INFORMATION SECURITY ASSIGNMENT 2

Sumsam Ali - 20k-1075

Q1: Based on these Videos briefly define How HIDS and NIDS is implemented.

Host Intrusion Detection Systems (HIDS) Implementation

Core Function of HIDS:

A HIDS is a fundamental part of any Security Information and Event Management (SIEM) platform. Its primary function is to aggregate data from multiple sources, identify deviations from normal activities, and take appropriate action based on those deviations.

Example Use Case:

For instance, a HIDS can be used to track remote logins to servers. Instead of manually checking log files on each server, a HIDS simplifies this by collecting and presenting logs in an easily readable and navigable format.

HIDS can be configured to alert on abnormal activities, such as multiple failed login attempts in a short time frame, unusual port listening activities, or unauthorized user additions to a server.

Tool Used for HIDS: Wazuh

1. **Wazuh Integration:**

   - Wazuh (referred to as 'wazoo'), a tool that can be used to implement a HIDS for free across various operating systems. Wazuh works in conjunction with the Elastic Stack to provide comprehensive monitoring and alerting capabilities.
   - Wazuh is a free and open-source security platform that unifies XDR and SIEM capabilities. It protects workloads across on-premises, virtualized, containerized, and cloud-based environments.
   - Wazuh helps organizations and individuals to protect their data assets against security threats. It is widely used by thousands of organizations worldwide, from small businesses to large enterprises.

2. **Components of Wazuh:**
   - **Wazuh Agent:** Installed on servers to monitor and collect event data. Compatible with a variety of operating systems.
   - **Wazuh Manager**: Receives logs from the Wazuh Agent. It contains rules to evaluate these logs and determine actions (like logging an event, triggering an alert, etc.).
   - **Integration with Elastic Stack**: Elastic Stack (ELK) - comprising Elasticsearch, Kibana, and Filebeat - is used in conjunction with Wazuh. Elasticsearch stores and indexes the logs, Kibana provides a UI for log visualization, and Filebeat is used for log transfer.

3. **Data Flow Process:**
   - The process starts with the Wazuh Agent collecting logs, which are then sent to the Wazuh Manager. The manager evaluates these logs and sends alerts to Elasticsearch via Filebeat. Kibana then accesses these logs for display and analysis.

4. **Benefits**:
    - This setup, combining Wazuh with the Elastic Stack, offers a powerful, insightful, and cost-effective solution for network security monitoring and intrusion detection.

5. **Community and Documentation:**
    - The text emphasizes the availability of extensive documentation and community support (like from OpenSecure), making it easier to implement and understand this technology.

Network Intrusion Detection Systems (HIDS) Implementation

Core Function of NIDS:

NIDS monitors network traffic in real-time to detect intrusion patterns. Focuses on packet-by-packet analysis, inspecting various protocol activities. Often part of an organization's perimeter security, working alongside firewalls.

Deployment

Positioned strategically to inspect entering and exiting traffic for malicious activities. NIDS sensors can be placed in different segments of the network for comprehensive coverage.

Tool Used for NIDS: Security Onion

1. **Definition and Purpose of Security Onion:**
    - It's a comprehensive, free, and open-source software suite for Network Security Monitoring (NSM) and Enterprise Security Monitoring (ESM).
    - NSM is about monitoring network events for security purposes, which can be proactive (like finding vulnerabilities) or reactive (such as during incident response).
    - ESM builds on NSM by adding endpoint visibility and other data sources, thus providing a fuller picture of an organization's security posture.

2. **Traffic Analysis:**
    - Security Onion can analyze both inbound/outbound (north/south) and internal (east/west) network traffic.
    - North/south monitoring helps detect external threats like adversarial entries or data exfiltration.
    - East/west monitoring focuses on internal threats and lateral movement within the network.
    - Endpoint telemetry supplements traffic analysis, especially as more traffic becomes encrypted.

3. **NSM Misconceptions:**
    - NSM is not a plug-and-play solution; it requires ongoing monitoring.
    - The platform emphasizes that while automation aids in identifying threats, human intelligence and vigilance are irreplaceable in threat detection.

