IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology(IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303256 |

Cyber Fusion -An Ethical Hacking Suite

CH.Mounika[1], M.Amith[2], N.Sita Samhitha[3], SK.Abdul Kalam[4]

U.G. Student[1], Department of Computer Engineering (CIC), Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

U.G. Student[2], Department of Computer Engineering (CIC), Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

U.G. Student[3], Department of Computer Engineering (CIC), Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

U.G. Student[4], Department of Computer Engineering (CIC), Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

ABSTRACT: In the realm of cybersecurity, the development of web applications for network security assessment has emerged as a critical endeavor. This paper presents a meticulously designed workflow for such an application, aimed at offering a comprehensive and efficient approach to network security assessment. The workflow is structured to leverage advanced technologies and user-provided data, facilitating thorough analysis and actionable insights. The workflow initiates with users inputting essential target details, including URLs for WHOIS IP address retrieval, target IP addresses, and curated username/password lists for SSH and FTP access. Subsequently, the application retrieves IP addresses associated with provided URLs using WHOIS, laying the groundwork for network scanning. The network scanning phase employs sophisticated techniques such as port scanning and service enumeration to uncover vulnerabilities and open ports within the target systems. Simultaneously, if SSH or FTP ports are open, the application seamlessly transitions into the password cracking module, utilizing user-provided credentials to bolster network defenses. The culmination of the workflow is the comprehensive display of assessment results to users. Through intuitive visualization and informative reporting, users gain insights into the security posture of target systems. Additionally, users are granted access to target systems via a terminal interface, empowering them to undertake informed actions for security remediation. This meticulously orchestrated workflow epitomizes a fusion of cutting-edge technology and user-driven insights, aspiring to elevate network security practices and fortify defenses against evolving cyber threats.

KEYWORDS: Information Gathering, Vulnerability Scanning, Exploitation, Hydra, SSH(Secure shell), Nmap

I.INTRODUCTION

In an era defined by relentless digital innovation, the protection of networks against cyber threats emerges as an imperative. Traditional security protocols often prove inadequate, leaving organizations vulnerable to malicious actors and data breaches. Recognizing the urgency of fortifying defenses, the demand for advanced tools for network scanning, password cracking, IP address discovery, and WHOIS lookup integration escalates.This ambitious initiative sets out to meet these exigencies head-on by spearheading the development of a state-of-the-art web application. Harnessing the power of machine learning algorithms, predictive analytics, and cloud computing, the project aims to revolutionize cybersecurity practices. Through meticulous network scans, exhaustive password analysis, and precise IP address identification via WHOIS lookup, the application promises unparalleled insight into network vulnerabilities.Moreover, by incorporating dynamic threat intelligence feeds and anomaly detection mechanisms, the application will proactively anticipate and mitigate emerging cyber threats. The fusion of these advanced functionalities will empower security professionals and system administrators with a multifaceted toolkit to fortify defenses comprehensively.Beyond mere detection, the application envisions proactive defense strategies, enabling organizations to stay one step ahead of cyber adversaries. By fostering a culture of resilience and adaptability, it aims to usher in a new era of cybersecurity excellence, where proactive risk management and continuous innovation are the cornerstones of digital .In essence, this project represents a paradigm shift in cybersecurity, where the boundaries of protection are extended, and vulnerabilities are transformed into opportunities for growth and resilience. By embracing

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303256 |

the cutting edge of technology and harnessing its transformative potential, the application stands as a beacon of hope in an ever-evolving digital landscape.

II. LITERATURE SURVEY

In [1] we integrated WHOIS, Nmap, and medusa tools for comprehensive Network Security Assessment. By consolidating these tools into unified interface, users can seamlessly transition between assessment phases, streamlining workflows and enhancing efficiency.
In [2] we enhanced Accessibility and Usability of Network Security Assessment Tools through Web Integration. This approach of web-based integration of WHOIS, Nmap, Medusa addresses accessibility and usability challenges by providing a user-friendly interface accessible from any device with an internet connection.
In [3] we observed that using standalone tools may lack centralized control and oversight, making it challenging for security administrators to monitor and manage assessment activities effectively, so to resolve the issue we come up with unified tool which offers centralized control and oversight of network security assessment activities through the web application interface.
In [4] we found out that manual execution and coordinating multiple network security assessment tools can be time-consuming and error-prone, so we automated execution and coordination of WHOIS, Nmap, Medusa withina unified web application.Hence this tool reduces the need for manual intervention and improve scalability of security assessment processes.This automated work flow streamline minimize errors,consumes time for users,enhance efficiency of security operations.

III. EXISTING SYSTEM

The existing system for network security assessment relies heavily on standalone tools and manual processes to identify vulnerabilities, assess network security posture, and mitigate potential risks. Security professionals typically utilize a variety of tools, such as WHOIS for domain registration information retrieval, Nmap for network mapping and port scanning, and Medusa for password cracking. These tools operate independently, requiring manual execution and coordination by security professionals. This manual approach involves inputting target information, configuring scan parameters, executing scans, and analyzing results, leading to a fragmented workflow with inefficiencies in managing data transfer and dependencies. Moreover, the command-line-based nature of many existing tools necessitates installation and configuration on local machines, limiting accessibility and usability, especially for non-technical users. Additionally, the lack of integration between tools results in disjointed assessment processes, reducing the effectiveness of identifying and mitigating security risks comprehensively. Manual execution and coordination of tools also pose scalability challenges, particularly in large-scale network environments, and may lack centralized control and oversight, increasing the risk of security breaches and unauthorized access. Overall, conducting network security assessments using standalone tools and manual processes can be resource-intensive in terms of time, effort, and personnel required to perform assessments and analyze results.

Disadvantages of Existing System:

1. Fragmented workflow – Leads to ineffeciencies and increased risk of errors.
2. Limited accessibility and usability – Hinder collaboration and knowledge sharing.
3. Lack of integration – Reduces the effectiveness of security assessments.
4. Scalable challenges – Obstruct the ability to conduct assessment at scale.
5. Security Risks – Lack of centralized control and oversight,increase risk of security breaches.

IV. PROPOSED SYSTEM

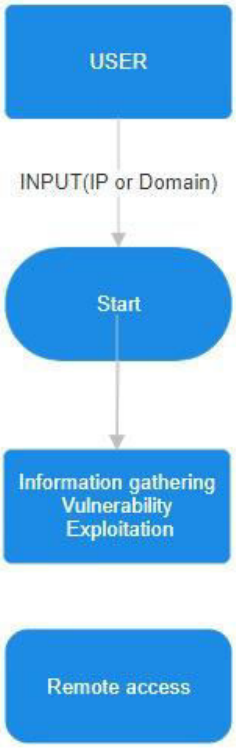
The proposed system for network security assessment represents a significant advancement over the existing system, aiming to overcome its limitations through a comprehensive, integrated, and automated approach to security testing. At its core, the proposed system offers an integrated platform that consolidates the functionality of multiple security assessment tools, including WHOIS, Nmap, and Medusa, into a unified interface. This integration streamlines the assessment process, eliminating the need for users to switch between different tools and facilitating seamless execution and coordination of assessment tasks. Moreover, the proposed system features a user-friendly web-based interface accessible from any device with an internet connection, enhancing accessibility and usability for both technical and non-technical users. Automation plays a pivotal role in the proposed system, with automated workflows enabling users to initiate assessments, configure parameters, and analyze results with minimal manual intervention. Centralized

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303256 |

control and oversight further enhance security by providing administrators with visibility into assessment processes and results, allowing for enforcement of access controls, monitoring of activity logs, and ensuring compliance with security policies and standards. Scalability and performance considerations are paramount in the design of the proposed system, with cloud-based infrastructure and distributed computing resources enabling dynamic scaling to accommodate large-scale network environments and handle concurrent assessment tasks efficiently. Security remains a top priority, with built-in features such as encryption, authentication mechanisms, and role-based access controls ensuring the confidentiality, integrity, and availability of assessment data and tools. Additionally, the proposed system generates comprehensive reports detailing assessment findings and recommended remediation actions, providing stakeholders with actionable insights to enhance the security posture of their network infrastructure effectively. Overall, the proposed system represents a holistic and advanced solution to network security assessment, addressing the shortcomings of the existing system and empowering organizations to proactively manage and mitigate security risks.



V. METHODOLOGY

STEP 1 : USER INPUT

In this step user simply inputs the URL of the target website. This URL serves as the starting point for the application to gather further details about target's infrastructure.

STEP 2 : IP ADDRESS RETRIEVAL

This step looks up the IP addresses linked to the provided URLs using WHOIS which helps understand the target's infrastructure better.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303256 |

STEP 3 : NETWORK SCANNING

Using the obtained IP addresses, the app scans the network extensively to find vulnerabilities and open ports, which could be potential entry points for hackers.

