CHAPTER

Becoming a CISSP

This chapter presents the following:

- Description of the CISSP certification
- Reasons to become a CISSP
- What the CISSP exam entails
- The Common Body of Knowledge and what it contains
- The history of $(ISC)^2$ and the CISSP exam
- An assessment test to gauge your current knowledge of security

This book is intended not only to provide you with the necessary information to help you gain a CISSP certification, but also to welcome you into the exciting and challenging world of security.

The Certified Information Systems Security Professional (CISSP) exam covers ten different subject areas, more commonly referred to as *domains*. The subject matter of each domain can easily be seen as its own area of study, and in many cases individuals work exclusively in these fields as experts. For many of these subjects, you can consult and reference extensive resources to become an expert in that area. Because of this, a common misconception is that the only way to succeed at the CISSP exam is to immerse yourself in a massive stack of texts and study materials. Fortunately, an easier approach exists. By using this sixth edition of the *CISSP All-in-One Exam Guide*, you can successfully complete and pass the CISSP exam and achieve your CISSP certification. The goal of this book is to combine into a single resource all the information you need to pass the CISSP exam and help you understand how the domains interact with each other so that you can develop a comprehensive approach to security practices. This book should also serve as a useful reference tool long after you've achieved your CISSP certification.

Why Become a CISSP?

As our world changes, the need for improvements in security and technology continues to grow. Security was once a hot issue only in the field of technology, but now it is becoming more and more a part of our everyday lives. Security is a concern of every organization, government agency, corporation, and military unit. Ten years ago *computer and information security* was an obscure field that only concerned a few people. Because the risks were essentially low, few were interested in security expertise.

Things have changed, however, and today corporations and other organizations are desperate to recruit talented and experienced security professionals to help protect the resources they depend on to run their businesses and to remain competitive. With a CISSP certification, you will be seen as a security professional of proven ability who has successfully met a predefined standard of knowledge and experience that is well understood and respected throughout the industry. By keeping this certification current, you will demonstrate your dedication to staying abreast of security developments.

Consider the reasons for attaining a CISSP certification:

- To meet the growing demand and to thrive in an ever-expanding field
- To broaden your current knowledge of security concepts and practices
- To bring security expertise to your current occupation
- To become more marketable in a competitive workforce
- To show a dedication to the security discipline
- To increase your salary and be eligible for more employment opportunities

The CISSP certification helps companies identify which individuals have the ability, knowledge, and experience necessary to implement solid security practices; perform risk analysis; identify necessary countermeasures; and help the organization as a whole protect its facility, network, systems, and information. The CISSP certification also shows potential employers you have achieved a level of proficiency and expertise in skill sets and knowledge required by the security industry. The increasing importance placed on security in corporate success will only continue in the future, leading to even greater demands for highly skilled security professionals. The CISSP certification shows that a respected third-party organization has recognized an individual's technical and theoretical knowledge and expertise, and distinguishes that individual from those who lack this level of knowledge.

Understanding and implementing security practices is an essential part of being a good network administrator, programmer, or engineer. Job descriptions that do not specifically target security professionals still often require that a potential candidate have a good understanding of security concepts as well as how to implement them. Due to staff size and budget restraints, many organizations can't afford separate network and security staffs. But they still believe security is vital to their organization. Thus, they often try to combine knowledge of technology and security into a single role. With a CISSP designation, you can put yourself head and shoulders above other individuals in this regard.

The CISSP Exam

Because the CISSP exam covers the ten domains making up the CISSP Common Body of Knowledge (CBK), it is often described as being "an inch deep and a mile wide," a reference to the fact that many questions on the exam are not very detailed and do not require you to be an expert in every subject. However, the questions do require you to be familiar with many *different* security subjects.

