Introduction

Namespace IDSApp

Classes

IDSCore

Main Intrusion Detection System core engine that coordinates packet capture, processing, rule matching, and alert generation. Provides real-time network traffic analysis and threat detection using signature-based and behavioral analysis techniques.

Key Responsibilities:

- Packet capture from network interfaces or PCAP files
- Multi-threaded packet processing with worker queues
- Rule-based threat detection using enhanced signature engine
- Protocol parsing and analysis (HTTP, DNS, SSH, FTP, etc.)
- Alert generation and security event logging
- Performance monitoring and system statistics collection
- Flow tracking and behavioral analysis
- DDoS and port scan detection
- Resource management and cleanup

PacketCaptureWrapper

Wrapper class for packet capture data that provides structured access to packet information and metadata for efficient processing

PerformanceMonitor

Monitors and reports system performance metrics including packet processing statistics, memory usage, and rule matching performance. Generates periodic performance reports to help identify bottlenecks and optimize system performance.