

# DUMPSBOSS.COM

## CompTIA Advanced Security Practitioner (CASP+)

CompTIA CAS-004

Version Demo

Total Demo Questions: 15

Total Premium Questions: 254

Buy Premium PDF

<https://dumpsboss.com>

[support@dumpsboss.com](mailto:support@dumpsboss.com)

dumpsboss.com

**QUESTION NO: 1**

An organization is establishing a new software assurance program to vet applications before they are introduced into the production environment, Unfortunately, many Of the applications are provided only as compiled binaries. Which Of the following should the organization use to analyze these applications? (Select TWO).

- A. Regression testing
- B. SAST
- C. Third-party dependency management
- D. IDE SAST
- E. Fuzz testing
- F. IAST

**ANSWER: D E****QUESTION NO: 2**

A security analyst observes the following while looking through network traffic in a company's cloud log:

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

- A. Quarantine 10.0.5.52 and run a malware scan against the host.
- B. Access 10.0.5.52 via EDR and identify processes that have network connections.
- C. Isolate 10.0.50.6 via security groups.
- D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

**ANSWER: D****QUESTION NO: 3**

A company wants to quantify and communicate the effectiveness of its security controls but must establish measures. Which of the following is MOST likely to be included in an effective assessment roadmap for these controls?

- A. Create a change management process.
- B. Establish key performance indicators.
- C. Create an integrated master schedule.
- D. Develop a communication plan.
- E. Perform a security control assessment.

**ANSWER: C**

#### QUESTION NO: 4

An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

- A. Document interpolation
- B. Regular expression pattern matching
- C. Optical character recognition functionality
- D. Baseline image matching
- E. Advanced rasterization
- F. Watermarking

**ANSWER: A C**

#### QUESTION NO: 5

An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data. Which of the following commands should

the analyst run to BEST determine whether financial data was lost?

- A. `grep -v '^4[0-9]{12}(:[0-9]{3})?$' file`
- B. `grep '^4[0-9]{12}(:[0-9]{3})?$' file`
- C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`
- D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

- A. Option A

- B. Option B
- C. Option C
- D. Option D

**ANSWER: C**

#### QUESTION NO: 6

A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users.

Which of the following would be BEST for the developer to perform? (Choose two.)

- A. Utilize code signing by a trusted third party.
- B. Implement certificate-based authentication.
- C. Verify MD5 hashes.
- D. Compress the program with a password.
- E. Encrypt with 3DES.
- F. Make the DACL read-only.

**ANSWER: A C**

#### QUESTION NO: 7

An auditor is reviewing the logs from a web application to determine the source of an incident. The web application architecture includes an Internet-accessible application load balancer, a number of web servers in a private subnet, application servers, and one database server in a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

```
web server logs
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET ../../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/" HTTP/1.1" 200 453 Safari/536.36

application server logs
14/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
14/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing

database server logs
14/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
14/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self signed.
```

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

- A. Enable the x-Forwarded-For header at the load balancer.
- B. Install a software-based HIDS on the application servers.

- C. Install a certificate signed by a trusted CA.
- D. Use stored procedures on the database server.
- E. Store the value of the `$_server ( ' REMOTE_ADDR ' ]` received by the web servers.

**ANSWER: C**

### QUESTION NO: 8

A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from `/var/log/auth.log: graphic.ssh_auth_log`.

Which of the following actions would BEST address the potential risks by the activity in the logs?

- A. Alerting the misconfigured service account password
- B. Modifying the AllowUsers configuration directive
- C. Restricting external port 22 access
- D. Implementing host-key preferences

**ANSWER: B**

#### Explanation:

Reference: <https://www.rapid7.com/blog/post/2017/10/04/how-to-secure-ssh-server-using-port-knocking-on-ubuntu-linux/>

### QUESTION NO: 9

A security architect is reviewing the following proposed corporate firewall architecture and configuration:

```
DMZ architecture
Internet-----70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

Web servers must receive all updates via HTTP/S from the corporate network.

Web servers should not initiate communication with the Internet.

Web servers should only connect to preapproved corporate database servers.

Employees' computing devices should only connect to web services over ports 80 and 443.

Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

- A. Add the following to Firewall\_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
- B. Add the following to Firewall\_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443
- C. Add the following to Firewall\_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
- D. Add the following to Firewall\_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
- E. Add the following to Firewall\_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535
- F. Add the following to Firewall\_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

**ANSWER: A D**

#### QUESTION NO: 10

A software company wants to build a platform by integrating with another company's established product. Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?

- A. Data sovereignty
- B. Shared responsibility
- C. Source code escrow
- D. Safe harbor considerations

**ANSWER: B**

#### Explanation:

When drafting an agreement between two companies, it is important to clearly define the responsibilities of each party. This is particularly relevant when a software company is looking to integrate with an established product. A shared responsibility agreement ensures that both parties understand their respective responsibilities and are able to work together efficiently and effectively. For example, the software company might be responsible for integrating the product and ensuring it meets user needs, while the established product provider might be responsible for providing ongoing support and maintenance. By outlining these responsibilities in the agreement, both parties can ensure that the platform is built and maintained successfully. References: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

#### QUESTION NO: 11

A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.

Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

- A. Perform additional SAST/DAST on the open-source libraries.
- B. Implement the SDLC security guidelines.
- C. Track the library versions and monitor the CVE website for related vulnerabilities.
- D. Perform unit testing of the open-source libraries.

**ANSWER: D**

**Explanation:**

Reference: <https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/>

**QUESTION NO: 12**

A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form? (Select TWO.)

- A. Text editor
- B. OOXML editor
- C. Event Viewer
- D. XML style sheet
- E. SCAP tool
- F. Debugging utility

**ANSWER: B D**

**QUESTION NO: 13**

A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.

Which of the following is t he NEXT step of the incident response plan?

- A. Remediation
- B. Containment
- C. Response
- D. Recovery

**ANSWER: B**

**Explanation:**

Reference: <https://www.sciencedirect.com/topics/computer-science/containment-strategy>

**QUESTION NO: 14**

An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

- A. Document interpolation
- B. Regular expression pattern matching
- C. Optical character recognition functionality
- D. Baseline image matching
- E. Advanced rasterization
- F. Watermarking

**ANSWER: A C****QUESTION NO: 15**

A company has moved its sensitive workloads to the cloud and needs to ensure high availability and resiliency of its web-based application. The cloud architecture team was given the following requirements

- The application must run at 70% capacity at all times
- The application must sustain DoS and DDoS attacks.
- Services must recover automatically.

Which of the following should the cloud architecture team implement? (Select THREE).

- A. Read-only replicas
- B. BCP
- C. Autoscaling
- D. WAF
- E. CDN
- F. Encryption
- G. Continuous snapshots
- H. Containerization

**ANSWER: C D F**

**Explanation:**

The cloud architecture team should implement Autoscaling (C), WAF (D) and Encryption (F). Autoscaling (C) will ensure that the application is running at 70% capacity at all times. WAF (D) will protect the application from DoS and DDoS attacks. Encryption (F) will protect the data from unauthorized access and ensure that the sensitive workloads remain secure.

DUMPSBOSS.COM