iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60230

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

ScanMaster: Holistic Network Scanning Toolset

Yerramsetti Sri Uday Kiran Sai Mahesh[1], Manthena Srihari[2], Tammala Aravind[3], Gajele Manisha [4], Reddyvari Venkateswara Reddy[5]

[1, 2, 3] *Student, Department of CSE (Cyber Security), CMR College Of Engineering & Technology, Hyderabad, India*
[4]*Assistant Professor, Department of CSE (Cyber Security), CMR College Of Engineering & Technology, Hyderabad, India*
[5]*Associate Professor, Department of CSE (Cyber Security), CMR College Of Engineering & Technology, Hyderabad, India*

Abstract: ***The SCANMASTER introduces an innovative network scanning tool that overcomes limitations in tools like Nmap and Wireshark. Notably, it features a user-friendly interface for enhanced accessibility and focuses on HTTP information gathering, offering insights beyond traditional network scanning. Unique timing and performance options allow users to customize scan speeds, potentially providing an edge in different network environments. Emphasizing efficiency, the tool facilitates quick scans for rapid network assessments without compromising depth. In summary, our tool offers a distinctive blend of simplicity, specific functionality, and efficient network analysis.***

Keywords: ***SCANMASTER, Network scanning tool, Nmap alternative, Wireshark alternative, User-friendly interface, HTTP information gathering, Customizable scan speeds, Performance options, Rapid network assessments, Efficiency in network analysis, Quick scans, Enhanced accessibility, Unique timing options, Specific functionality, Depth in network analysis, Distinctive blend, Network environment optimization, Enhanced insights, Efficient network scanning, Simplified network analysis.***

I. INTRODUCTION

In today's rapidly evolving digital landscape, businesses face significant challenges in managing their expanding digital presence. The complex network architectures that emerge from this growth present formidable obstacles to effectively monitoring and securing digital assets. Existing solutions, while diverse, often falter due to integration complexities, real-time capability shortcomings, and limited customization options. This results in a noticeable gap in proactive network security implementation, leaving organizations exposed to evolving threats. Consequently, there is a critical need for a network scanning tool that offers reliability and flexibility surpassing current solutions. Such a tool must seamlessly adapt to diverse network environments, integrate smoothly with existing infrastructures, and provide real-time monitoring and customizable features. Addressing these challenges is imperative for organizations to bolster their defenses against emerging threats and confidently navigate the dynamic digital landscape.

II. LITERATURE REVIEW

A. Zahoor Ahmed Soomro, Mahmood Hussain Shah, Javed Ahmed (2016)

In relation to SCANMASTER, it examines managerial roles in information security management (ISM). It lists the essential tasks for an efficient ISM, including training, policy creation, and business alignment. It emphasizes a comprehensive strategy and provides guidance on how to include SCANMASTER into ISM procedures. useful for both scholars and practitioners.

B. Akira Tanaka, Chansu Han, Takeshi Takahashi (2023)

For SCANMASTER to be effective in network security, methods for identifying and characterizing port scanning activity must be examined in the literature review. It draws attention to the difficulty in gleaning insights from aggregate traffic because different scanning algorithms are used. The study suggests a technique for recognizing distinct scanning patterns, sometimes known as "fingerprints," which include stealth scan patterns. It makes a connection between threat intelligence and fingerprints, improving SCANMASTER's capacity to identify scanning efforts. useful for incorporating cutting-edge detection techniques for proactive network defense into SCANMASTER.

C. Erik Larsson, Zehang Xiang, Prathamesh Murali (2021)

Reconfigurable scan networks (RSNs) are a useful tool for efficiently accessing on-chip instruments in contemporary integrated circuits (ICs). It suggests a hardware block to dynamically manage malfunctioning RSNs, making it easier to locate, test, and fix malfunctioning scan chains. The approach's viability is demonstrated by implementations, which also provide information on how to include fault management into SCANMASTER for better IC testing and maintenance.

