

Information Security

Prepared by Dr. Ahmed Omar

IT373
Information Security

Lecture 9



Intrusion Detection & Cybercrime

Lecture 9

IT373
Information Security

Prepared by
Dr. Ahmed Omar



Agenda

- ☐ **Intrusion Detection**
- ☐ **Types of Intrusion Detection Systems**
- ☐ **Detection Methodologies**
- ☐ **Understanding Cybercrime**
- ☐ **Categories of Cybercrime**
- ☐ **Best Practices for Organizations**

Intrusion Detection

What is an Intrusion?

- ❑ An intrusion in information security refers to any ***unauthorized access, use, or manipulation*** of computer systems, networks, or data.
- ❑ It represents a **violation** of an organization's security policy and can range from simple unauthorized access to sophisticated, multi-stage attacks.

Intrusion Detection

❑ What is Intrusion Detection?

An Intrusion Detection System (IDS) is a security technology that **monitors network traffic, system activities, and user behaviors** to identify suspicious activities that may indicate **security breaches, policy violations, or malicious attacks**. Unlike preventive security measures, IDS serves as a **detective** control that alerts administrators to potential threats.

Intrusion Detection

Core Functions of IDS

- ❑ **Monitoring:** Continuous observation of network traffic and system events
- ❑ **Analysis:** Processing collected data to identify patterns and anomalies
- ❑ **Detection:** Recognizing potential security incidents based on predefined rules or behavioral analysis
- ❑ **Alerting:** Notifying security personnel of detected threats
- ❑ **Logging:** Maintaining detailed records for forensic analysis and compliance

Intrusion Detection

IDS vs. Other Security Technologies

- ❑ **IDS vs. Firewall:** Firewalls prevent unauthorized access; IDS detects and reports intrusions that may have bypassed preventive measures
- ❑ **IDS vs. IPS:** Intrusion Prevention Systems (IPS) actively block detected threats, while IDS primarily monitors and alerts

Types of Intrusion Detection Systems

Network-Based IDS (NIDS)

❑ Characteristics:

- ✓ **Monitors network traffic in real-time**
- ✓ **Analyzes packets flowing through network segments**
- ✓ **Typically deployed at network perimeters or critical network points**

Types of Intrusion Detection Systems

Network-Based IDS (NIDS)

❑ Advantages:

- ✓ **Can detect attacks targeting multiple hosts**
- ✓ **Difficult for attackers to detect or disable**
- ✓ **Provides network-wide visibility**

Types of Intrusion Detection Systems

Network-Based IDS (NIDS)

❑ Limitations:

- ✓ **Cannot analyze encrypted traffic effectively**
- ✓ **May struggle with high-speed networks**
- ✓ **Limited visibility into host-specific activities**

Types of Intrusion Detection Systems

Host-Based IDS (HIDS)

Characteristics:

- ✓ **Installed on individual systems or servers**
- ✓ **Monitors system calls, file modifications, and user activities**
- ✓ **Analyzes local system logs and events**

Types of Intrusion Detection Systems

Host-Based IDS (HIDS)

Advantages:

- ✓ **Can detect insider threats and local attacks**
- ✓ **Monitors encrypted communications at the host level**
- ✓ **Provides detailed system-specific information**

Types of Intrusion Detection Systems

Host-Based IDS (HIDS)

Limitations:

- ✓ **Requires installation and maintenance on each host**
- ✓ **Consumes system resources**
- ✓ **Limited network visibility**

Types of Intrusion Detection Systems

Hybrid IDS

Combines both **NIDS** and **HIDS** capabilities to provide comprehensive coverage, correlating information from multiple sources for enhanced detection accuracy.

Detection Methodologies

1. Signature-Based Detection



Mechanism:

- Uses predefined patterns or signatures of known attacks
- Matches observed activities against a database of attack signatures
- Similar to antivirus signature detection

Detection Methodologies



1. Signature-Based Detection

☐ Advantages:

- High accuracy for known attacks
- Low false positive rates
- Fast detection and response

☐ Disadvantages:

- Cannot detect zero-day or unknown attacks
- Requires constant signature updates
- Vulnerable to evasion techniques

Detection Methodologies

2. Anomaly-Based Detection

☐ Mechanism:

- Establishes baselines of normal system/network behavior
- Identifies deviations from established baselines
- Uses statistical analysis, machine learning, or behavioral modeling

Detection Methodologies

2. Anomaly-Based Detection

Advantages:

- Can detect previously unknown attacks
- Adapts to changing environments
- Effective against insider threats

Disadvantages:

- Higher false positive rates
- Requires extensive training periods
- May be circumvented by gradual behavioral changes

Detection Methodologies

3. Modern Intrusion Detection

☐ Pattern Recognition

ML algorithms excel at identifying complex patterns in network traffic and system behaviors that would be impossible for humans to detect manually.

