**Info Security ASSIGNMENT 2**

**Hammad Shakeel 20k-0368**

**Qno1:**

Ans.

SIEM systems aim to gather data from various sources, identify deviations from normal patterns, and take appropriate actions. Host-based Intrusion Detection Systems (HIDS) facilitate readable, understandable, navigable, and fast log presentations. Wazuh, a free and open-source security platform, unifies Extended Detection and Response (XDR) with SIEM protection, addressing endpoints and cloud workloads. SIEM helps organizations detect, analyze, and respond to security threats before they disrupt business operations.

The primary function of every SIEM system is to aggregate data from various sources, identify anomalies, and take necessary actions. Host-based Intrusion Detection Systems (HIDS) present logs in a user-friendly, fast, and comprehensible manner. Wazuh, an open-source security platform, integrates Extended Detection and Response (XDR) with SIEM to safeguard endpoints and cloud workloads. SIEM solutions aid organizations in preemptively detecting, analyzing, and mitigating security threats before impacting business operations.

**Extended Detection and Response (XDR)**

XDR collects and automatically correlates data across multiple security layers, such as email, endpoint, server, cloud workload, and network. This enables quicker threat detection and improved response times through enhanced security analysis.

**Key Features of Wazuh**

* Wazuh supports various Operating Systems.
* The Wazuh manager receives logs from Wazuh agents and contains rules evaluated against received logs. Users can also add their own rules.
* It generates alerts and handles log storage and viewing using the Elastic Stack (ELK stack).
* The ELK stack includes Elastic Search (a log database), Kibana (a web UI for log visualization and filtering), and FileBeat (used to send alerts from Wazuh manager to Elastic Search).
* Communication between Wazuh agent and Wazuh manager occurs through TCP ports 1514 and 1515.
* Deployment methods include all-in-one and distributed options, offering resource allocation, fault-tolerance, redundancy, and scalability, where memory plays a crucial role.
* Clustering for Wazuh manager and Elastic Search enhances fault tolerance and processing power.
* Decoders are used to parse log files if they differ from standard JSON files or syslogs.

**Setting Up Elasticsearch, Kibana, and Filebeat for Wazuh Deployment**

Elasticsearch acts as a virtual library, organizing and quickly retrieving log information. Kibana, a user-friendly interface, aids in data exploration and visualization. Filebeat efficiently ensures log delivery to Elasticsearch.

**Security Onion Overview:**

• Security Onion serves purposes like threat hunting, enterprise security monitoring, and log management.

• Analyst workflows encompass alert triage, case creation, threat hunting, and detection engineering.

• Oracle Linux stands as the sole supported OS.

Deployment Modes:

• Important Node for Forensic Analysis

• Security Onion Desktop/Analyst Workstation

• Evaluation mode for testing

Deployment Modes include Standalone and Distributed configurations.

• Standalone: A production environment where all components are installed on a single system.

• Distributed: Also a production environment, but components are installed on different systems, each termed a node, forming a grid. Distributed mode is preferred over standalone.

**Introduction to Analyst Tools:**

Accessing the Web Console (SOC):

• Access the Security Onion Console or SOC.

• Overview of available analyst tools without detailed exploration; future sessions will delve into specific workflows.

SOC Interface Overview:

User Icon Dropdown:

• Options like Dark Mode/Light Mode, Release Notes, Documentation, Cheat Sheet, Blog, Settings.

SOC Main Menu:

• Modules/Components integrated into Security Onion, Tools accessible as separate applications.

**Overview of Components and Functionality:**

Grid Overview:

• Displays deployment nodes with IP address, version, and status details.

• Provides node-specific information and access to performance metrics via InfluxDB.

Upload PCAP or EVTX:

• File uploads processed by applications like Zeek and Suricata for metadata and alerts.

Replay Test Data:

• Ingests test data into sensor nodes for validation, may require further log investigation in case of timeouts.

Alerts and Cases:

• Alerts generated from ingested data, options for further case investigation.

Dashboards, Hunt Interface, PCAP Viewer:

• Pre-designed visualizations, slicing/dicing data, detailed PCAP information.

Downloads, Administration, Tools Section:

• Management functionalities for users, roles, configurations, Elastic Agent installers, Kibana for visualization, and various security analysis tools.

**Qno2:**

**Section 8.4 and Playlist 1:**

Both (the Section 8.4 and video playlist 1) the concept of Host Intrusion Detection Systems (HIDS) and share common elements and techniques.

Following are some important point:

1. Detection of Intrusions: The main purpose of HIDS is to detect intrusions or suspicious behavior on a host system. They highlight the importance of monitoring system activity and analyzing data to identify unauthorized actions.

2. Data Sources: It discusses various data sources used in HIDS. They mention the collection of system call traces, audit logs, file integrity checksums, and registry access as potential sources of information for detecting intrusions.

3. Anomaly-Based Detection: Section 8.4 specifically focuses on anomaly-based HIDS techniques. It explains the use of algorithms like Sequence Time-Delay Embedding (STIDE), Hidden Markov Models (HMM), Artificial Neural Networks (ANN), Support Vector Machines (SVM), and Extreme Learning Machines (ELM) for classifying system behavior as normal or anomalous. These techniques aim to identify deviations from expected patterns and detect potential intrusions.

4. Operating System Considerations: There are differences in implementing HIDS on different operating systems. It mentions the challenges of system call traces on Windows systems due to the use of Dynamic Link Libraries (DLLs) and also discussing the limitations of system call traces in Windows and proposing alternative approaches, such as monitoring DLL function calls.

5. Monitoring and Analysis: They highlight the importance of monitoring and analyzing system activity to detect intrusions. They discuss the need for specialized security software, such as Elasticsearch, Kibana, and Filebeat, to collect and analyze data, log events, and generate alerts.

In short, they highlight the need for specialized security software that can log events, detect unauthorized actions, and send alerts. They also discuss the use of data sources and sensors for collecting information, such as system call traces, audit logs, file integrity checksums, and registry access.

**Section 8.5 and playlist 2:**

Security Onion Essentials is based on a Network Intrusion Detection System (NIDS). Security Onion is a specialized Linux distribution that serves as a platform for network security monitoring and includes various open-source tools for network intrusion detection, log management, and analysis.

Following are the techniques that are discussed in section 8.5 and is related to Security Onion Essential (playlist 2)

1. NIDS Functionality: Security Onion Essentials, being a network security monitoring platform, monitors network traffic for suspicious or malicious activities.

2. Traffic Examination: NIDS examines network, transport, and/or application-level protocol activity to identify potential intrusion attempts. Security Onion includes various tools like Suricata, Zeek, and Snort, which inspect network traffic at multiple levels for anomalies and known attack patterns.

3. Sensors Deployment: Security Onion can utilize different sensor types (inline or passive) to monitor network traffic either by actively inspecting traffic flow or by passively analyzing copies of network packets.

4. Anomaly Detection and Signature Detection: Security Onion incorporates various detection techniques, including signature-based detection through tools like Snort and Suricata, as well as anomaly-based detection methods to identify abnormal behavior within the network.

5. Logging and Alerts: Section 8.5 emphasizes logging alerts generated by NIDS sensors, which include information such as timestamps, event types, network protocols, IP addresses, ports, and payload data. Security Onion collects logs and alerts generated by the deployed tools, providing visibility into potential security events for further analysis.