Intrusion Detection Systems (IDS) Cheatsheet

A quick reference guide to Intrusion Detection Systems (IDS), covering types, components, detection methods, and response strategies. Ideal for security professionals and system administrators.

IDS Fundamentals

IDS Definition

An Intrusion Detection System (IDS) is a security tool that monitors network or system activities for malicious behavior or policy violations. It identifies potential security breaches and reports them to security personnel.

Types of IDS

Network Intrusion Detection System (NIDS)	Monitors network traffic for suspicious activity. It analyzes packets traversing the network and compares them against a database of known threats.
Host Intrusion Detection System (HIDS)	Runs on individual hosts or endpoints. It monitors system calls, application logs, file system modifications, and other host activities for malicious behavior.
Hybrid IDS	Combines elements of both NIDS and HIDS to provide a more comprehensive security solution.

IDS Components

Sensors: Collect data from network traffic or host systems.
Analysis Engine: Analyzes the collected data for suspicious patterns.
Signature Database: Contains known threat signatures.
Reporting Console: Provides alerts and reports to security personnel.

Detection Methods

Signature-Based Detection

Compares network traffic or system activity against a database of known attack signatures. If a match is found, an alert is triggered. Effective for detecting known threats, but less effective against new or unknown attacks (zero-day exploits).

Anomaly-Based Detection

Establishes a baseline of normal network or system behavior and identifies deviations from this baseline as potential intrusions. Can detect unknown attacks, but may also generate false positives due to legitimate, but unusual, activity.

Stateful Protocol Analysis

Monitors network protocols for deviations from expected behavior. It analyzes the context of network traffic and detects anomalies based on the state of the protocol. Helps identify attacks that exploit protocol vulnerabilities.

Reputation-Based Detection

Uses reputation feeds and threat intelligence to identify malicious IP addresses, domains, and URLs. It blocks or alerts on traffic to or from entities with a poor reputation. Enhances detection accuracy and reduces false positives.

IDS Implementation

Placement Strategies

NIDS Placement	Strategically place NIDS sensors at critical network chokepoints, such as the perimeter, DMZ, and internal network segments, to monitor traffic flow and detect intrusions. Ensure adequate network visibility and coverage.
HIDS Placement	Deploy HIDS agents on critical servers, workstations, and endpoints to monitor local system activity and detect host-based intrusions. Protect sensitive data and prevent lateral movement.

Configuration and Tuning

Properly configure and tune IDS settings to minimize false positives and false negatives. Adjust sensitivity levels, customize rules, and whitelist trusted traffic to optimize detection accuracy.

Log Management

Implement centralized log management to collect, store, and analyze IDS logs. Correlate IDS events with other security logs to gain a comprehensive view of security incidents and improve incident response capabilities.

IDS vs. IPS

Key Differences

Intrusion Detection System (IDS)	Detects malicious activity and alerts administrators, but does not actively prevent or block intrusions. Primarily a monitoring tool.
Intrusion Prevention System (IPS)	Detects and actively prevents or blocks malicious activity in real-time. Can automatically take actions such as dropping malicious packets or terminating connections. An active security control.

Response Strategies

Upon detecting a security incident, follow established incident response procedures to contain, eradicate, and recover from the attack. Investigate the root cause, implement corrective actions, and enhance security measures to prevent future incidents.

Integration with Other Security Tools

Integrate IDS with other security tools, such as firewalls, SIEM systems, and threat intelligence platforms, to enhance security visibility, improve threat detection capabilities, and streamline incident response workflows. Enables a layered security approach.