The CISSP exam comprises 250 multiple-choice questions, and you have up to six hours to complete it. The questions are pulled from a much larger question bank to ensure the exam is as unique as possible for each entrant. In addition, the test bank constantly changes and evolves to more accurately reflect the real world of security. The exam questions are continually rotated and replaced in the bank as necessary. Each question has four answer choices, only one of which is correct. Only 225 questions are graded, while 25 are used for research purposes. The 25 research questions are integrated into the exam, so you won't know which go toward your final grade. To pass the exam, you need a minimum raw score of 700 points out of 1,000. Questions are weighted based on their difficulty; not all questions are worth the same number of points. The exam is not product- or vendor-oriented, meaning no questions will be specific to certain products or vendors (for instance, Windows, Unix, or Cisco). Instead, you will be tested on the security models and methodologies used by these types of systems.

$(ISC)^2$, which stands for International Information Systems Security Certification Consortium, has also added scenario-based questions to the CISSP exam. These questions present a short scenario to the test taker rather than asking the test taker to identify terms and/or concepts. The goal of the scenario-based questions is to ensure that test takers not only know and understand the concepts within the CBK, but also can apply this knowledge to real-life situations. This is more practical because in the real world, you won't be challenged by having someone asking you "What is the definition of collusion?" You need to know how to detect and prevent collusion from taking place, in addition to knowing the definition of the term.

After passing the exam, you will be asked to supply documentation, supported by a sponsor, proving that you indeed have the type of experience required to obtain this certification. The sponsor must sign a document vouching for the security experience you are submitting. So, make sure you have this sponsor lined up prior to registering for the exam and providing payment. You don't want to pay for and pass the exam, only to find you can't find a sponsor for the final step needed to achieve your certification.

The reason behind the sponsorship requirement is to ensure that those who achieve the certification have real-world experience to offer organizations. Book knowledge is extremely important for understanding theory, concepts, standards, and regulations, but it can never replace hands-on experience. Proving your practical experience supports the relevance of the certification.

A small sample group of individuals selected at random will be audited after passing the exam. The audit consists mainly of individuals from $(ISC)^2$ calling on the candidates' sponsors and contacts to verify the test taker's related experience.

What makes this exam challenging is that most candidates, although they work in the security field, are not necessarily familiar with all ten CBK domains. If a security professional is considered an expert in vulnerability testing or application security, for example, she may not be familiar with physical security, cryptography, or forensics. Thus, studying for this exam will broaden your knowledge of the security field.

The exam questions address the ten CBK security domains, which are described in Table 1-1.

Domain	Description
Access Control	This domain examines mechanisms and methods used to enable administrators and managers to control what subjects can access, the extent of their capabilities after authorization and authentication, and the auditing and monitoring of these activities. Some of the topics covered include • Access control threats • Identification and authentication technologies and techniques • Access control administration • Single sign-on technologies • Attack methods
Telecommunications and Network Security	This domain examines internal, external, public, and private communication systems; networking structures; devices; protocols; and remote access and administration. Some of the topics covered include • OSI model and layers • Local area network (LAN), metropolitan area network (MAN), and wide area network (WAN) technologies • Internet, intranet, and extranet issues • Virtual private networks (VPNs), firewalls, routers, switches, and repeaters • Network topologies and cabling • Attack methods
Information Security Governance and Risk Management	This domain examines the identification of company assets, the proper way to determine the necessary level of protection required, and what type of budget to develop for security implementations, with the goal of reducing threats and monetary loss. Some of the topics covered include • Data classification • Policies, procedures, standards, and guidelines • Risk assessment and management • Personnel security, training, and awareness
Software Development Security	This domain examines secure software development approaches, application security, and software flaws. Some of the topics covered include • Data warehousing and data mining • Various development practices and their risks • Software components and vulnerabilities • Malicious code
Cryptography	This domain examines cryptography techniques, approaches, and technologies. Some of the topics covered include • Symmetric versus asymmetric algorithms and uses • Public key infrastructure (PKI) and hashing functions • Encryption protocols and implementation • Attack methods