STEP 4 : PASSWORD CRACKING

If open SSH or FTP ports are found, the tool tries to crack passwords using the provided username and password lists, aiming to identify weak credentials.

STEP 5 : RESULT DISPLAY

Finally, the app presents the assessment results to users, allowing them to access target systems' terminals to execute commands and take actions. This helps users understand the security status and make informed decisions for enhancing cybersecurity.

VI. IMPLEMENTATION

1.FrontEnd Design

The frontend design focuses on creating a user-friendly interface that facilitates seamless interaction and efficient workflow management. Key features include:

- Input Forms: Intuitive forms for users to input target details, username lists, and password lists.
- Result Display: Clear and concise display of network scanning results, open ports, services, and potential vulnerabilities.
- User Authentication: Secure login mechanisms to authenticate users and provide access control based on user roles.

2. Backend Development

The backend development utilizes Django for routing, Celery for asynchronous task processing, and Python for scripting and integration. Key components of the backend include:

- Task Queue: Celery task queue for managing asynchronous tasks such as network scanning and password cracking.
- Task Scheduler: Scheduled tasks to automate recurring processes and ensure timely execution.
- Integration with Medusa: Seamless integration with Medusa for efficient password cracking attempts and vulnerability testing.

3. Database Management

MySQL is used as the database management system to store and manage application data securely. Key aspects of database management include:

- User Credentials: Secure storage of user credentials, encrypted passwords, and authentication tokens.
- System Logs: Logging mechanisms to track user activities, system events, and audit trails for security analysis.
- Data Protection: Measures to ensure data confidentiality, integrity, and availability within the database.

4. Testing

4.1 Unit Testing

Unit testing is conducted to validate individual components, including input validation, task execution, and data processing. Key aspects of unit testing include:

- Input Validation Testing: Testing input forms to ensure proper validation of user input and prevention of malicious input.
- Task Execution Testing: Validating task execution, asynchronous processing, and task completion under various scenarios.
- Data Processing Testing: Verifying data processing logic, database interactions, and data retrieval functionalities.

4.2 Integration Testing

Integration testing focuses on validating the interaction between frontend and backend components, including data flow, task integration, and system communication. Key aspects of integration testing include:

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303256 |

- Frontend-Backend Interaction: Testing communication between frontend elements and backend services, including form submissions, data retrieval, and result display.
- Task Integration: Ensuring seamless integration of Celery tasks, task queues, and task execution within the application.
- System Communication: Verifying API calls, data transfers, and inter-component communication for smooth operation.

4.3 Security Testing

Security testing is conducted to identify vulnerabilities, assess security measures, and ensure robust security posture. Key aspects of security testing include:

- Penetration Testing: Conducting penetration tests to identify potential vulnerabilities, injection attacks, and security loopholes.
- Authentication Testing: Testing authentication mechanisms, user sessions, and access control mechanisms for security compliance.
- Data Protection Testing: Validating data encryption, secure data storage, and data access controls to protect sensitive information.

VII. RESULTS

The results of the project showcase the successful implementation of network scanning and password cracking functionalities, a user-friendly interface, and robust security measures. Key outcomes include:

- Effective Network Scanning: The application accurately identifies open ports, services, and potential vulnerabilities in target systems.
- Efficient Password Cracking: Medusa integration enables efficient password cracking attempts, enhancing password security assessment.