D. Rodney R Rohrmann, Vincent J Ercolani, Mark W Patton (2015)

This paper addresses Tor's scalability issues by investigating the use of third-party data sources for anonymous, targeted IPv4 address scans utilizing parallelized scanners. Through anonymization of the scanning process, researchers can efficiently gather data from internet scans without running the danger of reprisals. The study shows that this strategy is feasible and provides SCANMASTER with useful information for enhanced scanning that preserves anonymity.

E. Min Huang, Jingyang Wang, Huiyong Wang (2010)

This article argues in favor of real-time data transport, pointing out the drawbacks of HTTP's pull approach, particularly in applications such as message and monitoring systems. It suggests leveraging HTTP-based persistent connections for real-time data transfer in a CORBA-based network management application. The method has benefits including increased security, adaptability, and versatility. SCANMASTER could be developed with the help of this literature to provide better real-time capabilities.

F. Saminda Wattuhewa 2023)

This evaluation emphasizes how important it is for network devices to have open ports as well as how useful tools like Nmap are for network administration and cybersecurity. The capacity of Nmap to detect open ports facilitates in-depth network examination and assists in evaluating security and resolving issues. If SCANMASTER had similar functionality, it might be more useful for port scanning and network evaluation.

J. Asokan, K.R. Aravind Britto, P. Valarmathi, M. Sundar Prakash Balaji, G. Sasi, V. Elamaran (2023)

This study focuses on the Nmap security scanning tool's capability and adaptability in evaluating network security. Nmap's versatility in conducting several kinds of scans makes it possible to thoroughly inspect hosts and services on a network, which helps to find potential vulnerabilities. The study highlights the applicability of Nmap in professional security assessments by concentrating on evaluating security flaws in over fifty Indian government websites. SCANMASTER's security scanning and vulnerability detection skills might be improved by incorporating a comparable feature.

G. Andrea Tundis , Wojciech Mazurczyk , Max Mühlhäuser (2018)

The review talks about how important it is to find system vulnerabilities in light of how quickly the Internet is growing. It draws attention to the availability of programs like Censys and Shodan, which automatically search the Internet for security flaws and make the results available to the public. These programs don't really touch the targeted devices; instead, they give prospective attackers reconnaissance data. The purpose of this study is to present an overview of the many publicly available network vulnerability scanning tools, classifying, characterizing, and emphasizing their benefits and drawbacks. By incorporating the knowledge gained from this assessment, SCANMASTER may be better able to detect and address network issues.

H. M. Sprengers, J. van Haaster (2016)

The evaluation of the literature offers information on network scanning technologies, highlighting their significance in locating active hosts and evaluating vulnerabilities. It talks about how difficult it is to swiftly scan big networks and emphasizes how important tools like Nmap are for effective scanning. It also discusses how to use network scanning to find endpoints and possible security concerns, including useful examples and enumeration tools such as "nmap". In order to effectively monitor network security and identify vulnerabilities, "SCANMASTER" can be developed and implemented with significant input from this thorough overview of network scanning tools and processes.

I. Ethan Harris, Lily Parker (2023)

Within the context of network security products, ScanMaster is evaluated in this comparative analysis. It gives information on its benefits over competitors by contrasting its features, functionality, and usability with those of other instruments of a like kind.

III. METHODOLOGY

A. SCANMASTER

Represents a comprehensive solution designed to address the evolving challenges of network security assessment and vulnerability management. By leveraging a combination of advanced scanning techniques, customizable parameters, and intuitive user interfaces, SCANMASTER aims to provide network administrators and cybersecurity professionals with a powerful toolset to proactively

identify and mitigate security risks within their network infrastructure. Through its versatile target selection options, SCANMASTER enables users to tailor scans to their specific environments, whether it's a single host, a range of IPs, or an entire subnet. The integration of the Nmap Scripting Engine (NSE) allows for the execution of custom scripts, enhancing the tool's capability to detect vulnerabilities and misconfigurations across diverse network environments. Additionally, SCANMASTER's support for various output formats facilitates seamless integration with existing security workflows, streamlining the process of analysis and reporting. Overall, SCANMASTER serves as a proactive solution to bolster network security posture, providing users with the insights and tools needed to fortify their networks against potential cyber threats.

B. Key Features

1) *Target Selection:* SCANMASTER allows users to select targets using various options such as single IP, host, range of IPs, or a subnet. Additionally, users can scan targets listed in a text file.
2) *Port Selection:* Users have flexibility in specifying the ports to scan, including single ports, ranges, or scanning all 65,535 ports. This feature enables users to focus their scans based on specific port configurations.
3) *Scan Types:* SCANMASTER supports different scan types, including TCP connect scans, TCP SYN scans, and UDP port scans. Users can choose the appropriate scan type based on their requirements for accuracy and efficiency.
4) *Service and OS Detection:* The tool provides functionality for detecting operating systems and services running on target hosts. Users has the capability to collect intricate details regarding detected services and operating systems to assess potential vulnerabilities.
5) *Output Formats:* SCANMASTER offers multiple output formats, including text files and XML, to cater to users' preferences for result presentation and analysis. This ensures compatibility with various analysis tools and workflows.
6) *NSE Scripts:* Users can leverage Nmap Scripting Engine (NSE) scripts to extend SCANMASTER's capabilities for in-depth analysis and vulnerability detection. SCANMASTER supports running default, custom, or predefined NSE scripts for specific scanning tasks.
7) *HTTP Service Information:* The tool includes features for gathering information from HTTP services, such as retrieving page titles, HTTP headers, and identifying web applications from known paths.
8) *Timing and Performance:* SCANMASTER allows users to adjust scan timing and performance settings based on their network environment and requirements. Options range from cautious scans suitable for intrusion detection system evasion to aggressive scans for rapid results.

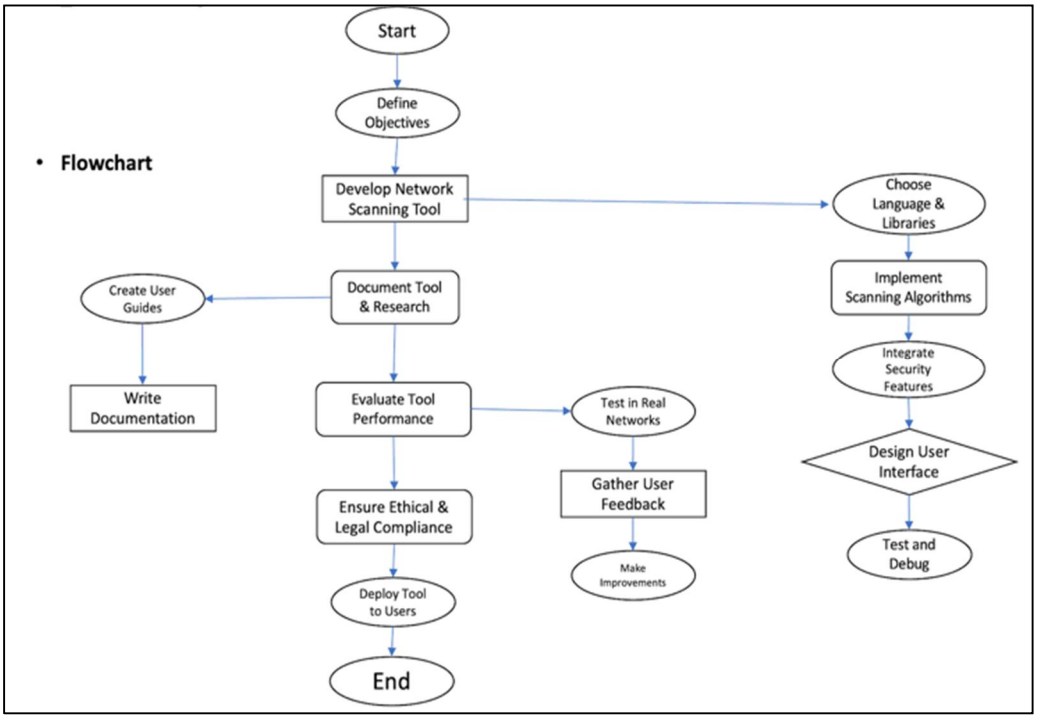


Fig: 1 Flowchart

IV. BENEFITS

1) *Comprehensive Security Assessment:* SCANMASTER offers an all-encompassing approach to network security assessment and vulnerability management. It provides a wide range of scanning techniques and customizable parameters to effectively identify and mitigate security risks within network infrastructures.
2) *Ease of Use:* With intuitive user interfaces and versatile target selection options, SCANMASTER is user-friendly and accessible to network administrators and cybersecurity professionals. Its straightforward design simplifies the process of initiating scans and interpreting results.
3) *Customization and Flexibility:* SCANMASTER allows users to tailor scans to their specific environments by selecting targets, specifying ports, and choosing appropriate scan types. This customization capability ensures that scans are focused and efficient, maximizing the utility of the tool.
4) *Integration with Existing Workflows:* SCANMASTER supports various output formats, facilitating seamless integration with existing security workflows. This compatibility enables users to incorporate SCANMASTER into their current processes for analysis and reporting without disruption.
5) *Enhanced Detection Capabilities:* By leveraging the Nmap Scripting Engine (NSE) and HTTP service information gathering features, SCANMASTER enhances detection capabilities for vulnerabilities and misconfigurations across diverse network environments. This empowers users to conduct in-depth analysis and identify potential security threats effectively.
6) *Performance Optimization:* SCANMASTER offers options to adjust scan timing and performance settings, allowing users to optimize scans based on their network environment and requirements. Whether conducting cautious scans for intrusion detection system evasion or aggressive scans for rapid results, users have the flexibility to adapt SCANMASTER to suit their needs.

V. OBJECTIVES

The objective of SCANMASTER is to provide users with a powerful yet user-friendly tool for enhancing network security and conducting comprehensive vulnerability assessments. By offering a range of features and functionalities, SCANMASTER aims to enable users to proactively identify and address potential security risks within their network environment. The intuitive interface permits users to perform targeted scans, select specific ports, and choose from various scan types to suit their unique needs.

Furthermore, SCANMASTER facilitates informed decision-making by presenting scan results in a clear and actionable format. Supporting multiple output formats and detailed reporting features, it empowers users to interpret findings effectively and prioritize remediation efforts accordingly. SCANMASTER also prioritizes user proficiency and confidence by providing comprehensive guidance, explanations of menu options, and best practices.

Ultimately, SCANMASTER strives to be a trusted ally in the fight against cyber threats, continuously evolving to address emerging challenges in the cybersecurity landscape. Through its commitment to excellence and user-centric approach, SCANMASTER aims to contribute to a more secure and resilient digital ecosystem.

VI. SYSTEM REQUIREMENTS

A. *Hardware*

1) *Processor:* A multi-core processor (e.g., Intel Core i5 or equivalent) to handle parallel scanning tasks efficiently.
2) *RAM:* At least 4 GB of RAM to ensure smooth performance during scans and data processing.
3) *Storage:* A minimum of 20 GB of available storage space for the tool and its associated data.
4) *Network Adapter:* A standard network interface card (NIC) to facilitate network communication.
5) *Display:* A monitor with a resolution of 1024x768 or higher for the graphical user interface (if applicable).

B. *Operating System*

Kali Linux, Windows

C. *Network Requirements*

Internet Connectivity: While not always required, internet connectivity can be essential for downloading updates, vulnerability databases, or additional data for the tool. These are general minimum system requirements, and they can be adjusted based on the specific features and capabilities of your network scanning tool. Keep in mind that more complex and resource-intensive tools may require higher system specifications to function optimally. Additionally, users may appreciate the capability to run the tool on systems with better hardware for improved performance and speed.

