NETWORK INTRUSTION DETECTION SYSTEM

ABSTRACT

With the rapid expansion of computer networks and internet-based applications, effective monitoring and analysis of network traffic have become essential for ensuring network performance, reliability, and security. A Network Protocol Analyzer is a vital tool used to capture, inspect, and analyze network packets to understand communication patterns and detect potential issues or malicious activities.

This project focuses on the design and development of a Network Protocol Analyzer that captures real-time network traffic and analyzes various network protocols such as TCP, UDP, ICMP, HTTP, and FTP. The system examines packet-level details including source and destination IP addresses, port numbers, packet size, protocol type, and timestamps. By analyzing these parameters, the tool provides insights into network behavior, bandwidth usage, and protocol distribution.

The proposed analyzer is developed using Python and leverages packet capturing libraries to monitor live network traffic. The system presents analyzed data through a user-friendly interface, enabling users to visualize network activity, identify suspicious packets, and troubleshoot network performance issues. Key features include protocol filtering, traffic statistics, and packet logging for further analysis.

This Network Protocol Analyzer assists network administrators and security professionals in diagnosing network problems, improving performance, and enhancing security by enabling early detection of abnormal or unauthorized network activities. The project demonstrates the practical application of network monitoring techniques and serves as an effective learning platform for understanding network protocols and traffic analysis.

MODULES

1. Packet Capture Module

- Capture live network packets
- Support for TCP, UDP, ICMP, HTTP, FTP, etc.
- Interface selection for monitoring

2. Packet Filtering Module

- Filter packets based on protocol type
- Filter by source/destination IP and port
- Reduce unnecessary traffic data

3. Packet Analysis Module

- Analyze packet headers and payload
- Extract protocol-specific information
- Identify packet size, flags, and timestamps

4. Protocol Classification Module

- Classify packets by protocol
- Display protocol distribution
- Identify protocol usage patterns

5. Traffic Statistics Module

- Calculate bandwidth usage
- Monitor packet counts and flow rates
- Generate network performance metrics

6. Visualization Module

- Display real-time network traffic
- Graphs for protocol and bandwidth analysis
- Tabular packet details

7. Alert & Detection Module

- Detect abnormal or suspicious traffic
- Generate alerts for unusual patterns
- Support basic intrusion indicators

8. Logging & Reporting Module

- Store captured packet data
- Generate analysis reports
- Export logs for future investigation

9. User Interface Module

- Interactive dashboard
- Real-time packet monitoring
- Easy navigation and filtering options