Table 1-1 Security Domains That Make Up the CISSP CBK

Domain	Description
Security Architecture and Design	This domain examines ways that software should be designed securely. It also covers international security measurement standards and their meaning for different types of platforms. Some of the topics covered include • Operating states, kernel functions, and memory mapping • Security models, architectures, and evaluations • Evaluation criteria: Trusted Computer Security Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), and Common Criteria • Common flaws in applications and systems • Certification and accreditation
Security Operations	This domain examines controls over personnel, hardware, systems, and auditing and monitoring techniques. It also covers possible abuse channels and how to recognize and address them. Some of the topics covered include • Administrative responsibilities pertaining to personnel and job functions • Maintenance concepts of antivirus, training, auditing, and resource protection activities • Preventive, detective, corrective, and recovery controls • Security and fault-tolerance technologies
Business Continuity and Disaster Recovery Planning	This domain examines the preservation of business activities when faced with disruptions or disasters. It involves the identification of real risks, proper risk assessment, and countermeasure implementation. Some of the topics covered include • Business resource identification and value assignment • Business impact analysis and prediction of possible losses • Unit priorities and crisis management • Plan development, implementation, and maintenance
Legal, Regulations, Investigations, and Compliance	This domain examines computer crimes, laws, and regulations. It includes techniques for investigating a crime, gathering evidence, and handling procedures. It also covers how to develop and implement an incident-handling program. Some of the topics covered include • Types of laws, regulations, and crimes • Licensing and software piracy • Export and import laws and issues • Evidence types and admissibility into court • Incident handling • Forensics

Table 1-1 Security Domains That Make Up the CISSP CBK *(continued)*

Domain	Description
Physical (Environmental) Security	This domain examines threats, risks, and countermeasures to protect facilities, hardware, data, media, and personnel. This involves facility selection, authorized entry methods, and environmental and safety procedures. Some of the topics covered include • Restricted areas, authorization methods, and controls • Motion detectors, sensors, and alarms • Intrusion detection • Fire detection, prevention, and suppression • Fencing, security guards, and security badge types

Table 1-1 Security Domains That Make Up the CISSP CBK *(continued)*

(ISC)^2 attempts to keep up with changes in technology and methodologies in the security field by adding numerous new questions to the test question bank each year. These questions are based on current technologies, practices, approaches, and standards. For example, the CISSP exam given in 1998 did not have questions pertaining to wireless security, cross-site scripting attacks, or IPv6.

Other examples of material not on past exams include security governance, instant messaging, phishing, botnets, VoIP, and spam. Though these subjects weren't issues in the past, they are now.

The test is based on internationally accepted information security standards and practices. If you look at the (ISC)^2 website for test dates and locations, you may find, for example, that the same test is offered this Tuesday in California and next Wednesday in Saudi Arabia.

If you do not pass the exam, you have the option of retaking it as soon as you like. (ISC)^2 used to subject individuals to a waiting period before they could retake the exam, but this rule has been removed. (ISC)^2 keeps track of which exam version you were given on your first attempt and ensures you receive a different version for any retakes. (ISC)^2 also provides a report to a CISSP candidate who did not pass the exam, detailing the areas where the candidate was weakest. Though you could retake the exam soon afterward, it's wise to devote additional time to these weak areas to improve your score on the retest.

CISSP: A Brief History

Historically, the field of computer and information security has not been a structured and disciplined profession; rather, the field has lacked many well-defined professional objectives and thus has often been misperceived.

In the mid-1980s, members of the computer security profession recognized that they needed a certification program that would give their profession structure and provide ways for security professionals to demonstrate competence and to present evidence of their qualifications. Establishing such a program would help the credibility of the security profession as a whole and the individuals who comprise it.

In November 1988, the Special Interest Group for Computer Security (SIG-CS) of the Data Processing Management Association (DPMA) brought together several organi-

zations interested in forming a security certification program. They included the Information Systems Security Association (ISSA), the Canadian Information Processing Society (CIPS), the Computer Security Institute (CSI), Idaho State University, and several U.S. and Canadian government agencies. As a voluntary joint effort, these organizations developed the necessary components to offer a full-fledged security certification for interested professionals. (ISC)^2 was formed in mid-1989 as a nonprofit corporation to develop a security certification program for information systems security practitioners. The certification was designed to measure professional competence and to help companies in their selection of security professionals and personnel. (ISC)^2 was established in North America, but quickly gained international acceptance and now offers testing capabilities all over the world.

Because security is such a broad and diversified field in the technology and business world, the original consortium decided on an information systems security CBK composed of ten domains that pertain to every part of computer, network, business, and information security. In addition, because technology continues to rapidly evolve, staying up-to-date on security trends, technology, and business developments is required to maintain the CISSP certification. The group also developed a Code of Ethics, test specifications, a draft study guide, and the exam itself.

How Do You Sign Up for the Exam?

To become a CISSP, start at www.isc2.org, where you will find an exam registration form you must fill out and send to (ISC)^2. You will be asked to provide your security work history, as well as documents for the necessary educational requirements. You will also be asked to read the (ISC)^2 Code of Ethics and to sign a form indicating that you understand these requirements and promise to abide by them. You then provide payment along with the completed registration form, where you indicate your preference as to the exam location. The numerous testing sites and dates can be found at www.isc2.org.

What Does This Book Cover?

This book covers everything you need to know to become an (ISC)^2-certified CISSP. It teaches you the hows and whys behind organization's development and implementation of policies, procedures, guidelines, and standards. It covers network, application, and system vulnerabilities; what exploits them; and how to counter these threats. The book explains physical security, operational security, and why systems implement the security mechanisms they do. It also reviews the U.S. and international security criteria and evaluations performed on systems for assurance ratings, what these criteria mean, and why they are used. This book also explains the legal and liability issues that surround computer systems and the data they hold, including such subjects as computer crimes, forensics, and what should be done to properly prepare computer evidence associated with these topics for court.

While this book is mainly intended to be used as a study guide for the CISSP exam, it is also a handy reference guide for use after your certification.

Tips for Taking the CISSP Exam

The exams are monitored by CISSP proctors, if you are taking the Scantron test. They will require that any food or beverage you bring with you be kept on a back table and not at your desk. Proctors may inspect the contents of any and all articles entering the test room. Restroom breaks are usually limited to allowing only one person to leave at a time, so drinking 15 cups of coffee right before the exam might not be the best idea.

NOTE (ISC)^2 still uses the physical Scantron tests that require you to color in bubbles on a test paper. The organization is moving towards providing the exam in a digital format through Pearson Vue centers.

You will not be allowed you to keep your smartphones and mobile devices with you during the testing process. You may have to leave them at the front of the room and retrieve them when you are finished with the exam. In the past too many people have used these items to cheat on the exam, so precautions are now in place.

Many people feel as though the exam questions are tricky. Make sure to read the question and its answers thoroughly instead of reading a few words and immediately assuming you know what the question is asking. Some of the answer choices may have only subtle differences, so be patient and devote time to reading through the question more than once.

As with most tests, it is best to go through the questions and answer those you know immediately; then go back to the ones causing you difficulty. The CISSP exam is not computerized (although (ISC)^2 is moving to a computerized model), so you will receive a piece of paper with bubbles to fill in and one of several colored exam booklets containing the questions. If you scribble outside the lines on the answer sheet, the machine that reads your answers may count a correct answer as wrong. I suggest you go through each question and mark the right answer in the booklet with the questions. Repeat this process until you have completed your selections. Then go through the questions again and fill in the bubbles. This approach leads to less erasing and fewer potential problems with the scoring machine. You are allowed to write and scribble on your question exam booklet any way you choose. You will turn it in at the end of your exam with your answer sheet, but only answers on the answer sheet will be counted, so make sure you transfer all your answers to the answer sheet.

Other certification exams may be taking place simultaneously in the same room, such as exams for certification as an SSCP (Systems Security Certified Professional), ISSAP or ISSMP (Architecture and Management concentrations, respectively), or ISSEP (Engineering concentration), which are some of (ISC)^2's other certification exams. These other exams vary in length and duration, so don't feel rushed if you see others leaving the room early; they may be taking a shorter exam.

When finished, don't immediately turn in your exam. You have six hours, so don't squander it just because you might be tired or anxious. Use the time wisely. Take an extra couple of minutes to make sure you answered every question, and that you did not accidentally fill in two bubbles for the same question.

Unfortunately, exam results take some time to be returned. (ISC)² states it can take up to six weeks to get your results to you, but on average it takes around two weeks to receive your results through e-mail and/or the mail.

If you passed the exam, the results sent to you will not contain your score—you will only know that you passed. Candidates who do not pass the test are always provided with a score, however. Thus, they know exactly which areas to focus more attention on for the next exam. The domains are listed on this notification with a ranking of weakest to strongest. If you do not pass the exam, remember that many smart and talented security professionals didn't pass on their first try either, chiefly because the test covers such a broad range of topics.

One of the most commonly heard complaints is about the exam itself. The questions are not long-winded, like many Microsoft tests, but at times it is difficult to distinguish between two answers that seem to say the same thing. Although (ISC)² has been removing the use of negatives, such as "not," "except for," and so on, they do still appear on the exam. The scenario-based questions may expect you to understand concepts in more than one domain to properly answer the question.

Another complaint heard about the test is that some questions seem a bit subjective. For example, whereas it might be easy to answer a technical question that asks for the exact mechanism used in Secure Sockets Layer (SSL) that protects against man-in-the-middle attacks, it's not quite as easy to answer a question that asks whether an eight-foot perimeter fence provides low, medium, or high security. Many questions ask the test taker to choose the "best" approach, which some people find confusing and subjective. These complaints are mentioned here not to criticize (ISC)² and the test writers, but to help you better prepare for the test. This book covers all the necessary material for the test and contains many questions and self-practice tests. Most of the questions are formatted in such a way as to better prepare you for what you will encounter on the actual test. So, make sure to read all the material in the book, and pay close attention to the questions and their formats. Even if you know the subject well, you may still get some answers wrong—it is just part of learning how to take tests.

Familiarize yourself with industry standards and expand your technical knowledge and methodologies outside the boundaries of what you use today. I cannot stress enough that just because you are the top dog in your particular field, it doesn't mean you are properly prepared for every domain the exam covers. Take the assessment test in this chapter to gauge where you stand, and be ready to read a lot of material new to you.

How to Use This Book

Much effort has gone into putting all the necessary information into this book. Now it's up to you to study and understand the material and its various concepts. To best benefit from this book, you might want to use the following study method:

1. Study each chapter carefully and make sure you understand each concept presented. Many concepts must be fully understood, and glossing over a couple here and there could be detrimental to you. The CISSP CBK contains thousands of individual topics, so take the time needed to understand them all.

2. Make sure to study and answer all of the questions at the end of the chapter, as well as those on the CD-ROM included with the book and the Appendix of Comprehensive Questions. If any questions confuse you, go back and study those sections again. Remember, some of the questions on the actual exam are a bit confusing because they do not seem straightforward. I have attempted to draft several questions in the same manner to prepare you for the exam. So do not ignore the confusing questions, thinking they're not well worded. Instead, pay even closer attention to them because they are there for a reason.
3. If you are not familiar with specific topics, such as firewalls, laws, physical security, or protocol functionality, use other sources of information (books, articles, and so on) to attain a more in-depth understanding of those subjects. Don't just rely on what you think you need to know to pass the CISSP exam.
4. After reading this book, study the questions and answers, and take the practice tests. Then review the $(ISC)^2$ study guide and make sure you are comfortable with each bullet item presented. If you are not comfortable with some items, revisit those chapters.
5. If you have taken other certification exams—such as Cisco, Novell, or Microsoft—you might be used to having to memorize details and configuration parameters. But remember, the CISSP test is "an inch deep and a mile wide," so make sure you understand the concepts of each subject *before* trying to memorize the small, specific details.
6. Remember that the exam is looking for the "best" answer. On some questions test takers do not agree with any or many of the answers. You are being asked to choose the best answer out of the four being offered to you.

Questions

To get a better feel for your level of expertise and your current level of readiness for the CISSP exam, run through the following questions:

1. Which of the following provides an incorrect characteristic of a memory leak?
   - **A.** Common programming error
   - **B.** Common when languages that have no built-in automatic garbage collection are used
   - **C.** Common in applications written in Java
   - **D.** Common in applications written in C++
2. Which of the following is the best description pertaining to the "Trusted Computing Base"?
   - **A.** The term originated from the Orange Book and pertains to firmware.
   - **B.** The term originated from the Orange Book and addresses the security mechanisms that are only implemented by the operating system.
   - **C.** The term originated from the Orange Book and contains the protection mechanisms within a system.

D. The term originated from the Rainbow Series and addressed the level of significance each mechanism of a system portrays in a secure environment.

3. Which of the following is the best description of the security kernel and the reference monitor?

   A. The reference monitor is a piece of software that runs on top of the security kernel. The reference monitor is accessed by every security call of the security kernel. The security kernel is too large to test and verify.

   B. The reference monitor concept is a small program that is not related to the security kernel. It will enforce access rules upon subjects who attempt to access specific objects. This program is regularly used with modern operating systems.

   C. The reference monitor concept is used strictly for database access control and is one of the key components in maintaining referential integrity within the system. It is impossible for the user to circumvent the reference monitor.

   D. The reference monitor and security kernel are core components of modern operating systems. They work together to mediate all access between subjects and objects. They should not be able to be circumvented and must be called upon for every access attempt.

4. Which of the following models incorporates the idea of separation of duties and requires that all modifications to data and objects be done through programs?

   A. State machine model

   B. Bell-LaPadula model

   C. Clark-Wilson model

   D. Biba model

5. Which of the following best describes the hierarchical levels of privilege within the architecture of a computer system?

   A. Computer system ring structure

   B. Microcode abstraction levels of security

   C. Operating system user mode

   D. Operating system kernel mode

6. Which of the following is an untrue statement?

   i. Virtual machines can be used to provide secure, isolated sandboxes for running untrusted applications.

   ii. Virtual machines can be used to create execution environments with resource limits and, given the right schedulers, resource guarantees.

   iii. Virtualization can be used to simulate networks of independent computers.

   iv. Virtual machines can be used to run multiple operating systems simultaneously: different versions, or even entirely different systems, which can be on hot standby.

A. All of them

B. None of them

C. i, ii

D. ii, iii

7. Which of the following is the best means of transferring information when parties do not have a shared secret and large quantities of sensitive information must be transmitted?

   A. Use of public key encryption to secure a secret key, and message encryption using the secret key

   B. Use of the recipient's public key for encryption, and decryption based on the recipient's private key

   C. Use of software encryption assisted by a hardware encryption accelerator

   D. Use of elliptic curve encryption

8. Which algorithm did NIST choose to become the Advanced Encryption Standard (AES) replacing the Data Encryption Standard (DES)?

   A. DEA

   B. Rijndael

   C. Twofish

   D. IDEA

Use the following scenario to answer questions 9–11. John is the security administrator for company X. He has been asked to oversee the installation of a fire suppression sprinkler system, as recent unusually dry weather has increased the likelihood of fire. Fire could potentially cause a great amount of damage to the organization's assets. The sprinkler system is designed to reduce the impact of fire on the company.

9. In this scenario, fire is considered which of the following?

   A. Vulnerability

   B. Threat

   C. Risk

   D. Countermeasure

10. In this scenario, the sprinkler system is considered which of the following?

    A. Vulnerability

    B. Threat

    C. Risk

    D. Countermeasure

11. In this scenario, the likelihood and damage potential of a fire is considered which of the following?

    A. Vulnerability

    B. Threat

C. Risk

D. Countermeasure

Use the following scenario to answer questions 12–14. A small remote facility for a company is valued at $800,000. It is estimated, based on historical data and other predictors, that a fire is likely to occur once every ten years at a facility in this area. It is estimated that such a fire would destroy 60 percent of the facility under the current circumstances and with the current detective and preventative controls in place.

