Security Onion Certified Professional version 1 Exam Blueprint

Design and Architecture – Approximately 15% of the questions

This domain will focus on the tasks administrators must understand to design and install a Security Onion 2 grid successfully. 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 different deployment modes.

- Architecture:
- Configuration:
- Hardware:
- Miscellaneous:

Grid Management – Approximately 20% of the questions.

This domain will focus on the tasks administrators must understand to administer and maintain a Security Onion 2 grid successfully. Topics for this section include but are not limited: user management, firewall management, understanding the key components of Saltstack, executing tasks using Salt commands, SaLt State (SLS) files, yaml formatting, docker, log pipelines, alert management, and managing and configuring the different applications contained in the various Security Onion nodes.

- Salt:
- User management
- Firewall management:
- Log pipelines:
- Miscellaneous:

Grid Monitoring – Approximately 10% of the questions.

This domain will focus on the tasks administrators must understand to identify potential issues in a Security Onion 2 grid successfully. Topics for this section include but are not limited to: navigating the Grid and Grafana interfaces, the purpose and functionality of tools such as Telegraph and Influxdb, building notification channels, and configuring alerts in Grafana.

- Grafana:
- Grid Interface:
- Telegraph:
- Influxdb:
- Miscellaneous:

Grid Tuning – Approximately 20% of the questions.

This domain will focus on the task administrators must understand and perform correctly to ensure a Security Onion 2 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 application to specific CPU cores, adding additional disks to LVM, tuning af_packet ring size, Elasticsearch shard management, Redis memory tuning, and Logstash pipeline batch size tuning.

- Berkeley Packet Filters:
- Zeek:
- Suricata:
- Elasticsearch:
- Logstash:
- Redis:
- LVM:
- af_packet:
- Alert management
- Miscellaneous:

Troubleshooting – Approximately 10% of the questions.

This domain will focus on the tasks administrators must understand to perform basic grid troubleshooting. Topics for this section include but are not limited to: understanding the purpose of the different so-* scripts, using Salt to assist in troubleshooting, location of the correct log files on the correct node and using standard Linux command-line tools like grep, tail, and cat.

- so-scripts:
- Troubleshooting with Salt:
- Application logs:
- Miscellaneous:

Analyst Tools – Approximately 25% of the questions.

This domain will focus on the different tools, and techniques analysts need to understand to properly investigate alerts and hunt for adversaries using Security Onion 2. Topics for this section include but are not limited to: the use of applications or tools available on Security Onion 2, to include the Security Onion Analyst node.

- osquery & Wazuh:
- Workflows:
- Hunt:
- PCAP:
- Playbook:
- TheHive:
- Alerts:
- Miscellaneous: