Examcollection

http://www.ipass4sure.com/examcollection.htm

http://www.ipass4sure.com

CAS-001

CompTIA

CompTIA Advanced Security Practitioner

http://www.ipass4sure.com/exams.asp?examcode=CAS-001

The CAS-001 practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The CAS-001 Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently.
The CAS-001 exam is very challenging, but with our CAS-001 questions and answers practice exam, you can feel confident in obtaining your success on the CAS-001 exam on your FIRST TRY!

CompTIA CAS-001 Exam Features

- Detailed questions and answers for CAS-001 exam
- Try a demo before buying any CompTIA exam
- CAS-001 questions and answers, updated regularly
- Verified CAS-001 answers by Experts and bear almost 100% accuracy
- CAS-001 tested and verified before publishing
- CAS-001 examcollection vce questions with exhibits
- CAS-001 same questions as real exam with multiple choice options

Acquiring CompTIA certifications are becoming a huge task in the field of I.T. More over these exams like CAS-001 exam are now continuously updating and accepting this challenge is itself a task. This CAS-001 test is an important part of CompTIA certifications. We have the resources to prepare you for this. The CAS-001 exam is essential and core part of CompTIA certifications and once you clear the exam you will be able to solve the real life problems yourself.Want to take advantage of the Real CAS-001 Test and save time and money while developing your skills to pass your CompTIA CAS-001 Exam? Let us help you climb that ladder of success and pass your CAS-001 now!

DEMO EXAM

For Full Version visit

http://www.ipass4sure.com/allexams.asp

QUESTION: 1
You need to ensure that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future?

A. Perfect forward secrecy
B. Secure socket layer
C. Secure shell
D. Security token

Answer: A

Explanation:
Perfect forward secrecy (or PFS) is the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.Forward secrecy has been used as a synonym for perfect forward secrecy, since the term perfect has been controversial in this context. However, at least one reference distinguishes perfect forward secrecy from forward secrecy with the additional property that an agreed key will not be compromised even if agreed keys derived from the same long-term keying material in a subsequent run are compromised. Answer option C is incorrect. Secure Shell (SSH) is a program that is used for logging into a remote computer over a network. Secure Shell can be used to execute commands on a remote machine and to move files from one machine to another. SSH uses strong authentication and secure communications over insecure channels. Answer option B is incorrect. Secure Sockets Layer (SSL) is a protocol that was developed by Netscape for transmitting private documents via the Internet. It uses a cryptographic system thatuses public and private keys to encrypt data. A public key is globally available and a private key is known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support the SSL protocol. Several web sites use this protocol to obtain confidential user information. When the SSL protocol is used to connect to a Web site, the URL must begin with https instead of http. Answer option D is incorrect. Security token can be a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens. Security tokens are used to prove one's identity electronically (as in the case of a customer trying to access his bank account). The token is used in addition to or in place of a password to prove that the customer is who he claims to be. The token acts like an electronic key to access something.

QUESTION: 2
The Security Development Lifecycle (SDL) consists of various security practices that are grouped under seven phases. Which of the following security practices are included in the Requirements phase? Each correct answer represents a complete solution. Choose all that apply.

A. Incident Response Plan
B. Create Quality Gates/Bug Bars

C. Attack Surface Analysis/Reduction
D. Security and Privacy Risk Assessment

Answer: B, D

Explanation:
The Requirements phase of the Security Development Lifecycle (SDL) includes the following security practices:
• Security and Privacy Requirements
• Create Quality Gates/Bug Bars
• Security and Privacy Risk Assessment
Answer option C is incorrect. Attack Surface Analysis/Reduction is a security practice included in the Design phase of the Security Development Lifecycle (SDL). Answer option A is incorrect. Incident Response Plan is a security practice included in the Release phase of the Security Development Lifecycle (SDL).

QUESTION: 3
Which of the following components of a VoIP network is frequently used to bridge video conferencing connections?

