Tools Used

- Nmap – Port scanning and service enumeration
- theHarvester – Open-source intelligence (OSINT) collection
- Shodan – Device and port exposure search engine
- Nikto – Web server vulnerability scanner
- SSL Labs – TLS/SSL configuration evaluation

Steps Performed

1. OSINT Collection

- Collected emails, subdomains, and metadata with theHarvester.
- Searched Shodan for any exposed devices or known services.

2. Port Scanning

- Ran nmap -A example.com to identify open ports and services.

3. Vulnerability Scanning

- Used Nikto to detect common web server vulnerabilities.
- Analyzed HTTPS configuration with SSL Labs.

Key Findings

- Open Ports: 80, 443, 22
- Services: Apache 2.4.29, OpenSSH 7.6p1
- Issues Identified:
- Outdated software
- Weak SSL ciphers
- Exposed HTTP headers

Recommendations

- Update outdated software packages
- Disable weak SSL/TLS protocols
- Remove unnecessary HTTP headers
- Restrict access to non-essential ports

Lessons Learned

This project enhanced my understanding of:

- Reconnaissance and enumeration techniques
- OSINT tools and their use cases
- Vulnerability scanning basics
- Writing concise, technical reports