NETWORK IDS DEFENSE

Securing Your Digital World

What is network Intrusion Detection System

A Network Intrusion Detection System (IDS) monitors network traffic in real time to detect and alert on suspicious or malicious activity

Why Network Security Matters ?

1. Detects malicious activity early
2. Prevents service disruption
3. Protects data from cyber attacks
4. Ensures business continuity

Types of Cyber Threats

1. Port Scanning
2. DDoS Attacks
3. Brute Force Attacks
4. Suspicious IP Activity

Detection Mechanisms

1

Port scans: threshold of 10+ ports per host

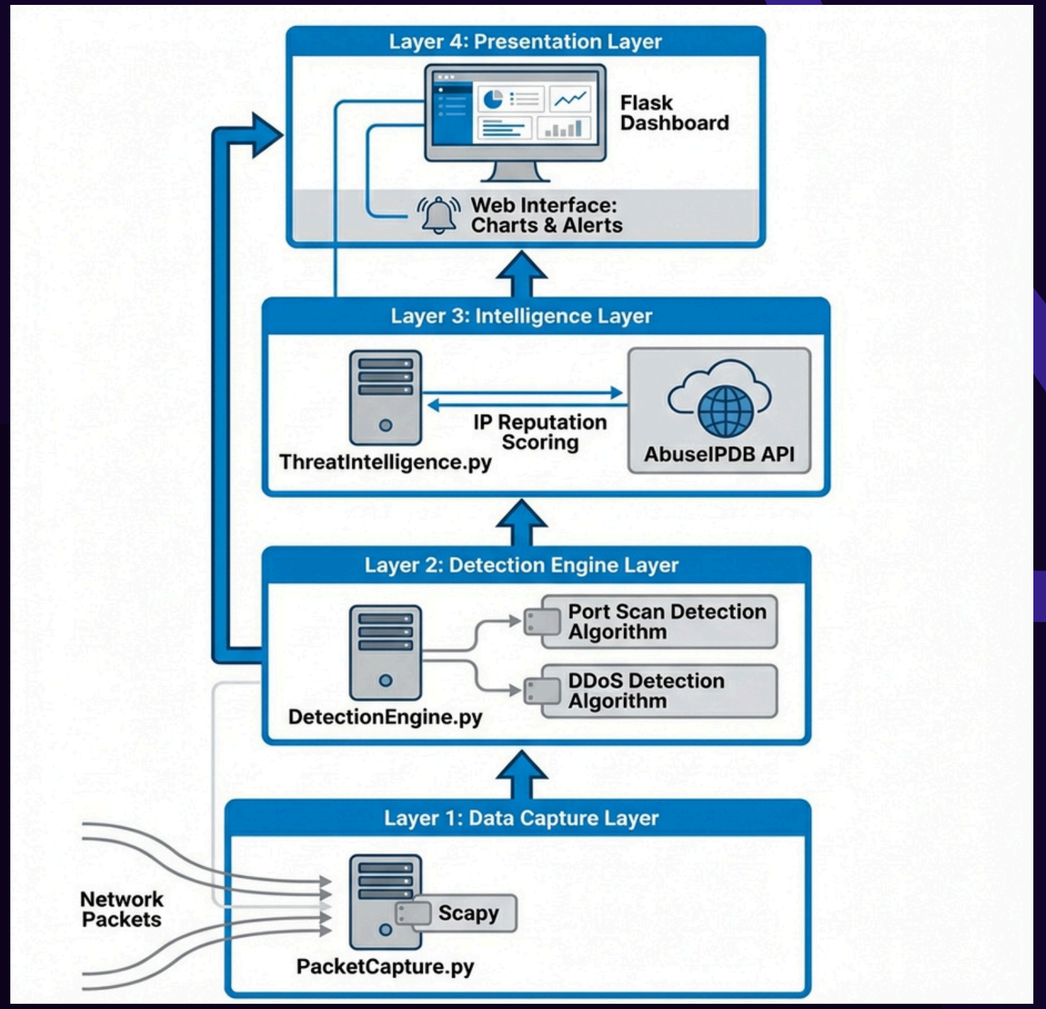
2

DDoS: >100 requests/sec triggers alert

3

Alerts enriched with IP reputation score

System Architecture



Web Dashboard

Total Alerts
100
All time

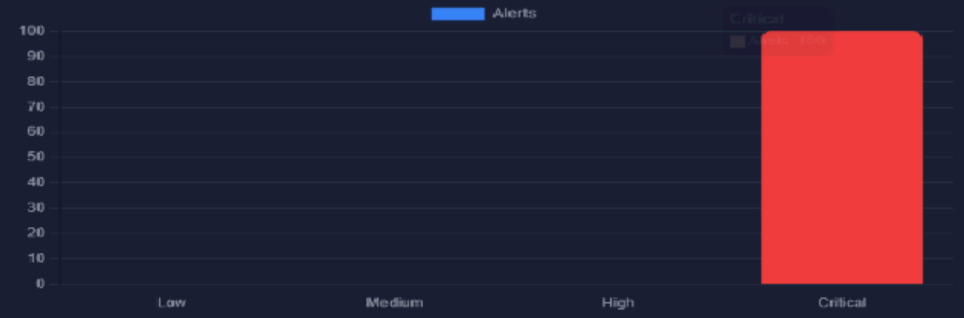
Critical Threats
100
High confidence

System Status
ACTIVE
Monitoring network

Active Rules
2
Port Scan, DDoS

Threat Distribution

Severity Breakdown



FILTERS: Search IP address... All Types Apply Export CSV

