JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

"Comprehensive Network Security and Monitoring Tool"

Dr. Prakasha S, Abdul Razak, Dheeraj S, Gayithri L M, Janardhan S
Department of Information Science
RNS Institute of Technology, Bengaluru

Abstract: Network security remains one of the most critical aspects of modern digital infrastructure, given the ever-increasing sophistication of cyber threats. This survey focuses on three key pillars of network security: packet sniffing, network scanning, and automated firewall management. By consolidating insights from multiple research papers and aligning them with practical implementations, the survey explores current trends, methodologies, and challenges in these domains. Moreover, this work seeks to provide a basis for creating a unified solution to enhance network security comprehensively. It underlines the importance of adopting innovative approaches and integrated strategies to address the ever-evolving landscape of cybersecurity threats.

I. INTRODUCTION

In today's interconnected world, networks form the backbone of almost every sector, from healthcare and finance to entertainment and education. This growing dependence on digital infrastructure has made networks a prime target for attackers. Cybersecurity threats, including malware, phishing, denial-of-service attacks, and unauthorized access, have grown exponentially in sophistication.

Traditional security mechanisms often operate in silos, addressing specific vulnerabilities without considering the broader network environment. For instance, packet sniffing tools focus on capturing and analysing traffic, while network scanners probe for vulnerabilities. Firewalls, on the other hand, enforce access control but lack real-time threat detection capabilities. The fragmented nature of these tools highlights the need for an integrated solution that combines their strengths.

This survey aims to address the following questions:

[1] What are the limitations of existing packet sniffing, network scanning, and firewall management solutions?

[2] In what ways can progress in these domains be merged to design a comprehensive network security solution?

[3] Which emerging trends are expected to influence the evolution of unified network security frameworks?

II. LITERATURE SURVEY

[A] Packet Sniffing Techniques

Packet sniffing is a crucial component of network security, allowing administrators to observe and analyse traffic as it occurs. It involves intercepting packets as they travel across a network, providing visibility into potential threats such as unauthorized data transfers or malware communications.

Key Studies:

[1] Unity is Strength: Improving Wi-Fi Passive Measurements Through Sniffer Redundancy introduces the concept of using redundant sniffers to enhance packet capture accuracy, particularly in high-traffic or noisy environments.

[2] Network Monitoring: By using Packet Sniffing methods compares the performance of popular sniffing tools like Wireshark and Tcpdump, emphasizing their utility in identifying anomalies.

Limitations:

- Missing of packet during prime hours can lead to incomplete data analysis.
- Encryption renders many packets unreadable, limiting the effectiveness of sniffing in secure networks.
- Packet sniffers are passive tools and cannot act to prevent threats in real time.

B. Network Scanning and Detection

Network scanning is useful in identifying vulnerabilities, rogue devices, and open ports. It provides a proactive measure to reduce any sort of danger by mapping network resources and identifying weak points before they are exploited.

Key Studies:

[1] Detecting Network Scanning Through Monitoring and Manipulation of DNS Traffic presents an innovative approach to detecting stealthy scans by analysing DNS query behaviours.

[2] Improving Network Clarity and Safety with Improved Port Scanning Methods integrates dynamic and idle scanning methods, leveraging programmable hardware for enhanced performance.

Advanced Techniques:

- Active Scanning: Involves sending probes like SYN or ACK packets to elicit responses from network devices, revealing open ports and services.

- Passive Scanning: Monitors traffic without sending probes, making it stealthier but less comprehensive.
- Hybrid Approaches: Combine active and passive methods for a balanced trade-off between visibility and subtlety.

Challenges:

- Traditional scanning tools are often slow and resource-intensive.
- Sometimes gives out incorrect read, leading to unnecessary alerts and wasted resources.
- Stealthy scans, such as those using slow probing rates, are difficult to detect with conventional methods.

C. Automated Firewall Management

Firewalls are a critical component of any network security strategy, providing a barrier between trusted and untrusted networks. However, manual configuration of firewalls can be error-prone and time-consuming, particularly in complex network environments.

Key Studies:

[1] Automated Firewall Configuration in Virtual Networks explores rule-based automation to improve accuracy and scalability.

[2] Research on Computer Network Security Based on Firewall Technology highlights the importance of centralized management for distributed networks.

Benefits of Automation:

- Reduces the likelihood of misconfigurations, which are a leading cause of security breaches.
- Adapts dynamically to changing network conditions, such as the addition of new devices or services.
- Improves scalability, making it feasible to manage large, complex networks.

III. OBJECTIVES

1. To evaluate existing packet sniffing technologies for their effectiveness in real-time threat detection.
2. To analyze the capabilities of advanced network scanning techniques in identifying vulnerabilities.
3. To assess the role of automation in enhancing firewall management efficiency.
4. To design an integrated tool that combines these functionalities into a seamless, user-friendly system.

IV. PROPOSED SYSTEM

The proposed system combines the strengths of packet sniffing, network scanning, and automated firewalls into a single framework.

A. Packet Sniffing

- Deploy multiple sniffers in a redundant configuration to minimize packet loss.
- Use advanced filters to capture only relevant traffic, reducing overhead.

B. Network Scanning

- Employ DNS-based scanning techniques to detect stealthy intrusions.
- Integrate active scans for comprehensive vulnerability assessments.

C. Firewall Automation

- Develop algorithms to automate rule creation and deployment based on detected threats.
- Implement a centralized dashboard for monitoring and controlling firewall activity.

Integration

- A unified interface will provide administrators with real-time insights into network activity, alerts for potential threats, and tools for immediate response.

V. ADVANTAGES OF PROPOSED SYSTEM

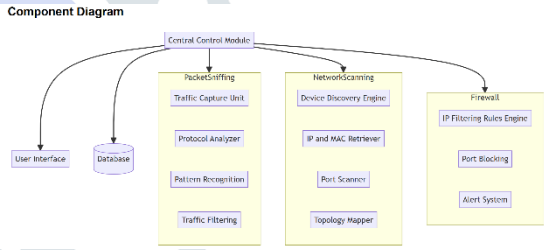
- Comprehensive Security: Integrates three critical components into a cohesive system.
- Scalability: Adapts to networks of varying sizes and complexities.
- Efficiency: Reduces manual effort and minimizes human error.
- User-Friendly Interface: Provides clear, actionable insights for non-expert users.

VI. PROPOSED METHODOLOGY

While the proposed system addresses current challenges, future work could explore:

- **AI Integration**: Using machine learning to predict and prevent potential threats.
- **Cloud Compatibility**: Extending functionalities to cloud-based networks.
- **Performance Optimization**: Enhancing the speed and accuracy of detection mechanisms.

VII. SYSTEM ARCHITECTURE



VIII. CONCLUSION

This survey highlights the critical role of packet sniffing, network scanning, and firewall automation in modern network security. By integrating these technologies into a single framework, the proposed system offers a robust solution to address today's cybersecurity challenges. Future developments will focus on refining the system and evaluating its performance in real-world scenarios

IX. REFERENCES

[1] Unity is Strength: Improving Wi-Fi Passive Measurements Through Sniffer Redundancy, Ad Hoc Networks.

[2] Ethical Approaches to Network Monitoring Using Packet Sniffing Tools, IEEE Access.

[3] Detecting Network Scanning Through Monitoring and Manipulation of DNS Traffic, IEEE Access.

[4] Increasing Network Clarity and Safety with Modern Port Examine Techniques, Sensors.

[5] Automated Firewall Configuration in Virtual Networks, IEEE Transactions on Dependable and Secure Computing.

[6] Research on Computer Network Security Based on Firewall Technology, Journal of Physics: Conference Series.