VII. RESULTS

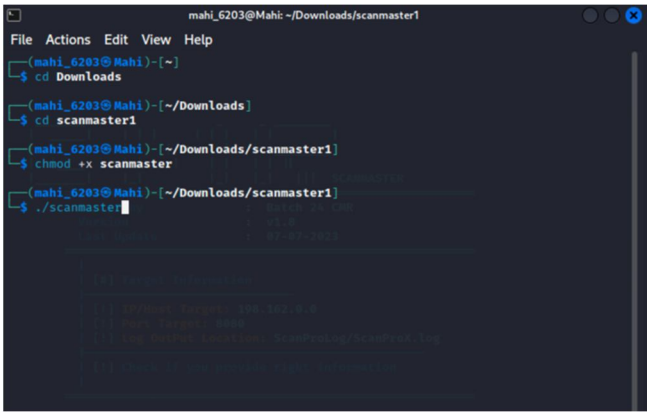


Fig:2 Locating the path

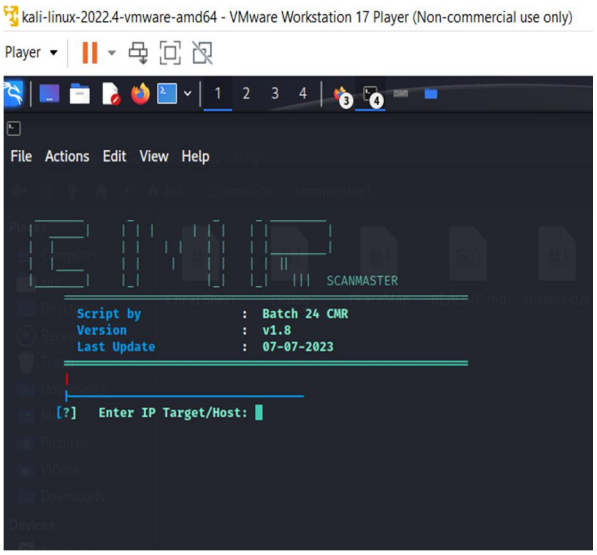


Fig:3 Enter IP

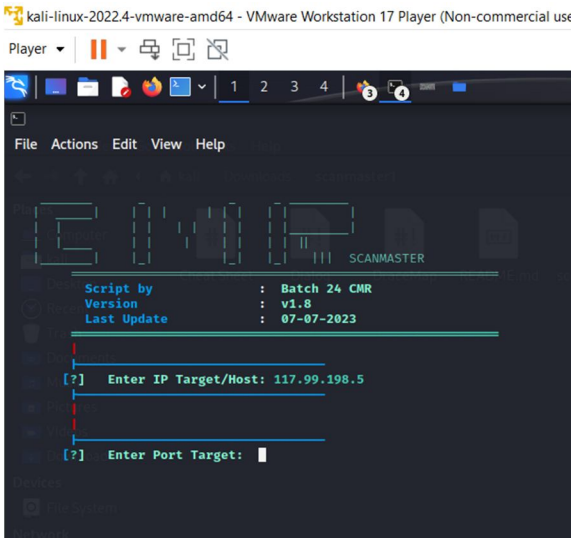


Fig:4 Enter Port Target

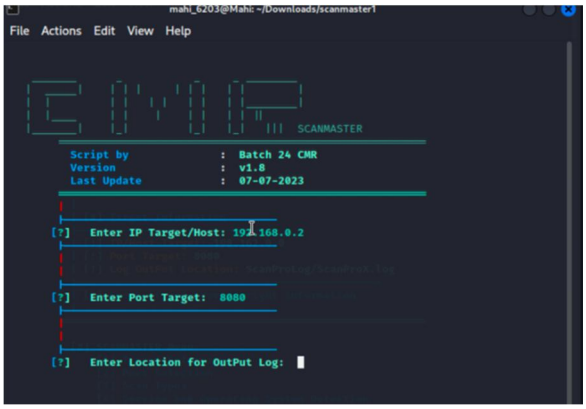


Fig:5 Main Page Of SCANMASTER

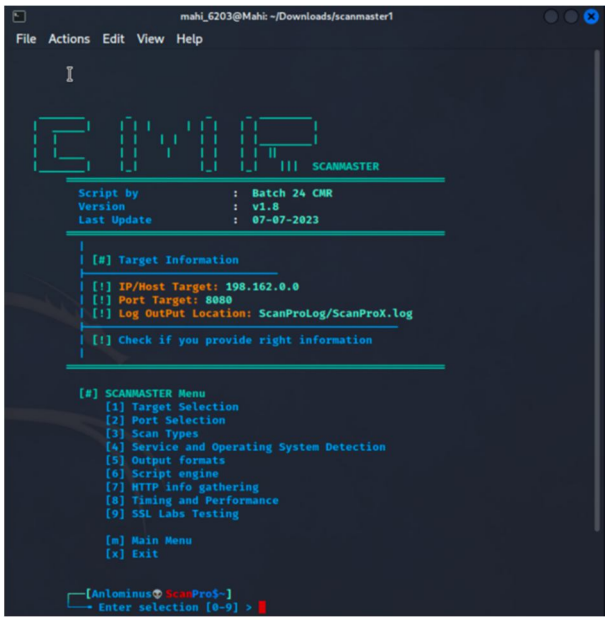


Fig:6 Menu of SCANMASTER

VIII. CONCLUSION

In conclusion, SCANMASTER emerges as a robust and versatile network scanning tool designed to bolster cybersecurity measures effectively. With its array of features, SCANMASTER empowers users to conduct thorough vulnerability assessments, enabling proactive identification and mitigation of potential security risks within network infrastructures.

