Review: Quiz 11 - Investigation on the SIEM (Digital Forensics 152361)

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

1

When investigating a potential e-mail crime, what is your first step in the investigation? *

- ○ Trace the IP address to its origin
- ○ Write a report
- ○ Determine whether a crime was actually committed
- ◉ Recover the evidence ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

2

During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore, you report this evidence. This type of evidence is known as *

- ○ Inculpatory evidence
- ○ Mandatory evidence
- ◉ Exculpatory evidence ✓
- ○ Terrible evidence

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

3

Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report? *

- TIFF-8
- DOC
- WPD
- PDF ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

4

To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong? *

- Post-investigation Phase
- Reporting Phase
- Pre-investigation Phase ✓
- Investigation Phase

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

5

Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section? *

- Speculation or opinion as to the cause of the incident ✓
- Purpose of the report
- Author of the report
- Incident summary

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

6

What is the role of logstash components in a SIEM system? (Choose all that apply) *

- [ ] Install on the server to collect logs.
- [x] Process logs ✓
- [x] Forward logs to OpenSearch for indexing ✓
- [ ] Storage logs

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

7

Which plugin needs to be installed for Logstash to send data to OpenSearch? *

- ( ) logstash-input-opensearch
- (•) logstash-output-opensearch ✓
- ( ) logstash-output-elasticsearch
- ( ) logstash-input-elasticsearch

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

8

What is the purpose of the following command? tar -zxvf logstash-8.8.2-linux-x86_64.tar.gz *

- ( ) Install logstash
- ( ) Compress the file
- (•) Extract the file ✓
- ( ) Uninstall logstash

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

9

What does the following configuration indicate? (Choose all that apply) *

```
opensearch {
  hosts => ["https://opensearch:9200"]
  index => "opensearch-logstash-docker-%{+YYYY.MM.dd}"
  user => "admin"
  password => "admin"
  ssl => true
  ssl_certificate_verification => false
}
```

- [x] The account used to configure the OpenSearch service is admin ✓
- [ ] The OpenSearch service is using port 5601
- [x] OpenSearch will automatically create a new index for this log source every day ✓
- [x] The OpenSearch service has been configured to use SSL/TLS ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

10

What types of logs does the following winlogbeat configuration collect? (Choose all that apply) *

```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

  - name: Security

  - name: Microsoft-Windows-Sysmon/Operational

  - name: Windows PowerShell
    event_id: 400, 403, 600, 800

  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106
```

- [x] All events in System logs ✓
- [x] All events in Security logs ✓
- [ ] All events in PowerShell logs
- [x] All events in Sysmon logs ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

11

Is the following statement true or false: "Filebeat can be installed on servers and workstations to collect all text-based log files and send them to the SIEM system (OLD)?" *

- (●) True ✓
- ( ) False

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

12

Can Logstash be configured to send data to two destination addresses simultaneously? *

- ○ No
- ◉ Yes ✓
- ○ It depends on the version

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

13

Lệnh DQL sau có nhiệm vụ làm gì? Chọn đáp án đúng nhất. **process.executable: ping** *

- ○ The command has a syntax error
- ○ Search for the value of the field start with the keyword ping
- ◉ Search for the value of the field contain the keyword ping ✓
- ○ Search for the value of the field end with the keyword ping

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

14

What does the following command mean? **sudo systemctl enable opensearch** *

- ○ Verify that OpenSearch launched correctly
- ○ Start the OpenSearch service
- ◉ Enable OpenSearch as a service ✓
- ○ Uninstall OpenSearch service

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

15

What service port does OpenSearch use? *

- 9000
- 9200 ✓
- 5601
- 5044

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

16

Which of the following commands allows you to install OpenSearch Dashboards? *

- sudo systemctl enable opensearch-dashboards
- sudo systemctl start opensearch-dashboards
- dpkg -i opensearch-dashboards-2.18.0-linux-arm64.deb ✓
- dpkg -u opensearch-dashboards-2.18.0-linux-arm64.deb

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

17

What does setting network.host: 0.0.0.0 in the opensearch.yml file mean? *

- It allows OpenSearch to be accessed from any IP address ✓
- It only allows access to OpenSearch from the local address
- Disable access to the OpenSearch service over the network

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

18

What does setting the index **auditbeat-*** mean? *

- ( ) It only allows searching with indices named auditbeat-*.
- ( ) The index name is invalid
- (•) It allows searching across all indices that begin with auditbeat ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

19

Which of the following tasks can Logstash fulfill without using other components of the SIEM (OLD)? (Choose three.) *

- [x] Receive log data from remote systems. ✓
- [ ] Store log data persistently.
- [x] Process log data to extract information. ✓
- [x] Forward log data to other services ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

20

Which of the following filters in Logstash allows parsing and structuring unstructured data? *

- ( ) geoip
- (•) grok ✓
- ( ) json
- ( ) split