4. **Capabilities of Security Onion:**
    - **Intrusion Detection:** Utilizes NIDS, specifically Suricata, to generate alerts from network traffic based on known signatures.

- **Network Metadata:** Provides detailed logs of network activity using Zeek or Suricata, which can be more informative than signature-based detection alone.
- **Full Packet Capture:** Offers a complete recording of network traffic, like a surveillance system, which is invaluable for forensic analysis and is handled by Stenographer.
- **File Analysis:** Files transferred across the network are extracted and analyzed by Strelka for additional insights.
- **Intrusion Detection Honeypot**: Incorporates a node that simulates common network services to trap and identify malicious interactions.

5. **Enterprise Security Monitoring:**
   - Ingests telemetry from endpoints using agents like Beats, osquery, and Wazuh.
   - For devices that cannot host agents, Security Onion can consume and analyze standard Syslog data.

6. **Integrated Analysis Tools:**
   - **Security Onion Console (SOC):** The primary user interface for accessing alerts, dashboards, and case management features.
   - **CyberChef**: A versatile tool for complex data analysis tasks such as decoding and decompressing.
   - **Playbook:** A feature for creating and managing detection strategies and documentation for security events.

7. **Workflow Efficiency:**
   - Security Onion provides an integrated workflow, guiding the user from alert triage to in-depth analysis and case resolution.
   - Users are encouraged to review alerts, analyze dashboards, expand hunts, inspect packet captures, utilize CyberChef for deep analysis, escalate noteworthy findings to cases, and create plays in Playbook for future alerts.

8. **Deployment Flexibility:**
   - The platform offers different deployment scenarios to accommodate various network architectures, with a setup wizard for easy configuration.

9. **Engagement and Learning:**
   - Security Onion demands active engagement from defenders to review alerts, monitor network activity, and continuously learn and adapt to the evolving security landscape.

Security Onion NIDS architechture

- **Adversary**: Represents a potential threat actor trying to penetrate the network.

- **North-South TAP:** This is a network tap (Test Access Point) that captures traffic between the internal network and the wider internet, often referred to as 'north-south' traffic because it typically involves data moving in and out of the network.

- **East-West TAP:** Another network tap that captures 'east-west' traffic, which is the traffic that occurs inside a network, as data moves laterally from server to server or device to device.

- **Security Onion:** Central to the diagram, this represents the Security Onion platform. It is connected to both the North-South and East-West TAPs, indicating that it monitors and analyzes traffic from both directions.

- **Logs:** There are dashed arrows labeled "Logs" pointing from the Security Onion to a server rack icon and a desktop computer icon. This implies that Security Onion collects and potentially aggregates logs from various network devices and endpoints.

- **Server Rack and Desktop Computer**: These icons are likely to represent the network infrastructure and end-user devices, respectively. The logs from these devices are being monitored by Security Onion.

Q1: How is this related to techniques outlined in textbook chapter # 8 IDS, sections 8.4 and 8.5?

Wazuh and Security Onion are tools that integrate and utilize the principles and techniques of Host-Based Intrusion Detection Systems (HIDS) and Network-Based Intrusion Detection Systems (NIDS) discussed in sections 8.4 and 8.5.

Wazuh:

Wazuh is often used as a HIDS, as outlined in section 8.4. It fulfills the role of monitoring sensitive systems from within by:

Monitoring System Call Traces: Wazuh can keep an eye on the system calls made by processes, which is a fundamental technique mentioned for HIDS. For example, if an unexpected system call is made that could indicate a breach, Wazuh can log this as a suspicious event.

Analyzing Audit Records: It can analyze log files generated by the operating system to detect unusual activities. If an attacker tries to elevate privileges or execute unauthorized commands, Wazuh would detect these changes in the audit logs.

File Integrity Monitoring: Wazuh includes file integrity monitoring features, which compare current file states with good baselines (similar to Tripwire). For instance, if a system binary changes unexpectedly, Wazuh can alert administrators to potential tampering.

