CAS-004$^{Q\&As}$

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.pass4itsure.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:

1.

Some developers can directly publish code to the production environment.

2.

Static code reviews are performed adequately.

3.

Vulnerability scanning occurs on a regularly scheduled basis per policy.

Which of the following should be noted as a recommendation within the audit report?

A. Implement short maintenance windows.

B. Perform periodic account reviews.

C. Implement job rotation.

D. Improve separation of duties.

Correct Answer: D

QUESTION 2

An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports. Which of the following historian server locations will allow the business to get the required reports in an ?? and IT environment?

A. In the ?? environment, use a VPN from the IT environment into the ?? environment.

B. In the ?? environment, allow IT traffic into the ?? environment.

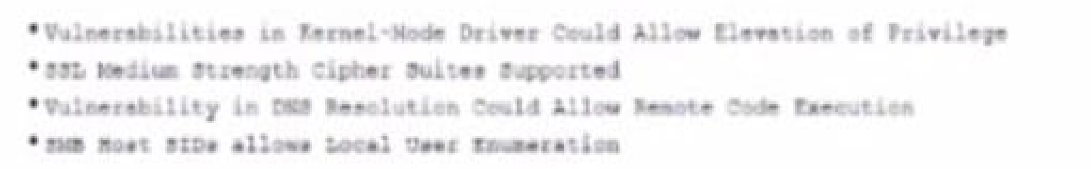
C. In the IT environment, allow PLCs to send data from the ?? environment to the IT environment.

D. Use a screened subnet between the ?? and IT environments.

Correct Answer: D

QUESTION 3

An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:



- Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
- SSL Medium Strength Cipher Suites Supported
- Vulnerability in DNS Resolution Could Allow Remote Code Execution
- SMB Host SIDs allows Local User Enumeration

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker

B. Port scanner

C. Account enumerator

D. Exploitation framework

Correct Answer: A

QUESTION 4

Due to locality and budget constraints, an organization\\'s satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.

Which of the following would be the BEST option to implement?

A. Distributed connection allocation

B. Local caching

C. Content delivery network

D. SD-WAN vertical heterogeneity

Correct Answer: C

QUESTION 5

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 the NEXT step of the incident response plan?

A. Remediation

B. Containment

C. Response

D. Recovery

Correct Answer: B

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

QUESTION 6

A company wants to improve the security of its web applications that are running on in-house servers. A risk assessment has been performed, and the following capabilities are desired:

1.

Terminate SSL connections at a central location

2.

Manage both authentication and authorization for incoming and outgoing web service calls

3.

Advertise the web service API

4.

Implement DLP and anti-malware features

Which of the following technologies will be the BEST option?

A. WAF

B. XML gateway

C. ESB gateway

D. API gateway

Correct Answer: D

QUESTION 7

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company\\'s Chief Financial Officer loses a phone multiple times a year.

Which of the following will MOST likely secure the data on the lost device?

A. Require a VPN to be active to access company data.

B. Set up different profiles based on the person\\'s risk.

C. Remotely wipe the device.

D. Require MFA to access company applications.

Correct Answer: C

QUESTION 8

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

Correct Answer: BC

QUESTION 9

A hospital is deploying new imaging softwares that requires a web server for access to image 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:

1.

The imaging server IP is 192.168.101.24

2.

The domain controller IP is 192.168.100.1

3.

The client machine IP is 192.168.200.37

Which of the following should be used to confirm this is the only open post 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

Correct Answer: B

QUESTION 10

A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.

Which of the following technologies would BEST meet this need?

A. Faraday cage

B. WPA2 PSK

C. WPA3 SAE

D. WEP 128 bit

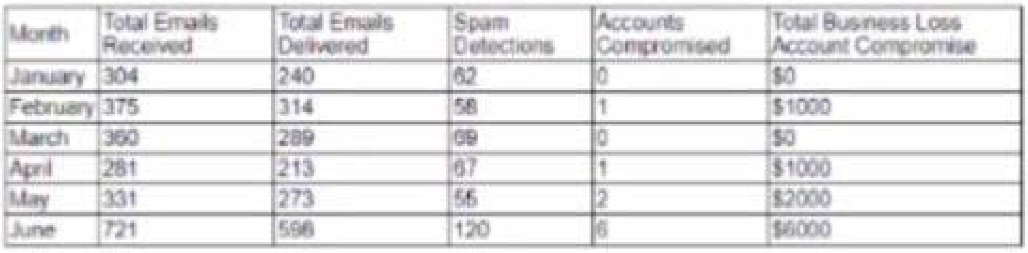
Correct Answer: C

WPA3 SAE prevents brute-force attacks.

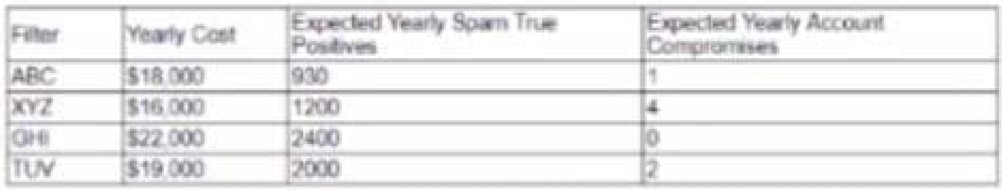
Reference: https://support.enplug.com/hc/en-us/articles/205160175-Setting-your-WiFi-encryption-as-WPA2-PSK

QUESTION 11

A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:



Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	56	2	$2000
June	721	598	120	6	$6000



Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

Which of the following meets the budget needs of the business?

A. Filter ABC

B. Filter XYZ

C. Filter GHI

D. Filter TUV

Correct Answer: C

QUESTION 12

A security team is concerned with attacks that are taking advantage of return-oriented programming against the company\\'s public facing applications. Which of the following should the company implement on the public-facing servers?

A. WAF

B. ASLR

C. NX

D. HSM

Correct Answer: B

According to Intel, the answer is ASLR (B).

"Areas of strength for ROP attacks includes the ability to circumvent data execution prevention (NX)"... meaning C is not the correct answer. See page 8 at link below.

"Existing solutions to ROP attacks include Address Space Layout Randomization: ASLR is the state-of-the-art protection against ROP attacks." See page 9 at link below.

https://www.intel.com/content/dam/develop/external/us/en/documents/catc17-anti-rop-moving-target-defense-844137.pdf

QUESTION 13

A security architect is designing a solution for a new customer who requires significant security capabilities in its environment. The customer has provided the architect with the following set of requirements:

1.

Capable of early detection of advanced persistent threats.

2.

Must be transparent to users and cause no performance degradation.

3.

Allow integration with production and development networks seamlessly.

4.

Enable the security team to hunt and investigate live exploitation techniques.

Which of the following technologies BEST meets the customer\\'s requirements for security capabilities?

A. Threat Intelligence

B. Deception software

C. Centralized logging

D. Sandbox detonation

Correct Answer: B

QUESTION 14

A company security engineer arrives at work to face the following scenario:

1) Website defacement 2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand 3) A Job offer from the company\\'s competitor 4) A security analyst\\'s investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data

Which of the following threat actors Is MOST likely involved?

A. Organized crime

B. Script kiddie

C. APT/nation-state

D. Competitor

Correct Answer: C

QUESTION 15

Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

A. The image must be password protected against changes.

B. A hash value of the image must be computed.

C. The disk containing the image must be placed in a seated container.

D. A duplicate copy of the image must be maintained

Correct Answer: B

CAS-004 VCE Dumps CAS-004 Practice Test CAS-004 Study Guide