



# CAS-003<sup>Q&As</sup>

CompTIA Advanced Security Practitioner (CASP+)

## Pass CompTIA CAS-003 Exam with 100% Guarantee

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

<https://www.passapply.com/cas-003.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

The Chief Information Officer (CIO) wants to establish a non-binding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a formal partnership. Which of the following would MOST likely be used?

- A. MOU
- B. OLA
- C. NDA
- D. SLA

Correct Answer: A

### QUESTION 2

A security researcher at an organization is reviewing potential threats to the VoIP phone system infrastructure, which uses a gigabit Internet connection. The researcher finds a vulnerability and knows placing an IPS in front of the phone system will mitigate the risk. The researcher gathers the following information about various IPS systems:

IPS vendor	False positive rate	Maximum throughput	Latency added	Installation fee	Yearly cost
Vendor 1	12 per 1,000 hits	100Mbps	8ms	\$1,000	\$12,000
Vendor 2	18 per 1,000 hits	1000Mbps	5ms	\$500	\$18,000
Vendor 3	10 per 1,000 hits	1000Mbps	8ms	\$200	\$11,000
Vendor 4	2 per 1,000 hits	1000Mbps	12ms	\$750	\$10,000
Vendor 5	14 per 1,000 hits	100Mbps	10ms	\$2,000	\$15,000

The organization is concerned about cost, but call quality is critical to its operations. Which of the following vendors would be BEST for the organization to choose?

- A. Vendor 1
- B. Vendor 2
- C. Vendor 3
- D. Vendor 4
- E. Vendor 5

Correct Answer: C

### QUESTION 3



A company's chief cybersecurity architect wants to configure mutual authentication to access an internal payroll website. The architect has asked the administration team to determine the configuration that would provide the best defense against MITM attacks. Which of the following implementation approaches would BEST support the architect's goals?

- A. Utilize a challenge-response prompt as required input at username/password entry.
- B. Implement TLS and require the client to use its own certificate during handshake.
- C. Configure a web application proxy and institute monitoring of HTTPS transactions.
- D. Install a reverse proxy in the corporate DMZ configured to decrypt TLS sessions.

Correct Answer: C

---

#### QUESTION 4

Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:

Involve business owners and stakeholders  
Create an applicable scenario  
Conduct a biannual verbal review of the incident response plan  
Report on the lessons learned and gaps identified

Which of the following exercises has the CEO requested?

- A. Parallel operations
- B. Full transition
- C. Internal review
- D. Tabletop
- E. Partial simulation

Correct Answer: C

---

#### QUESTION 5

Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin her investigative work, she runs the following nmap command string: `user@hostname:~$ sudo nmap 192.168.1.54` Based on the output, nmap is unable to identify the OS running on the node, but the following ports are open on the device: TCP/22 TCP/111 TCP/512-514 TCP/2049 TCP/32778 Based on this information, which of the following operating systems is MOST likely running on the unknown node?

- A. Linux
- B. Windows
- C. Solaris
- D. OSX



Correct Answer: C

TCP/22 is used for SSH; TCP/111 is used for Sun RPC; TCP/512-514 is used by CMD like exec, but automatic authentication is performed as with a login server, etc. These are all ports that are used when making use of the Sun Solaris operating system.

[CAS-003 VCE Dumps](#)

[CAS-003 Practice Test](#)

[CAS-003 Study Guide](#)