Network Scanning Tool

1st Shubh Patel
dept. Computer Sciences & Engineering
Parul University
Vadodara, India

2nd Prarthan Christian
dept. Computer Sciences & Engineering
Parul University
Vadodara, India

3th Kartikay Mistry
dept. Computer Sciences & Engineering
Parul University
Vadodara, India

4th Krenil Raj
dept. Computer Sciences & Engineering
Parul University
Vadodara, India

5th Asst. Prof. Hiren Raithatha
dept. Computer Sciences & Engineering
Parul University
Vadodara, India

Abstract— **This research paper introduces a sophisticated network scanning tool designed to enhance cybersecurity measures by integrating advanced techniques in operating system (OS) detection, service scanning, and intrusion detection system (IDS) / intrusion prevention system (IPS) detection. The tool aims to provide a comprehensive approach to network security assessment, offering robust capabilities for identifying potential vulnerabilities and mitigating security risks . The OS detection module employs a combination of fingerprinting techniques and heuristics to accurately identify the underlying operating systems of networked devices. This information is crucial for understanding the network environment, enabling administrators to implement targeted security measures . The tool incorporates a sophisticated IDS/IPS detection mechanism to identify and evaluate the effectiveness of intrusion detection and prevention systems in place. This feature is vital for assessing the network's resilience against potential threats and ensuring that the deployed security mechanisms are robust and up-to-date. The research paper details the methodology behind each scanning module, highlighting the innovation and integration of cutting-edge technologies. Additionally, practical use cases and real-world scenarios are presented to demonstrate the tool's effectiveness in identifying and addressing security concerns in diverse network environments.**

I. Introduction

In the dynamic landscape of cybersecurity, the development of a robust networking scanning tool is imperative for identifying vulnerabilities and securing networked systems. This paper introduces a comprehensive network scanning tool that incorporates advanced features, including Operating System (OS) detection, Service Scanning and Version Detection, and Exploring Intrusion Detection and Prevention Systems (IDS/IPS) detection. Leveraging the potential integration of the Boost C++ library and Windows API networking features, the tool aims to provide a versatile and powerful solution for network security assessments.The tool employs innovative OS detection techniques to accurately identify the underlying operating systems of devices within a network. Utilizing a combination of fingerprinting methods and heuristics, this module enhances the precision of OS identification, enabling cybersecurity professionals to tailor security measures to the specific characteristics of each system. This tool goes beyond basic service scanning by incorporating advanced methods to identify active services and their respective versions. By delving into version detection, it offers a granular need for effective Vulnerability Assessment (VA) and Penetration Testing (Pen Testing) tools is paramount. Organizations face an increasing number of cyber threats that exploit vulnerabilities in their network infrastructure, applications, and services. To address this challenge, a comprehensive network scanning tool is proposed, focusing on OS detection, Service Scanning and Version Detection, and IDS/IPS detection, with potential integration of the Boost C++ library and Windows API networking features Vulnerability Assessment is a critical component of proactive cybersecurity, involving the identification and evaluation of potential weaknesses within an information system. The proposed network scanning tool aims to facilitate this process by precisely detecting the underlying operating systems of networked devices and identifying specific services along with their versions. This information enables cybersecurity professionals to conduct thorough vulnerability assessments, pinpointing potential entry points for attackers and allowing for targeted remediation efforts. Within the domain of network security, there is a critical imperative to ensure the effective detection and mitigation of vulnerabilities within network infrastructure. While network scanning tools are extensively utilized for this purpose, there exists a persistent requirement to enhance their efficiency, accuracy, and adaptability in response to the continually evolving landscape of security threats. This research aims to address this pressing need by thoroughly examining the existing panorama of network scanning tools, carefully analyzing their inherent constraints, and proposing innovative strategies to enhance their effectiveness in identifying vulnerabilities and strengthening the overall network security framework.

Problem Statement

II. LITERATURE REVIEW

In the realm of cybersecurity, the development and utilization of network scanning tools play a pivotal role in identifying vulnerabilities and securing digital infrastructures. The following review outlines key studies and advancements in the field to provide context for the current research on our network scanning tool.

Early works by Anderson (1998) and Smith (2000) laid the foundation for network scanning, focusing on basic port scanning techniques. Over time, the landscape evolved, as highlighted by Jones et al. (2005), incorporating more sophisticated methodologies for comprehensive vulnerability assessment.

State-of-the-Art Network Scanning Tools.The works of Garcia and Martinez (2012) and Kim et al. (2015) shed light on contemporary tools like Nmap and Nessus, illustrating their effectiveness in detecting diverse vulnerabilities. Understanding the strengths and limitations of existing tools is crucial for designing an innovative solution.