☐ Explainable AI (XAI)

Modern IDS integrates XAI to provide transparency in decisionmaking, helping analysts understand why specific alerts were triggered

Detection Methodologies

3. Modern Intrusion Detection

❑ AI/ML in IDS: Benefits

- Higher detection accuracy (85-95%)
- Reduced false positives
- Real-time threat identification
- Ability to detect evolving threats
- Automation of analysis

Detection Methodologies

3. Modern Intrusion Detection

❑ AI/ML in IDS: Challenges

- Model training requirements
- Adversarial attacks against AI
- Data quality dependencies
- Interpretability concerns
- Computational resource demands

Security Information & Event Management (SIEM)

- ❑ SIEM is a cybersecurity solution that combines security information management (**SIM**) and security event management (**SEM**) to provide organizations with a centralized platform to collect, analyze, and respond to security threats in real time.
- ❑ SIEM systems aggregate **log** and **event data** from across an organization's entire IT infrastructure—including endpoints, servers, applications, networks, cloud environments, and security devices such as firewalls , IDS, and antivirus software. This data consolidation allows security teams to detect behavioral anomalies, identify potential threats, and respond swiftly before disruptions occur.

Security Information & Event Management (SIEM)

SIEM Main Functions

- ☐ Collects & analyzes log data from across network
- ☐ Aggregates IDS alerts with other security events
- ☐ Provides correlation between multiple security signals
- ☐ Creates contextual view of security incidents

Security Orchestration, Automation, and Response (SOAR)

- ❑ SOAR is a set of integrated cybersecurity technologies designed to help organizations **collect** security threat data, **automate** response actions, and coordinate workflows across disparate security tools with minimal human intervention.
- ❑ SOAR platforms integrate numerous security tools such as **SIEM, firewalls, endpoint protection, threat intelligence feeds, and vulnerability scanners** into a unified platform to streamline detection, investigation, and response to security incidents

Security Orchestration, Automation, and Response (SOAR)

SOAR Main Functions

- ☐ Automates response to detected threats
- ☐ Orchestrates actions across multiple security tools
- ☐ Reduces response time from hours to minutes/seconds
- ☐ Follows predefined playbooks for consistent response

SIEM & SOAR: Integrating IDS with Incident Response

Benefits of Integration

- ✓ Faster threat response
- ✓ Reduced alert fatigue
- ✓ Improved detection accuracy



Real-World IDS Use Cases

Scenario: A major bank needs to monitor its internal network for suspicious activities and compliance requirements.

Solution:

Deploy a hybrid IDS architecture combining:

- NIDS at network perimeters to monitor external traffic
- HIDS on critical servers (database, application servers)
- Signature-based detection for known financial malware
- Anomaly detection to identify unusual transaction patterns

IDS Architecture and Deployment

Centralized Architecture	Distributed Architecture	Hierarchical Architecture
▪ Single management console controls multiple sensors ▪ Central database stores all events and alerts ▪ Suitable for smaller networks with centralized management	▪ Multiple IDS components operate independently ▪ Local processing and decision-making capabilities ▪ Better scalability for large, geographically distributed networks	▪ Combines centralized and distributed elements ▪ Multi-tier management structure ▪ Regional managers report to central authority

IDS Architecture and Deployment

Deployment Considerations

- **Network Positioning:** Strategic placement for maximum coverage
- **Traffic Mirroring:** Using network taps or switch port mirroring
- **Performance Impact:** Minimizing disruption to network operations
- **Scalability:** Planning for network growth and increased traffic

Understanding Cybercrime

Criminal activities carried out using computers, networks, or digital technologies, violating applicable laws and subject to legal prosecution.

Key Characteristics:

- **Legal Violation:** Breaks specific criminal laws
- **Criminal Intent:** Intent to commit illegal activities
- **Prosecutable:** Subject to law enforcement investigation
- **Jurisdictional:** Falls under specific legal frameworks

Understanding Cybercrime

☐ **Cyber-dependent crimes**

Crimes that can be committed only using computers (e.g., DDoS attacks, malware distribution).

☐ **Cyber-enabled crimes**

Traditional crimes amplified in scale or reach by digital means (e.g., online fraud, intellectual property theft).

Categories of Cybercrime

Crimes Against Individuals

- ❑ **Identity Theft:** Unauthorized use of personal information for fraudulent purposes
- ❑ **Cyberstalking:** Persistent harassment using digital communications
- ❑ **Online Fraud:** Deceptive schemes to obtain money or personal information
- ❑ **Cyberbullying:** Intentional and repeated harm through digital platforms

Categories of Cybercrime

Crimes Against Organizations

- ❑ **Corporate Espionage:** Theft of trade secrets and confidential business information
- ❑ **Data Breaches:** Unauthorized access to sensitive organizational data
- ❑ **Ransomware Attacks:** Encrypting systems and demanding payment for decryption
- ❑ **Financial Fraud:** Manipulating financial systems for illegal gain

Cybercriminal Profiles and Motivations

Script Kiddies

Characteristics:

- Limited technical skills
- Use pre-written tools and scripts
- Often motivated by curiosity or desire for recognition

Typical Activities:

- Website defacements
- Simple denial-of-service attacks
- Social media harassment

Cybercriminal Profiles and Motivations

Script Kiddies

- ❑ **Real Example:** In 2019, a **16-year**-old used readily available DDoS tools to attack his school's network, causing several hours of downtime. The attack was traced through network logs showing the use of a known botnet tool.

Cybercriminal Profiles and Motivations

Organized Criminal Groups

Characteristics:

- ☐ Professional criminals with advanced skills
- ☐ Well-funded and organized operations
- ☐ Profit-driven motivations

Typical Activities:

- ☐ Large-scale financial fraud
- ☐ Ransomware operations
- ☐ Human trafficking facilitation

Cybercriminal Profiles and Motivations

Organized Criminal Groups

Case Study - Carbanak Banking Malware (2013-2015): Perpetrators: Organized criminal group from Russia and Ukraine

Method: Spear-phishing emails, lateral movement, ATM manipulation

Impact: \$1 billion stolen from over 100 banks worldwide

Detection Timeline:

- Initial infection often went undetected for months
- Lateral movement mimicked legitimate admin activities
- Unusual ATM dispensing patterns eventually triggered alerts

Digital Forensics: Fundamentals & Role in Cybercrime

Digital Forensics

Digital forensics is the process of collecting, preserving, and analyzing digital evidence to reconstruct security incidents. This investigation helps identify root causes and gather evidence for legal proceedings.

Role in Prosecution and Attribution

Digital forensics provides crucial evidence for identifying perpetrators, establishing intent, linking suspects to crimes, and supporting legal proceedings in cybercrime cases.

Digital Forensics: Fundamentals & Role in Cybercrime

Key Stages in Digital Forensics:

☐ **Evidence Collection**

Identifying and securing digital devices and data sources while maintaining chain of custody. Includes seizing computers, mobile devices, storage media, and cloud data.

☐ **Preservation**

Creating forensic copies and hashes of digital evidence to prevent alteration. Ensures evidence integrity through write-blockers and documented procedures.

Digital Forensics: Fundamentals & Role in Cybercrime

Key Stages in Digital Forensics:

☐ **Analysis**

Examining evidence using specialized tools to recover deleted files, extract metadata, analyze network traffic, and reconstruct timelines of events.

☐ **Reporting & Presentation**

Documenting findings in detailed reports and presenting evidence in court. Must adhere to legal standards for admissibility and expert testimony.

Best Practices for Organizations

☐ **Strategic IDS Deployment & Tuning**

Place IDS sensors at strategic network points, regularly update signatures, and fine-tune to reduce false positives while maintaining detection capabilities.

☐ **SIEM Integration & Log Management**

Integrate IDS with SIEM solutions for centralized monitoring, implement proper log management, and establish correlation rules for enhanced threat detection

☐ **Develop Incident Response Playbooks**

Create detailed response playbooks for common threats, establish clear roles and responsibilities, and implement the NIST IR framework (Preparation, Detection, Containment, Eradication, Recovery)

☐ **Staff Training & Awareness**

Conduct regular security awareness training for all staff, specialized technical training for security teams, and tabletop exercises to simulate incident scenarios

Summary

- ❑ Intrusion Detection
- ❑ Types of IDS
- ❑ Detection Methodologies
- ❑ Cybercrime



Thank You

