Host and Network-based IDS & SIEM Tools

Outline

- Host-based IDS
  - How does it work
  - Use cases
  - Advantages and disadvantages
- Network-based IDS
  - How does it work
  - Use cases
  - Advantages and disadvantages

Intrusion Detection Systems

- An IDS is a system that monitors network or system activity for malicious activity

- Can be used to detect unauthorized access, misuse of privileges, or attempts to compromise system security

- Its primary purpose is to identify potential security threats or incidents and generate alerts or take automated actions to mitigate them

Host-based IDS

Host-based IDS

- Designed to monitor and analyze the activity on individual computers or hosts within a network
- Focus on identifying signs of malicious or unauthorized activity at the host level

- Monitors system activity
  - File changes
  - Process and system activity
  - Network connections

Host-based IDS

- Can use signature and anomaly detection
- Require the installation of agent software on each host
- Can be used in conjunction with firewalls and antivirus software
- Deployment on several devices such as servers, workstations, laptops

How host-based IDS works

1. **Data collection and normalization**
   - System calls, logs, audit trails, network traffic, file integrity
2. **Anomaly detection**
   - Normal behavior establishment
   - Comparison of real-time activities with the baseline
3. **Signature detection**
   - Comparison of observed behavior against a database of known attack signatures

How host-based IDS works

4. **Alert and logging**
    - Logs of incidents include details of the event, affected host, and user or process involved

5. **Response**
    - By sending real-time alerts, security teams can promptly initiate response actions

6. **Reporting and analysis**
    - Provides analysis tools to assess the scope and impact of security incidents

Use cases for host-based IDS

- **Server protection**
  - *Web servers*: Monitor unexpected changes to web application files, or unauthorized access attempts
  - *Database servers*: Detects changes to the database structure or data

- **Endpoint security**
  - *Workstations*: Detects malware infections, unauthorized software installations, suspicious user behavior, etc.
  - *Point-of-sale systems*: Protects against data breaches, ensuring the confidentiality of customer payment information

Use cases for host-based IDS

- **Virtual environments**
  - Monitor VMs by detecting unauthorized changes, network traffic, or security breaches within the virtualized infrastructure
- **Cloud Security**
  - Security of virtual servers and applications running in a cloud environment, by detecting cloud-specific threats and vulnerabilities
- **Insider threat detection**
  - By monitoring employees' activities against suspicious behavior

Advantages and limitations of HIDS

Advantages

- Deep visibility into host activities
- Local threat detection
- Granular monitoring
- Customizable policies
- Real-time alters
- Forensic capabilities

Limitations and Challenges

- Agent installation
- Agent overhead
- Complexity
- Blind spots
- Log volume
- Limited network visibility

Advantages and limitations of HIDS

Advantages

- Insider threat detection
- Compliance support
- Low false positives
- Integration with SIEM tools

Limitations and Challenges

- Complexity of Threats
- Maintenance overhead
- Privacy concerns
- Cost

Network-based IDS

Network-based IDS

- Designed to monitor and analyze network traffic for signs of malicious activities
- Operates at the network level, providing a broader view of network security

- **Key features**
  - Packet analysis
    - Capture and analyze network packets in real time
  - Protocol analysis
    - Can analyze several network protocols
    - Identifies unauthorized protocol usage and policy violations
  - Traffic Logging
    - Including details such as source and destination IP, ports, timestamps

Network-based IDS

- **Key features**
  - Network traffic visualization
    - Visualization capabilities such as network flow diagrams
  - Scalability
    - Can monitor network traffic in large complex environments

  - Signature and anomaly detection
  - Alerting
  - Integration with other security tools

How network-based IDS works

1. **Traffic capture and data collection**
   - Captures network traffic as it traverses the network and collects data from captured packets, including header information, payload data, and metadata

2. **Anomaly detection**
3. **Signature detection**

4. **Real-time analysis**
   - Continuously analyze network traffic

How network-based IDS works

5. Alert and logging

- Alerts provide details about the detected threats, such as source and destination IP, port, and timestamps
- Logs of incidents include details about network traffic and threat detected

6. Incident response

- By sending real-time alerts, security teams can promptly initiate response actions

7. Scalability

- Can be scaled to handle large volumes of network traffic

Use cases for network-based IDS

- **Network perimeter defense**
  - Commonly deployed at the network perimeter as a first line of defense
  - Monitors incoming and outgoing traffic
- **Malware detection**
  - Can identify patterns and behaviors associated with malware infections in network traffic
- **Internal network monitoring**
  - Detect threats from within the organization (insider threats)

Use cases for network-based IDS

- **Critical infrastructure protection**
  - Detection of network-level attacks on ICS’

- **Multi-site organizations**
  - Provides centralized network security monitoring and threat detection across all sites

- **Cloud security**
  - Can be extended to monitor network traffic in cloud environments, securing the cloud infrastucture

Advantages and disadvantages of NIDS

Advantages

- Real-time monitoring
- Network-wide coverage
- Centralized threat detection
- Signature and anomaly-based detection
- Reduced false positives

Limitations and challenges

- Blind spots in encrypted traffic
- Complex threats
- High network speeds
- False negatives
- Protocol-specific limitations
- Complexity of network traffic

Advantages and disadvantages of NIDS

Advantages

- Scalability
- Automated alerting
- Integration with other security tools

Limitations and challenges

- Privacy concerns
- Maintenance overhead
- Overwhelmed by alerts

SIEM Tools

Security Information and Event Management

- SIEM stands for Security Information and Event Management
- A SIEM is a comprehensive cybersecurity solution that combines the capabilities of Security Information Management (SIM) and Security Event Management (SEM)
- Provides real-time analysis of security alerts generated by various hardware and software infrastructure

