ROBUST AUTOMATION RECON PENETRATION TESTING TOOL

Haseeb Biya, Student, Bharati Vidyapeeth (Deemed to be University),Department Of Engineering And Technology, Navi Mumbai, Maharashtra, India

Parth Agashe, Student, Bharati Vidyapeeth (Deemed to be University), Department Of Engineering And Technology, Navi Mumbai, Maharashtra, India

Bhuvnesh Trivedi, Student, Bharati Vidyapeeth (Deemed to be University), Department Of Engineering And Technology, Navi Mumbai, Maharashtra, India

Shweta Patil, Professor, Dept. Of Computer Science & Business Systems, Bharati Vidyapeeth (Deemed to be University), Department Of Engineering And Technology, Navi Mumbai, Maharashtra, India

ABSTRACT:

With increased cyber threats in sophistication and prevalence, it's increasingly essential to utilize tools that assist with penetration testing to be effective as well as efficient. The "Robust Automation Recon Penetration Testing Tool" is what serves this purpose. It eases network security analysis by providing automation of central processes such as IP scanning, obtaining IP data, DNS examination, and the detection of vulnerabilities. Through the elimination of manual tasks, it enables security teams to spend more time on making wiser decisions yet continue to deliver precise and consistent results. What's unique about this tool is that it's scalable. It's built to keep up with emerging cybersecurity threats by introducing new features as necessary so that it remains useful regardless of how things evolve. Its modular structure means it can easily deal with threats yet to come. In addition, the tool has a straightforward and easy-to-use interface, making it a suitable option for both veteran professionals and students such as ourselves who are just entering the profession. It's a practical and effective means of bolstering defences against emerging online threats.

Keywords— cyber threats, penetration testing, vulnerability detection

INTRODUCTION:

The Penetration Testing Tool is a versatile web-based application developed to support cybersecurity professionals, ethical hackers, and IT administrators in evaluating the security of web domains and applications. With the increasing reliance on online platforms, ensuring the security and resilience of digital assets has become paramount. This project serves as a centralized platform, offering a comprehensive suite of tools to identify vulnerabilities, gather critical information, and assess potential security risks associated with a target domain.

The tool integrates a user-friendly interface and a modular structure, allowing users to perform a wide range of security testing operations. Key functionalities include retrieving the IP address of a domain, conducting port scans to identify open ports, performing DNS lookups for domain information, and detecting broken links that could indicate neglected vulnerabilities. Additionally, the platform enables users to enumerate subdomains, analyze directory listings, and identify potential HTML injection points, which are crucial for detecting injection-based security flaws.

Beyond these essential capabilities, the tool also includes advanced features like the exploration of a domain's history through the Wayback Machine and the execution of Google Dorking queries for uncovering sensitive information indexed by search engines. By consolidating these functions into a single application, the project ensures that users can access a comprehensive set of tools without needing to rely on multiple disparate systems.

This project is designed to be accessible to a broad range of users, from seasoned cybersecurity experts to individuals with limited technical expertise. Its clean and intuitive interface simplifies the process of security assessment, enabling users to focus on identifying and addressing vulnerabilities effectively. The Penetration Testing Tool underscores the importance of proactive measures in maintaining the security of digital infrastructure and aims to contribute to the broader effort of strengthening online safety and resilience.

PROPOSED SYSTEM

Penetration testing tools play a vital role in evaluating system security by simulating real-world cyber threats. Among the most prominent tools, Metasploit and Burp Suite are highly regarded for their effectiveness in security assessments.

Metasploit is a versatile framework that empowers cybersecurity professionals to discover, exploit, and validate system vulnerabilities. Its extensive library of exploits and payloads makes it an indispensable asset for ethical hackers.

Meanwhile, Burp Suite excels in web application security testing, offering advanced features such as an intercepting proxy, scanner, and repeater to analyze and modify web traffic. These tools are instrumental in ethical hacking, allowing organizations to proactively detect and remediate security flaws before they can be leveraged by cybercriminals.

SYSTEM ARCHITECTURE OVERVIEW:

Frontend Layer

The frontend is designed to deliver a seamless and interactive user experience, utilizing HTML (Jinja templates), Tailwind CSS, and JavaScript. It features a well-structured and intuitive interface, enabling users to perform security assessments with ease. Key functionalities include IP Scanning, IP Retrieval, IP Lookup, Port Scanning, and DNS Lookup, all accessible through interactive and user-friendly components. Additionally, Chart.js is employed for dynamic data visualization, while AOS (Animate on Scroll) enhances UI responsiveness and engagement.