A. MCU
B. Videoconference station
C. IP Phone
D. Call agent

Answer: A

Explanation:
A Multipoint Control Unit (MCU) is a device frequently used to bridge video conferencing connections. The Multipoint Control Unit is an endpoint on the LAN that provides the ability for 3 or more terminals and gateways to participate in a multipoint conference. The MCU consists of a mandatory Multipoint Controller (MC) and optional Multipoint Processors (MPs). Answer option C is incorrect. IP Phones provide IP endpoints for voice communication. Answer option D is incorrect. A call agent provides call control for IP phones, CAC, bandwidth control and management, and address translation. Unlike a gatekeeper, which in a Cisco environment typically runs on a router, a call agent typically runs on a server platform. Cisco Unified Communications Manager is an example of a call agent. The call agent controls switching logic and calls for all the sites under the central controller. A central gateway controller includes both centralized configuration and maintenance of call control functionality, when new functionality needs to be added, only the controller needs to be updated. Answer option B is incorrect. A videoconference station provides access for end-user involvement in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. A user can view video streams and hear audio that originates at a remote user station.

QUESTION: 4
Which of the following is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies?

A. SAML
B. SOAP
C. SPML
D. XACML

Answer: D

Explanation:
XACML stands for extensible Access Control Markup Language. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies. Latest version 2.0 was ratified by OASIS standards organization on 1 February 2005. The planned version 3.0 will add generic attribute categories for the evaluation context and policy delegation profile (administrative policy profile). Answer option B is incorrect. SOAP, defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks, it relies on extensible Markup Language as its message format, and usually relies on other Application Layer protocols for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built. Answer option C is incorrect. Service Provisioning Markup Language (SPML) is an XML-based framework developed by OASIS (Organization for the Advancement of Structured Information Standards). It is used to exchange user, resource and service provisioning information between cooperating organizations. SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations. SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations. Answer option A is incorrect. Security Assertion Markup Language (SAMLJ is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

QUESTION: 5

You work as a Network Administrator for uCertify Inc. You want to allow some users to access a particular program on the computers in the network. What will you do to accomplish this task?

A. Apply remote access policies
B. Apply NTFS permissions
C. Apply group policies
D. Apply account policies

Answer: C

Explanation:
In order to accomplish the task, you should apply group policy in the network. A group policy that is created by an administrator affects all users on a computer or all users on a domain. Group policies can be used for defining, customizing, and controlling the functioning of network resources, computers, and operating systems. They can be set for a single computer with multiple users, for users in workgroups, or for computers in a domain. Administrators can configure group policy settings for users as well as for computers in many ways. Group policies can be used to allow or restrict the access of a particular program by a particular user. It can also be used to configure the desktop, the Start menu, the taskbar. the Control Panel, security settings, among other things. In Windows XP, group policies can be configured by using the Group Policy Console dialog box, which can be opened by running the GPEDIT.MSC command from the Start menu. Answer option D is incorrect. An account policy controls the password expiration policy, the lockout policy, and other password features. Answer option B is incorrect. NTFS permissions are attributes of the folder or file for which they are configured. These include both standard and special levels of settings. The standard settings are combinations of the special permissions which make the configuration more efficient and easier to establish. Answer option A is incorrect. A remote access policy specifies how remote users can connect to the network and the requirements for each of their systems before they are allowed to connect. It defines the methods users can use to connect remotely such as dial up or VPN. This policy is used to prevent damage to the organizational network or computer systems and to prevent compromise or loss of data.

QUESTION: 6
Which of the following is the most secure authentication scheme and uses a public key cryptography and digital certificate to authenticate a user?

