DUMPSARENA

CompTIA Advanced Security Practitioner (CASP) CAS-003

CompTIA CAS-003

Version Demo

Total Demo Questions: 20

Total Premium Questions: 547

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Company leadership believes employees are experiencing an increased number of cyber attacks; however, the metrics do not show this. Currently, the company uses “Number of successful phishing attacks” as a KRI, but it does not show an increase.

Which of the following additional information should be the Chief Information Security Officer (CISO) include in the report?

A. The ratio of phishing emails to non-phishing emails

B. The number of phishing attacks per employee

C. The number of unsuccessful phishing attacks

D. The percent of successful phishing attacks

ANSWER: C

QUESTION NO: 2

The finance department has started to use a new payment system that requires strict PII security restrictions on various network devices. The company decides to enforce the restrictions and configure all devices appropriately. Which of the following risk response strategies is being used?

A. Avoid

B. Mitigate

C. Transfer

D. Accept

ANSWER: B

QUESTION NO: 3

A Chief Information Security Officer (CISO) is creating a security committee involving multiple business units of the corporation.

Which of the following is the BEST justification to ensure collaboration across business units?

A. A risk to one business unit is a risk avoided by all business units, and liberal BYOD policies create new and unexpected avenues for attackers to exploit enterprises.

B. A single point of coordination is required to ensure cybersecurity issues are addressed in protected, compartmentalized groups.

C. Without business unit collaboration, risks introduced by one unit that affect another unit may go without compensating controls.

D. The CISO is uniquely positioned to control the flow of vulnerability information between business units.

ANSWER: C

QUESTION NO: 4

A systems analyst is concerned that the current authentication system may not provide the appropriate level of security. The company has integrated WAYF within its federation system and implemented a mandatory two-step authentication system. Some accounts are still becoming compromised via phishing attacks that redirect users to a fake portal, which is automatically collecting and replaying the stolen credentials. Which of the following is a technical solution that would BEST reduce the risk of similar compromises?

A. Security awareness training

B. Push-based authentication

C. Software-based TOTP

D. OAuth tokens

E. Shibboleth

ANSWER: C

QUESTION NO: 5

A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

- The tool needs to be responsive so service teams can query it, and then perform an automated response action.
- The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
- The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Scalability

B. Latency

C. Availability

D. Usability

E. Recoverability

F. Maintainability

ANSWER: B C E

QUESTION NO: 6

A company is not familiar with the risks associated with IPv6. The systems administrator wants to isolate IPv4 from IPv6 traffic between two different network segments. Which of the following should the company implement? (Choose two.)

A. Use an internal firewall to block UDP port 3544.

B. Disable network discovery protocol on all company routers.

C. Block IP protocol 41 using Layer 3 switches.

D. Disable the DHCPv6 service from all routers.

E. Drop traffic for ::/0 at the edge firewall.

F. Implement a 6in4 proxy server.

ANSWER: A C

QUESTION NO: 7

The results of an external penetration test for a software development company show a small number of applications account for the largest number of findings. While analyzing the content and purpose of the applications, the following matrix is created:

Application Name	Externally accessible	PHI	PII	Medium Findings	High Findings	Critical Findings
Application 1	No	No	Yes	135	175	226
Application 2	Yes	Yes	No	38	20	11
Application 3	No	No	No	175	108	82
Application 4	Yes	No	No	250	35	22
Application 5	No	Yes	Yes	200	75	62

The findings are then categorized according to the following chart:

Application Name	Missing OS Patches	Coding Errors	Credential Non-compliance	Missing Software Patches
Application 1	175	0	21	329
Application 2	2	55	0	12
Application 3	37	227	5	96
Application 4	110	5	0	192
Application 5	24	169	0	144

Which of the following would BEST reduce the amount of immediate risk incurred by the organization from a compliance and legal standpoint? (Choose two.)

A. Place a WAF in line with Application 2

B. Move Application 3 to a secure VLAN and require employees to use a jump server for access

C. Apply the missing OS and software patches to the server hosting Application 4

D. Use network segmentation and ACLs to control access to Application 5

E. Implement an IDS/IPS on the same network segment as Application 3

F. Install a FIM on the server hosting Application 4

G. Enforce Group Policy password complexity rules on the server hosting Application 1

ANSWER: D E

QUESTION NO: 8

A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

A. OTA updates

B. Remote wiping

C. Side loading

D. Sandboxing

E. Containerization

F. Signed applications

ANSWER: E F

QUESTION NO: 9

An incident responder wants to capture volatile memory comprehensively from a running machine for forensic purposes. The machine is running a very recent release of the Linux OS.