Backend Layer:

The backend is developed using Python (Flask framework) to efficiently manage server-side operations, core logic processing, and data handling. It integrates key libraries such as:

- SQL Alchemy for database management (SQLite as the storage solution).
- Requests for seamless API communication and data exchange. This architecture ensures real-time execution of security-related tasks while maintaining scalability and performance.

API Layer:

The system employs RESTful APIs to facilitate efficient communication between the frontend and backend. These APIs enhance functionality by enabling smooth data exchange, integration with external security services, and streamlined execution of security evaluations.

PROBLEM STATEMENT:

In the fast-changing world of cybersecurity today, organizations are subjected to more and more security threats, vulnerabilities, and cyber-attacks. The old penetration testing process involves extensive manual labor, time, and knowledge, and therefore it is hard to conduct frequent and detailed security audits.

We require a powerful, automated penetration testing and reconnaissance tool that simplifies the process of finding security vulnerabilities, conducting vulnerability analysis, and recommending remediation.

The tool must incorporate diverse reconnaissance methods, exploit detection functionality, and reporting features to advance security audits.

The objective of this project is to create an automation-based penetration testing tool that effectively collects intelligence, identifies vulnerabilities, and conducts security audits with less human intervention. The tool must be capable of multi-layered security testing, such as network, web application, and system-level penetration testing, to enable organizations to detect and prevent possible threats proactively.

RELATED WORK:

Mamilla, S.R. (2021) [1] conducted a study on penetration testing processes and tools, specifically analyzing Nmap, Dmitry, Unicorn scan, and Sparta within a Kali Linux environment. The research aimed to compare these tools to determine their efficiency in network scanning and vulnerability detection. The findings emphasized the advantages of each tool in identifying security weaknesses. However, the study was constrained by the limited number of tools tested and time restrictions. The author suggested future research involving a broader range of tools and testing across diverse environments to enhance the findings.Shah, K. [2] conducted a study on Vulnerability Assessment and Penetration Testing, emphasizing the significance of combining both approaches to enhance system security. The paper explores various tools and techniques used to detect and mitigate security threats, providing insights into their effectiveness. Additionally, the study highlights challenges faced during implementation and suggests best practices to strengthen cybersecurity measures.

Kumar, K., & Chawda, R. (2019) [3] presented the paper "A Survey about Port Numbers and Its Applications," which explores the role of port numbers in network communications. The study defines port numbers as unique identifiers that facilitate data transmission between a system and its applications. It explains how 16-bit port numbers can be assigned automatically by the operating system, manually configured by users, or predefined for widely used applications. The paper also highlights the interaction between port numbers and networking protocols like TCP and UDP, ensuring proper data routing. Additionally, the authors differentiate between well-known port numbers (e.g., port 80 for HTTP) and transient port numbers, which are assigned temporarily for communication sessions. The study traces the historical development of port numbers, from early ARPANET implementations to their standardized use in modern networks.Mamilla, S.R. (2021) [4] authored the paper "A Study of Penetration Testing Processes and Tools," which emphasizes the growing importance of cybersecurity in light of increasing cybercrimes such as data breaches and hacking. The study advocates for penetration testing as an effective method to evaluate the robustness of an organization's security measures.

It highlights the necessity for penetration testers to consider factors like budget, time constraints, and the specific scope of an organization's needs when selecting appropriate tools for each phase of the testing process.

DEPLOYMENT DIAGRAM :

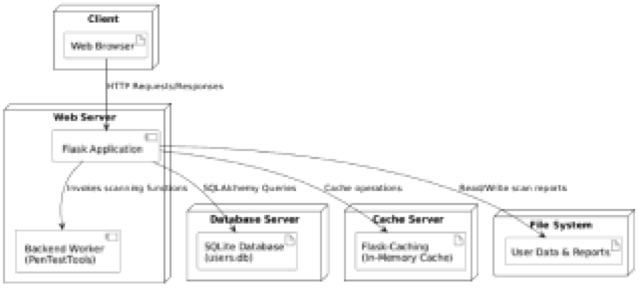

Fig 1 Deployment Diagram

At the forefront, the Client represents a web browser that communicates with the Web Server through HTTP requests and responses. The Web Server hosts a Flask Application, which acts as the core processing unit, handling client requests and coordinating different operations. This application interacts with a Backend Worker (Pen Test Tools) to execute scanning functions for security assessments.

