IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"NETWORK ANALYZER"

DR. S.M. PATIL
Department of Computer Engineering
SKNSITS, Lonavala

Ganesh Gudewar
Department of Computer Engineering,
SKN Sinhgad Institute Of Technology and Science,
Lonavala, India

Rushikesh Ingale
Department of Computer Engineering,
SKN Sinhgad Institute Of Technology and Science,
Lonavala, India

Dhananjay Korde
Department of Computer Engineering,
SKN Sinhgad Institute Of Technology and Science,
Lonavala, India

Shivam Koli
Department of Computer Engineering,
SKN Sinhgad Institute Of Technology and Science,
Lonavala, India

Abstract: In the ever-expanding realm of modern technology, the stability and efficiency of communication networks have become vital to our daily lives, the continuity of businesses, and the functioning of entire industries. To meet the growing demands of network management and optimization, the Network Analyzer Project emerges as a pioneering endeavour. This project envisions the development of a comprehensive system tailored to empower network professionals and administrators in their mission to monitor, analyze, and enhance network performance.

The Network Analyzer Project is committed to the creation of that components include data collection and log capture mechanisms, robust data storage and management systems, visualization tools, real-time network monitoring capabilities, and an array of troubleshooting and diagnostic utilities.

Keywords :- Computer Network, Network Analyzer, Port Scanning, IP Blocking, Packet sniffing, Network Troubleshooting

I. INTRODUCTION

In an ever-evolving technological landscape, this project stands at the nexus of innovation, with its core objectives encompassing both hardware and software components. These include cutting-edge data collection, storage and management systems, real-time network monitoring, and an array of diagnostic utilities.

In addition to its monitoring and analysis capabilities, the Network Analyzer Project offers insight into the active network system. Users can access vital information such as system name, version, and active ports, ensuring a comprehensive view of the network's current state.

The Network Analyzer Project represents a pivotal step in the evolution of network management, aiming to enhance network reliability, security, and performance. As we embark on this journey, we anticipate a future where network administrators possess the tools they need to ensure the seamless operation of our interconnected world.

II. OBJECTIVES

Create an intuitive user interface for Network Monitoring and Analysis, featuring a user-friendly dashboard with interactive visuals, customizable widgets, and easy navigation. The interface provides a

quick overview of network performance, logs, and security alerts while allowing in-depth data analysis.

Establish real-time network monitoring with continuous data collection, processing, and dynamic reporting, including historical trend analysis for long-term network optimization.

Strengthen network security analysis by integrating an IP blocklist feature to proactively identify and list malicious IP addresses that could threaten system integrity and data security.

Provide essential diagnostic tools for network administrators and engineers, including a traceroute for network mapping and a ping utility for the device reachability checks.

Improve data management by enabling seamless export of network log data in CSV and TXT formats for analysis and reporting, along with support for data import to facilitate historical analysis.

III. LITERATURE SURVEY

The development of application software and technology changes gradually. In order to meet the

customers' specific requirements and ensure the robustness and efficiency of the application software, various functions are packaged as a whole. Network Analyzer Tool provides the ideal blend of conceptual instruction and work to give administrators and users a quick start in monitoring network systems using the operating system. [1]

Networking concepts and theories mainly deal with the server and client sides, Network Analyzer provides effective network monitoring systems. Designing and maintenance of a fully functioning network monitoring system that is less expensive. This allows users to monitor networks and allows a person to see the traffic.[3]

With the rise of Internet usage, network attacks have become more frequent, and Distributed Denial of Service (DDoS) attacks make up a big fraction of these attacks. Consequently, multiple studies have been conducted to model attacks and enhance network security.[4]

The authors in [9] for example, are able to process streaming data and provide intuitive analysis to facilitate the detection of attacks in real-time. However, these methods of visualization remain inefficient (not scalable) when the amount of data is large. [9]

Packet sniffing is a process that is used to intercept and log traffic passing over a network.[11] We can use JPcap and Winpcap to capture these packets from the network. We use the Python network packet capture method to collect all packets.[11]

IV. SYSTEM OVERVIEW AND DESIGN

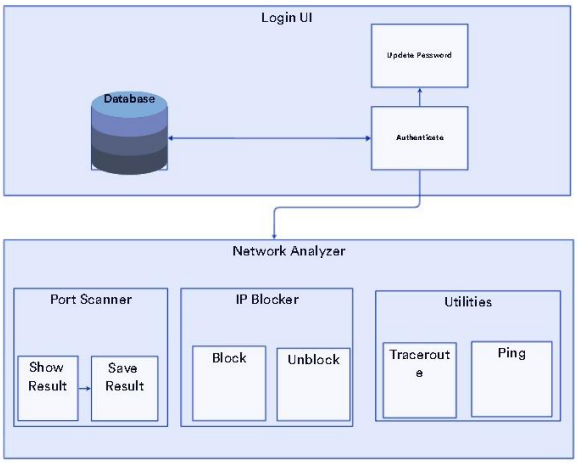

Figure 1 : Architecture Diagram

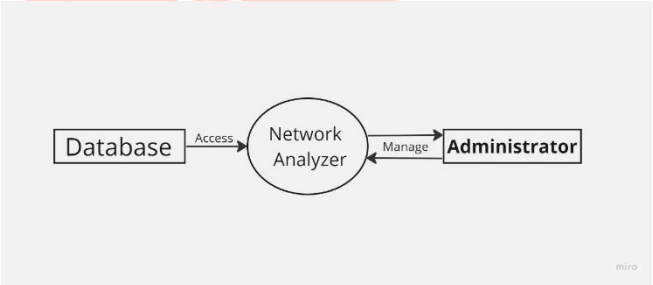

Figure 2 : DFD LEVEL 0

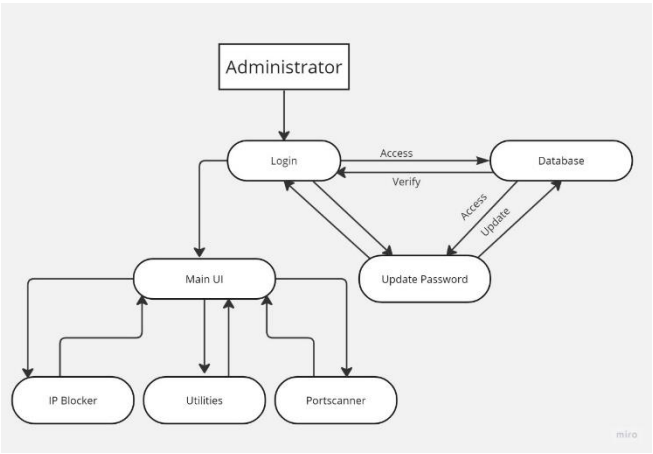

Figure 3 : DFD LEVEL 1

V. METHODOLOGY

1. USER AUTHENTICATION AND AUTHORIZATION SYSTEM:

Design and implement a secure user authentication system, including role-based access control, to ensure authorized access to the application. Reference: Implemented user authentication and authorization mechanisms based on best practices.

2. INTERFACE SELECTION AND DATA COLLECTION:

Develop a module allowing users to select specific network interfaces for monitoring. Implement mechanisms to collect and store network data, including DNS, application, and NetFlow logs. Reference: Utilized established data collection protocols for DNS, application, and NetFlow logs.

3. DATA PROCESSING AND ANALYSIS:

Design algorithms and methods for processing collected data, filtering based on various criteria, and performing real-time analysis. Integrate tools for diagnosing network issues using traceroute, ping, and packet capture functionalities. Reference: Developed algorithms for real-time data analysis using principles from network traffic analysis literature.

4. USER INTERFACE DEVELOPMENT:

Create an intuitive user interface, presenting real-time monitoring data, diagnostic tools, and network analytics in a user-friendly manner. Include customizable dashboards and visualizations to enhance data representation. Reference: Designed the user interface following principles of user-centred design.

