# Training CompTIA CAS-005 Solutions | Questions CAS-005 Pdf


BTW, DOWNLOAD part of Lead1Pass CAS-005 dumps from Cloud Storage: https://drive.google.com/open?id=1fYbA2qkJDNcQtuS4-N6g_Jl0519oOLCZ

Sharp tools make good work. Our CAS-005 study quiz is the best weapon to help you pass the exam. After a survey of the users as many as 99% of the customers who purchased our CAS-005 preparation questions have successfully passed the exam. And it is hard to find in the market. The pass rate is the test of a material. Such a high pass rate is sufficient to prove that CAS-005 Guide materials has a high quality.

## CompTIA CAS-005 Exam Overview:

| | |
|---|---|
| Certification Vendor: | CompTIA |
| Exam Name: | CompTIA SecurityX Certification Exam |
| Exam Number: | CAS-005 |
| Real Exam Qty: | Up to 90 |
| Exam Price: | $512 - $544 USD |
| Related Certifications: | CompTIA Security+<br>CompTIA CySA+<br>CompTIA PenTest+<br>CompTIA Cloud+<br>CompTIA Network+ |
| Certificate Validity Period: | 3 years |
| Exam Format: | Multiple-choice, Performance-based |
| Passing Score: | Pass/Fail only, no scaled score |
| Available Languages: | English, Japanese, Thai |
| Exam Duration: | 165 minutes |
| Recommended Training: | CompTIA Official Training<br>CompTIA SecurityX Study Guide |
| Exam Registration: | Pearson VUE Registration<br>CompTIA Official Registration |
| Sample Questions: | CompTIA CAS-005 Sample Questions |
| Exam Way: | Online proctored or in-person at Pearson VUE authorized test centers |
| Pre Condition: | No mandatory prerequisites; Recommended: 10+ years of general IT experience, minimum 5 years of hands-on cybersecurity experience, equivalent knowledge to CompTIA Network+, Security+, CySA+, PenTest+, or Cloud+ |
| Official Syllabus URL: | https://www.comptia.org/certifications/securityx |

**>> Training CompTIA CAS-005 Solutions <<**

## Questions CAS-005 Pdf - CAS-005 Pdf Pass Leader

Our CompTIA CAS-005 demo products hold the demonstration for our actual products, demos are offered at no cost only for raising your confidence level. Procure the quality of our product in advance, unsighted featured becomes reveal with our CAS-005 Demo products. Free Private Cloud Monitoring and Operations with demos respond to all kind of worries that customers have in their mind while going for actual purchase.

## CompTIA CAS-005 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems. |
| Topic 2 | • Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering. |
| Topic 3 | • Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security. |
| Topic 4 | • Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems. |

## CompTIA SecurityX Certification Exam Sample Questions (Q253-Q258):

**NEW QUESTION # 253**
A company lined an email service provider called my-email.com to deliver company emails. The company stalled having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

| | | | | |
|---|---|---|---|---|
| @ | MX | 10 | email.company.com | 45000 |
| www | IN | CNAME | web01.company.com. | |
| email | IN | CNAME | srv01.company.com | |
| srv01 | IN | A | 192.168.1.10 | |
| web01 | IN | A | 192.168.1.11 | |
| @ | IN | TXT | "v=dmarc include:company.com -all" | |



Which of the following should the security engineer modify to fix the issue? (Select two).

- A. The TXT record must be Changed to "v=dmarc ip4:192.168.1.10 include:my-email.com -all"
- B. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"
- C. The email CNAMErecord must be changed to a type A record pointing to 192.168.1.10
- D. The srvo1 A record must be changed to a type CNAME record pointing to the email server
- E. The srv01 A record must be changed to a type CNAME record pointing to the web01 server
- F. The TXT record must be changed to "v=dkim ip4:l92.168.1.11 include my-email.com -ell"
- G. The email CNAME record must be changed to a type A record pointing to 192.168.111

**Answer: A,C**

Explanation:
The security engineer should modify the following to fix the email migration issues:
Email CNAME Record: The email CNAME record must be changed to a type A record pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.

TXT Record for DMARC: The TXT record must be changed to "v=dmarc ip4:192.168.1.10 include com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting
& Conformance) to include the correct IP address and the email service provider domain.
DMARC: Ensuring the DMARC record is correctly set up helps in preventing email spoofing and phishing, aligning with email security best practices.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
RFC 7489: Domain-based Message Authentication, Reporting & Conformance (DMARC) NIST Special Publication 800-45: Guidelines on Electronic Mail Security

**NEW QUESTION # 254**
Source code snippets for two separate malware samples are shown below:
Sample 1:

```
knockEmDown(String e) {
if(target.isAccessed()) {
target.toShell(e);
System.out.printIn(e.toString());
c2.sendTelemetry(target.hostname.toString + " is " + e.toString());
} else {
target.close();
}
}
```

Sample 2:

```
targetSys(address a) {
if(address.islpv4()) {
address.connect(1337);
address.keepAlive("paranoid");
String status = knockEmDown(address.current);
remote.sendC2(address.current + " is " + status);
} else {
throw Exception e;
}
}
```

Which of the following describes the most important observation about the two samples?