Anomaly and Signature Detection: Wazuh employs both anomaly detection and signature-based detection to monitor and alert on suspicious activity. If a known malware signature is detected or if a user's behavior deviates from their normal pattern, Wazuh can flag these events.

Security Onion:

Security Onion incorporates many NIDS features as discussed in section 8.5, such as:

Network Traffic Analysis: It provides tools like Suricata, which can analyze network traffic packet by packet for intrusion patterns. For example, if there's an unusual spike in traffic or specific patterns of data that match known attack signatures, Security Onion can raise an alert.

Log Management: Security Onion can aggregate logs from various sources (like NIDS sensors) to provide context and situational awareness, a key principle in network-based intrusion detection. An example would be correlating an alert from Suricata with log data from a web server to confirm a potential web application attack.

Types of Sensors: Security Onion can deploy both inline and passive sensors for network monitoring, which can inspect traffic for signatures of known attacks or anomalies, such as a sudden increase in data packets to a particular IP address that might suggest a DDoS attack.

Deployment and Analysis Tools: Security Onion offers a comprehensive suite of tools for detecting, analyzing, and logging network events. This includes a console for managing alerts, dashboards for data visualization, and full packet capture for detailed forensic analysis.

Together, Wazuh and Security Onion provide a layered defense strategy, combining the strengths of both HIDS and NIDS. Wazuh focuses on individual host systems, monitoring their internal states and changes, while Security Onion looks at the broader network traffic, seeking to identify threats that are moving across the network. The integration of these tools allows for a robust security posture, offering both depth in the form of host-level monitoring and breadth through network traffic analysis.

Below is a comparison table illustrating how Wazuh and Security Onion align with the principles outlined in sections 8.4 (Host-Based Intrusion Detection Systems, HIDS) and 8.5 (Network-Based Intrusion Detection Systems, NIDS):

FEATURE/ASPECT	SECTION 8.4 (HIDS)	WAZUH (HIDS IMPLEMENTATION)	SECTION 8.5 (NIDS)	SECURITY ONION (NIDS IMPLEMENTATION)
PRIMARY FUNCTION	Monitors individual host systems for suspicious activity	Monitors hosts, captures system logs, file integrity	Monitors network traffic for intrusion patterns	Analyzes network traffic using tools like Suricata
Deployment	Deployed on critical or vulnerable systems	Installed on servers and endpoints	Deployed at strategic network points	Deployed as part of the network infrastructure
Data Sources	System calls, audit records, file integrity	System call analysis, log inspection, file monitoring	Packet analysis, protocol activity	Packet capture, protocol analysis, log aggregation
Detection Methodology	Anomaly detection, signature/heuristic detection	Signature-based detection, anomaly detection	Signature detection, anomaly detection, SPA	Signature detection, anomaly detection
Action on Detection	Logs events, sends alerts	Generates alerts, performs active response	Sends alerts, logs information	Generates alerts, visualizes data, logs events
Scope of Protection	Internal system activities	Internal system and application integrity	Network traffic entering and exiting the network	Entire network traffic, both internal and external

Types of Attacks Detected	Both external and internal intrusions	Malware, unauthorized changes, policy violations	Mainly external intrusions, some internal capabilities	External intrusions, lateral movement, policy violations
Response Capabilities	Can halt or mitigate damage on the host	Can respond to threats with active countermeasures	Typically, cannot halt traffic, but can alert	Can halt traffic if configured with inline tools
Suitability for Encryption Traffic	Not directly applicable	Not directly applicable	Limited due to encrypted traffic	Limited; may use endpoint agents for visibility
Platform	Operating system specific	Multi-platform (Windows, Linux, macOS)	Platform-agnostic (focuses on network protocols)	Multi-platform, with focus on network analysis
Example Tools	Tripwire, OSSEC	Wazuh agent	Snort, Bro/Zeek	Suricata, Snort, integrated tools like CyberChef

This table contrasts the key attributes and functionalities of HIDS and NIDS as conceptualized in academic literature with their practical applications in Wazuh and Security Onion, respectively. It demonstrates how each tool embodies the principles and techniques of its associated detection system type.