Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

SSCP MCQs
SSCP TestPrep
SSCP Study Guide
SSCP Practice Test
SSCP Exam Questions



ISC2

SSCP

Systems Security Certified Practioner

A Black Hat is someone who uses his skills for offensive purpose. They do not seek authorization before they attempt to comprise the security mechanisms in place. "Grey Hats" are people who sometimes work as a White hat and other times they will work as a "Black Hat", they have not made up their mind yet as to which side they prefer to be.
The following are incorrect answers:
All the other choices could be possible reasons but the best one today is really for financial gains.
References used for this question:
http://library.thinkquest.org/04oct/00460/crimeMotives.html and
http://www.informit.com/articles/article.aspx?p=1160835 and
http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb006.pdf

QUESTION: 371
What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?

A. Data fiddling
B. Data diddling
C. Salami techniques
D. Trojan horses

Answer: C

Explanation:
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 644.

QUESTION: 372
Java is not:

A. Object-oriented.
B. Distributed.
C. Architecture Specific.
D. Multithreaded.

Answer: C

Explanation:
JAVA was developed so that the same program could be executed on multiple hardware and operating system platforms, it is not Architecture Specific.
The following answers are incorrect:

Object-oriented. Is not correct because JAVA is object-oriented. It should use the object- oriented programming methodology.
Distributed. Is incorrect because JAVA was developed to be able to be distrubuted, run on multiple computer systems over a network.
Multithreaded. Is incorrect because JAVA is multi-threaded that is calls to subroutines as is the case with object-oriented programming.
A virus is a program that can replicate itself on a system but not necessarily spread itself by network connections.

QUESTION: 373
What is malware that can spread itself over open network connections?

A. Worm
B. Rootkit
C. Adware
D. Logic Bomb

Answer: A

Explanation:
Computer worms are also known as Network Mobile Code, or a virus-like bit of code that can replicate itself over a network, infecting adjacent computers.
A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
A notable example is the SQL Slammer computer worm that spread globally in ten minutes on January 25, 2003. I myself came to work that day as a software tester and found all my SQL servers infected and actively trying to infect other computers on the test network.
A patch had been released a year prior by Microsoft and if systems were not patched and exposed to a 376 byte UDP packet from an infected host then system would become compromised.
Ordinarily, infected computers are not to be trusted and must be rebuilt from scratch but the vulnerability could be mitigated by replacing a single vulnerable dll called sqlsort.dll.
Replacing that with the patched version completely disabled the worm which really illustrates to us the importance of actively patching our systems against such network mobile code.
The following answers are incorrect:
- Rootkit: Sorry, this isn't correct because a rootkit isn't ordinarily classified as network mobile code like a worm is. This isn't to say that a rootkit couldn't be included in a worm, just that a rootkit isn't usually classified like a worm. A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of

certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.
- Adware: Incorrect answer. Sorry but adware isn't usually classified as a worm. Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.
- Logic Bomb: Logic bombs like adware or rootkits could be spread by worms if they exploit the right service and gain root or admin access on a computer.
The following reference(s) was used to create this question:
The CCCure CompTIA Holistic Security+ Tutorial and CBT and
http://en.wikipedia.org/wiki/Rootkit and
http://en.wikipedia.org/wiki/Computer_worm and
http://en.wikipedia.org/wiki/Adware

QUESTION: 374
Which of the following technologies is a target of XSS or CSS (Cross-Site Scripting) attacks?

A. Web Applications
B. Intrusion Detection Systems
C. Firewalls
D. DNS Servers

Answer: A

Explanation:
XSS or Cross-Site Scripting is a threat to web applications where malicious code is placed on a website that attacks the use using their existing authenticated session status. Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.
An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information

retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.
Mitigation:
Configure your IPS - Intrusion Prevention System to detect and suppress this traffic.
Input Validation on the web application to normalize inputted data.
Set web apps to bind session cookies to the IP Address of the legitimate user and only permit that IP Address to use that cookie.
See the XSS (Cross Site Scripting) Prevention Cheat Sheet See the Abridged XSS Prevention Cheat Sheet
See the DOM based XSS Prevention Cheat Sheet
See the OWASP Development Guide article on Phishing.
See the OWASP Development Guide article on Data Validation. The following answers are incorrect:
Intrusion Detection Systems: Sorry. IDS Systems aren't usually the target of XSS attacks but a properly-configured IDS/IPS can "detect and report on malicious string and suppress the TCP connection in an attempt to mitigate the threat.
Firewalls: Sorry. Firewalls aren't usually the target of XSS attacks.
DNS Servers: Same as above, DNS Servers aren't usually targeted in XSS attacks but they play a key role in the domain name resolution in the XSS attack process.
The following reference(s) was used to create this question:
CCCure Holistic Security+ CBT and Curriculum and
https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

QUESTION: 375
Which of the following should be performed by an operator?

