdated)

- Missing Security Headers:

* • X-Frame-Options (Clickjacking Risk)
* • X-Content-Type-Options (MIME Sniffing Risk)

- Directory Indexing Enabled:

* • Multiple endpoints allow directory listing if no index page is present

- Allowed HTTP Methods: GET, POST, OPTIONS, HEAD

- Web Publisher Vulnerabilities:

* • Server may allow file browsing via open directory features
* • Referenced CVEs include CVE-1999-0269 and CVE-2002-1078

# Lessons Learned

This lab demonstrated how misconfigurations such as outdated software, missing headers, and enabled directory listings can introduce serious security risks. Tools like Nikto can effectively identify these vulnerabilities. Mitigation strategies include applying updates, disabling unused methods, and setting proper HTTP security headers.