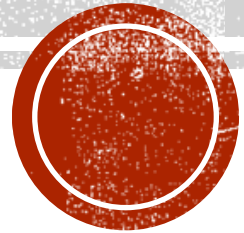
NSHIELD — SCAN. DETECT. SECURE:

AI-DRIVEN AUTOMATED TOOL FOR SECURITY ANALYSIS AND REMEDIATION



Name : Jackie Kim

Student ID : 300376300

Course : CSIS4495-001 Applied Research Project

INTRODUCTION

- Rapidly growing and evolving cybersecurity threats
- Increasing reliance on digital platforms across industries
- Traditional defenses (e.g., firewalls, antivirus) are no longer sufficient
- Proactive approaches are essential to secure sensitive data

WHAT IS PENETRATION TESTING ?

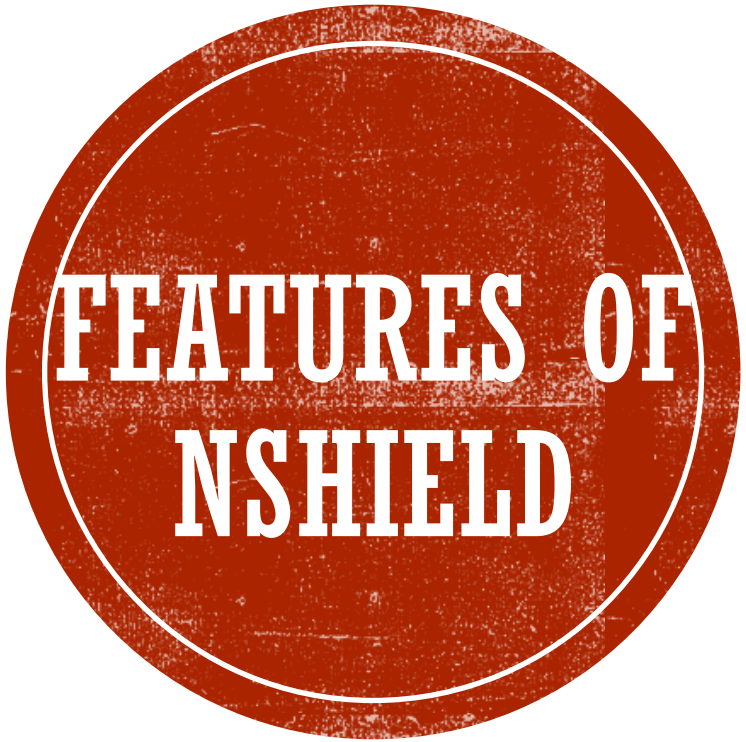
- Authorized, simulated cyberattacks to evaluate security posture
- Mimics real-world attacker techniques
- Identifies vulnerabilities before malicious actors can exploit them
- Supports stronger defense strategies and compliance

CHALLENGES IN TRADITIONAL PEN TESTING

- Time-consuming and expensive for SMEs
- Difficulty analyzing complex reports
- Reports may become outdated quickly
- Risk of false positives or missed threats in automation

NShield

Scan, Detect, Secure



NShield is a Flask-based automated penetration testing tool

Targets network security & web application vulnerabilities

Accessible via an intuitive web interface

Designed for professionals, students, and ethical hackers

INTEGRATED TOOLS & FUNCTIONALITY

Nmap Integration

- Automates port scanning, OS detection, and CVE vulnerability checks
- Uses powerful NSE scripts for detailed network assessments

Nikto Integration

- Scans web servers for misconfigurations, outdated software, and dangerous files

NMAP COMMANDS

Scan Name	Command	Description	Importance	Risks Identified
Full Port Scan	nmap -p- -sV -O -A <target>	Scans all 65,535 TCP ports, detects services, OS, and performs aggressive probing.	Offers a comprehensive network overview, uncovering hidden or unexpected services.	Unauthorized services, unpatched apps, exposed admin panels, or backdoors.
SMB & RDP Vulnerability Scan	nmap --script smb-vuln-ms17-010,smb-vuln-ms08-067,smb-enum-shares,smb-enum-users,smb-os-discovery -p 445 <target>	Targets SMB/RDP vulnerabilities including EternalBlue, user enumeration, and OS discovery.	Identifies lateral movement vectors and legacy protocols often exploited in ransomware campaigns.	MS17-010, MS08-067, weak share permissions, exposed user credentials, OS fingerprinting.
Web & FTP Vulnerability Scan	nmap --script http-vuln-cve2017-5638,http-vuln-cve2014-3704,http-vuln-misfortune-cookie -p 80,443 <target>	Detects common web app and server vulnerabilities including Apache Struts and Drupal flaws.	Essential for spotting remote code execution vectors and injection flaws in common CMS or frameworks.	CVE-2017-5638 (Apache Struts), CVE-2014-3704 (Drupal SQLi), Misfortune Cookie (session hijacking).
SMTP & DNS Security Scan	nmap --script smtp-vuln-cve2011-1720,ftp-anon,samba-vuln-cve-2012-1182,dns-zone-transfer -p 21,25,53,139,445 <target>	Examines vulnerabilities in SMTP, FTP, Samba, and DNS services.	Protects sensitive internal data from exposure via anonymous access and insecure DNS zone transfers.	CVE-2011-1720, CVE-2012-1182, anonymous FTP, full DNS zone leaks.
Comprehensive Vulnerability Scan	nmap --script vulners -sV <target>	Matches detected services against public CVE databases using the vulners NSE script.	Supports patch management and audit-readiness by mapping services to known vulnerabilities.	Known CVEs tied to outdated services (e.g., Apache, OpenSSH, MySQL).

