Implementation of Network Intrusion and Host Intrusion Detection System Using Wazuh

Roll no: 20k-0409 – Mukand Krishna

The Security Onion Essentials course covers key aspects such as infrastructure, deployment modes, analyst tools, and common workflows.

Security Onion infrastructure components include Docker containers orchestrated by Salt Stack. Elastic components, Redis for queuing, InfluxDB for metrics, and data generators like Elastic Agent, Steno, Cerakata, Zeke, and Stroka form the robust components of the system.

Analyst Tools:

It provides access to a myriad of tools, including Alerts Queue, Hunt Interface, Dashboards, Cases, Cyber Chef, Playbook, Elastic Fleet, Attack Navigator, and Elastic Kibana. These tools allow analysts to efficiently monitor, analyze, and respond to security events.

Deployment Modes:

It offers various deployment modes catering to different needs. These include Import Node for forensic analysis, Security Onion Desktop for a secure analysis environment, Evaluation Mode for testing, and Production Deployment Options like Standalone and Distributed.

Installation Process begins with downloading and verifying the Security Onion ISO. Hardware requirements for an evaluation installation emphasize the need for two network interfaces. It includes setting up a virtual machine in VMware Workstation, configuring specifications, and booting from the Security Onion ISO.

Security Onion Setup Process involves configuring node types, acknowledging the Elastic license, network configuration, and platform configuration. It includes setting up the Security Onion console, accessing the web console, and performing a health check.

Introduction to Analyst Tools:

The web console overview tell about user settings, the grid overview, InfluxDB metrics, and functionalities like uploading pcap/evtx files. Video tells about the Alerts and Cases components, dashboards, the Hunt Interface, PCAP analysis, and the administration section for user management. A comprehensive overview of tools includes Kibana, Elastic Fleet, OSQuery Manager, CyberChef, Playbook, and Attack Navigator.

In conclusion, the implementation of NIDS using Security Onion involves a deployment process, robust infrastructure components, and a comprehensive suite of analyst tools.

Implementation of HIDS and Its Importance in Network Security

A Host Intrusion Detection System (HIDS) plays a crucial role in network security by monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces. This system is essential for the detection of security breaches, unauthorized activities, and policy violations. The implementation of HIDS is a cornerstone in a comprehensive security framework, providing real-time analysis and alerting for potential threats.

1. Wazuh is a powerful open-source tool for HIDS. It comprises several key components: the Wazuh agent, installed on the monitored servers; the Wazuh manager, which collects and analyzes data from the agents; and the Elastic Stack, consisting of Elasticsearch, Filebeat, and Kibana, for data storage, filtering, and visualization. Each of these components plays a vital role in the effective functioning of a HIDS, offering a comprehensive solution for network security.

2. Architecture of a Wazuh-Based HIDS is designed to provide a scalable and effective solution for intrusion detection. The Wazuh agent, installed on each server, monitors and collects various events, which are then sent to the Wazuh manager. The manager evaluates these logs against predefined rules and generates alerts. The Elastic Stack (ELK) plays a crucial role in storing, filtering, and visualizing these alerts, making it easier for administrators to monitor and respond to potential security incidents.

3. Wazuh can be deployed in various configurations depending on the needs of the environment. A setup, where all components are on a single server, is suitable for small deployments or testing environments. In contrast, a distributed deployment, with separate servers for the manager, Elasticsearch, and Kibana, is ideal for larger, production environments. This separation allows for better resource allocation and scalability.

4. Installation and Configuration of a Wazuh-based HIDS involves setting up each component of the system. The installation process includes configuring the Wazuh manager and agents, as well as setting up the Elastic Stack components. Proper configuration of these elements is crucial for effective monitoring and analysis. This includes specifying network settings, configuring log paths, and setting up rules and decoders for log analysis.

5. HIDS Implementation involves several critical steps.

The primary goal of HIDS is to monitor and analyze activities on individual hosts within a network, thereby identifying any deviations from normal behavior. It is important in detecting potential security threats and taking action to mitigate them.