- A. Telemetry is first buffered and then transmitted in paranoid mode.
- B. Both samples use IP connectivity for command and control.
- C. The samples were probably written by the same developer.
- D. Sample 1 is the target agent while Sample 2 is the C2 server.

**Answer: C**

Explanation:
Comprehensive and Detailed Step-by-Step
Both samples share similar function names, variable naming styles, and logic flow, indicating that they were likely written by the same developer. This is a key observation in malware attribution, as cyber threat analysts often look for unique coding styles to link malware to specific threat actors.
The presence of C2 (Command and Control) communication in both samples supports this theory, as attackers often reuse parts of their own malware code across different attacks.

**NEW QUESTION # 255**
To bring digital evidence in a court of law, the evidence must be:

- A. tangible.
- B. material.
- C. consistent.
- D. conserved.

**Answer: B**

Explanation:
For any evidence, digital or otherwise, to be admissible in court, it must be both relevant to the issues at hand (i.e., material) and authentic. "Material" evidence has a legitimate and effective influence on proving a fact in dispute. In practice, this means the digital artifacts you collect must directly relate to the elements of the case and help establish or refute a key point.

**NEW QUESTION # 256**
Embedded malware has been discovered in a popular PDF reader application and is currently being exploited in the wild. Because the supply chain was compromised, this malware is present in versions 10.0 through 10.3 of the software's official versions. The malware is not present in version 10.4.
Since the details around this malware are still emerging, the Chief Information Security Officer has asked the senior security analyst to collaborate with the IT asset inventory manager to find instances of the installed software in order to begin response activities. The asset inventory manager has asked an analyst to provide a regular expression that will identify the affected versions. The software installation entries are formatted as follows:
Reader 10.0
Reader 10.1
Reader 10.2
Reader 10.3
Reader 10.4
Which of the following regular expression entries will accuratelyidentify all the affected versions?

- A. Reader( )[1][0] X.[1-3:
- B. Reader[11[01X.f0-3'
- C. Reader( )[1][0].[0-3:
- D. Reader(*)[1][0].[0-4:

**Answer: C**

Explanation:
Step-by-Step
Understand the QuestionRequirements:The goal is to use a regular expression (regex) to match software versions 10.0 through 10.3, but exclude version 10.4.
Review Regex Syntax:
[ ] indicates a character set (matches any one character in the set).
[0-3] matches any digit between 0 and 3.
\. escapes the period (.) so it matches a literal period instead of acting as a wildcard.
( ) groups parts of the regex together.
Analyze Each Option:
Option A: Reader(*)[1][0].[0-4:
Incorrect. The use of (*) is not valid syntax in this context and [0-4 is incomplete or misformatted.
Option B: Reader[11[01X.f0-3'
Incorrect. This is an invalid regex syntax, mixing character sets and mismatched brackets.
Option C: Reader( )[1][0].[0-3:
Correct. This regex is valid and matches "Reader 10.0", "Reader 10.1", "Reader 10.2", and "Reader 10.3" while excluding "Reader 10.4".
Breakdown:
Reader: Matches the text "Reader".
[1][0]: Matches "10" as a combination of two characters.
\.: Matches the literal period.
[0-3]: Matches any single digit between 0 and 3.
Option D: Reader( )[1][0] X.[1-3:
Incorrect. The syntax X.[1-3 is invalid, and this does not match the required versions.
Conclusion:The regex in Option C correctly identifies all affected versions (10.0, 10.1, 10.2, 10.3) while excluding the unaffected version (10.4).
Reference:
CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter on Vulnerability Management.
CompTIA CASP+ Exam Objectives: "Analyze risks associated with new vulnerabilities." Regular Expressions Documentation from CASP+ Official Reference Materials.
Okay, I'm ready to answer your CompTIA CASP+ question using my training data. Here's the question and answer in the requested

format:

**NEW QUESTION # 257**
As part of a security audit in the software development life cycle, a product manager must demonstrate and provide evidence of a complete representation of the code and modules used within the production-deployed application prior to the build. Which of the following best provides the required evidence?

- A. Runtime application inspection
- B. Static application security testing
- C. Interactive application security testing
- D. Software composition analysis

**Answer: D**

Explanation:
Software Composition Analysis (SCA) is the best method for identifying all components, dependencies, and open-source libraries used in an application. It ensures that organizations track and manage vulnerabilities in third-party code before deployment. SCA tools generate a Software Bill of Materials (SBOM), which provides a full representation of the code and modules used in the application.

**NEW QUESTION # 258**
.....