

CAS-004 Exam Simulations, CAS-004 Interactive Course



BONUS!!! Download part of Itexamguide CAS-004 dumps for free: https://drive.google.com/open?id=1aJtVaLUyVl_phQqw_Q8Qe66Uu8T1vf_8

With the help of our CAS-004 training guide, your dream won't be delayed anymore. Because, we have the merits of intelligent application and high-effectiveness to help our clients study more leisurely on our CAS-004 practice questions. If you prepare with our CompTIA CASP actual exam for 20 to 30 hours, the exam will become a piece of cake in front of you. And the pass rate of our CAS-004 learning guide is high as 98% to 100%, you will be satisfied with it if you buy it.

We provide the update freely of CAS-004 exam questions within one year and 50% discount benefits if buyers want to extend service warranty after one year. The old client enjoys some certain discount when buying other exam materials. We update the CAS-004 guide torrent frequently and provide you the latest study materials which reflect the latest trend in the theory and the practice. So you can master the CAS-004 Test Guide well and pass the exam successfully. While you enjoy the benefits we bring you can pass the exam. Don't be hesitated and buy our CAS-004 guide torrent immediately!

>> CAS-004 Exam Simulations <<

CAS-004 Interactive Course | Formal CAS-004 Test

If you want to pass the exam with the shortest time, choosing us, we will achieve this for you. Our CAS-004 study materials contain the knowledge points you need to learn, through the practicing, and you will master the CAS-004 exam dumps. You just need to spend 48 to 72 hours on studying, and you can pass the exam. CAS-004 Study Materials are of high-quality, since the experienced professionals compile them, and they were quite familiar with the questions types of the exam centre.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q196-Q201):

NEW QUESTION # 196

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. Remotely wipe the device.**
- C. Set up different profiles based on the person's risk.
- D. Require MFA to access company applications.

Answer: B

Explanation:

Remotely wiping the device is the best way to secure the data on the lost device, as it would erase all the data and prevent unauthorized access. Requiring a VPN to be active to access company data may not protect the data on the device itself, as it could be stored locally or cached. Setting up different profiles based on the person's risk may not prevent data loss or theft, as it depends on the level of access and encryption. Requiring MFA to access company applications may not protect the data on the device itself, as it could be stored locally or cached. Verified References: <https://www.comptia.org/blog/what-is-byod>
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION # 197

Which of the following BEST describe the importance of maintaining chain of custody in forensic evidence collection? (Choose two.)

- **A. It ensures the integrity of the collected evidence.**
- **B. It increases the likelihood that evidence will be deemed admissible in court.**
- C. It provides automated attestation for the integrity of the collected evidence.
- D. It attests to how recently evidence was collected by recording date/time attributes.
- E. It ensures confidentiality and the need-to-know basis of forensically acquired evidence.
- F. It authenticates personnel who come in contact with evidence after collection.

Answer: A,B

Explanation:

Forensic evidence is most useful when it's complete and verifiably authentic. You can achieve the first with an expansive collection approach, even if you must pare it down later. The second requires a chain of custody documenting where the evidence was discovered, who collected it, how it was collected, and every person who handled it from then until its presentation in court. The chain of custody exists to ensure the evidence was collected legally and was not subsequently altered.

NEW QUESTION # 198

Device event logs sources from MDM software as follows:

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

- A. Resource leak; recover the device for analysis and clean up the local storage.
- **B. Impossible travel; disable the device's account and access while investigating.**
- C. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
- D. Falsified status reporting; remotely wipe the device.

Answer: B

Explanation:

The device event logs show that the device was in two different locations (New York and London) within a short time span (one hour), which indicates impossible travel. This could be a sign of a compromised device or account. The best response action is to disable the device's account and access while investigating the incident. Malicious installation of an application is not evident from the logs, nor is resource leak or falsified status reporting. Verified References: <https://www.comptia.org/blog/what-is-impossible-travel>

NEW QUESTION # 199

A systems administrator was given the following IOC to detect the presence of a malicious piece of software communicating with its command-and-control server:

post /malicious. php

User-Agent: Malicious Tool V 1.0

Host: www.malicious.com

The IOC documentation suggests the URL is the only part that could change. Which of the following regular expressions would allow the systems administrator to determine if any of the company hosts are compromised, while reducing false positives?

- A. `Host: [a-z]*\.malicious\.com`
- B. `www\. malicious\. com/malicious. php`
- C. `POST /malicious\. php`
- D. `malicious. *`
- E. `User-Agent: Malicious Tool. *`

Answer: A

Explanation:

In this case, the systems administrator should use the regex `Host: [a-z]*.malicious.com` to determine if any of the company hosts are compromised, while reducing false positives, because this regex would:

Match the Host header in the HTTP request, which specifies the domain name of the command-and-control server.

Allow any subdomain under the malicious.com domain, by using the character class `[a-z]*`, which matches zero or more lowercase letters.

Escape the dot character in the domain name, by using the backslash, which prevents it from being interpreted as a wildcard that matches any character.

Not match any other parts of the IOC that could change, such as the URL path, the User-Agent header, or the HTTP method.

NEW QUESTION # 200

Following a recent security incident on a web server the security analyst takes HTTP traffic captures for further investigation.

The analyst suspects certain jpeg files have important data hidden within them.

Which of the following tools will help get all the pictures from within the HTTP traffic captured to a specified folder?

- A. dd
- B. memdump
- C. nbtstat
- D. **tshark**

Answer: D

NEW QUESTION # 201

.....

Just choose the right Itexamguide CompTIA Advanced Security Practitioner (CASP+) Exam Questions formats and download quickly and start CAS-004 exam preparation without wasting further time. The countless CAS-004 exam candidates have already passed their dream CompTIA CAS-004 Certification Exam and they all have got help from Itexamguide CAS-004 exam questions. You can also trust Itexamguide CAS-004 exam practice test questions and start preparation right now.

CAS-004 Interactive Course: https://www.itexamguide.com/CAS-004_braindumps.html

CompTIA CAS-004 Exam Simulations We hope you can feel that we have cudgeled our brains for providing you the best study materials, CompTIA CAS-004 Exam Simulations (In case you do not receive any massage, please notice us at your available time, do not forget to check junk mailbox.) Dear examinees, firstly we feel heartfelt to meet you, and welcome to browse our website and products, Many candidates are under severe strain during the CompTIA CAS-004 examination.

A story is not done until the acceptance tests pass for all scenarios, CAS-004 This relieves any sort of anxiety in the candidate's mind before the purchase of CompTIA Advanced Security Practitioner (CASP+) Exam certification exam preparation material.

Efficient CompTIA CAS-004 Exam Simulations | Try Free Demo before Purchase

We hope you can feel that we have cudged our brains CAS-004 Test Torrent for providing you the best study materials, (In case you do not receive any massage, please notice us at your available time, do not forget to check junk mailbox.) New CAS-004 Exam Pattern Dear examinees, firstly we feel heartfelt to meet you, and welcome to browse our website and products.

Many candidates are under severe strain during the CompTIA CAS-004 examination, In this way, we have the latest CAS-004 guide torrent, Secondly, the price of the CAS-004 study materials is favourable.

- [illegible]

2026 Latest IteXamguide CAS-004 PDF Dumps and CAS-004 Exam Engine Free Share: https://drive.google.com/open?id=1aJtVaLUyVl_phQqw_Q8Qe66Uu8T1vf_8