

➤ **Vendor: CompTIA**

➤ **Exam Code: CAS-003**

➤ **Exam Name: CompTIA Advanced Security Practitioner (CASP)**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [Dec./2020](#))**

Visit Braindump2go and Download Full Version CAS-003 Exam Dumps

QUESTION 693

Following the merger of two large companies the newly combined security team is overwhelmed by the volume of logs flowing from the IT systems.

The company's data retention schedule complicates the issue by requiring detailed logs to be collected and available for months.

Which of the following designs BEST meets the company's security and retention requirement?

- A. Forward logs to both a SIEM and a cheaper longer-term storage and then delete logs from the SIEM after 14 days
- B. Reduce the log volume by disabling logging of routine maintenance activities or failed authentication attempts
- C. Send logs to a SIEM that correlates security data and store only the alerts and relevant data arising from that system.
- D. Maintain both companies' logging and SIEM solutions separately but merge the resulting alerts and reports.

Answer: C

QUESTION 694

As part of a systems modernization program, the use of a weak encryption algorithm is identified in a web services API. The client using the API is unable to upgrade the system on its end which would support the use of a secure algorithm set.

As a temporary workaround the client provides its IP space and the network administrator limits access to the API via an ACL to only the IP space held by the client.

Which of the following is the use of the ACL in this situation an example of?

- A. Avoidance
- B. Transference
- C. Mitigation
- D. Acceptance
- E. Assessment

Answer: C

QUESTION 695

A new employee is plugged into the network on a BYOD machine but cannot access the network.

Which of the following must be configured so the employee can connect to the network?

- A. Port security
- B. Firewall
- C. Remote access

[CAS-003 Exam Dumps](#) [CAS-003 Exam Questions](#) [CAS-003 PDF Dumps](#) [CAS-003 VCE Dumps](#)

<https://www.braindump2go.com/cas-003.html>

D. VPN

Answer: D

QUESTION 696

A company has deployed MFA. Some employees, however, report they are not getting a notification on their mobile device.

Other employees report they downloaded a common authenticator application but when they tap the code in the application it just copies the code to memory instead of confirming the authentication attempt.

Which of the following are the MOST likely explanations for these scenarios? (Select TWO)

- A. The company is using a claims-based authentication system for MFA
- B. These are symptoms of known compatibility issues with OAuth 1.0
- C. OpenID Connect requires at least one factor to be a biometric
- D. The company does not allow an SMS authentication method
- E. The WAYF method requires a third factor before the authentication process can complete
- F. A vendor-specific authenticator application is needed for push notifications

Answer: CE

QUESTION 697

A company wants to secure a newly developed application that is used to access sensitive information and data from corporate resources.

The application was developed by a third-party organization, and it is now being used heavily despite lacking the following controls:

- Certificate pinning
- Tokenization
- Biometric authentication

The company has already implemented the following controls:

- Full device encryption
- Screen lock
- Device password
- Remote wipe

The company wants to defend against interception of data attacks.

Which of the following compensating controls should the company implement NEXT?

- A. Enforce the use of a VPN when using the newly developed application.
- B. Implement a geofencing solution that disables the application according to company requirements.
- C. Implement an out-of-band second factor to authenticate authorized users
- D. Install the application in a secure container requiring additional authentication controls.

Answer: A

QUESTION 698

A security engineer is looking at a DNS server following a known incident.

The engineer sees the following command as the most recent entry in the server's shell history:

`id ^f=iev/sda of=/dev/sdb`

Which of the following MOST likely occurred?

- A. A tape backup of the server was performed.
- B. The drive was cloned for forensic analysis.
- C. The hard drive was formatted after the incident.
- D. The DNS log files were rolled daily as expected

Answer: B

QUESTION 699

The security configuration management policy states that all patches must undergo testing procedures before being moved into production.

The security analyst notices a single web application server has been downloading and applying patches during non-business hours without testing.

There are no apparent adverse reaction, server functionality does not seem to be affected, and no malware was found after a scan.