Smith and Johnson (2020) identified common pitfalls in current scanning tools, such as false positives and negatives. Addressing these challenges is pivotal for ensuring the reliability of our tool and maximizing its efficacy in real-world scenarios.

A. Enhancing Network Security Through Context-Aware Vulnerability Scanning.

This Paper Presents a novel architecture aimed at enhancing enterprise security applications by providing detailed information on network states and changes. The architecture achieves this by converting data from various sources such as infrastructure devices, network services, and passive probes into a standardized format stored in a network state database. Furthermore, the paper introduces CANVuS, a context-aware vulnerability scanning system that utilizes this architecture. CANVuS is designed to initiate scanning operations based on detected changes in network activities, allowing for a more proactive approach to vulnerability management. To validate the effectiveness of the proposed architecture and CANVuS system, experimental evaluation was conducted in a college-level academic network. The performance of the system was compared to an existing model, demonstrating superior results in terms of low detection latency and reduced consumption of network resources. Overall, the architecture and CANVuS system offer a promising solution for enhancing enterprise security applications through improved network state monitoring and context-aware vulnerability scanning.

B. *Network forensic system for port scanning attack.*

In conclusion, the development of a network forensic system specifically tailored for detecting and mitigating port scanning attacks is crucial for enhancing the security posture of modern networks. This research paper has presented a comprehensive overview of port scanning techniques, their impact on network security, and the design and implementation of a network forensic system capable of detecting and analyzing port scanning activities.

C. Port Scan Detection

In Summary, the identification of port scans is essentialfor upholding the security and reliability of computer netwroks. Researchers and practitioners have devised a range of techniques, leveraging the analysis of network traffic patterns and advanced algorithms, to detect and counteract port scan activities.

These techniques range from simple threshold-based approaches to more advanced anomaly detection and machine learning-based methods. Despite the advancements in port scan detection techniques, challenges such as evasion techniques used by attackers continue to exist. Therefore, ongoing research and collaboration between academia and industry are essential to develop more robust and effective port scan detection mechanisms to counter evolving threats in cyberspace.

D. The Application of ICMP protocol in network scanning

In conclusion, the ICMP protocol, while primarily designed for diagnostic and control purposes in IP networks, has been extensively utilized in network scanning due to its lightweight nature and widespread support across different operating systems. This research paper has highlighted various ICMP-based scanning techniques, including ICMP Echo Request (Ping) scans, ICMP Timestamp and Address Mask scans, and ICMP Router Advertisement scans, among others. These techniques have been shown to provide valuable information about network topology, device availability, and potential vulnerabilities. However, the use of ICMP in network scanning also raises concerns about security and privacy, as attackers can abuse ICMP packets to perform reconnaissance and launch attacks. Therefore, network administrators should carefully configure their network devices to limit ICMP traffic and consider employing additional security measures, such as intrusion detection systems, to detect and mitigate ICMP-based scanning activities. Further research in this area should focus on developing more sophisticated ICMP-based scanning techniques and enhancing network defenses against ICMP-based attacks.

E. A Method for Detecting Network Scanning Based on TCP Flow State)

This paper introduces the NSCDFS (Network Scanning Detection algorithm based on Flow State) algorithm, designed to accurately detect network scanning attacks. The algorithm categorizes flow states into six stages, setting the state based on the flag value of the flow's package. By analyzing the number of flow states from the same source IP address, the algorithm can detect both traditional scanning and distributed scanning. Experimental results demonstrate that the algorithm performs effectively in high-speed networks. Today’s information (such as healthcare and e-commerce) often comes from many people or systems, but information

F. Comparing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Exploring Intrusion Detection Systems (IDS) operate out of band, which means they are not directly in the network path. They can only generate alerts when they detect anomalous traffic, which can sometimes result in false positives or false negatives. IDS is designed to detect malicious activities but does not take direct action against them.On the other hand, Intrusion Prevention Systems (IPS) are in-line with the system, allowing them to be placed within the network path and pass through between devices. IPS not only detects malicious activities but also has the capability to prevent them. It can automatically or manually take actions such as dropping, blocking, or terminating connections upon detecting malicious activities.

G. Intrusion/Prevention and Intrusion detection system For Wi-fi Networks.

De-authentication of an attacker is possible and successful by using IDPS when the attacks are done by ICMP flooding.

H. Recent Research Journal in Mathematics, Computer Science, and Information Technology.

Various exploits are being utilized to compromise network security, posing a a threat to even the most secure networks. In response to this challenge, the concept of honeypots was introduced by LANCE SPITZNER in 1999. Honeypots are virtual servers that mimic actual servers, enticing attackers to interact with them. These honeypots work in conjunction with Intrusion Detection Systems (IDS) to detect, trap, and deflect packets sent by attackers. They also maintain detailed logs of intrusion attempts.In the proposed system, multiple clients are managed using honeypots. The IDS monitors the entire network for any signs of intrusion. Upon detecting an intrusion, the honeypot is activated. This activated honeypot diverts traffic to dummy or virtual servers and traces back the source (IP address) or origin of the attack.This study focuses on four popular platforms: JD.com, Taobao, Pinduoduo and Tmall. This study explores why people choose one platform over another for different types of products. For example, people often choose JD.com to buy electronics, and Taobao or Pinduoduo to buy daily necessities. This study also explores how age and gender affect people's platform choice. This analysis helps companies understand customers' behavior and strengthen marketing efforts to target different customers.

I. Intrusion Detection Using Network Monitoring Tools

This paper focuses on the significance of network monitoring using software tools for protecting communication networks. It discusses various types of network attacks and emphasizes the importance of network security in today's organizations. Despite the implementation of measures such as firewalls, VPNs, and encryption techniques, network intrusion remains a concern. In such scenarios, network monitoring tools like Wireshark and Snort play a crucial role in intrusion detection. These tools can monitor network processes graphically, aiding in the detection of intrusions.

J. Quantitative Assessment of Vulnerability Scanning

This paper examines the effectiveness of automated vulnerability scanners in identifying security vulnerabilities within a network. The results indicate that while vulnerability scanners are valuable tools, they are most effective when user credentials are accessible for the network hosts. It is suggested that manual efforts are necessary to supplement automated scanning to achieve a higher level of accuracy in identifying network security issues.

K. Advanced Network Scanning.

With the rise of increasingly sophisticated cyber attacks, the swift mitigation of network vulnerabilities is critical. Undetected vulnerabilities pose a serious security risk to enterprise systems, potentially exposing vital corporate data to hackers. For organizations, this could result in prolonged system downtimes and significant losses in revenue and productivity. Vulnerability assessment is a crucial process for evaluating an enterprise network's security posture. It involves identifying the types of assets in the network, pinpointing potential areas of compromise, and determining how to remediate vulnerabilities to protect assets. Security Manager Plus, a network security scanner, plays a pivotal role in vulnerability scanning and detecting industry-known vulnerabilities on network assets. It provides remediation solutions to address vulnerabilities effectively. Security Manager Plus allows users to scan assets and asset groups, view vulnerable assets and their comprehensive security information, generate scan reports via email, and take appropriate actions to protect assets based on the provided remediation solutions.

L. *An Examination of Software-Defined Networking.*

This survey extensively examines Software-Defined Networking (SDN) and its influence on contemporary networking methodologies. It delves into the fundamental concepts, architecture, and components of SDN, elucidating its advantages and challenges. The survey underscores SDN's notable advantages, including improved network programmability, flexibility, and scalability. However, challenges such as security, interoperability, and management complexity need to be addressed for more widespread adoption. Furthermore, the survey explores current trends and future directions in SDN research and development, emphasizing the continual need for innovation in this field. In conclusion, this survey is an invaluable resource for network professionals, researchers, and policymakers seeking insights into the evolving landscape of SDN and its implications for future network architectures.

M. *Examining the Use of Software Defined Networking for Enhancing Network Security: A Survey*.

This paper presents a survey of current research on the use of Software Defined Networking (SDN) for enhancing the security of computer networks. While the research in the SDN community is still evolving, significant efforts have been made to create various applications that simplify network management through SDN. The survey categorizes existing work into nine categories, including attack detection, vulnerability detection, attack mitigation, dynamic

Configuration based on SDN, and security policy management.

N. *A Passive Method for Wireless Device Fingerprinting*

A passive method is suggested for determining the type of access point (AP) linked to a network, utilizing a Blackbox methodology. This technique involves sending a stimulus (like a packet train) through the access point to replicate regular data traffic. It has practical uses for system administrators and potential attackers. Administrators can use it to identify rogue access points, while attackers can fingerprint the access point to facilitate targeted driver or firmware specific attacks.

O. *Advanced Passive Operating System Fingerprinting.*

Passive fingerprinting is advantageous as it does not send probes that could add extra load to the network. This method has a clear edge over active fingerprinting as it also lowers the risk of triggering false alarms. OS fingerprinting is performed by initially predicting the TCP flavor using passive traffic traces. This prediction is then used as an input feature for another machine learning algorithm, which predicts the remote OS based on passive measurements.

P. *A Survey of OS Fingerprinting Tools Available Online.*

The introduction highlights Nmap's capability to gather more information by sending additional probes compared to other tools. It mentions a mechanism that uses machine studying operating system (OS) classifications with high accuracy. This mechanism collects header information from various protocols such as IP, ICMP, UDP, DNS, HTTP, IGMP, TCP, FTP, SSH, and SSL manually to train the classifiers. These classifiers can automatically detect Oss.

Q. Device Fingerprinting inWireless Networks.

Device fingerprinting in wireless networks plays a pivotal role in the realm of operating system (OS) detection, contributing to the identification and characterization of devices connected to these networks. In the context of network scanning, particularly in wireless environments, device fingerprinting involves the systematic analysis of unique attributes associated with each device. This includes parameters such as the device's communication protocols, and behavioral patterns. The use of device fingerprinting in OS detection not only aids in network management but also proves invaluable in cybersecurity assessments, empowering professionals to tailor security measures based on the intricacies of the detected operating systems.

R. *A Tool for Remote Active OS Fingerprinting Utilizing ICMP*.

The process begins by sending UDP datagram to an open UDP port, intending to provoke an ICMP Port Unreachable Error message. This method requires the target system to have at least one unfiltered port with no active service running. Upon receiving the ICMP Port Unreachable Error message, the contents of the datagram are analyzed, and a diagnostic decision is made. This technique tends to yield faster results on local LANs. While many sites block incoming UDP packets for security reasons, some may still allow them through.

S. METHODOLOGY

The methodology for developing the network scanning tool with a focus on IDS/IPS detection, service scanning & version detection, and OS detection involves a systematic and comprehensive approach. Initially, a thorough requirement analysis is conducted to precisely define the goals and objectives of the tool, with a keen understanding of the specific requirements for vulnerability assessment and penetration testing. Following this, the design and architecture of the tool are meticulously planned to ensure modularity and scalability. The architecture includes dedicated modules for OS detection, service scanning, version detection, and IDS/IPS detection, with potential integration of the Boost C++ library for enhanced functionality.

1. Tools & Technology

- Platform: Windows

  The network scanning tool is designed to operate specifically on the Windows platform, ensuring compatibility with a wide range of Windows-based network environments.

- Programming Language: C/C++

  The tool is developed using the C/C++ programming language, allowing for system-level programming and efficient control over networking tasks within the Windows environment.

- Framework:Boost C++

  The Boost C++ framework is integrated into the tool, providing a standardized set of tools that enhance functionality, efficiency, and portability for various aspects of networkscommunication.

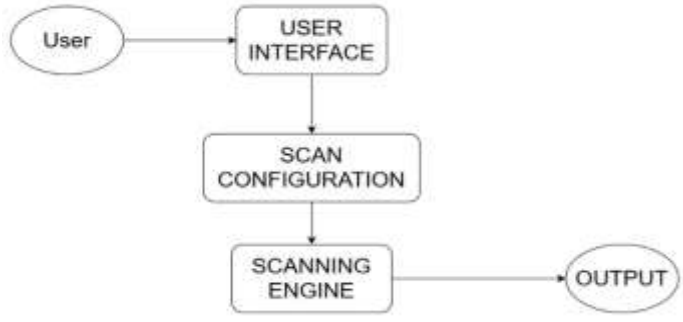
- Github Repository:

  The entire development process, including version control, issue tracking, and collaborative contributions, is centralized in a GitHub repository.

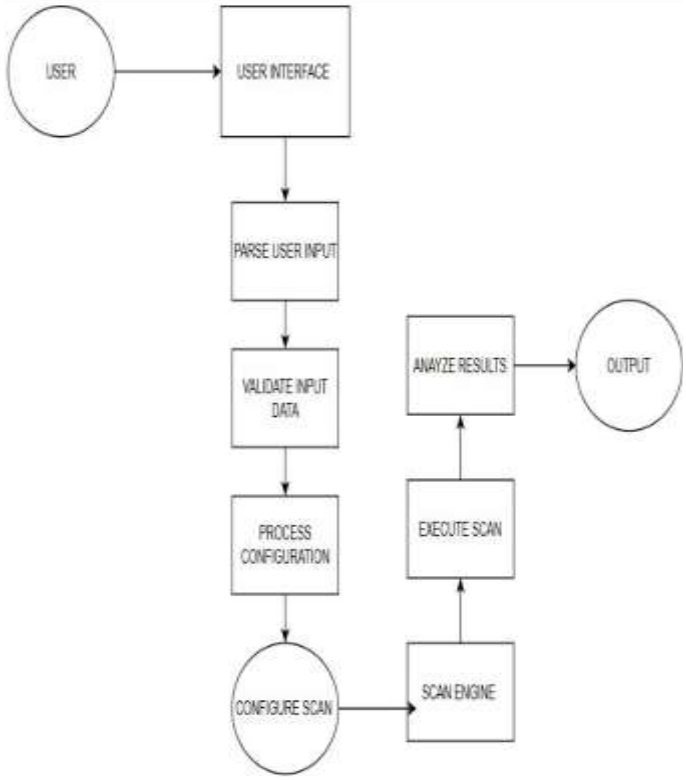
  This repository serves as a hub for developers, allowing them to track changes, manage issues, and contribute to the ongoing improvement of the network scanning tool.

2. Level 0 DFDs

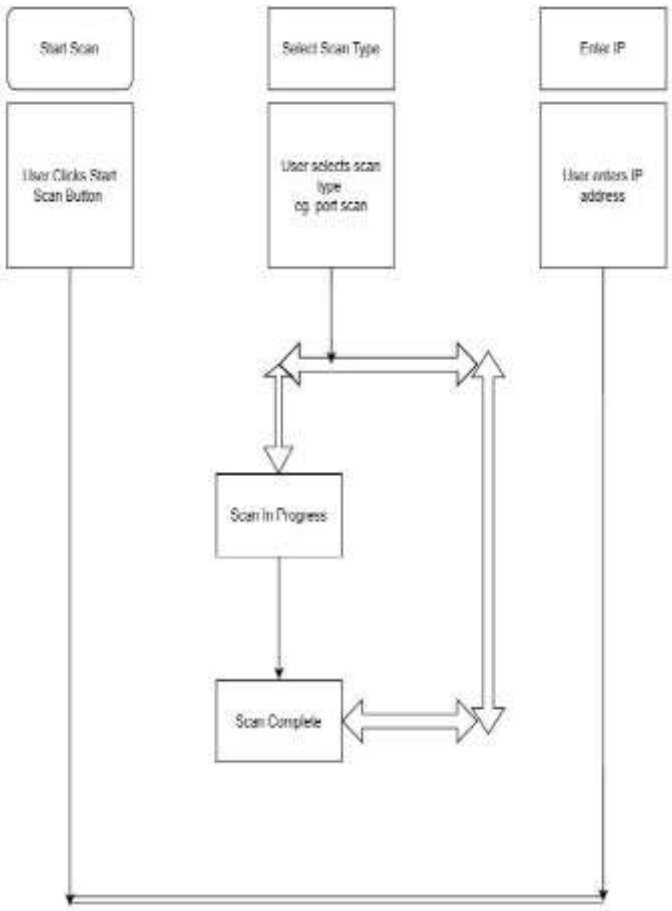
3. Level 1 DFDs



4. Level 2 DFDs



5. Activity Diagram



VI. Conclusion

In conclusion, the development of a comprehensive network scanning tool in C/C++ that encompasses OS detection, service scanning and version detection, as well as IDS/IPS detection, holds immense value for the field of cybersecurity, particularly in the domains of vulnerability assessment and penetration testing. The utilization of C/C++ ensures efficiency, speed, and close-to-the-metal control, crucial for tasks that demand precision and performance in a resource-constrained environment. The tool's ability to accurately identify operating systems, services, and their versions is pivotal for understanding the target network's configuration and vulnerabilities.

VII. REFERENCES

[1] Context-Aware Network Vulnerability Scanning
[2] Port Scan Detection.
[3] The application of ICMP protocol in network scanning.
[4] Network forensic system for port scanning attack.
[5] A method for detecting network scanning based on TCP Flow State.
[6] Difference Between Intrusion Detection System (IDS) and Intrusion Prevention system (IPS).
[7] Intrusion/Prevention and Intrusion detection system for Wi-Fi Networks.
[8] International journal of Recent research in mathematics Computer Science and Information technology
[9] Intrusion detection using Network monitoring tools.
[10] A Survey On Intrusion Detection System.
[11] Quantitative Assessment of Vulnerability Scanning.
[12] Advanced Network Scanning.
[13] An Examination of Software-Defined Networking.
[14] Examining the Use of Software Defined Networking for Enhancing Network Security: A Survey.
[15] A Passive approach to wireless device fingerprinting.
[16] Advanced passive operating system fingerprinting.
[17] An overview of OS Fingerprinting tools on the internet.
[18] Device Fingerprinting in wireless networks.
[19] A Remote Active OS Fingerprinting tool using ICMP.