VIII. RESULT ANALYSIS

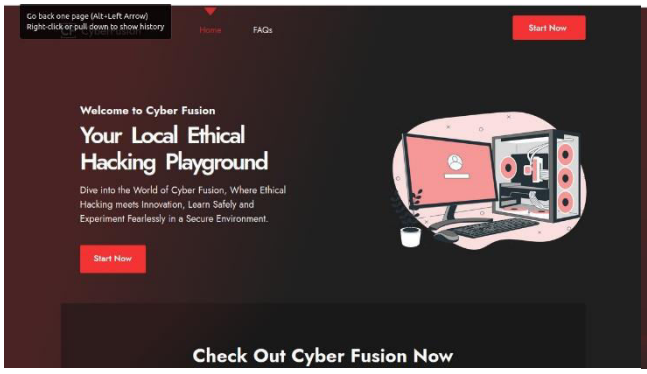


Fig 1 : Home page

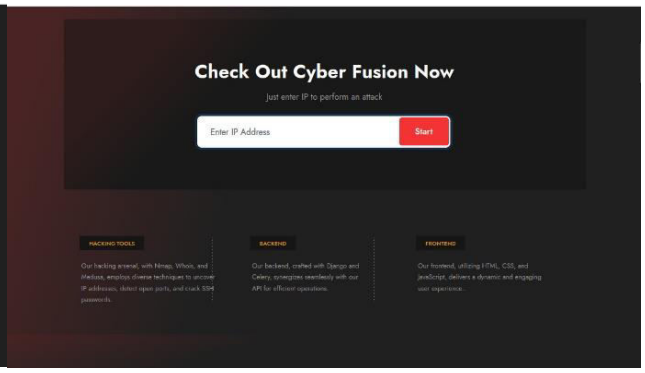


Fig 2 : User input

Fig 3 : Execution of Cyber Fusion

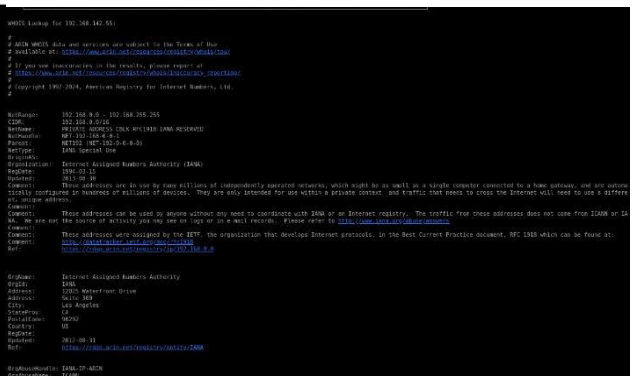


Fig 4 : Information gathering using WHOIS

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303256 |

Fig 5 : Checking for open ports using Nmap and password Cracking using hydra and getting access to target machine

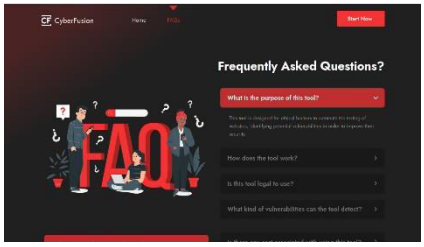


Fig 6 : FAQ page

IX. CONCLUSION

In conclusion, the development of the web application for network scanning, password cracking, and IP address retrieval through WHOIS represents a significant step towards enhancing cybersecurity practices and fortifying network defenses. The project's successful implementation of advanced technologies, robust security measures, and user-friendly design contributes to:

Improved Security Posture: Organizations can leverage the application to not only identify and mitigate potential vulnerabilities and strengthen password security but also to retrieve IP addresses associated with URLs using WHOIS data. This multifaceted approach enhances the overall security posture by providing a comprehensive view of potential risks and vulnerabilities.

Efficient Workflow: The application streamlines the network scanning, password cracking, and IP address retrieval processes. It automates task execution, providing security professionals and system administrators with actionable insights derived from comprehensive scans and WHOIS data analysis. This efficiency accelerates threat detection and response, ultimately fortifying network defenses.

User Trust and Confidence: The integration of security measures, data protection mechanisms, and user authentication instills trust and confidence among users. Additionally, the ability to retrieve IP addresses using WHOIS data adds another layer of transparency and reliability to the application. Users can be assured of a secure and dependable environment for conducting cybersecurity operations.

Future Development: Future iterations of the application can explore additional features, enhancements, and integrations to further enhance network security. Integration with WHOIS for IP address retrieval opens up possibilities for deeper analysis, such as identifying potential threat actors and tracing malicious activities back to their source. This continuous evolution ensures that the application remains at the forefront of addressing emerging cybersecurity challenges, providing organizations with the tools they need to adapt and respond effectively to evolving threats."

REFERENCES

[1] https://ieeexplore.ieee.org/document/8673520
[2] https://www2.cs.arizona.edu/~collberg/Teaching1466-566/2012/Resources/presentations/2012/topic7-final/report.pdf
[3] Bhushan B. Gupta, "Requirements Based Web Application Security Testing–A Preemptive Approach!", 2017
[4] Whois(1) — whois — Debian stretch — Debian Manpages". Archived from the original on 2021-04-01. Retrieved 2020-12-27
[5] Password Cracking. Open Web Application Security Project (OWASP). Available online: https://owasp.org/www-community/password-cracking
[6] Web Application Security Testing Methodologies." OWASP. Available online: https:// owasp.org/www-project-web-security-testing-guide/
[7] Whois Documentation. Available online: https://www.whois.net/
[8] Nmap Documentation. Available online: https://nmap.org/book/
[9] Medusa Documentation. Available online: https://github.com/jmk-foofus/medusa

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details