By offering flexible target selection options, SCANMASTER caters to various network configurations, allowing users to tailor scans to their specific needs. The tool's ability to scan an extensive variety of ports and support different scan types ensures comprehensive coverage and accuracy in identifying potential vulnerabilities.

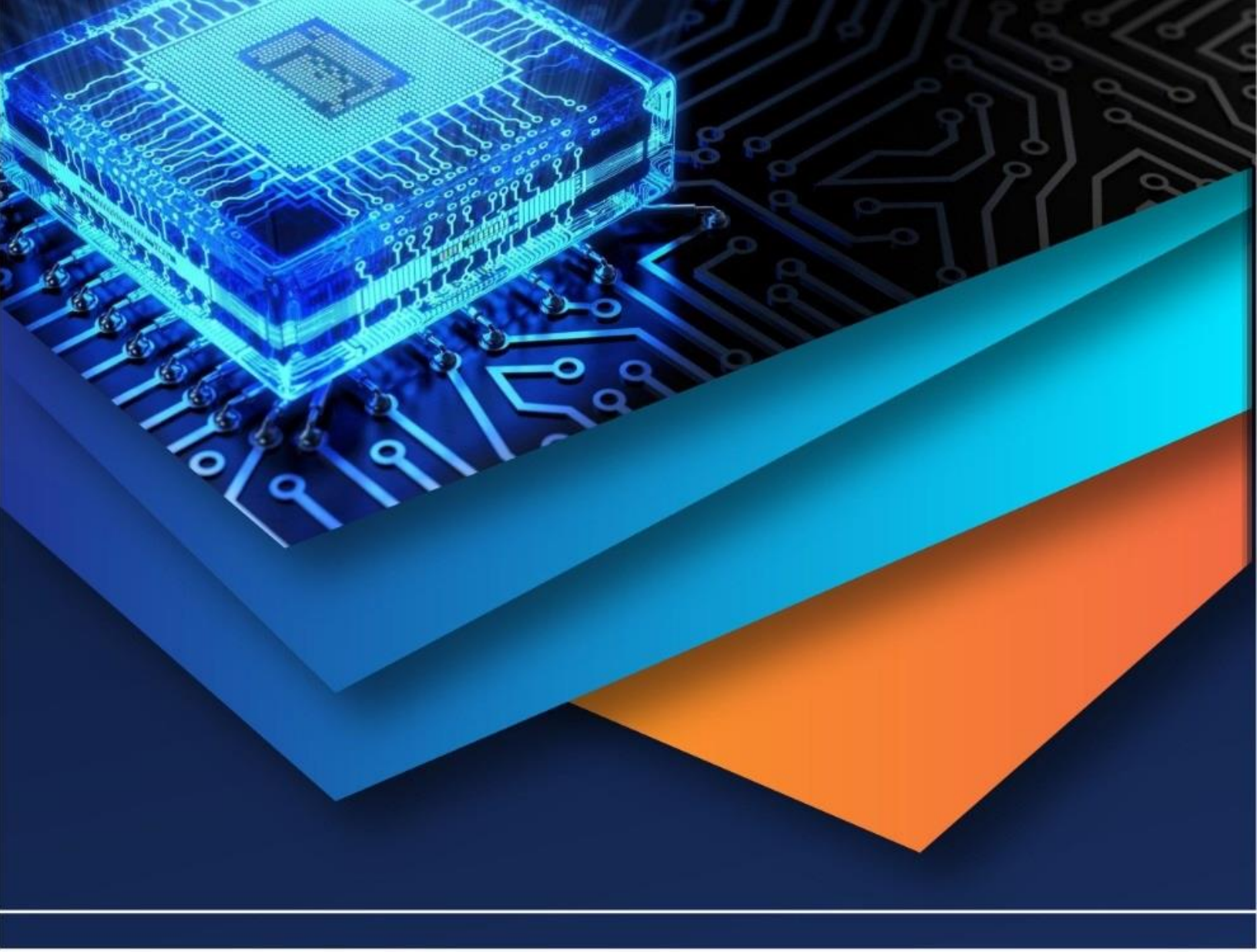
Furthermore, SCANMASTER's support for service and operating system detection, coupled with its integration of Nmap Scripting Engine (NSE) scripts, enhances its capability for in-depth analysis and vulnerability detection. The tool's diverse output formats facilitate effortless integration with the current analysis workflows, facilitating efficient post-scan analysis and reporting.