To manage user data and authentication, the Flask application performs SQL Alchemy queries to interact with an SQLite database housed on a Database Server. Additionally, to enhance performance, a Cache Server utilizing Flask-Caching (In-Memory Cache) is integrated, allowing for efficient handling of frequently accessed data through caching operations.

The system also includes a File System that is responsible for storing user data and generated scan reports. The web server reads from and writes to this storage, ensuring that reports and other relevant information are preserved for further analysis.

CLASS DIAGRAM

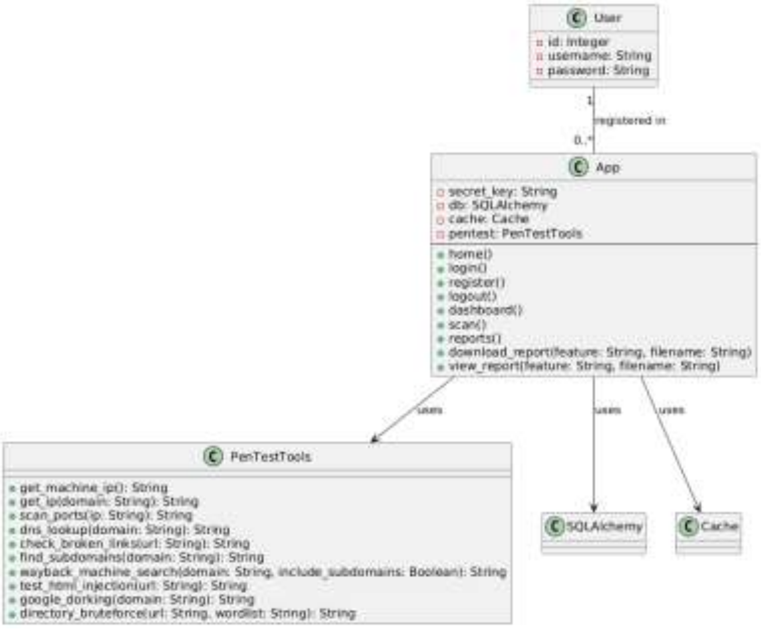
User
id: Integer
username: String
password: String
1
registered in
0..*
App
secret_key: String
db: SQLAlchemy
cache: Cache
pentest: PenTestTools
home()
login()
register()
logout()
dashboard()
scan()
reports()
download_report(feature: String, filename: String)
view_report(feature: String, filename: String)
uses
uses
uses
PenTestTools
get_machine_ip(): String
get_ip(domain: String): String
scan_ports(ip: String): String
dns_lookup(domain: String): String
check_broken_links(url: String): String
find_subdomains(domain: String): String
wayback_machine_search(domain: String, include_subdomains: Boolean): String
test_html_injection(url: String): String
google_dorking(domain: String): String
directory_bruteforce(url: String, wordlist: String): String
SQLAlchemy
Cache

Fig 2 Class Diagram

The diagram represents a modular class structure for an application designed to integrate user management, penetration testing, and reporting functionalities. The User class handles user data with attributes like id, username, and password, while the App class acts as the core of the system, managing user sessions, database interactions using SQLAlchemy, and caching with the Cache class. The App class also provides methods for authentication (login, register, logout), initiating scans (scan), and managing reports (report, download report, view report), ensuring seamless interaction between users and the application's core features. Additionally, it securely manages user credentials and session states. At the heart of the penetration testing capabilities is the PenTestTools class, which offers methods for various security tasks such as port scanning (scan_ports), DNS lookups (dns_lookup), subdomain discovery (find_subdomains), and vulnerability detection. It supports threading and performance optimization using tools like _load_wordlist and lock. The Main class serves as the entry point, orchestrating the application's flow by instantiating components like App and PenTestTools. This design ensures a clean separation of concerns, making the system scalable, maintainable, and efficient for penetration testing workflows. It also allows for easy expansion of functionalities, ensuring the framework remains adaptable to future requirements.

