New CISSP Braindumps Ebook & CISSP Training For Exam

2026 Latest RealValidExam CISSP PDF Dumps and CISSP Exam Engine Free Share: https://drive.google.com/open?id=14A64N64TlenDmvFL6dxBiNoNADN1RUpE

Preparing authentic ISC CISSP questions in the form of a PDF file is significant because it is the only choice that guarantees your success in the CISSP exam. ISC CISSP PDF questions are accessible without any installation. You will need a few days to prepare successfully for the CISSP Exam if you have RealValidExam's ISC Exam PDF Questions. This PDF file of ISC CISSP questions is supported by any device like laptops, tablets, and smartphones.

The CISSP exam is offered by the International Information System Security Certification Consortium (ISC) and is designed for professionals who have at least five years of experience in the information security field. Certified Information Systems Security Professional (CISSP) certification is highly valued by employers as it demonstrates an individual’s knowledge and expertise in information security. In addition, it provides a competitive edge to professionals seeking career advancement in this field.

The ISC CISSP exam consists of 250 multiple-choice questions, which are designed to test the candidate's knowledge and skills in eight security domains. These domains include security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security. CISSP Exam is designed to be challenging, and candidates are required to have a minimum of five years of professional experience in at least two of the eight domains or four years of experience with a relevant degree. Passing the exam requires a score of 700 out of 1000 points, and the certification is valid for three years.

>> New CISSP Braindumps Ebook <<

CISSP Training For Exam - CISSP Certification Book Torrent

With our numerous advantages of our CISSP latest questions and service, what are you hesitating for? Our company always serves our clients with professional and precise attitudes on our CISSP exam questions, and we know that your satisfaction is the most important thing for us. We always aim to help you pass the CISSP Exam smoothly and sincerely hope that all of our candidates can enjoy the tremendous benefit of our CISSP exam material, which might lead you to a better future! And the high pass rate of CISSP learning material as 99% to 100% won't let you down.

To become a CISSP, candidates must demonstrate a minimum of five years of professional experience in the information security industry. They must also pass the CISSP exam, which consists of 250 multiple-choice questions and takes six hours to complete. CISSP Exam is challenging, and only those who have a solid understanding of the various domains of information security can pass it.

ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q1813-Q1818):

NEW QUESTION # 1813
Which of the following is NOT a common integrity goal?

- A. Maintain internal and external consistency.
- B. Prevent paths that could lead to inappropriate disclosure.
- C. Prevent unauthorized users from making modifications.
- D. Prevent authorized users from making improper modifications.

Answer: B

Explanation:
Inappropriate disclosure is a confidentiality, not an integrity goal.
All of the other choices above are integrity goals addressed by the Clark-Wilson integrity model.
The Clark-Wilson model is an integrity model that addresses all three integrity goals:
1. prevent unauthorized users from making modifications,
2. prevent authorized users from making improper modifications, and
3. maintain internal and external consistency through auditing.
NOTE: Biba address only the first goal of integrity above
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill. Kindle Edition.

NEW QUESTION # 1814
What is the 802.11 standard related to?

- A. Wireless network communications
- B. The OSI/ISO model
- C. Public Key Infrastructure (PKI)
- D. Packet-switching technology

Answer: A

Explanation:
The 802.11 standard outlines how wireless clients and APs communicate, lays out
the specifications of their interfaces, dictates how signal transmission should take place, and
describes how authentication, association, and security should be implemeted.
The following answers are incorrect:
Public Key Infrastructure (PKI) Public Key Infrastructure is a supporting infrastructure to manage
public keys. It is not part of the IEEE 802 Working Group standard.
Packet-switching technology A packet-switching technology is not included in the IEEE 802
Working Group standard. It is a technology where-in messages are broken up into packets, which
then travel along different routes to the destination.
The OSI/ISO model The Open System Interconnect model is a sevel-layer model defined as an
international standard describing network communications.
The following reference(s) were/was used to create this question:
Source: Shon Harris - "All-in-One CISSP Exam Guide" Fourth Edition; Chapter 7 -
Telecommunications and Network Security: pg. 624.
802.11 refers to a family of specifications developed by the IEEE for Wireless LAN technology.
802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997. There are several specifications in the 802.11 family:
802.11 # applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). 802.11a # an extension to 802.11 that applies to wireless

LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS. 802.11b (also referred to as 802.11 High Rate or Wi-Fi) # an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4
GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11
standard, allowing wireless functionality comparable to Ethernet.
802.11g # applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.
Source: 802.11 Planet's web site.

NEW QUESTION # 1815
In most security protocols that support authentication, integrity and confidentiality,

- A. Public key cryptography is used to create digital signatures.
- B. Private key cryptography is used to create digital signatures.
- C. DES is used to create digital signatures.
- D. Digital signatures are not implemented.

Answer: A

Explanation:
The correct answer is "Public key cryptography is used to create digital signatures.".
Answer "Private key cryptography is used to create digital signatures" is incorrect because private key cryptography does not create digital signatures.
Answer "DES is used to create digital signatures" is incorrect because DES is a private key system and, therefore, follows the same logic as in "Private key cryptography is used to create digital signatures"; and answer "Digital signatures are not implemented" is incorrect because digital signatures are implemented to obtain authentication and integrity.

NEW QUESTION # 1816
What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?

- A. Accountability controls
- B. Assurance procedures
- C. Administrative controls
- D. Mandatory access controls

Answer: B

Explanation:
Controls provide accountability for individuals accessing information. Assurance procedures ensure that access control mechanisms correctly implement the security policy for the entire life cycle of an information system. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION # 1817
Which of the following technologies is a target of XSS or CSS (Cross-Site Scripting) attacks?

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

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:
https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

NEW QUESTION # 1818
......

id=14A64N64TlenDmvFL6dxBiNoNADN1RUpE