QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

CompTIA

CAS-003

CompTIA Advanced Security Practitioner (CASP)

DEMO

Find some pages taken from full version

Killexams CAS-003 questions and answers are collected from CompTIA certified professionals who recently took and pass their exam. Our CAS-003 Exam PDF contain Organized dumps of questions and answers with references and explanations (where applicable). Our target to assemble the guide is not only to pass the exam at first attempt, but really improving your knowledge about the exam topics you are dealing with.

Following pages are for demo purpose only. Demo pages are randomly taken from full version. Full version can be different from the demo version.
You can request the updated Demo by contacting support@killexams.com.

For Details about Full version Click http://killexams.com/pass4sure/exam-detail/CAS-003

QUESTION: 93
A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

A. Begin a chain-of-custody on for the user's communication. Next, place a legal hold on the user's email account.
B. Perform an e-discover using the applicable search terms. Next, back up the user's email for a future investigation.
C. Place a legal hold on the user's email account. Next, perform e-discovery searches to collect applicable emails.
D. Perform a back up of the user's email account. Next, export the applicable emails that match the search terms.

Answer: C

Explanation:
A legal hold is a process that an organization uses to maintain all forms of pertinent information when legal action is reasonably expected. E-discovery refers to discovery in litigation or government investigations that manages the exchange of electronically stored information (ESI). ESI includes email and office documents, photos, video, databases, and other filetypes.

QUESTION: 94
A company is in the process of implementing a new front end user interface for its customers, the goal is to provide them with more self-service functionality. The application has been written by developers over the last six months and the project is currently in the test phase. Which of the following security activities should be implemented as part of the SDL in order to provide the MOST security coverage over

the solution? (Select TWO).

A. Perform unit testing of the binary code
B. Perform code review over a sampling of the front end source code
C. Perform black box penetration testing over the solution
D. Perform grey box penetration testing over the solution
E. Perform static code review over the front end source code

Answer: D, E

Explanation:
With grey box penetration testing it means that you have limited insight into the devise which would most probable by some code knowledge and this type of testing over the solution would provide the most security coverage under the circumstances.
A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization. With a static code review it is assumed that you have all the sources available for the application that is being examined. By performing a static code review over the front end source code you can provide adequate security coverage over the solution.

QUESTION: 95
A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML
B. WAYF
C. LDAP
D. RADIUS
E. Shibboleth
F. PKI

Answer: C, D

Explanation:
RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices.
LDAP and RADIUS have something in common. They‘re both mainly protocols (more than a database) which uses attributes to carry information back and forth. They‘re clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together.
RADIUS is NOT a database. It’s a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database.
RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to not only perform user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There’s no way to perform any type of such complex decisions in a user database.

QUESTION: 96
A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.
B. Require each user to log passwords used for file encryption to a decentralized repository.
C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.
D. Allow encryption only by tools that use public keys from the existing escrowed corporate PKI.

Answer: D

Explanation:
Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network.
An e-discovery policy would define how data is archived and encrypted. If the data is archived in an insecure manor, a user could be able to delete data that the user does not want to be searched. Therefore, we need to find a way of securing the data in a way that

only authorized people can access the data.
A public key infrastructure (PKI) supports the distribution and identification of public encryption keys for the encryption of data. The data can only be decrypted by the private key.
In this question, we have an escrowed corporate PKI. Escrow is an independent and licensed third party that holds something (money, sensitive data etc.) and releases it only when predefined conditions have been met. In this case, Escrow is holding the private key of the PKI.
By encrypting the e-discovery data by using the PKI public key, we can ensure that the data can only be decrypted by the private key held in Escrow and this will only happen when the predefined conditions are met.

QUESTION: 97
A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

A. RAS
B. Vulnerability scanner
C. HTTP intercept
D. HIDS
E. Port scanner
F. Protocol analyzer

Answer: D, F

Explanation:
A protocol analyzer can be used to capture and analyze signals and data traffic over a communication channel which makes it ideal for use to assess a company's network from within under the circumstances.
HIDS is used as an intrusion detection system that can monitor and analyze the internal company network especially the dynamic behavior and the state of the computer systems; behavior such as network packets targeted at that specific host, which programs accesses what resources etc.