5. SECURITY ENHANCEMENT AND THREAT ANALYSIS:

Create an intuitive user interface, presenting real-time monitoring data, diagnostic tools, and network analytics in a user-friendly manner. Include customizable dashboards and visualizations to enhance data representation. Reference: Designed the user interface following principles of user-centred design.

6. EXPORT/IMPORT AND REPORTING:

Develop an efficient export/import module supporting data formats such as CSV and TXT to facilitate data sharing and historical analysis. Incorporate reporting features that generate detailed reports on network performance and traffic.

VI. APPLICATION RESULT

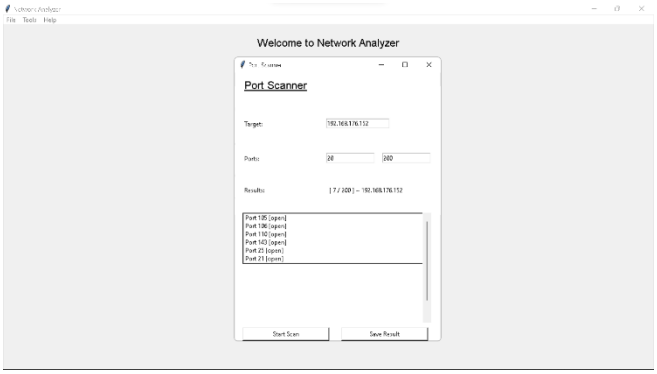

Figure 4 : Port Scanner

A port scanner looks through your whole IP address block for active hosts inside the given IP address range.

These ports serve as communication channels between the host and other network devices. This program then searches ports to see whether services are running on them and to detect open ports.

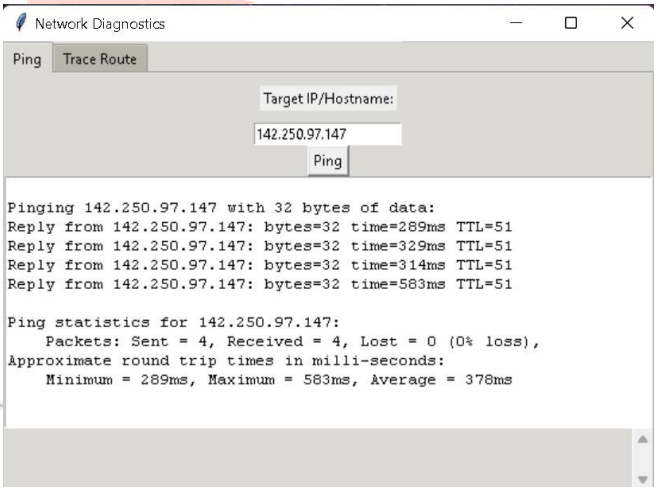

Figure 5 : Ping

Ping is a word used in internet speed test results to determine how quickly a data signal goes from one network device to another. It is critical to determining how long it takes for a packet of data to go from your device to a server and then back to your device.

Ping is an excellent tool for checking network connectivity by delivering data packets and monitoring response time. It is used to diagnose network difficulties by determining whether a device can communicate with another device on the local network or the internet.

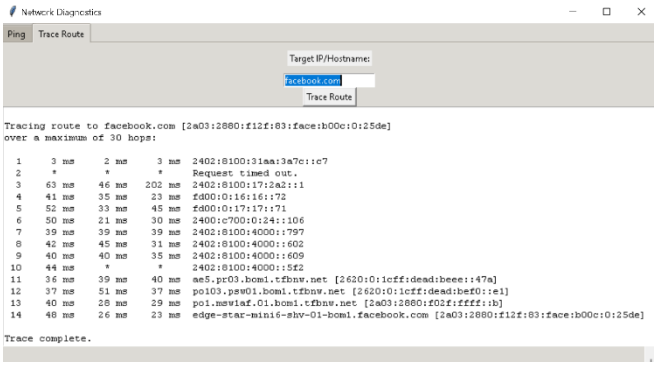

Figure 6 : Traceroute

Get the whole path taken by a packet to reach its destination. Learn the names and identities of the routers and devices in the path. Determine how long it takes to send and receive data from each device in the path.