12. What is the single loss expectancy (SLE) for the facility suffering from a fire?

A. $80,000

B. $480,000

C. $320,000

D. 60 percent

13. What is the annualized rate of occurrence (ARO)?

A. 1

B. 10

C. .1

D. .01

14. What is the annualized loss expectancy (ALE)?

A. $480,000

B. $32,000

C. $48,000

D. .6

15. Which of the following is not a characteristic of Protected Extensible Authentication Protocol?

A. Authentication protocol used in wireless networks and point-to-point connections

B. Designed to provide improved secure authentication for 802.11 WLANs

C. Designed to support 802.1x port access control and Transport Layer Security

D. Designed to support password-protected connections

16. Which of the following best describes the Temporal Key Integrity Protocol's (TKIP) role in the 802.11i standard?

A. It provides 802.1x and EAP to increase the authentication strength.

B. It requires the access point and the wireless device to authenticate to each other.

C. It sends the SSID and MAC value in ciphertext.

D. It adds more keying material for the RC4 algorithm.

17. Vendors have implemented various solutions to overcome the vulnerabilities of the wired equivalent protocol (WEP). Which of the following provides an incorrect mapping between these solutions and their characteristics?
    - **A.** LEAP requires a PKI.
    - **B.** PEAP only requires the server to authenticate using a digital certificate.
    - **C.** EAP-TLS requires both the wireless device and server to authenticate using digital certificates.
    - **D.** PEAP allows the user to provide a password.
18. Encapsulating Security Payload (ESP), which is one protocol within the IPSec protocol suite, is primarily designed to provide which of the following?
    - **A.** Confidentiality
    - **B.** Cryptography
    - **C.** Digital signatures
    - **D.** Access control
19. Which of the following redundant array of independent disks implementations uses interleave parity?
    - **A.** Level 1
    - **B.** Level 2
    - **C.** Level 4
    - **D.** Level 5
20. Which of the following is not one of the stages of the dynamic host configuration protocol (DHCP) lease process?
    - **i.** Discover
    - **ii.** Offer
    - **iii.** Request
    - **iv.** Acknowledgment
    - **A.** All of them
    - **B.** None of them
    - **C.** i
    - **D.** ii
21. Which of the following has been deemed by the Internet Architecture Board as unethical behavior for Internet users?
    - **A.** Creating computer viruses
    - **B.** Monitoring data traffic
    - **C.** Wasting computer resources
    - **D.** Concealing unauthorized accesses

22. Most computer-related documents are categorized as which of the following types of evidence?
    - **A.** Hearsay evidence
    - **B.** Direct evidence
    - **C.** Corroborative evidence
    - **D.** Circumstantial evidence
23. During the examination and analysis process of a forensics investigation, it is critical that the investigator works from an image that contains all of the data from the original disk. The image must have all but which of the following characteristics?
    - **A.** Byte-level copy
    - **B.** Captured slack spaces
    - **C.** Captured deleted files
    - **D.** Captured unallocated clusters
24. _____ is a process of interactively producing more detailed versions of objects by populating variables with different values. It is often used to prevent inference attacks.
    - **A.** Polyinstantiation
    - **B.** Polymorphism
    - **C.** Polyabsorbtion
    - **D.** Polyobject
25. Tim is a software developer for a financial institution. He develops middleware software code that carries out his company's business logic functions. One of the applications he works with is written in the C programming language and seems to be taking up too much memory as it runs over a period of time. Which of the following best describes what Tim needs to look at implementing to rid this software of this type of problem?
    - **A.** Bounds checking
    - **B.** Garbage collection
    - **C.** Parameter checking
    - **D.** Compiling
26. _____ is a software testing technique that provides invalid, unexpected, or random data to the inputs of a program.
    - **A.** Agile testing
    - **B.** Structured testing
    - **C.** Fuzzing
    - **D.** EICAR

27. Which type of malware can change its own code, making it harder to detect with antivirus software?
    - **A.** Stealth virus
    - **B.** Polymorphic virus
    - **C.** Trojan horse
    - **D.** Logic bomb
28. What is derived from a passphrase?
    - **A.** A personal password
    - **B.** A virtual password
    - **C.** A user ID
    - **D.** A valid password
29. Which access control model is user-directed?
    - **A.** Nondiscretionary
    - **B.** Mandatory
    - **C.** Identity-based
    - **D.** Discretionary
30. Which item is not part of a Kerberos authentication implementation?
    - **A.** A message authentication code
    - **B.** A ticket-granting ticket
    - **C.** Authentication service
    - **D.** Users, programs, and services
31. If a company has a high turnover rate, which access control structure is best?
    - **A.** Role-based
    - **B.** Decentralized
    - **C.** Rule-based
    - **D.** Discretionary
32. In discretionary access control, who/what has delegation authority to grant access to data?
    - **A.** A user
    - **B.** A security officer
    - **C.** A security policy
    - **D.** An owner
33. Remote access security using a token one-time password generation is an example of which of the following?
    - **A.** Something you have
    - **B.** Something you know

C. Something you are
D. Two-factor authentication

34. What is a crossover error rate (CER)?
A. A rating used as a performance metric for a biometric system
B. The number of Type I errors
C. The number of Type II errors
D. The number reached when Type I errors exceed the number of Type II errors

35. What does a retina scan biometric system do?
A. Examines the pattern, color, and shading of the area around the cornea
B. Examines the patterns and records the similarities between an individual's eyes
C. Examines the pattern of blood vessels at the back of the eye
D. Examines the geometry of the eyeball

36. If you are using a synchronous token device, what does this mean?
A. The device synchronizes with the authentication service by using internal time or events.
B. The device synchronizes with the user's workstation to ensure the credentials it sends to the authentication service are correct.
C. The device synchronizes with the token to ensure the timestamp is valid and correct.
D. The device synchronizes by using a challenge-response method with the authentication service.

37. What is a clipping level?
A. The threshold for an activity
B. The size of a control zone
C. Explicit rules of authorization
D. A physical security mechanism

38. Which intrusion detection system would monitor user and network behavior?
A. Statistical/anomaly-based
B. Signature-based
C. Static
D. Host-based

39. When should a Class C fire extinguisher be used instead of a Class A?
A. When electrical equipment is on fire
B. When wood and paper are on fire
C. When a combustible liquid is on fire
D. When the fire is in an open area

40. How does halon suppress fires?
    - **A.** It reduces the fire's fuel intake.
    - **B.** It reduces the temperature of the area.
    - **C.** It disrupts the chemical reactions of a fire.
    - **D.** It reduces the oxygen in the area.
41. What is the problem with high humidity in a data processing environment?
    - **A.** Corrosion
    - **B.** Fault tolerance
    - **C.** Static electricity
    - **D.** Contaminants
42. What is the definition of a power fault?
    - **A.** Prolonged loss of power
    - **B.** Momentary low voltage
    - **C.** Prolonged high voltage
    - **D.** Momentary power outage
43. Who has the primary responsibility of determining the classification level for information?
    - **A.** The functional manager
    - **B.** Middle management
    - **C.** The owner
    - **D.** The user
44. Which best describes the purpose of the ALE calculation?
    - **A.** It quantifies the security level of the environment.
    - **B.** It estimates the loss potential from a threat.
    - **C.** It quantifies the cost/benefit result.
    - **D.** It estimates the loss potential from a threat in a one-year time span.
45. How do you calculate residual risk?
    - **A.** Threats × risks × asset value
    - **B.** (Threats × asset value × vulnerability) × risks
    - **C.** SLE × frequency
    - **D.** (Threats × vulnerability × asset value) × control gap
46. What is the Delphi method?
    - **A.** A way of calculating the cost/benefit ratio for safeguards
    - **B.** A way of allowing individuals to express their opinions anonymously

C. A way of allowing groups to discuss and collaborate on the best security approaches
D. A way of performing a quantitative risk analysis

47. What are the necessary components of a smurf attack?
A. Web server, attacker, and fragment offset
B. Fragment offset, amplifying network, and victim
C. Victim, amplifying network, and attacker
D. DNS server, attacker, and web server

48. What do the reference monitor and security kernel do in an operating system?
A. Intercept and mediate a subject attempting to access objects
B. Point virtual memory addresses to real memory addresses
C. House and protect the security kernel
D. Monitor privileged memory usage by applications

Answers

1. C
2. C
3. D
4. C
5. A
6. B
7. A
8. B
9. B
10. D
11. C
12. B
13. C
14. C
15. D
16. D
17. A
18. A

19. D
20. B
21. C
22. A
23. A
24. A
25. B
26. C
27. B
28. B
29. D
30. A
31. A
32. D
33. A
34. A
35. C
36. A
37. A
38. A
39. A
40. C
41. A
42. D
43. C
44. D
45. D
46. B
47. C
48. A