Which of the following technical approaches would be the MOST feasible way to accomplish this capture?

A. Run the memdump utility with the -k flag.

B. Use a loadable kernel module capture utility, such as LiME.

C. Run dd on/dev/mem.

D. Employ a stand-alone utility, such as FTK Imager.

ANSWER: D

QUESTION NO: 10

One of the objectives of a bank is to instill a security awareness culture. Which of the following are techniques that could help to achieve this? (Choose two.)

A. Blue teaming

B. Phishing simulations

C. Lunch-and-learn

D. Random audits

E. Continuous monitoring

F. Separation of duties

ANSWER: B E

QUESTION NO: 11

First responders, who are part of a core incident response team, have been working to contain an outbreak of ransomware that also led to data loss. In a rush to isolate the three hosts that were calling out to the NAS to encrypt whole directories, the hosts were shut down immediately without investigation and then isolated. Which of the following were missed? (Choose two.)

A. CPU, process state tables, and main memory dumps

B. Essential information needed to perform data restoration to a known clean state

C. Temporary file system and swap space

D. Indicators of compromise to determine ransomware encryption

E. Chain of custody information needed for investigation

ANSWER: D E

QUESTION NO: 12

The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.

Which of the following BEST meets the needs of the board?

A. KRI:
- Compliance with regulations
- Backlog of unresolved security investigations
- Severity of threats and vulnerabilities reported by sensors- Time to patch critical issues on a monthly basis KPI:
- Time to resolve open security items
- % of suppliers with approved security control frameworks
- EDR coverage across the fleet
- Threat landscape ratingB. KRI:
- EDR coverage across the fleet
- Backlog of unresolved security investigations
- Time to patch critical issues on a monthly basis- Threat landscape rating KPI:
- Time to resolve open security items
- Compliance with regulations
- % of suppliers with approved security control frameworks
- Severity of threats and vulnerabilities reported by sensors

B. KRI:
- EDR coverage across the fleet
- % of suppliers with approved security control framework
- Backlog of unresolved security investigations
- Threat landscape ratingKPI:
- Time to resolve open security items
- Compliance with regulations
- Time to patch critical issues on a monthly basis
- Severity of threats and vulnerabilities reported by sensors

C. KPI:
- Compliance with regulations
- % of suppliers with approved security control frameworks
- Severity of threats and vulnerabilities reported by sensors- Threat landscape rating KRI:
- Time to resolve open security items
- Backlog of unresolved security investigations
- EDR coverage across the fleet
- Time to patch critical issues on a monthly basis

ANSWER: A

QUESTION NO: 13

A factory-floor system uses critical, legacy, and unsupported application software to enable factory operations. A latent vulnerability was recently exposed, which permitted attackers to send a specific string of characters followed by arbitrary code for execution. Patches are unavailable, as the manufacturer is no longer in business. Which of the following would be the BEST approach the company should take to mitigate the risk of this vulnerability and other latent vulnerability exploits? (Choose two.)

A. Configure a host-based firewall on the application server and restrict access to necessary ports and services.

B. Create a factory-floor enclave segregated from direct LAN/WAN reachability.

C. Implement a proxy that will sanitize input provided to the application.

D. Install server-side X.509 certificates and enable TLS 1.0 or later for client access.

E. Install network and host-based IDS, feeding logs to SIEM, and alerts to SOC operators.

F. Create a hunt team focused on the factory-floor operations.

ANSWER: B C

QUESTION NO: 14 - (SIMULATION)

SIMULATION

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

To select multiple protocols, use CTRL+CLICK.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


NMAP Scan Output
Devices Discovered (0)
Add Device For
10.1.45.65
10.1.45.66
10.1.45.67
10.1.45.68

ANSWER: See the explanation below.

