Anomaly-based IDS - Concepts & Background

Concepts & Background: IDS & Anomaly Detection

1 Basics of Cybersecurity

Cybersecurity protects computers & networks from attacks that can steal or damage data.

2 What is Network Traffic?

All communication over a network (packets, flows) between devices.

3 What are Cyberattacks & Intrusions?

Unauthorized activities like hacking, data theft, malware installation, DoS.

4 What is an IDS?

An IDS is a system that detects intrusions by monitoring and analyzing network or host activity.

5 Types of IDS

Signature-based: Detects known attack patterns

Anomaly-based: Learns normal behavior, flags deviations

6 Why use ML for IDS?

ML can detect novel attacks that dont match known signatures.

7 How does ML-based Anomaly Detection work?

Train ML on normal data test on new data flag high deviations as anomalies.

8 Key ML Algorithms

Isolation Forest: Detects outliers by isolating points

Autoencoder: Neural network learns to reconstruct normal data, high error anomaly

One-Class SVM: Separates normal from abnormal in feature space

9 Features of Network Traffic

Examples:

- Duration of connection
- Protocol type (TCP/UDP/ICMP)
- Number of bytes sent/received
- Flags set (SYN, ACK, etc.)
- Number of failed login attempts

Common Datasets

NSL-KDD: Benchmark dataset, cleaned version of KDD99

CICIDS2017: Large, realistic with modern attack scenarios