Live Threat Feed

TIMESTAMP	SEVERITY	TYPE	SOURCE IP	REPUTATION	TARGET IP	CONFIDENCE
6:36:10 PM 1/4/2026	CRITICAL	DDOS	172.27.252.208	✓ CLEAN	216.239.36.223	90%
6:36:10 PM 1/4/2026	CRITICAL	DDOS	172.27.252.208	✓ CLEAN	216.239.36.223	90%
6:35:30 PM 1/4/2026	CRITICAL	DDOS	172.27.252.208	✓ CLEAN	34.54.84.110	90%
6:35:30 PM 1/4/2026	CRITICAL	DDOS	172.27.252.208	✓ CLEAN	34.54.84.110	90%
6:35:30 PM 1/4/2026	CRITICAL	DDOS	172.27.252.208	✓ CLEAN	34.54.84.110	90%
6:35:30 PM 1/4/2026	CRITICAL	DDOS	172.27.252.208	✓ CLEAN	216.239.36.223	90%

Challenges Overcome

Session management with persistent secret keys

Threshold calibration for accurate detection

Optimizing real-time performance

Key Achievements

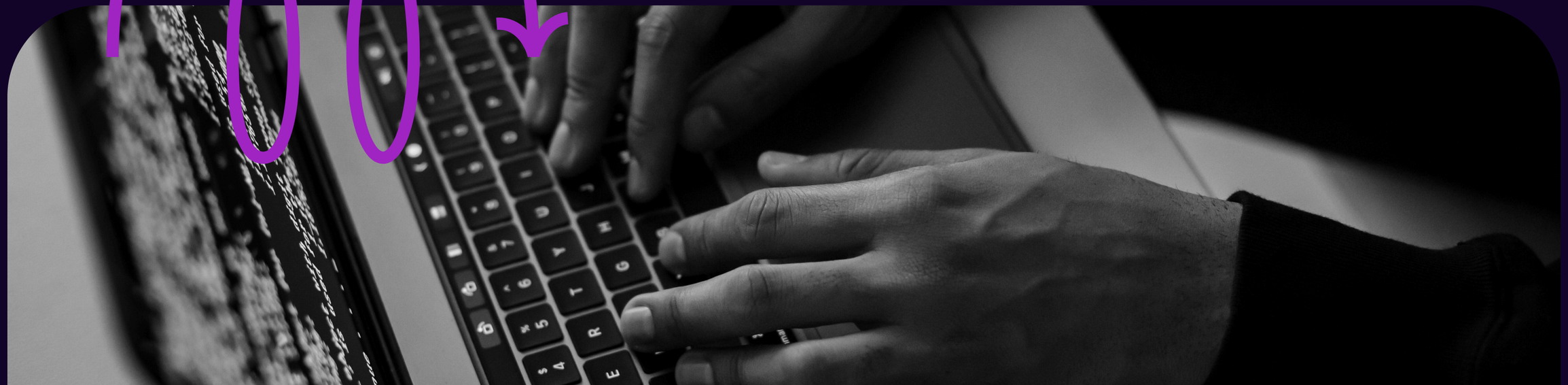
Modular and extensible architecture

Low false positive rate

Production-ready for small/medium networks

Conclusion and Next Steps

- New detection rules (DNS tunneling, SSH brute-force)
- Multi-threaded packet processing for scalability
- Firewall integration for automated response



THANK YOU!