A. Changing profiles
B. Approving changes
C. Adding and removal of users
D. Installing system software

Answer: D

Explanation:
Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment.
Source: MOSHER, Richard & ROTHKE, Ben, CISSP CBK Review presentation on domain 7.

QUESTION: 376
At which of the basic phases of the System Development Life Cycle are security requirements formalized?

A. Disposal
B. System Design Specifications

C. Development and Implementation
D. Functional Requirements Definition

Answer: D

Explanation:
During the Functional Requirements Definition the project management and systems development teams will conduct a comprehensive analysis of current and possible future functional requirements to ensure that the new system will meet end-user needs. The teams also review the documents from the project initiation phase and make any revisions or updates as needed. For smaller projects, this phase is often subsumed in the project initiation phase. At this point security requirements should be formalized.
The Development Life Cycle is a project management tool that can be used to plan, execute, and control a software development project usually called the Systems Development Life Cycle (SDLC).
The SDLC is a process that includes systems analysts, software engineers, programmers, and end users in the project design and development. Because there is no industry-wide SDLC, an organization can use any one, or a combination of SDLC methods.
The SDLC simply provides a framework for the phases of a software development project from defining the functional requirements to implementation. Regardless of the method used, the SDLC outlines the essential phases, which can be shown together or as separate elements. The model chosen should be based on the project. For example, some models work better with long-term, complex projects, while others are more suited for short-term projects. The key element is that a formalized SDLC is utilized.
The number of phases can range from three basic phases (concept, design, and implement) on up.
The basic phases of SDLC are:
Project initiation and planning Functional requirements definition System design specifications Development and implementation
Documentation and common program controls
Testing and evaluation control, (certification and accreditation) Transition to production (implementation)
The system life cycle (SLC) extends beyond the SDLC to include two additional phases: Operations and maintenance support (post-installation)
Revisions and system replacement
System Design Specifications
This phase includes all activities related to designing the system and software. In this phase, the system architecture, system outputs, and system interfaces are designed. Data input, data flow, and output requirements are established and security features are designed, generally based on the overall security architecture for the company.
Development and Implementation
During this phase, the source code is generated, test scenarios and test cases are developed, unit and integration testing is conducted, and the program and system are documented for maintenance and for turnover to acceptance testing and production. As well as general care for software quality, reliability, and consistency of operation,

particular care should be taken to ensure that the code is analyzed to eliminate common vulnerabilities that might lead to security exploits and other risks.

Documentation and Common Program Controls

These are controls used when editing the data within the program, the types of logging the program should be doing, and how the program versions should be stored. A large number of such controls may be needed, see the reference below for a full list of controls.

Acceptance

In the acceptance phase, preferably an independent group develops test data and tests the code to ensure that it will function within the organization's environment and that it meets all the functional and security requirements. It is essential that an independent group test the code during all applicable stages of development to prevent a separation of duties issue. The goal of security testing is to ensure that the application meets its security requirements and specifications. The security testing should uncover all design and implementation flaws that would allow a user to violate the software security policy and requirements. To ensure test validity, the application should be tested in an environment that simulates the production environment. This should include a security certification package and any user documentation.

Certification and Accreditation (Security Authorization)

Certification is the process of evaluating the security stance of the software or system against a predetermined set of security standards or policies. Certification also examines how well the system performs its intended functional requirements. The certification or evaluation document should contain an analysis of the technical and nontechnical security features and countermeasures and the extent to which the software or system meets the security requirements for its mission and operational environment.

Transition to Production (Implementation)

During this phase, the new system is transitioned from the acceptance phase into the live production environment. Activities during this phase include obtaining security accreditation; training the new users according to the implementation and training schedules; implementing the system, including installation and data conversions; and, if necessary, conducting any parallel operations.

Revisions and System Replacement

As systems are in production mode, the hardware and software baselines should be subject to periodic evaluations and audits. In some instances, problems with the application may not be defects or flaws, but rather additional functions not currently developed in the application. Any changes to the application must follow the same SDLC and be recorded in a change management system. Revision reviews should include security planning and procedures to avoid future problems. Periodic application audits should be conducted and include documenting security incidents when problems occur. Documenting system failures is a valuable resource for justifying future system enhancements.

Below you have the phases used by NIST in it's 800-63 Revision 2 document

As noted above, the phases will vary from one document to another one. For the purpose of the exam use the list provided in the official ISC2 Study book which is presented in short form above. Refer to the book for a more detailed description of activities at each of the phases of the SDLC.

However, all references have very similar steps being used. As mentioned in the official book, it could be as simple as three phases in it's most basic version (concept,

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.