CAS-003$^{\text{Q\&As}}$

CompTIA Advanced Security Practitioner (CASP+)

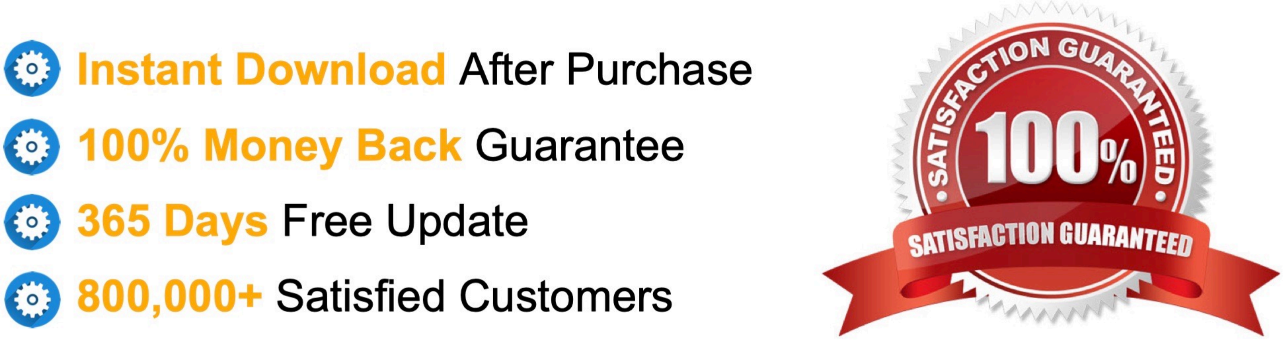
Pass CompTIA CAS-003 Exam with 100% Guarantee

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

https://www.leads4pass.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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

The email administrator must reduce the number of phishing emails by utilizing more appropriate security controls. The following configurations already are in place:

1.

Keyword blocking based on word lists

2.

URL rewnting and protection

3.

Stopping executable files from messages

Which of the following is the BEST configuration change for the administrator to make?

A. Configure more robust word lists for blocking suspicious emails

B. Configure appropriate regular expression rules per suspicious email received

C. Configure Bayesian filtering to block suspicious inbound email

D. Configure the mail gateway to strip any attachments.

Correct Answer: B

Reference: https://www ibm.com/docs/en/rsoa-and-rD/36?tODic=Darsing-extension-customization

QUESTION 2

A company is in the process of re-architecting its sensitive system infrastructure to take advantage of on-demand computing through a public cloud provider The system to be migrated is sensitive with respect to latency availability, and integrity The infrastructure team agreed to the following

1.

Application and middleware servers will migrate to the cloud"; Database servers will remain on-site

2.

Data backup wilt be stored in the cloud

Which of the following solutions would ensure system and security requirements are met?

A. Implement a direct connection from the company to the cloud provider

B. Use a cloud orchestration tool and implement appropriate change control processes

C. Implement a standby database on the cloud using a CASB for data-at-rest security

D. Use multizone geographic distribution with satellite relays

Correct Answer: A

QUESTION 3

A development team releases updates to an application regularly. The application is compiled with several standard open-source security products that require a minimum version for compatibility. During the security review portion of the development cycle, which of the following should be done to minimize possible application vulnerabilities?

A. The developers should require an exact version of the open-source security products, preventing the introduction of new vulnerabilities.

B. The application development team should move to an Agile development approach to identify security concerns faster

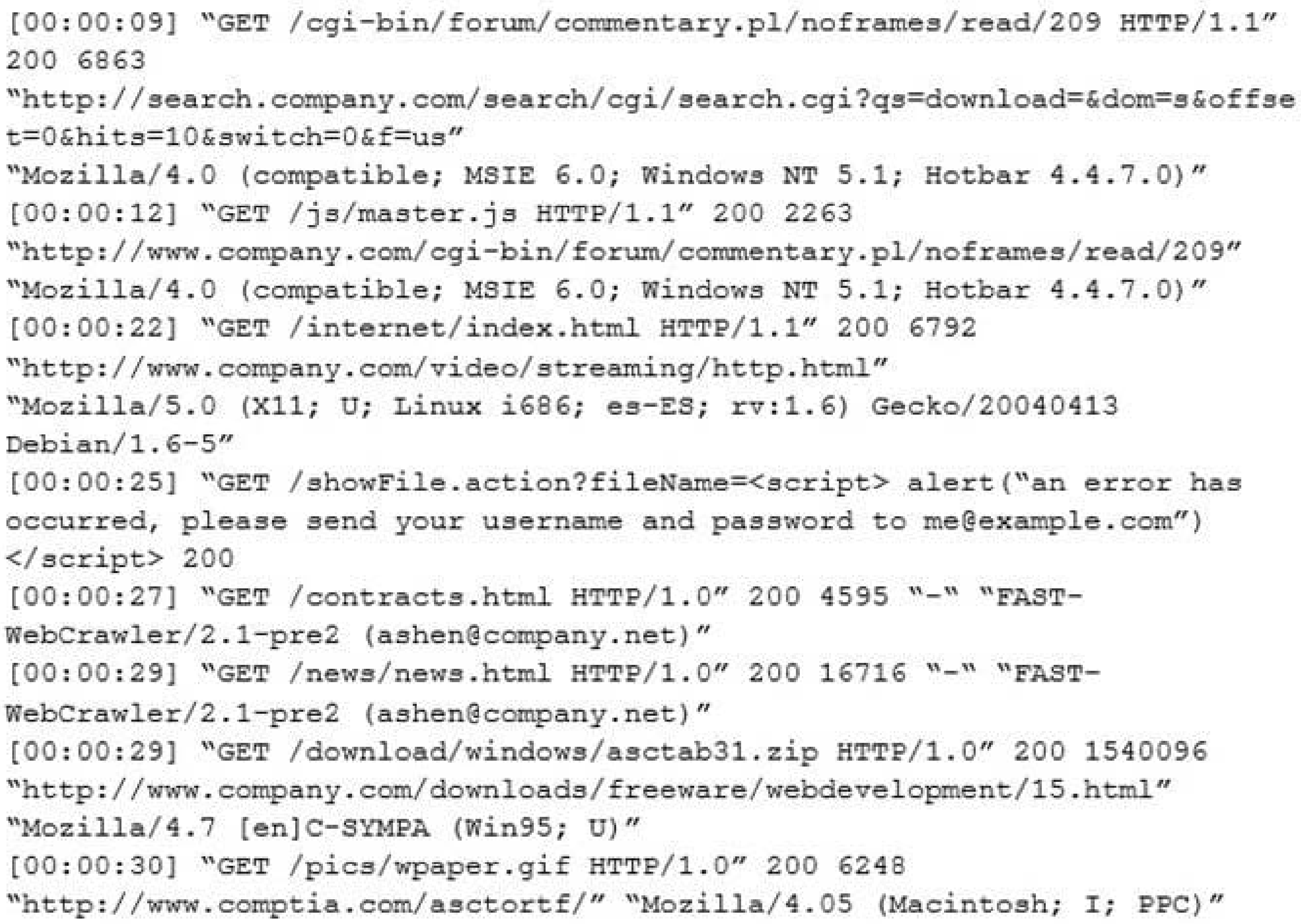
C. The change logs for the third-party libraries should be reviewed for security patches, which may need to be included in the release.

D. The application should eliminate the use of open-source libraries and products to prevent known vulnerabilities from being included.