NIKTO COMMANDS

Scan Name	Command	Description	Importance	Risks Identified
Basic Scan	nikto -h <target>	Performs general web scan to detect outdated software, default files, and common misconfigs.	Useful for quick reconnaissance and identifying low-hanging fruit in web servers.	Default server files, missing security headers, outdated server software.
SSL Scan	nikto -h <target> -ssl	Forces HTTPS connection to assess SSL/TLS implementation and cryptographic flaws.	Ensures secure channel setup, detecting deprecated protocols and cipher weaknesses.	Weak SSL ciphers, support for SSLv2/SSLv3, MITM vulnerabilities.
Verbose Scan	nikto -h <target> -Display V	Produces detailed output with HTTP request/response and test results.	Helpful for manual review or when debugging application/server issues.	Depends on server config—may reveal full request/response details.
XSS & SQL Injection Scan	nikto -h <target> -Tuning 1,6	Targets web vulnerabilities related to Cross-Site Scripting and SQL Injection.	Crucial for application-layer security—prevents unauthorized data access and script execution.	Stored/reflected XSS, SQLi allowing data extraction or DB control.
File Inclusion & RCE Scan	nikto -h <target> -Tuning 4,5	Tests for inclusion vulnerabilities and Remote Code Execution flaws.	High-risk detection—can lead to full system compromise if exploited.	Local/Remote File Inclusion, code execution from user-controlled inputs.
Server Vulnerability Scan	nikto -h <target> -Tuning 3	Focuses on web server software issues based on version and platform.	Highlights server misconfigurations or outdated platforms that may allow attacks.	Known server flaws in Apache, Nginx, IIS; outdated modules/plugins.

AI-ENHANCED REPORTING

- Post-scan analysis via Ollama + Llama3
- Each scan includes:
  - Risk explanation
  - Severity rating (color-coded)
  - Remediation recommendations
- Easy to understand for all skill levels

SYSTEM ARCHITECTURE OF NSHIELD

Modular Architecture

- app.py: Routes user input and orchestrates scanning & reporting
- net_scan.py & web_scan.py: Isolated logic for Nmap and Nikto scans
- Easy to extend for future vulnerabilities and tools

Web Interface Pages

- index.html:
  - Central navigation hub
- install.html:
  - Setup progress tracker (25% step increments)
- net.html & web.html:
  - User-selectable scan categories
- results.html:
  - Raw + analyzed results in a professional report view

VALIDATION AND EVALUATION OVERVIEW

Validation Platforms

- TryHackMe – Used for network security validation
- OWASP Juice Shop – Used for web application security validation

Evaluation Parameters

- Functionality & Coverage
- Accuracy & Effectiveness
- Performance & Speed
- Usability & User Experience

VALIDATION HIGHLIGHTS – NETWORK

Detected Security

- Open ports
- Services (SSH, HTTP)

Missed

- SMB exploits (MS17-010, MS08-067)
- RDP (MS12-020)
- CVEs (HTTP CVE-2017-5638)

VALIDATION HIGHLIGHTS – WEB APP

Detected Security

- XSS
- SQL Injection
- SSL/TLS misconfigs
- Security misconfigs

Missed

- Insecure Deserialization

MANUAL TESTING COMPARISON

Automated Tool Output:

- Provides quick and accurate results for security scans.
- Identifies vulnerabilities like XSS, SQL Injection, SSL/TLS misconfigurations.

Manual Testing Output:

- Handcrafted tests produce the same exact results.
- Vulnerabilities such as XSS, SQL Injection, and SSL/TLS misconfigurations were detected.

Conclusion:

- Both the automated tool and manual testing produced identical outputs for the same commands.
- This confirms that the automated tool is accurate and aligns with manual testing results.

PERFORMANCE & USABILITY

- Network Scan: ~2 hours
- Web App Scan: ~4 hours
- Ollama + Hardware upgrade → Minimal speed improvement

- Beginner-friendly GUI
- Needs dynamic scan logic & faster feedback

REPORT QUALITY

- Structured, color-coded by severity
- Suggestions too general (e.g., “Apply latest patch”)
- Needs deeper technical remediation and risk correlation

LESSONS LEARNED

Beyond Scripting:	• Effective scanning requires not just running tools like Nmap/Nikto, but interpreting results and generating actionable, understandable reports.
Power of AI Integration:	• Incorporating Ollama enabled beginner-friendly analysis, helping bridge the gap between technical output and human understanding.
User-Centered Reporting:	• Visually intuitive with severity-based color coding • Detailed, with collapsible raw outputs and organized vulnerability tables • Accessible to both non-technical users and seasoned professionals
Validation is Crucial:	• Testing against TryHackMe and OWASP Juice Shop highlighted both strengths and gaps in the tool's detection capabilities.

CHALLENGES

Script Variability:	• Nmap and Nikto produced inconsistent outputs across environments, complicating parsing and report clarity.
Generalized AI Output:	• Ollama sometimes returned non-specific remediation lacking context or prioritization.
Performance Bottlenecks:	• Network scanning: ~2 hours • Web scanning: ~4 hours • Despite hardware boosts, execution time remained high
Detection Gaps:	• Missed certain vulnerabilities (e.g., SMB/RDP exploits, insecure deserialization)Indicated a need for improved detection logic and deeper analysis layers

CONCLUSION

- NShield achieved its core goal:
  - automate scanning, analyze findings with AI, and deliver clear, educational, and actionable reports.
- Key contributions:
  - Bridged detection and remediation
  - Enhanced accessibility of vulnerability data
  - Supported learning for junior analysts and educational use
- Future improvements:
  - Add CVSS scoring
  - Correlate cross-scan findings
  - Optimize scan performance
  - Expand AI interpretation capabilities


Q
A