Security Onion Certified Professional (SOCP) version 2.4.200 Exam Blueprint

1. Design and Architecture – Approximately 24% of the questions (12)

This domain will focus on the tasks administrators must understand to design and install a successful Security Onion 2.4 grid. They must demonstrate their ability to choose the correct deployment mode and appropriate Security Onion node(s) based on different scenarios. Topics for this section include, but are not limited to, understanding the purpose and functionality of the different node types, recommended minimum hardware requirements for each node type, the applications and services each node type utilizes, and the various deployment modes.

1.1. Explain the different deployment modes and node types, and the role of each node
- 1.1.1. Import
- 1.1.2. Evaluation
- 1.1.3. Standalone
- 1.1.4. Distributed
- 1.1.5. Manager
- 1.1.6. Search
- 1.1.7. Forward

1.2. Identify the core components and their functionality within the following Security Onion nodes
- 1.2.1. Manager
- 1.2.2. Search
- 1.2.3. Forward
- 1.2.4. Receiver
- 1.2.5. Intrusion Detection Honeypot (IDH)

1.3. Describe the function of the following components
- 1.3.1. Elasticsearch
- 1.3.2. Elastic Agent
- 1.3.3. Logstash
- 1.3.4. Redis
- 1.3.5. Strelka
- 1.3.6. Stenographer
- 1.3.7. Suricata
- 1.3.8. Zeek

1.4. Determine the minimum hardware requirements of the following Security Onion nodes
- 1.4.1. Standalone
- 1.4.2. Manager

1.4.3. Search
1.4.4. Forward

2. Grid Management – Approximately 16% of the questions. (8)

This domain will focus on the tasks administrators must understand to effectively administer and maintain a Security Onion 2.4 grid. Topics for this section include, but are not limited to: user management, firewall management, key components of SaltStack, and configuring several core components of the various Security Onion nodes.

2.1. Describe the following components of Saltstack and their functionality within a Security Onion 2.4 Grid
  2.1.1. Salt Master
  2.1.2. Salt Minions
  2.1.3. Salt states
2.2. Describe Role-Based Access Control (RBAC) and explain how to assign, modify, and remove roles assigned to SOC user accounts
2.3. Explain how to add, disable, update, and remove SOC user accounts using the Users Administration interface
2.4. Explain how to add, disable, update, and remove SOC user accounts using the so-users command-line utility
2.5. Describe Multi-factor Authentication (MFA) and explain how to enable, modify, and disable MFA for SOC user accounts
2.6. Describe how to add and remove a single IP address or subnets from the host firewall for the following roles using the Grid Configuration interface
  2.6.1. Analyst Web access to the SOC
  2.6.2. Elastic Agent Endpoints
  2.6.3. Security Onion Search Nodes
  2.6.4. Security Onion Forward/Sensor Nodes
2.7. Explain the process of adding and removing nodes from the Security Onion grid using the Grid Members interface in SOC

3. Grid Monitoring and Troubleshooting – Approximately 20% of the questions. (10)

This domain will focus on the tasks administrators must understand to successfully identify potential issues in a Security Onion 2.4 grid. Topics for this section include but are not limited to: navigating the Grid and InfluxDB interfaces, explaining the purpose and functionality of InfluxDB, building custom InfluxDB dashboards, configuring notification endpoints and rules, and configuring check/alerts within InfluxDB.

3.1. Identify the different metrics available in the Grid interface
3.2. Explain how to collect additional node metrics by pivoting from a node within the Grid interface to InfluxDB
3.3. Describe how to upload PCAP and EVTX files for analysis using the Grid interface

3.4. Explain the purpose of Telegraph in Security Onion 2.4
3.5. Explain the concept of buckets in InfluxDB
3.6. Describe how to perform the following tasks in InfluxDB
    3.6.1. Creating custom dashboards
    3.6.2. Adding custom cells to a dashboard
    3.6.3. Copying or moving cells between dashboards
    3.6.4. Enabling, disabling, and modifying pre-built checks
    3.6.5. Managing notation policies
    3.6.6. Manage notification rules
3.7. Determine the proper location of application logs on Security Onion nodes
3.8. Explain the tail and grep command-line tools and their use when analyzing log files

4. Grid Tuning – Approximately 20% of the questions. (10)

This domain will focus on the task administrators must understand and perform correctly to ensure a Security Onion 2.4 sensor grid is running efficiently. Topics for this section include but are not limited to: Berkeley Packet Filters (BPF), adding additional CPU cores or workers, pinning applications to specific CPU cores, adjusting Redis memory allotment, tuning Logstash pipeline batch size and workers, and tuning Network Intrusion Detection System (NIDS) rules.

4.1. Explain the function of Berkeley Packet Filters and identify the correct BPF syntax
4.2. Describe how BPFs are implemented in Security Onion 2.4
4.3. Explain the following tuning considerations for Zeek
    4.3.1. Purpose of Zeek workers (lb_procs)
    4.3.2. How to determine the correct number of Zeek workers based on the volume of analyzed network traffic
    4.3.3. How to configure the number of workers on a specific node
    4.3.4. How to enable and disable Zeek scripts on a specific node or globally on every node running Zeek
    4.3.5. How to configure CPU affinity for Zeek on a specific node
4.4. Explain the following tuning considerations for Suricata
    4.4.1. Purpose of Suricata threads
    4.4.2. How to determine the correct number of Suricata threads based on the volume of analyzed network traffic
    4.4.3. How to configure the number of threads on a specific node
    4.4.4. How to configure CPU affinity for Suricata on a specific node
4.5. Explain Logstash batch size and worker threads, and the effects they have on the data pipeline
4.6. Describe how to modify the amount of system memory Redis uses to store events as they pass through the data pipeline
4.7. Describe Elasticsearch data streams and how events are written to (indexed) and collected (queried) from data streams
4.8. Describe how Elasticsearch Index Lifecycle Management (ILM) is used to manage Elasticsearch data streams and indices

4.9. Describe the process of adding custom queries to the Hunt and Dashboards interfaces in the SOC
    4.9.1. Describe how to modify the preset values for the category, severity, TLP, PAP, tags, and status fields in a case
    4.9.2. Explain how to configure automatic observable extraction when an event is escalated or added to a case

5. Analyst Tools – Approximately 20% of the questions. (10)

This domain will focus on the different tools and techniques analysts need to understand to properly investigate alerts and hunt for malicious activity using Security Onion 2.4. Topics for this section include, but are not limited to: the use of applications or tools available on Security Onion 2.4, and describe the process of acknowledging and escalating events in the Alerts interface.

5.1. Describe the following Case management tasks
    5.1.1. Attaching new events to a case
    5.1.2. Adding Attachments and Observables
    5.1.3. Setting values such as assignee, status, Traffic Light Protocol (TLP), and Permissible Action Protocol (PAP)
5.2. Describe the process of creating one or more data tables or visualizations in the Group Metrics section of the Hunt and Dashboards interface
5.3. Explain the following options in the SOC context menu
    5.3.1. Include
    5.3.2. Exclude
    5.3.3. Only
    5.3.4. Group by
    5.3.5. New Group by
    5.3.6. Actions
        5.3.6.1. Correlate
        5.3.6.2. Hunt
        5.3.6.3. PCAP