The process begins with the deployment of Wazuh, a complete open-source HIDS solution. Wazuh is composed of many components. The **Wazuh agent** is installed on the servers that need to be monitored. These agents are responsible for collecting and sending event logs to the Wazuh manager.

The Wazuh manager, in turn, processes these logs, evaluates them against a set of predefined rules, and generates alerts if any anomalies are detected.

The Elastic Stack (contain Elasticsearch, Filebeat, and Kibana) plays role in managing and visualizing the data.

1. Elasticsearch acts as a database and search engine, storing the logs sent by Filebeat.
2. Filebeat is responsible for transporting alerts from the Wazuh manager to Elasticsearch.
3. Kibana, as a web user interface, enables users to view, filter, and analyze these logs in a user-friendly manner.

The deployment of Wazuh can change based on the needs of the environment. It can be set up as an all-in-one configuration for smaller setups or distributed across multiple servers for larger, more complex networks. This flexibility allows for better resource management and scalability.

Once deployed, the Wazuh agents need to be configured with details such as the manager's IP address and port. The agents then start monitoring the servers and sending logs to the manager. The manager evaluates these logs using rules and decoders. These rules cover many log sources and are designed to detect various types of security incidents.

For enhanced security, it's important to implement encryption for data in transit. This involves using SSL/TLS encryption to secure communication between the Wazuh manager, Elasticsearch, and Kibana. Configuring Elasticsearch and Kibana for HTTPS ensures that the data remains secure while being transmitted and accessed.

User authentication is another important aspect. This can be achieved by enabling X-Pack security in Elasticsearch and Kibana and setting up passwords for built-in users. Additionally, creating and managing individual user accounts in Kibana helps control access levels and maintains security within the system.

Regular updates, maintenance, and strong password policies are essential for keeping the system secure and functioning optimally.

In summary, implementing HIDS with Wazuh involves planning, deployment, configuration, and ongoing management to ensure that it effectively safeguards the network against intrusions and other security threats.

Related to techniques outlined in textbook chapter # 8 IDS, sections 8.4 and 8.5?

The information in the video is relevant to methods in the section 8.4 (HIDS).

HIDS adds a specialized layer of security to sensitive systems like database servers and administrative systems. Used to detect suspicious behavior. The primary benefit of HIDS is that it can detect both external and internal intrusions. HIDS can use anomaly or signature and heuristic approaches to detect unauthorized behavior on the monitored host.

There are some common things b/w video and section 8.4 for HIDS implementation:

Primary goal of HIDS is to detect intrusions, log suspicious events, and send alerts, to enhance security on vulnerable system. It is important in detecting potential security threats and taking action to mitigate them.

Audit (log file) records: collecting information on user activity. Collects and analyzes logs, providing insights into activities on servers. Wazoo manager receives logs, evaluates rules, and generates alerts.

Alerts: Wazuh is used as solution to employ rules to evaluate logs against predefined criteria for generating alerts.

Alerts are logged in and sent to the central manager, providing information such as source IP, port, and log location. Wazuh Architecture Component (Elasticsearch) acts like a database and search engine for logs and metadata.

It is also integrated with different components for more functionalities like the architecture of Distributed IDS: OS audit function, reformat function which comes in HAR.

The information in the video is relevant to methods in the section 8.5 (NIDS).

NIDS examines the traffic packet by packet in real time, or close to real time, to attempt to detect intrusion patterns.

Security Onion Components contain the Data Generators like Elastic Agent, Steno for pcap, Cerakata for alerts.

2 modes: inline and passive sensors are used to monitor the traffic within the sensor, that passes through device and monitors a copy of network traffic that don't pass through device.

Deployment Modes like Import Node (forensic analysis using pcap), Evaluation Model (testing with lower system requirements.

Some attacks suitable for Signature detection like application, transport, network layer attacks.