MODEL:

Fig 3. Landing Page

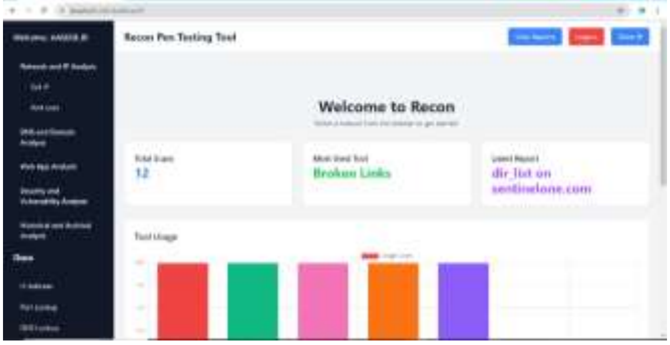

Fig 4. Dashboard

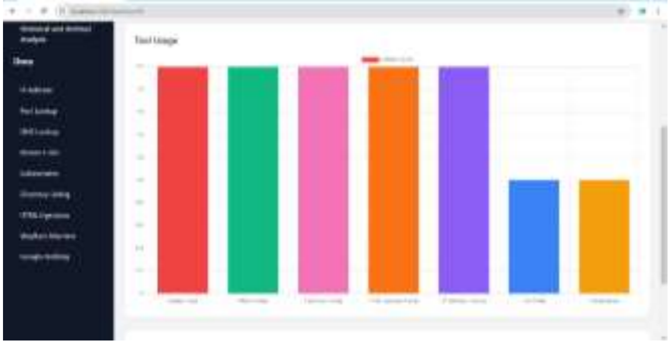

Fig 5. Feature Usage Bar Graph

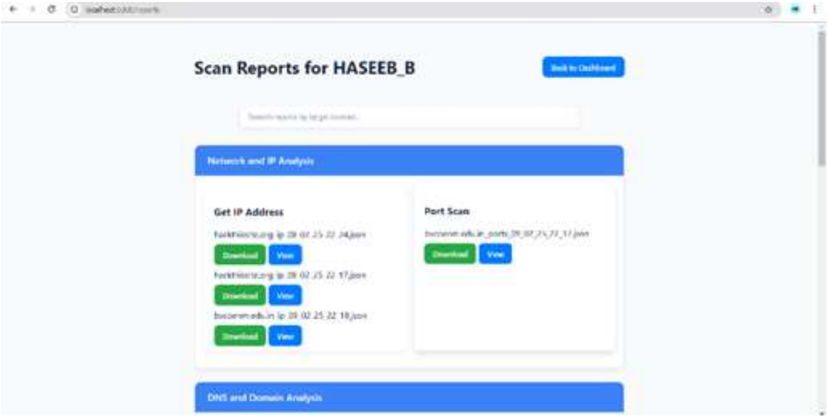

Fig 6. Report Pag

RESULT:

Fig 7. DNS Records

Fig 8. Subdomains of Hackthissite

Fig 9. BrokenLink's of Hackthissite

USE CASES AND APPLICATIONS :

The "Robust Automation Recon Penetration Testing Tool" is developed for use as a general-purpose tool for most cyber security issues. The use can span many domains and situations, as detailed below:

1. Network Vulnerability Assessment

The tool highlighted would therefore be useful because it identifies vulnerabilities in network configurations and open ports, and exposed services. Very useful to organizations that want to shield their internal and external networks from cyber threats.

2. Web Application Security Testing

The tool is used by penetration testers to analyze the security of web applications by performing DNS analysis and IP reconnaissance. Useful for detecting misconfigurations, DNS spoofing vulnerabilities, and weak security practices on hosted applications.

3. Small and Medium Enterprise (SME)

Security SMEs normally would not have the ability to undertake exhaustive security testing due to shortage of and other resources. This tool provides for a relatively low-cost and easy-to-use solution for securing their digital assets. Removes complicated steps that necessitate deeper specialized security expertise.

FUTURE SCOPE:

"Robust Automation Recon Penetration Testing Tool" is a morphable network security solution providing simple functionalities of IP scanning, DNS analysis, and IP search. The roadmap for future development is focusing on empowering the tool with more recent techniques and challenges in cyberspace security.

1. **Integration with Machine Learning for Threat Detection:**

Because cyber threats are resorting to increasingly insidious means, Machine Learning is playing a crucial role in detecting repeated or missed events and behaviors that traditional means might overlook. Future contender features could include employing ML algorithms for predictive threat analysis, anomaly detection, and risk assessment based on historical data.

2. **Global Threat Intelligence and Geolocation Integration:**

Combined, real-time global threat intelligence feed as well as geolocation could enable the tool to measure threats by location, source, and attack patterns.

3. **Advanced Reporting and Analytics:**

The tool could be advanced by reporting and analytics functions that generate comprehensive security assessment, risk report, and visualization of the attack surface to enable more informed decision-making.

COCNLUSION :

The Penetration Testing Tool is a comprehensive solution designed to simplify and enhance the process of identifying vulnerabilities in web domains. By integrating features like IP address retrieval, port scanning, DNS lookups, subdomain enumeration, and advanced tools such as Google Dorking and HTML injection detection, it equips users with essential capabilities for thorough security assessments.The tool’s intuitive interface and modular design ensure accessibility for a wide range of users, from cybersecurity experts to those with minimal technical expertise. It consolidates powerful features into one platform, saving time while delivering actionable insights to address potential risks effectively.In a rapidly evolving digital landscape, this tool plays a crucial role in fostering proactive security measures. It empowers users to safeguard their systems, contributing to the broader goal of strengthening cybersecurity in an increasingly interconnected world.

TABLE - I. TEST CASES

Test Case ID	Feature	Input	Expected Output	Actual Output	Status
1	Get IP address	www.hackthissite.org	Returns the IP address of the domain	137.74.187.103	PASS
2	Scan Port	www.hackthissite.org	Returns Open ports	Port 80 (HTTP), Port 443 (HTTPS)	PASS
3	DNS Lookup	www.hackthissite.org	Returns DNS Records	A, MX, NS, TXT Records	PASS
4	Find Subdomains	www.instagram.com	Returns list of subdomains	Multiple subdomains found	PASS
5	Broken Links	www.hackthissite.org	Returns list of	List of broken links	PASS

			broken links		
6	Directory Listing	www.hackthissite.org	Returns discovered directories	List of directories	FAIL
7	HTML Injection	www.hackthissite.org	Returns injection point details	Form fields susceptible	PASS
8	Google Dorking	www.hackthissite.org	Returns search results	List of search results	PASS
9	Wayback Machine Scan	www.hackthissite.org	Returns historical data	Historical website data	PASS

REFERENCES :

1. *A .Patil, "Research Paper on Cyber Security Challenges and Threats," International Journal of Advanced Research in Science Communication and Technology, 2024* *https://ijarsct.co.in/Paper15082.pdf*
2. *Shah, "Vulnerability assessment and penetration Testing by Khushi Shah," Scribd, 2023.* *https://www.scribd.com/document/775397616/Vulnerability-Assessment-and-Penetration-Testing-by-Khushi-Shah*
3. *F. Barman, N. Alkaabi, H. Almenhali, M. Alshedi, and R. Ikuesan, "A methodical framework for conducting reconnaissance and enumeration in the ethical hacking lifecycle," European Conference on Cyber Warfare and Security, vol. 22, no. 1, pp. 54–64, Jun. 2023*
4. *M. Saha and V. Adai kalam, "Information Gathering of Ethical Hacking using Reconnaissance Framework," 2022* https://www.ijset.in/wp-content/uploads/IJSET_V10_issue2_196.pdf
5. *Petar Lachkov and Smriti Bhatt, "Vulnerability assessment for applications security through penetration simulation and testing," Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing, May 2021.* *https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10251051*
6. *S. R. Mamilla, "A study of penetration testing processes and tools," CSUSB Scholar Works, 2021.*
7. *Rakesh R, "Autonomous Penetration Testing for Web Applications Using Raspberry Pi", pub. in International Journal of Engineering and Techniques - Volume 4 Issue 1, Jan – Feb 2018*
8. *Aleatha S., "Selection of penetration testing methodologies: A comparison and evaluation", pub. in proc. of AUSTRALIAN INFORMATION SECURITY MANAGEMENT CONFERENCE, 2018.*
9. *Aleatha S. "Selection of penetration testing methodologies: A comparison and evaluation", pub. in proc. of AUSTRALIAN INFORMATION SECURITY MANAGEMENT CONFERENCE, 2018* *https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1181&context=ism*
10. *Mahajan, R Kumar, and Kumar Khatri, "A study on web application security and detecting security vulnerabilities," IEEE Conference Publication | IEEE Xplore, Sep. 01, 2017* *https://www.researchgate.net/publication/324935252_A_study_on_web_application_security_and_detecting_security_vulnerabilities*
11. *Gupta and A. Anand, "Ethical hacking and hacking attacks," International Journal of Engineering and Computer Science, Apr. 2017* *https://www.researchgate.net/publication/316431977_Ethical_Hacking_and_Hacking_Attacks*
12. *Patil, Jangra, Bhale, Raina, and Kulkarni, "Ethical hacking: The need for cyber security," IEEE Conference Publication | IEEE Xplore, Sep. 01, 2017.*