Project Title:

Design and Evaluation of an Integrated Intrusion Detection and Firewall System Using C++

Research Motivation

Modern cybersecurity systems require both:

- Detection → Identify malicious behavior (IDS)
- Prevention → Block malicious traffic (Firewall)

Many security architectures combine these two components to form a layered defense strategy.

This project implements a simplified Integrated Network Defense System (INDS) that:

1. Detects DDoS attacks
2. Detects Port Scanning behavior
3. Automatically blocks malicious IPs
4. Logs security events
5. Evaluates system performance

This demonstrates core principles of real-world network defense architectures.

Objectives

1. Design and implement a packet abstraction using object-oriented C++.
2. Implement an Intrusion Detection System (IDS) to detect DDoS and Port Scanning behavior using threshold-based analysis.
3. Implement a Firewall Engine to block malicious IPs and restricted ports.
4. Log all security events to a persistent file.
5. Simulate network traffic and evaluate detection and prevention effectiveness.
6. Provide a research-oriented framework that can be extended for real-world applications.

System Architecture

The system is composed of:

1. **Packet Class** → Represents each network packet with IP and Port.
2. **IDS Engine** → Analyzes traffic for DDoS and Port Scan attacks using thresholds.
3. **Firewall Engine** → Blocks malicious traffic based on IDS alerts and predefined rules.
4. **Logging Module** → Stores alerts in security_log.txt.
5. **Evaluation Module** → Summarizes allowed vs blocked packets.

Methodology

1. **Packet Simulation:**
   Traffic is simulated using objects of Packet class.

2. **Threshold-based IDS Analysis:**
    - DDoS Detection: IP sending >5 packets triggers alert
    - Port Scan Detection: IP accessing >3 ports triggers alert
3. **Firewall Blocklist:**
    - Malicious IPs detected by IDS are added to firewall blocklist
    - Firewall also blocks predefined restricted ports
4. **Logging:**
    - All blocked packets and alerts are logged in security_log.txt
5. **Evaluation:**
    - The system counts allowed vs blocked packets
    - Performance is summarized in console output

Research Significance

- Demonstrates layered network security design
- Combines detection (IDS) with prevention (Firewall)
- Illustrates threshold-based anomaly detection
- Provides a foundation for future research:
    - Dynamic thresholds
    - Real-time traffic integration
    - AI-assisted threat detection

Tools & Technology

- C++ (Object-Oriented Programming)
- File Handling for logging
- Console-based simulation
- No external libraries (simple, portable, clear for research)

Future Work

- Dynamic rule updates for firewall
- Real-time network packet capture
- Integration with multiple IDS modules
- Multi-threaded processing
- Statistical anomaly detection and AI extension