Correct Answer: C

QUESTION 4

An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.



```
[00:00:09] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1"
200 6863
"http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offse
t=0&hits=10&switch=0&f=us"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:12] "GET /js/master.js HTTP/1.1" 200 2263
"http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:22] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5"
[00:00:25] "GET /showFile.action?fileName=<script> alert("an error has
occurred, please send your username and password to me@example.com")
</script> 200
[00:00:27] "GET /contracts.html HTTP/1.0" 200 4595 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA (Win95; U)"
[00:00:30] "GET /pics/wpaper.gif HTTP/1.0" 200 6248
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

Which of the following types of attack vector did the penetration tester use?

A. SQL injection

B. CSRF

C. Brute force

D. XSS

E. TOC/TOU

Correct Answer: B

QUESTION 5

A technician receives the following security alert from the firewall\\'s automated system:

Match_Time: 10/10/16 16:20:43 Serial: 002301028176 Device_name: COMPSEC1 Type: CORRELATION Scrusex: domain\samjones Scr: 10.50.50.150 Object_name: beacon detection Object_id: 6005 Category: compromised-host Severity: medium Evidence: host repeatedly visited a dynamic DNS domain (17 time) After reviewing the alert, which of the following is the BEST analysis?

A. the alert is a false positive because DNS is a normal network function.

B. this alert indicates a user was attempting to bypass security measures using dynamic DNS.

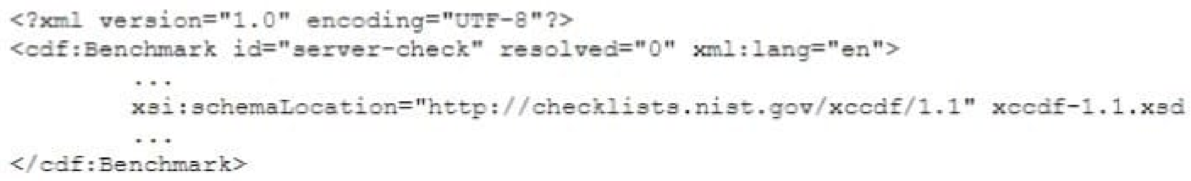
C. this alert was generated by the SIEM because the user attempted too many invalid login attempts.

D. this alert indicates an endpoint may be infected and is potentially contacting a suspect host.

Correct Answer: B

QUESTION 6

An engineer wants to assess the OS security configurations on a company\\'s servers. The engineer has downloaded some files to orchestrate configuration checks When the engineer opens a file in a text editor, the following excerpt appears:



```
<?xml version="1.0" encoding="UTF-8"?>
<cdf:Benchmark id="server-check" resolved="0" xml:lang="en">
        ...
        xsi:schemaLocation="http://checklists.nist.gov/xccdf/1.1" xccdf-1.1.xsd
        ...
</cdf:Benchmark>
```

Which of the following capabilities would a configuration compliance checker need to support to interpret this file?

A. Nessus

B. Swagger file

C. SCAP

D. Netcat

E. WSDL

Correct Answer: C

QUESTION 7

A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: "" and "". Which of the following tools BEST supports the use of these definitions?

A. HTTP interceptor

B. Static code analyzer

C. SCAP scanner

D. XML fuzzer

Correct Answer: D

QUESTION 8

A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

A. Insider threat

B. Network reconnaissance

C. Physical security

D. Industrial espionage

Correct Answer: C

If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.

However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security.

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

QUESTION 9

An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:

1.

Indemnity clauses have identified the maximum liability

2.

The data will be hosted and managed outside of the company\\'s geographical location

The number of users accessing the system will be small, and no sensitive data will be hosted in the solution. As the security consultant on the project, which of the following should the project\\'s security consultant recommend as the NEXT step?

A. Develop a security exemption, as it does not meet the security policies

B. Mitigate the risk by asking the vendor to accept the in-country privacy principles

C. Require the solution owner to accept the identified risks and consequences

D. Review the entire procurement process to determine the lessons learned

Correct Answer: C

QUESTION 10

A database administrator is required to adhere to and implement privacy principles when executing daily tasks. A manager directs the administrator to reduce the number of unique instances of PII stored within an organization\\'s systems to the greatest extent possible. Which of the following principles is being demonstrated?

A. Administrator accountability

B. PII security

C. Record transparency

D. Data minimization

Correct Answer: D

QUESTION 11

An organization is concerned that its hosted web servers are not running the most updated version of software. Which of the following would work BEST to help identify potential vulnerabilities?

A. hping3 -S comptia.org -p 80

B. nc -1 -v comptia.org -p 80

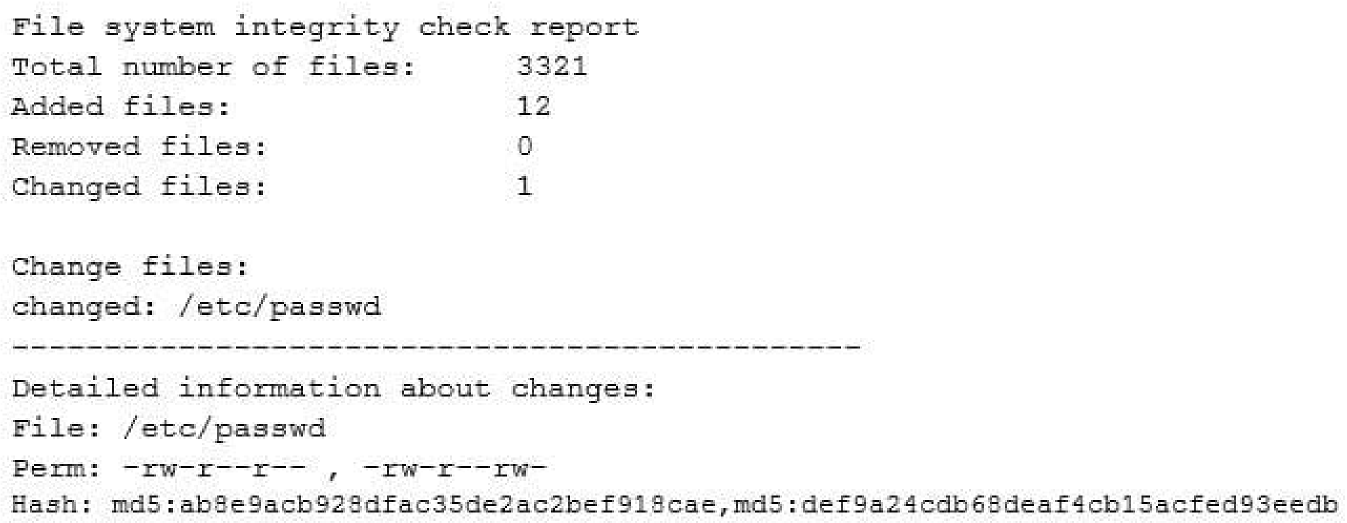
C. nmap comptia.org -p 80 -sV

D. nslookup -port=80 comptia.org

Correct Answer: C

QUESTION 12

While investigating suspicious activity on a server, a security administrator runs the following report:



```
File system integrity check report
Total number of files:      3321
Added files:                12
Removed files:              0
Changed files:              1

Change files:
changed: /etc/passwd
---------------------------------------------
Detailed information about changes:
File: /etc/passwd
Perm: -rw-r--r-- , -rw-r--rw-
Hash: md5:ab8e9acb928dfac35de2ac2bef918cae,md5:def9a24cdb68deaf4cb15acfed93eedb
```

In addition, the administrator notices changes to the /etc/shadow file that were not listed in the report. Which of the following BEST describe this scenario? (Choose two.)

A. An attacker compromised the server and may have used a collision hash in the MD5 algorithm to hide the changes to the /etc/shadow file

B. An attacker compromised the server and may have also compromised the file integrity database to hide the changes to the /etc/shadow file

C. An attacker compromised the server and may have installed a rootkit to always generate valid MD5 hashes to hide the changes to the /etc/shadow file

D. An attacker compromised the server and may have used MD5 collision hashes to generate valid passwords, allowing further access to administrator accounts on the server

E. An attacker compromised the server and may have used SELinux mandatory access controls to hide the changes to the /etc/shadow file

Correct Answer: D

QUESTION 13

A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:

The data is for internal consumption only and shall not be distributed to outside individuals The systems administrator should not have access to the data processed by the server The integrity of the kernel image is maintained

Which of the following host-based security controls BEST enforce the data owner\\'s requirements? (Choose three.)

A. SELinux

B. DLP

C. HIDS

D. Host-based firewall

E. Measured boot

F. Data encryption

G. Watermarking

Correct Answer: CEF

QUESTION 14

A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After invest the new vulnerability, it was determined that the web services providing are being impacted by this new threat. Which of the following data types a MOST likely at risk of exposure based on this new threat? (Select TWO)

A. Cardholder data

B. intellectual property

C. Personal health information

D. Employee records

E. Corporate financial data

Correct Answer: AC

QUESTION 15

A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

A. A separate physical interface placed on a private VLAN should be configured for live host operations.

B. Database record encryption should be used when storing sensitive information on virtual servers.

C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.

D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network.

Correct Answer: A

VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration.

When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

Latest CAS-003 Dumps CAS-003 Practice Test CAS-003 Braindumps