Security Information and Event Management

- SIEMs centralize the collection, analysis, and correlation of security data

- SIEM tools provide
  - Threat detection and response
  - Compliance management
  - Visibility and centralization
  - Alert prioritization
  - Incident investigation
  - Automated response

Components of a SIEM tool

- **Log management**
  - Focuses on the collection, storage, and retention of logs and security event data from various sources throughout an organization’s infrastructure
  - The key functions of log management are
    - Data collection
    - Normalization
    - Storage
    - Indexing
    - Data retention policies

Components of a SIEM tool

- **Security Information Management (SIM)**
  - Responsible for aggregating, analyzing, and presenting security-related data
  - Focuses on contextual analysis and provides insights into security events

  - The key functions of security information management are
    - Data analysis
    - Correlation
    - Alerting
    - Reporting
    - Dashboard and visualization

Components of a SIEM tool

- **Security Event Management (SIM)**
  - Focuses on real-time monitoring, immediate threat detection, and automated response to security events and incidents
  - The key functions of security event management are
    - Real-time monitoring
    - Alerting
    - Automated response
    - Integration
    - Incident response

How SIEM tools work

- **Data collection**
  - Collect data from a several sources within an organization’s infrastructure
    - Network devices
    - Security appliances
    - Operating systems
    - Applications
    - Cloud services
- **Normalization**
  - Processing and standardization of data into a common format

How SIEM tools work

- **Secure data storage and retention policies**
  - Storage of log and event data in centralized repositories, often encrypted and protected of unauthorized access
  - Policies to determine how long data should be retained, based on regulatory requirements and compliance standards

- **Analysis and correlation**
  - Analyze data to identify patterns, can be done using statistical analysis, machine learning, and behavioral analytics
  - Examine the relationships between different data points and events

How SIEM tools work

- **Generating alerts and notifications**
  - Generate alerts with security levels, contextual information, and details about detected incidents
  - Alerts are sent to security administrators, or a centralized management console
- **Dashboards and reporting**
  - Dashboards provide real-time visualizations and summaries of security events
  - Generate detailed reports for security administrators and compliance purposes

Advantages and limitations of SIEM tools

Advantages

- Improved threat detection and response
- Centralized visibility
- Correlation and contextual analysis
- Alert prioritization
- Compliance management

Limitations and challenges

- Data volume and complexity
- Customization and tuning
- Skilled personnel
- Integration complexity
- Alert fatigue
- Cost and budget constraints

Advantages and limitations of SIEM tools

Advantages

- Incident investigation and forensics
- Automated responses
- Risk mitigation

Limitations and challenges

- False positives and negatives
- Data privacy and compliance
- Scalability

SIEM Deployment

- **On-premises**
  - Installed and operated within an organization’s own data centers or infrastructure
  - All hardware and software are owned and managed internally
  - Advantages
    - Greater control over security and data handling
    - For organizations with strict regulatory requirements
  - Challenges
    - Requires significant upfront capital investment
    - Ongoing maintenance, updates, and scalability can be resource intensive

SIEM Deployment

- **Cloud-based**
  - Hosted and operated by third-party providers in the cloud
  - Access to the SIEM platform is via the internet

  - Advantages
    - Lower cost and reduced hardware management
    - Scalability and flexibility
  - Challenges
    - Data privacy and compliance considerations, for sensitive data in the cloud

SIEM Deployment

- **Hybrid**
  - Combination of both on-premises and cloud components
  - Deployment of certain functions on-premises while utilizing cloud services

  - Advantages
    - Flexibility to balance control and scalability based on specific needs
    - Allows to gradually transition to cloud-based SIEM
  - Challenges
    - Requires effective integration and coordination between on-premise and cloud components
    - May introduce complexity in management of the hybrid environment

Snort

- Open-source intrusion prevention system (IPS) that uses a rule-based engine to monitor network traffic for malicious activity

- Has three primary uses
  - Packet sniffer
  - Packet logger
  - Full network intrusion prevention system

- Some key features of snort are that is robust, extensible, multi-threaded

Suricata

- High-performance, open-source network analysis and threat detection software
- Uses a rule-based engine to monitor network traffic for malicious activity
- Suricata offers
  - Multi-threading
  - Protocol support
  - Rule language
  - Detection capabilities

Zeek

- Free and open-source network security monitoring (NSM) framework that can be used to monitor network traffic for malicious activity
- Some of the key features of Zeek include:
  - Anomaly detection
  - Correlation
  - Extensibility
  - Supports a wide range of protocols
  - Can be used to collect and analyze data from a variety of sources

Tripwire

- A security software suite that includes file integrity monitoring (FIM), security configuration management (SCM), and vulnerability management (VM) tools
- Some of the key features of Tripwire include:
  - File integrity monitoring
  - Security configuration management
  - Vulnerability management
  - Compliance reporting
  - Scalability
  - Ease of use

OSSEC

- Free, open-source host-based intrusion detection system
- Used to monitor a system's files, processes, and network connections for malicious activity
- Can detect a wide variety of threats, including malware infections, unauthorized access, and denial-of-service attacks
- OSSEC uses a variety of methods to detect malicious activity, including:
  - File integrity monitoring
  - Process monitoring
  - Network monitoring
  - Log analysis

AIDE

- Free and open-source file integrity checker that can be used to monitor a system's files and directories for changes
- AIDE uses a variety of methods to detect changes to files, including:
  - Checksums
  - Permissions
  - Timestamps

- Some of its key features include that is portable, extensible, and scalable

Advanced Intrusion Detection Environment

References

- Snort: https://www.snort.org/
- Suricata: https://suricata.io/
- Zeek: https://zeek.org/
- Tripwire: https://www.tripwire.com/
- OSSEC: https://www.ossec.net/
- AIDE: https://aide.github.io/