Traceroute traces the route of your information packets. So, you can see the whole journey that your data packets follow to get to their destination. The devices (hosts) that were used along the travel of your information packets will also be included in the tracing findings.

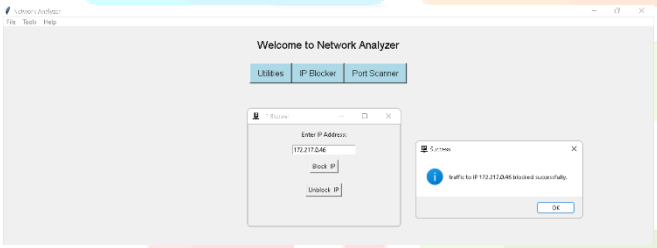

Figure7 : IP Blocker

An IP blocker feature is designed to prevent specific IP addresses from communicating with or accessing certain resources on a network.

It is a security feature that allows network administrators to control and restrict access to their network based on the source IP addresses of incoming traffic.

VII. CONCLUSION

Concluding Phase 1 of the Network Analyzer Project, we have achieved significant progress in establishing the groundwork for a comprehensive network analysis tool. Our team has effectively concluded the initial planning and design stages, thereby defining a clear direction for the forthcoming phases of the project. We have delineated the project's scope, identified key objectives, and laid the foundation for the project as a whole.

Throughout this phase, we conducted a thorough assessment of the project's feasibility and technical requirements, ensuring a robust grasp of the challenges and opportunities that lie ahead. The outstanding collaboration and communication within our team have fostered a shared sense of purpose and unity as we move forward.

VIII. FUTURE ENHANCEMENT

In summary, the successful completion of Phase 1 paves the way for the subsequent phases of the Network Analyzer Project. With a well-defined roadmap, a motivated team, and a comprehensive understanding of the project's scope, we are well prepared to advance to Phase 2.

Here, we will initiate further development and testing, bringing us one step closer to delivering a network analysis tool that fulfils the needs of our users.

IX. REFERENCES

1] SPACES-2015, Dept of ECE, K L UNIVERSITY 402 Performance Analysis of Network Monitoring Tool through Automated Software Engineering Approach. https://ieeexplore.ieee.org/document/7058294

2] Department of Computer Engineering, Florida Institute of Technology, FL, USA: Network Security Traffic Analysis Platform - Design and Validation. https://ieeexplore.ieee.org/document/10017862

8] https://www.cisco.com/c/en/us/products/security/what-is-network-traffic-analysis.html#~related-topics.

3] Research Gate April 2013, By Authors: Abdullahi S.B Mohammed University Sains Malaysia. https://www.researchgate.net/publication/327530819_Network_Traffic_Analysis_A_Case_Study_of_ABU_Network

4] Portable network analyser -ScholarWorks@UARK https://scholarworks.uark.edu/cgi/viewcontent.cgi?article=1004&context=csceuht

5]GEPRIS https://gepris.dfg.de/gepris/projekt/421687036?language=en

6] Machine learning techniques for network analysis; New Jersey Institute of Technology, https://digitalcommons.njit.edu/cgi/viewcontent.cgi?article=2647&context=dissertations29

7] Batfish - An open-source network configuration analysis tool, By Batfish https://juliopdx.com/2021/10/31/building-a-network-ci/cd-pipeline-part-4/

9] Network Packet Analyzer | Profile image of Joseph Brian M KasoziJoseph Brian M Kasozi. https://www.academia.edu/4007454/Network_Packet_Analyzer

10]_ https://www.elprocus.com/network-analyzer/

11] Portable network analyser by T. Warren. https://www.semanticscholar.org/paper/Portable-network_analyzer_Warren/720e4d1f606e4e688fb6ac1bf6127996d1298f16

12]Event_focused_network_analysis: https://www.tandfonline.com/doi/full/10.1080/14494035.2020.1716559