



# CAS-004<sup>Q&As</sup>

CompTIA Advanced Security Practitioner (CASP+)

## Pass CompTIA CAS-004 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/cas-004.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

A security analyst wants to keep track of all outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT. Which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

- A. X-Forwarded-Proto
- B. X-Forwarded-For
- C. Cache-Control
- D. Strict-Transport-Security
- E. Content-Security-Policy

Correct Answer: B

---

### QUESTION 2

A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt the data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

- A. Key rotation
- B. Key revocation
- C. Key escrow
- D. Zeroization
- E. Cryptographic obfuscation

Correct Answer: A

---

### QUESTION 3

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

1.

Unauthorized insertions into application development environments



2.

Authorized insiders making unauthorized changes to environment configurations

Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

- A. Perform static code analysis of committed code and generate summary reports.
- B. Implement an XML gateway and monitor for policy violations.
- C. Monitor dependency management tools and report on susceptible third-party libraries.
- D. Install an IDS on the development subnet and passively monitor for vulnerable services.
- E. Model user behavior and monitor for deviations from normal.
- F. Continuously monitor code commits to repositories and generate summary logs.

Correct Answer: AF

---

#### QUESTION 4

A large telecommunications equipment manufacturer needs to evaluate the strengths of security controls in a new telephone network supporting first responders. Which of the following techniques would the company use to evaluate data confidentiality controls?

- A. Eavesdropping
- B. On-path
- C. Cryptanalysis
- D. Code signing
- E. RF sidelobe sniffing

Correct Answer: A

---

#### QUESTION 5

An information security officer reviews a report and notices a steady increase in outbound network traffic over the past ten months. There is no clear explanation for the increase. The security officer interviews several business units and discovers an unsanctioned cloud storage provider was used to share marketing materials with potential customers.

Which of the following services would be BEST for the security officer to recommend to the company?

- A. NIDS
- B. HIPS



C. CASB

D. SFTP

Correct Answer: C

[CAS-004 PDF Dumps](#)

[CAS-004 VCE Dumps](#)

[CAS-004 Study Guide](#)