April 26, 2024

University of Sciences and Arts in Lebanon

Faculty of Sciences and Arts

Reconova

Computer Science Final Year Project – Cybersecurity

Hassan Shahrour

Ibrahim Hammoudi

Ahmad Sleem

Supervisor: Dr. Hisham Yassine

Abstract

This project aims to develop a web-based interface for an automated reconnaissance tool tailored for penetration testing. The tool allows users to input a domain name or IP address, upon which it initiates an automated reconnaissance scan using multiple integrated scanning tools to ensure accurate and comprehensive results. The gathered data is then analyzed using an AI model, such as ChatGPT via API integration, to detect potential vulnerabilities and misconfigurations. Based on the analysis, the system provides detailed insights and a recommended roadmap to guide penetration testers through subsequent phases of the security assessment process. In the second phase of the project, the platform will support scanning of individual computers by allowing users to input an IP address for host-based vulnerability assessment. Post-analysis, if security issues are found, the system generates a report and optionally offers automated remediation scripts suggested by the AI. Users can review and approve these scripts before execution. This dual-phase approach enhances the efficiency of reconnaissance and vulnerability management, providing actionable intelligence and automation for both network and host-level security assessments.

Table of Contents

Contents

1 Introduction

.1 Background

In the field of cybersecurity, reconnaissance is the initial and one of the most critical phases of penetration testing. It involves gathering information about a target system to identify potential vulnerabilities and misconfigurations before attempting exploitation. Traditionally, this process is manual, time-consuming, and fragmented across different tools. With the increasing complexity of systems and networks, the need for automated, intelligent reconnaissance solutions has become more apparent. Moreover, artificial intelligence (AI) is emerging as a powerful ally in interpreting complex scan data and recommending security improvements. By combining automation, multi-tool integration, and AI analysis, this project addresses the growing demand for smarter and more efficient reconnaissance workflows in cybersecurity.

.2 Objective

The primary objective of this project is to design and implement a web-based platform that automates the reconnaissance phase of penetration testing. The system will allow users to input a domain name or IP address and initiate a scan using multiple reconnaissance tools. The collected data will be analyzed by an AI model (e.g., ChatGPT) to identify vulnerabilities and misconfigurations and provide a roadmap for the next phases of penetration testing. In the second phase, the system will also support host-level scanning, where users can input an IP address to check for local vulnerabilities. If security issues are detected, the AI will generate remediation scripts, and users will be given the choice to apply these changes. The ultimate goal is to enhance the efficiency, accuracy, and decision-making process of penetration testers.

.3 Scope

Included in Scope:

- Development of a web interface for user input and result display.
- Integration of multiple reconnaissance tools (e.g., Nmap, Sublist3r, WhatWeb, etc.) for automated scanning.
- Use of AI (ChatGPT API) to analyze scan results for vulnerabilities and misconfigurations.
- Generation of a roadmap to guide penetration testers post-reconnaissance.
- Support for scanning individual computers based on IP address for local vulnerability assessment.
- Agents will be installed on these computers to open an encrypted channel for communicating.
- AI-suggested remediation scripts for identified issues.
- Option for the user to approve or reject automatic script execution.
- The script could run on that pc.

Excluded from Scope:

- Full exploitation of discovered vulnerabilities.
- Real-time monitoring or intrusion detection systems.
- Deep learning model training (AI will be used via API, not trained within the system).
- Full OS-specific patch management outside of proposed remediation scripts.

.1 Methodology

- The project will follow an incremental development methodology with the following approach:
- **Web Development**: A web interface will be built using asp .net core mvc or web api, enabling user interaction with the platform.
- **Tool Integration**: Open-source reconnaissance tools will be integrated into the backend for automation (e.g., Nmap, Whois, Nikto, Subfinder).
- **AI Analysis**: The results from the tools will be sent to ChatGPT (via API) for interpretation and vulnerability detection.
- **Roadmap Generation**: Based on AI insights, a structured roadmap will be created to assist penetration testers in further actions.
- **Host-Level Scanning**: Extend the system to scan a single host for vulnerabilities using tools like Lynis or OpenVAS.
- **Remediation Scripts**: The AI will suggest remediation scripts. Upon user approval, these scripts will be executed on the system.

Technologies and Tools:

1. asp .net core mvc
2. HTML/CSS/JavaScript for front-end
3. Nmap, Subfinder, WhatWeb, etc. for scanning
4. ChatGPT API for AI analysis
5. Bash scripting for remediation execution
6. Docker for isolation and testing
7. Git for version control

.2 Limitations

This project is subject to several limitations:

- **API Dependency**: The analysis relies heavily on third-party AI APIs like ChatGPT, which may introduce latency, rate limits, or cost issues.
- **Time Constraints**: Due to the academic calendar, full implementation of advanced features may not be feasible.
- **Security Concerns**: Executing remediation scripts automatically poses risks; this project includes user consent but does not fully mitigate all potential impacts.
- **Limited Real-Time Capabilities**: The platform performs on-demand scans but does not support real-time or continuous monitoring.
- **Legal Considerations**: The tool must only be used on authorized targets; testing on unauthorized systems could breach legal and ethical boundaries.

2 Related Research

2.1 Similar Existing Products

Several reconnaissance and vulnerability assessment tools already exist in the cybersecurity ecosystem, each offering varying levels of automation, depth, and usability. However, these tools, while individually effective, often operate in silos. Most lack integration with modern AI to assist in result interpretation or script generation for remediation. Additionally, they are typically either too complex for novice users or too limited in automation for advanced testers.

2.2 Project's Added Value

This project provides a unique combination of automation, AI integration, and user-friendly interface in the domain of cybersecurity reconnaissance and vulnerability management. Its key contributions include:

- **Unified Platform**: Unlike fragmented toolsets requiring separate setup and use, this platform consolidates various reconnaissance tools under a single, web-based interface.
- **AI-Driven Analysis**: By integrating ChatGPT, the platform introduces intelligent interpretation of scan results, helping even novice users understand technical vulnerabilities and misconfigurations.
- **Roadmap Generation**: Beyond detection, the system provides actionable insights and a step-by-step roadmap for further testing, something not offered by typical scanning tools.
- **Scripted Remediation Support**: Most platforms stop at vulnerability identification. This project takes it a step further by offering AI-suggested remediation scripts, bridging the gap between detection and resolution.
- **Interactive Consent and Execution**: The optional approval mechanism before script execution enhances safety, transparency,

and control for users—especially important in educational or training environments.

- **Dual-Layer Scanning**: With support for both network reconnaissance and host-level vulnerability scanning, the platform broadens its applicability in penetration testing scenarios.
- **Educational Utility**: The platform is particularly valuable for cybersecurity training and academic use, offering a guided and insightful experience for students and new professionals.