Which of the following action should the analyst take?

- A. Reschedule the automated patching to occur during business hours.
- B. Monitor the web application service for abnormal bandwidth consumption.
- C. Create an incident ticket for anomalous activity.
- D. Monitor the web application for service interruptions caused from the patching.

Answer: C

QUESTION 700

The Chief Financial Officer (CFO) of a major hospital system has received a ransom letter that demands a large sum of cryptocurrency be transferred to an anonymous account.

If the transfer does not take place within ten hours, the letter states that patient information will be released on the dark web.

A partial listing of recent patients is included in the letter.

This is the first indication that a breach took place.

Which of the following steps should be done FIRST?

- A. Review audit logs to determine the extent of the breach
- B. Pay the hacker under the condition that all information is destroyed
- C. Engage a counter-hacking team to retrieve the data
- D. Notify the appropriate legal authorities and legal counsel

Answer: D

QUESTION 701

A hospital's security team recently determined its network was breached and patient data was accessed by an external entity.

The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan.

The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients.

Which of the following is the MOST appropriate response?

- A. When it is mandated by their legal and regulatory requirements
- B. As soon as possible in the interest of the patients
- C. As soon as the public relations department is ready to be interviewed
- D. When all steps related to the incident response plan are completed
- E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

Answer: A

QUESTION 702

You are a security analyst tasked with interpreting an Nmap scan output from Company A's privileged network.

The company's hardening guidelines indicate the following:

- There should be one primary server or service per device.
- Only default ports should be used.

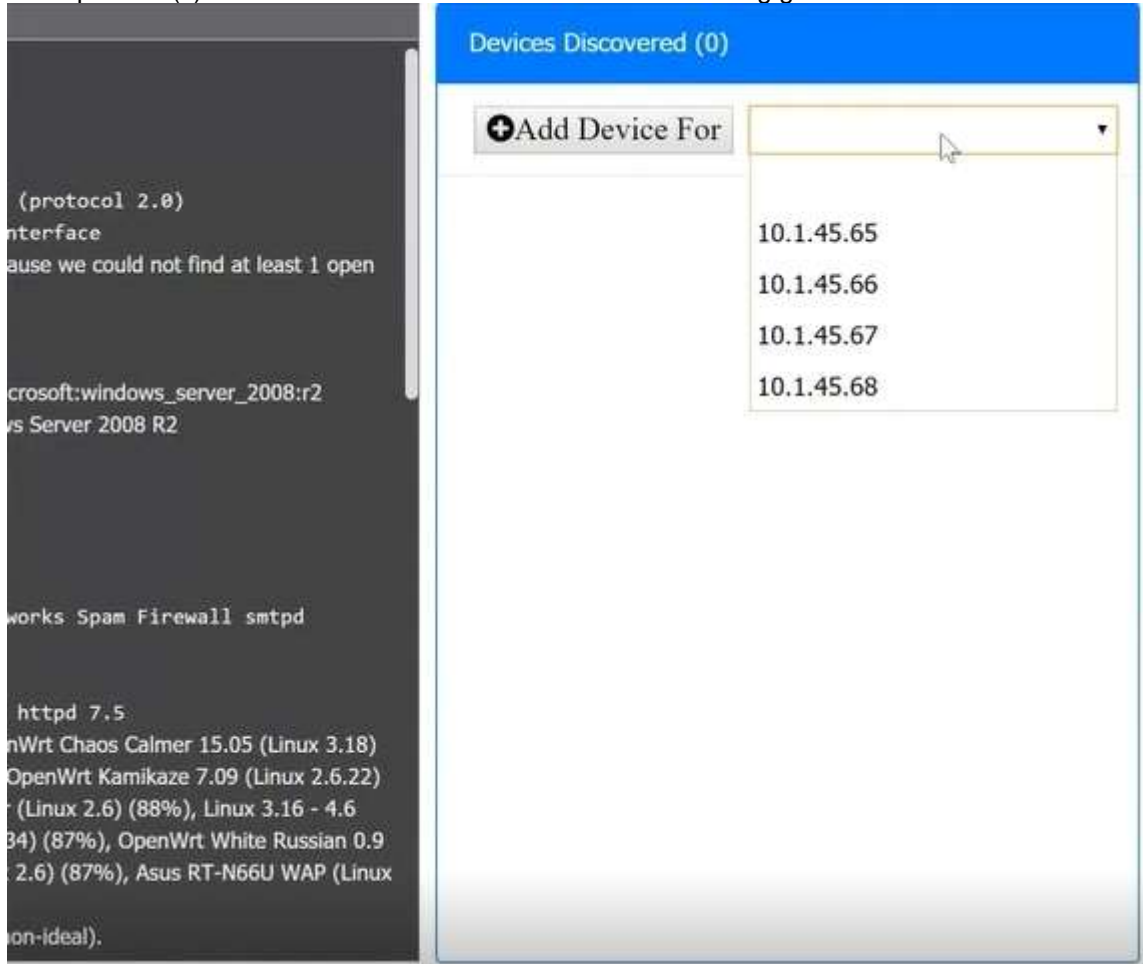
- Non-secure protocols should be disabled.

INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found, add a device entry to the Devices Discovered list, with the following information:

- The IP address of the device
- The primary server or service of the device
- The protocol(s) that should be disabled based on the hardening guidelines



The screenshot shows two side-by-side windows. The left window displays Nmap scan results, including the following text: (protocol 2.0), interface, cause we could not find at least 1 open, microsoft:windows_server_2008:r2, vs Server 2008 R2, works Spam Firewall smtpd, httpd 7.5, nWrt Chaos Calmer 15.05 (Linux 3.18), OpenWrt Kamikaze 7.09 (Linux 2.6.22), (Linux 2.6) (88%), Linux 3.16 - 4.6, 34) (87%), OpenWrt White Russian 0.9, 2.6) (87%), Asus RT-N66U WAP (Linux, on-ideal).

The right window is titled "Devices Discovered (0)". It features a button labeled "+ Add Device For" and a dropdown menu. The dropdown menu is open, showing a list of IP addresses: 10.1.45.65, 10.1.45.66, 10.1.45.67, and 10.1.45.68. A mouse cursor is pointing at the 10.1.45.66 entry.

Answer:

Add device for 10.1.45.66 as below:



Devices Discovered (1)

+ Add Device For

IP Address: 10.1.45.66

Role: FTP Server

Disable Protocols:

- 20/tcp
- 21/tcp
- 22/tcp
- 25/tcp
- 80/tcp
- 415/tcp
- 443/tcp
- 2001/tcp

QUESTION 703

A security analyst has received the following requirements for the implementation of enterprise credential management software.

- The software must have traceability back to an individual
- Credentials must remain unknown to the vendor at all times
- There must be forced credential changes upon ID checkout
- Complexity requirements must be enforced.
- The software must be quickly and easily scalable with max mum availability

Which of the following vendor configurations would BEST meet these requirements?

- A. Credentials encrypted in transit and then stored, hashed and salted in a vendor's cloud, where the vendor handles key management
- B. Credentials stored, hashed, and salted on each local machine
- C. Credentials encrypted in transit and stored in a vendor's cloud, where the enterprise retains the keys
- D. Credentials encrypted in transit and stored on an internal network server with backups that are taken on a weekly basis

Answer: B

QUESTION 704

To meet a SLA, which of the following documents should be drafted, defining the company's internal interdependent unit responsibilities and delivery timelines.

- A. BPA
- B. OLA
- C. MSA
- D. MOU

Answer: B

Explanation:

OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure

[CAS-003 Exam Dumps](#) **[CAS-003 Exam Questions](#)** **[CAS-003 PDF Dumps](#)** **[CAS-003 VCE Dumps](#)**

<https://www.braindump2go.com/cas-003.html>

that all the support groups provide the intended ServiceLevelAgreement.