IDS_Domain_Overview

Cybersecurity Internship Project

May 15, 2025

1. Introduction to Intrusion Detection Systems (IDS)

An **Intrusion Detection System (IDS)** is a cybersecurity solution that monitors and analyzes network traffic or system behavior to detect suspicious activities or policy violations. The primary goal of an IDS is to *detect cyberattacks* such as unauthorized access, misuse, or compromise of computer systems and networks.

There are two primary types of IDS based on their detection mechanisms: **Signature-Based Detection** and **Anomaly-Based Detection**.

2. Types of IDS Detection Techniques

2.1. Signature-Based Detection

Working Principle: Compares observed activities against a database of known attack signatures or patterns.

Advantages:

- High accuracy for known threats
- Low false positive rate

Disadvantages:

- Cannot detect unknown or zero-day attacks
- Requires constant updates of signature databases

Example: Detecting a specific malware file hash or known SQL injection pattern.

2.2. Anomaly-Based Detection

Working Principle: Establishes a baseline of ”normal” network behavior, then flags deviations as potential threats.

Advantages:

- Capable of detecting new and unknown attacks
- Suitable for dynamic environments

Disadvantages:

- Higher false positive rate
- Requires training and tuning

Example: A user suddenly accessing hundreds of files at midnight when they usually don’t.

3. Common IDS Techniques

Technique	Description
Signature Matching	Pattern matching with known threat signatures
Statistical Analysis	Anomaly detection using statistical thresholds
Machine Learning	Predictive modeling for behavior-based detection
Protocol Analysis	Detects protocol deviations and rule violations

4. Attack Types in the Dataset

Attack Type	Description
DDoS	Overloads network resources using multiple systems
Brute Force (SSH/FTP)	Attempts repeated login using password guessing
Port Scan	Scans network ports to find open vulnerabilities
Botnet Activity	Malicious automated agents performing attacks
Web Attacks	Exploits vulnerabilities in web applications (XSS, SQLi)
Infiltration	Unauthorized internal access via backdoors or malware
Heartbleed	Exploits OpenSSL vulnerability to read system memory

5. Relevance of IDS in Modern Cybersecurity

With the rise of complex and frequent cyberattacks, IDS plays a critical role in:

- Network Security Monitoring
- Incident Response
- Compliance Enforcement
- Threat Intelligence

By integrating machine learning with IDS, it becomes possible to build adaptive systems that can evolve with emerging threats.

6. Conclusion

Understanding the domain of IDS is crucial for building effective and intelligent defense mechanisms. The dataset offers diverse attack scenarios that help in developing ML-based systems capable of high-accuracy threat detection.

— *End of Report* —