A. Form-based authentication
B. Basic authentication
C. Digest authentication
D. Certificate-based authentication

Answer: D

Explanation:
Certificate-based authentication is the most secure authentication scheme. A certificate-based authentication scheme is a scheme that uses a public key cryptography and digital certificate to authenticate a user. A digital certificate is an electronic document that includes identification information, public key, and the digital signature of a certification authority based on that certification authority's private key. When a user connects to the server, he presents his digital certificate containing the public key and the signature of the certification authority. The server verifies the validity of the signature and whether the certificate has been provided by a trusted certificate authority or not. The server then authenticates the user by using public key cryptography to prove that the user truly holds the private key associated with the certificate. Answer option B is incorrect. Basic authentication is a simple method of authentication that provides minimum security. It should be used only when security is not critical because basic authentication requests are not encrypted. Answer option A is incorrect. Form-based authentication Form-based authentication allows users to create their own custom forms. It requires session tracking for the authentication, so that the container may use the login form. It is not a secure authentication scheme. Answer option C is incorrect. Digest authentication is a secure authentication method in which passwords are sent across a network as a hash value rather than as clear text. It is a more secure authentication method as compared to Basic authentication. Digest authentication works across proxy servers and firewalls.

QUESTION: 7
Which of the following security practices are included in the Implementation phase of the Security Development Lifecycle (SDL)? Each correct answer represents a complete solution. Choose two.

A. Establish Design Requirements
B. Perform Static Analysis
C. Use Approved Tools
D. Execute Incident Response Plan

Answer: A, B

Explanation:
Security practices performed during each phase of the Security Development Lifecycle (SDL) process are as follows:

Phases	Security Practices
Training	• Core Security Training
Requirements	• Security and Privacy Requirements • Create Quality Gates/Bug Bars • Security and Privacy Risk Assessment
Design	• Establish Design Requirements • Attack Surface Analysis/Reduction • Threat Modeling
Implementation	• Use Approved Tools • Deprecate Unsafe Functions • Perform Static Analysis
Verification	• Perform Dynamic Analysis • Fuzz Testing • Attack Surface Review
Release	• Incident Response Plan • Final Security Review • Release/Archive
Response	• Execute Incident Response Plan

C:\Documents and Settings\user-nwz\Desktop\1.JPG

QUESTION: 8
In which of the following activities an organization identifies and prioritizes technical, organizational, procedural, administrative, and physical security weaknesses?

A. Social engineering

B. Vulnerability assessment
C. White box testing
D. Penetration testing

Answer: B

Explanation:
A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed for include, but are not limited to, nuclear power plants, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems. Vulnerability is the most reliable weakness that any programming code faces.These programming codesmay be buffer overflow, xss, sql injection, etc. A piece of malware code that takes advantage of a newly announced vulnerability in a software application, usually the operating system or a Web server, is known as an exploit. Answer option C is incorrect. White box is one of the three levels of penetration testing performed for an organization or network. This final level simulates an attacker with extensive knowledge of the organization and its infrastructure and security controls. The knowledge would come either from independent research and information gathering or from a trusted inside source with full knowledge of the network and its defenses. Answer option A is incorrect. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user's computer or network. This method involves mental ability of people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name, password, computer name. IP address, employee ID, or other information that can be misused. Answer option D is incorrect. A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit.

QUESTION: 9
SDLC phases include a minimum set of security tasks that are required to effectively incorporate security in the system development process. Which of the following are the key security activities for the development/acquisition phase? Each correct answer represents a complete solution. Choose two.

A. Prepare initial documents for system certification and accreditation

Pass4sure Certification Exam Features;

- Pass4sure offers over **2500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **120** Global Certification Vendors Covered.
- Services of Professional & Certified Experts available via support.
- Free 90 days updates to match real exam scenarios.
- Instant Download Access! No Setup required.
- Price as low as $19, which is 80% more cost effective than others.
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (Android, iPhone, iPod, iPad)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- ***Guaranteed Success***.
- **Fast**, helpful support 24x7.

View list of All certification exams offered;
http://www.ipass4sure.com/allexams.asp

View list of All Study Guides (SG);
http://www.ipass4sure.com/study-guides.asp

View list of All Audio Exams (AE);
http://www.ipass4sure.com/audio-exams.asp

Download Any Certication Exam DEMO.
http://www.ipass4sure.com/samples.asp

To purchase Full version of exam click below;
http://www.ipass4sure.com/allexams.asp

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

and many others.. See complete list Here