Additionally, SCANMASTER's features for HTTP service information gathering and customizable timing and performance settings further enrich its functionality, making it an asset for network security professionals.

Overall, SCANMASTER stands out as a reliable and user-friendly solution for network security assessment, equipping users with the necessary tools to safeguard their network infrastructure against evolving cyber threats. Its comprehensive feature set, coupled with its intuitive interface, makes it an asset in the arsenal of cybersecurity professionals striving to maintain the integrity and resilience of their networks.

REFERENCES

[1] Zahoor Ahmed Soomro, Mahmood Hussain Shah, Javed Ahmed (https://www.researchgate.net/publication/284810509_Information_security_management_needs_more_holistic_approach_A_literature_review).
[2] Akira Tanaka, Chansu Han, Takeshi Takahashi (https://ieeexplore.ieee.org/document/10054012).
[3] Erik Larsson, Zehang Xiang, Prathamesh Murali (https://ieeexplore.ieee.org/document/9442850)
[4] Rodney R Rohrmann, Vincent J Ercolani, Mark W Patton (https://ieeexplore.ieee.org/document/8004906)
[5] Min Huang, Jingyang Wang, Huiyong Wang (https://ieeexplore.ieee.org/document/5486179)
[6] Saminda Wattuhewa (https://www.researchgate.net/publication/374135016_Network_Scanning_with_Nmap)
[7] J. Asokan, K.R. Aravind Britto, P. Valarmathi, M. Sundar Prakash Balaji, G. Sasi, V. Elamaran (https://ieeexplore.ieee.org/document/10335785)
[8] Andrea Tundis , Wojciech Mazurczyk , Max Mühlhäuser(https://dl.acm.org/doi/abs/10.1145/3230833.3233287)
[9] M. Sprengers, J. van Haaster (https://www.sciencedirect.com/topics/computer-science/network-scanning-tool)
[10] Masscan Project. (https://github.com/robertdavidgraham/masscan)
[11] Wireshark (https://www.wireshark.org/news/20201029.html)
[12] Zabbix - The Enterprise-Class Open Source Network Monitoring Solution. (https://www.zabbix.com/network_monitoring)
[13] Fing - Network Tools. (https://help.fing.com/hc/en-us/sections/7313339689746-Available-tools)
[14] Nmap Host Discovery(https://nmap.org/book/man-host-discovery.html).
[15] Nmap Port Scanning.(https://nmap.org/book/man-port-scanning-basics.html)
[16] Nmap Target Specification (https://nmap.org/book/man-target-specification.html)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY