Developing a Comprehensive Network Traffic Monitoring System: Approaches, Challenges, and Solutions

CS 4991 Capstone Report, 2024

Caleb Stoltz
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
cjs2pz@virginia.edu

ABSTRACT

The increase of cyberattacks poses a significant threat to the integrity of network infrastructure, requiring robust monitoring and alert systems. To resolve this issue, I proposed a basic network traffic monitoring and alert system designed to capture, analyze, and identify potentially malicious activity within network data. This project implementation includes sniffing tools and data analysis algorithms to examine network traffic for patterns indicating malicious intent. The proposal also includes a web-based interface for real-time data visualization and alerts. Anticipated results include an implemented system capable of efficiently flagging suspicious activities, offering a base to build upon. For future research, a system with an expanded algorithm to be scalable to larger network bases in critical infrastructure.

1. INTRODUCTION

In the current digital landscape, the security of personal data and networks has become paramount due to increasingly sophisticated cyberattacks. Such threats not only endanger sensitive information but also the functionality of essential services within the sectors of critical infrastructure. This project, conceived under the guidance of my mentor, who is a veteran consultant with extensive expertise in software development and cybersecurity, aims to address this presenting issue by proposing a network traffic monitoring and alert system.

The project covers essential aspects such as system design, programming across diverse languages, data management, full-stack development, risk assessment, intrusion detection, and security testing. This endeavor not only contributes to the construction of cybersecurity frameworks, but also marks a significant step in my immersion into the field of digital security.

2. RELATED WORKS

Before starting, I needed context and the history of current platforms that excel in network monitoring and alert systems. I found the open-source monitoring system proposed by Nagios. Kocjan & Beltowski (2016) state: “Nagios is an open-source tool for system monitoring. It…watches servers and other devices on your network and makes sure that they are working properly. Nagios constantly checks if other machines are working properly. It also verifies that various services on those machines are working properly. In addition, Nagios can accept information from other processes or machines regarding their status; for example, a web server can send information to Nagios if it is overloaded.”

With its robust system monitoring capabilities, Nagios provides a valuable foundation for the network traffic monitoring envisioned for the proposed project. One benefit of using Nagios in my project is the inclusion of an extensive plugin ecosystem that is provided, allowing a customizable range of network parameters and devices to be added. This not only eliminates many complications of connecting devices and parameters to a server but also promotes scalability, which is crucial for the evolving landscape of network threats.

In addition to Nagios' extensive monitoring system, the addition of a strong network protocol analyzer to add to Nagios was needed. Wireshark is the top of the line in relation to network protocol analysis, providing intricate and detailed tools for packet sniffing. In a previous internship, I was able to monitor the intricacies of Wireshark in an active monitoring environment and was impressed by the amount of detail it was able to provide.

Bock (2022) speaks on the different packet analyzers developed over the last twenty years, stating that Wireshark is solely a "packet sniffer used to analyze network traffic." Wireshark was the packet analysis tool to use for my project because of its portability with Nagios. The ability to trigger Wireshark tools in customizable Nagios alerts provides in-depth packet analysis, only when necessary.

3. SYSTEM DESIGN

This section reviews the details of the proposed network traffic monitoring and alert system, including its general operation, along with challenges and potential solutions.

3.1 Overview of System Architecture

The proposed system is designed as a comprehensive solution that uses both Nagios and Wireshark to provide detailed monitoring and web traffic analysis.

3.1.1 Data Capture

The system creates a local web server on a separate machine to run the Nagios monitoring system, while Wireshark attaches itself to the network itself. Nagios uses custom plugins to capture data while Wireshark uses network sniffers in combination to capture all inbound and outbound traffic.

3.1.2 Analysis and Monitoring

Nagios first retrieves the captured data packets and searches for performance issues or network anomalies. The initial analysis stage is for catching macro-level patterns that might lead to performance issues, potential security risks or misconfigurations.

3.1.3 Detailed Packet Analysis

When any detection system by Nagios is triggered, all packets of the issue are filtered to Wireshark, which then analyzes the frame, addresses, communication ports, and the data being transmitted. With this information, the software can determine whether the data packet is malicious or could cause issues

3.1.4 Alerts and Visualization

If a potential security threat is identified during the Wireshark analysis, the system can generate an alert. Alerts can be programmed in multiple ways including color coordination, visuals, etc. A web-based interface can display live data and alerts to the system admin through a dashboard from Wireshark.

3.2 Requirements

The system requirements for the proposed network trafficking and monitoring system were to be designed to meet high standards of performance and security. It is necessary that the system be able to handle larger volumes of network traffic at an efficient rate without compromising security. The combination of Nagios' large scale network monitoring and Wireshark's intricate detailed packet analysis creates a comprehensive system.

3.3 Challenges

During the development of the proposal, one of the projected primary challenges was managing immense amounts of data. The problem with using Nagios is that it is directly influenced by the performance of the server on which it is hosted. This means the scalability of data is completely dependent on the processor of the machine hosting the server. With a more substantial server, Nagios and Wireshark would both be able to filter for data per second and reduce latency issues within alert and visual generation.

Another challenge with the proposed system is the complexity of the system integration. Nagios and Wireshark use two different frameworks, which can cause problems, including tool communication, alert triggering between the two systems, and efficiency issues.

Configuration of the system and the ability to retrieve all genuine threats is a significant challenge. Improper configuration of the two software could lead to accuracy issues within detection, causing false positives and undetected threats.

4. ANTICIPATED RESULTS

The proposed network traffic monitoring system, designed to enhance cybersecurity measures by scanning and flagging malicious activity, is expected to deliver significant improvements in efficiency and security management. Using two different monitoring environments with precise configurations, the system integration would increase detection accuracy significantly. A developed interface to visualize and monitor packet sniffing would be implemented to improve the efficiency of the IT staff by decreasing their manual monitoring efforts and human error. Reductions in cost and time devoted to cybersecurity could be spent in other, more productive areas of a business.

5. CONCLUSION

This project proposes a comprehensive network traffic monitoring system designed to enhance cybersecurity measures through the integration of Nagios and Wireshark. The fusion of these tools, while challenging, provides a robust solution capable of detailed monitoring and analysis of potential threats. The network traffic monitoring system I propose recognizes the importance of innovative technology to address critical challenges in cybersecurity today, providing more of a general understanding of the topic and its shortcomings. This offers a scalable, efficient and effective solution aligned to make significant contributions to a business looking for a safer future.

The proposed project has offered me a significant professional development opportunity by enhancing my understanding of network security and system integration. The advice and feedback from my mentor also provided an invaluable experience and aided in my data analysis and software engineering skills. Ultimately, creating this proposal and partial implementation in my mentorship provided invaluable experience in versing through the realms of software engineering and cybersecurity. Equipping myself with the skills and insights required to immerse myself in the evolving landscape of digital threats will only benefit my career.

6. FUTURE WORK

The proposed network traffic monitoring and alert system, while complete in its design, can offer numerous avenues for future development and expansion. The first step of development would be to fully implement the proposed design using Nagios and Wireshark, testing it through a network.

A problem brought to attention by my mentor was that, due to their differing frameworks, the two systems will have serious difficulty working together as designed without precise configuration An important future enhancement would be to fully develop a singular framework that has the modularity of Nagios and the capabilities of Wireshark, able to easily work together in unison with specific configuration.

Finally, to broaden the currently proposed system, different iterations could explore specific industry adaptations like healthcare and finance where data is sensitive and require more security. This direction could not only enhance system utility but also increase its relevance for different sectors of business.

REFERENCES

Kocjan, W., & Beltowski, P. (2016). 1. In *Learning Nagios* (3rd ed.). essay, Packt Publishing.

Bock, L. (2022). 1. In *Learn Wireshark* (2nd ed.). essay, Packt Publishing.