Explanation:

10.1.45.65 – FTP Server – Disable 8080

10.1.45.66 – Email Serve – Disable 25 and 415

10.1.45.67 – Web Server – Disable 21, 80

10.1.45.68 – UTM Appliance – Disable 21

QUESTION NO: 15

A hospital is deploying new imaging software that requires a web server for access to images for both local and remote users. The web server allows user authentication via secure LDAP. The information security officer wants to ensure the server does not allow unencrypted access to the imaging server by using Nmap to gather additional information. Given the following:

- The imaging server IP is 192.168.101.24.
- The domain controller IP is 192.168.100.1.
- The client machine IP is 192.168.200.37.

Which of the following should be used to confirm this is the only open port on the web server?

A. nmap -p 80,443 192.168.101.24

B. nmap -p 80, 443,389,636 192.168.100.1

C. nmap —p 80,389 192.168.200.37

D. nmap -p- 192.168.101.24

ANSWER: D

QUESTION NO: 16 - (DRAG DROP)

DRAG DROP

A security consultant is considering authentication options for a financial institution. The following authentication options are available. Drag and drop the security mechanism to the appropriate use case.

Options may be used once.

Select and Place:

Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	
Authentication to cloud-based corporate portals will feature single sign-on	
Any infrastructure portal will require time-based authentication	
Customers will have delegated access to multiple digital services	

Kerberos	oAuth
OTP	SAML

ANSWER:

Explanation:

QUESTION NO: 17

A penetration testing manager is contributing to an RFP for the purchase of a new platform. The manager has provided the following requirements:

- Must be able to MITM web-based protocols
- Must be able to find common misconfigurations and security holes

Which of the following types of testing should be included in the testing platform? (Choose two.)

A. Reverse engineering tool

B. HTTP intercepting proxy

C. Vulnerability scanner

D. File integrity monitor

E. Password cracker

F. Fuzzer

ANSWER: B C

QUESTION NO: 18

Following a merger, the number of remote sites for a company has doubled to 52. The company has decided to secure each remote site with an NGFW to provide web filtering, NIDS/NIPS, and network antivirus. The Chief Information Officer (CIO) has requested that the security engineer provide recommendations on sizing for the firewall with the requirements that it be easy to manage and provide capacity for growth.

The tables below provide information on a subset of remote sites and the firewall options:

Location	# of Users	Connectivity	Bandwidth Utilization
St.Louis	18	50 Mbps	20 Mbps
Des Moines	12	25 Mbps	19 Mbps
Chicago	27	100 Mbps	41 Mbps
Rapid City	6	10 Mbps	8 Mbps
Indianapolis	7	12 Mbps	8 Mbps

Vendor	Maximum Recommended Devices	Firewall Throughput	Full UTM?	Centralized Management Available?
A	40	150 Mbps	Y	Y
B	60	400 Mbps	N	Y
C	25	200 Mbps	N	N
D	25	100 Mbps	Y	Y

Which of the following would be the BEST option to recommend to the CIO?

A. Vendor C for small remote sites, and Vendor B for large sites.

B. Vendor B for all remote sites

C. Vendor C for all remote sites

D. Vendor A for all remote sites

E. Vendor D for all remote sites

ANSWER: D

QUESTION NO: 19

A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregator and allows remote access to MSSP analysts. Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud. The data is then sent from the log aggregator to a public IP address in the MSSP's datacenter for analysis.

A security engineer is concerned about the security of the solution and notes the following:

- The critical devices send cleartext logs to the aggregator.
- The log aggregator utilizes full disk encryption.
- The log aggregator sends to the analysis server via port 80.
- MSSP analysts utilize an SSL VPN with MFA to access the log aggregator remotely. ▪ The data is compressed and encrypted prior to being archived in the cloud.

Which of the following should be the security engineer's GREATEST concern?

A. Hardware vulnerabilities introduced by the log aggregator server

B. Network bridging from a remote access VPN

C. Encryption of data in transit

D. Multitenancy and data remnants in the cloud

ANSWER: C

QUESTION NO: 20

A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:

- Store taxation-related documents for five years
- Store customer addresses in an encrypted format
- Destroy customer information after one year
- Keep data only in the customer's home country

Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

A. Capacity planning policy

B. Data retention policy

C. Data classification standard

D. Legal compliance policy

E. Data sovereignty policy

F. Backup policy

G. Acceptable use policy

H. Encryption standard

ANSWER: B E H