题目

第一章题目

1. A software program would be protected from illegal distribution under what law?
   A. Trademark
   B. Copyright
   C. Trade secret
   D. SPA
2. Which group states that the Internet is a privilege and should be treated and used with respect?
   A. Computer Ethics Institute
   B. Internet Standards Board
   C. GASSP Committee
   D. Internet Architecture Board
3. G8 has been involved with which of the following items?
   A. Fighting against cybercrime
   B. Legislating on economic espionage
   C. Protecting employee privacy rights
   D. Prosecuting software pirates
4. The golden arches of McDonald's are protected under what intellectual property law?
   A. Trademark
   B. Trade secret
   C. Logo Protection Law
   D. Copyright
5. Which is not true of the Federal Sentencing Guidelines enacted in 1991?
   A. Developed specifically to address white collar crimes.
   B. Detailed the specific responsibilites of senior executives within companies.
   C. Established a maximum fine of $100 million.
   D. Encouraged the implementation of security policies and a security program.
6. There are different categories for evidence depending upon what form it is in and possibly how it was collected. Which of the following is considered supporting evidence?
   A. Best evidence
   B. Corroborative evidence
   C. Conclusive evidence
   D. Direct evidence
7. Which type of law punishes the individuals with financial restitution instead of jail penalties?
   A. Tort
   B. Administrative
   C. Criminal
   D. Regulatory

8. Which of the following is an attack that uses tools to intercept electronic communication signals usually passively instead of actively?

A. Masquerading

B. Social engineering

C. Wiretapping

D. Salami

9. If a waiter tells his friends how the restaurant's famous secret sauce is made, what law has he violated?

A. No law was violated.

B. Trademark

C. Trade secret

D. Copyright

10. Which organization posts four primary Code of Ethics canons involving societal protection, individual honorability, diligent service, and professional development?

A. Computer Ethics Institute

B. (ISC)2

C. Internet Ethics Board

D. Internet Activities Board

11. A witness testimony would be classified as what type of evidence?

A. Real

B. Secondary

C. Best

D. Conclusive

12. Which of the following would protect a senior executive in a liability lawsuit brought on by an employee?

A. He is able to demonstrate that due diligence and due care were established and followed.

B. He was on vacation during the incident.

C. The incident was not covered in the company's security policy.

D. The employee was not in good standing.

13. Who usually blows the whistle on illegal software usage within companies?

A. IT administrators

B. CISSPs

C. Disgruntled employees

D. Managers

14. Which person would not be part of the Internet Architecture Board?

A. Software programmer

B. IT executive

C. Technology researcher

D. An appointed FCC representative

15. Typically, computer files are considered hearsay evidence. In which of the following scenarios would computer files be admissible?

A. When the file clearly proves guilt

B. When a forensic expert testifies that the evidence is trustworthy

C. When the computer output is done during regular business hours

D. It is never admissible.

16. The investigation process of a computer crime is very similar to investigating many other types of crime. What is the "who" and "why" of a crime?

A. Motivations

B. Opportunities

C. Means

D. Capabilities

17. Which famous crime involved tricking phone switches with a 2600 Hz tone generator that enabled free long distance charges?

A. Blue Boxing

B. Red Boxes

C. Chaos Computer Club

D. Cult of the Dead Cow

18. Which of the following cannot be presented in a court as evidence?

A. The original computer system that was violated

B. A crime scene investigator's notebook

C. Videotapes from the monitoring system

D. Original documentation

19. Legally and ethically making a system attractive to a potential attacker and logging an attacker's actions for use in future prosecution is called_____.

A. Entrapment

B. Enticement

C. Encouragment

D. Proximate causation

20. Different evidence categories describe different types of evidence and the weight they can hold in a court case. Which of the following would be deemed real evidence?

A. An eyewitness testimony

B. A captured Trojan horse virus from the victim's computer

C. A videotape from the company's closed-circuit TV system

D. The oral testimony of a forensic expert

21. Which regulation forces financial institutions to communicate privacy options to its customers that give them the option of allowing their personal information to be shared with third parties?

A. Federal Privacy Act of 1974

B. Gramm-Leech-Bliley Act of 1999

C. Federal Sentencing Guidelines

D. Computer Security Act of 1987

22. What is the benefit of a person obtaining a patent for their invention?

A. Full ownership for as long as that invention is in use

B. Full owneship for exactly five years

C. Full ownership of the invention for a specified time period

D. Allows others to use the invention

23. What is the name of the technique in Qualitative Risk Analysis that uses the anonymous opinions of all individuals?

A. Consensus approach

B. Delphi techinque

C. Group mentality

D. Group discussion phase

24. Which of the following is a policy that outlines the directives dictated by management and is more technically focused?

A. System-specific

B. Technical-specific

C. Organizational

D. Issue-specific

25. Which is not an example of security awareness?

A. Security training

B. Security bulletin board notes

C. Security access control lists (ACLs)

D. Security objectives in an employee's performance review

26. Identifying, assessing, and reducing risk to an acceptable level and maintaining the achieved level is referred to as _____.

A. Risk planning

B. Risk management

C. Security management

D. Operations management

27. Assigning a dollar figure to a single event assumed by the company if a threat occurred is called what?

A. Single loss expectancy (SLE)

B. Exposure factor (EF)

C. Qualitative Risk Analysis

D. Quantitative Risk Analysis

28. Companies should set up different types of baselines for individual departments and the company as a whole. This can include physical, technical, and administrative security baselines. Which of the following defines a baseline?

A. Rules indicating what should and should not be done

B. A minimum level of security required

C. Step-by-step instructions used to complete a task

D. Recommendations

29. A company cannot eliminate all risk. The risk that remains is referred to as residual risk and the company must determine if this corresponds with their acceptable level of risk. Which of the following defines residual risk?

A. Asset value × exposure factor

B. Single loss expectancy (SLE) × annualized rate of occurrence (ARO)

C. (Threats × vulnerability × asset value) × control gap

D. Threats × vulnerability × asset value

30. The department or individual responsible for protecting and maintaining a company's computer-related assets is called a _____.

A. Data owner

B. Data custodian

C. Data keeper

D. Data user

31. Companies must understand how often a specific threat is likely to occur. Which of the following is a value that represents the likelihood of an event taking place within the span of a year?

A. Annualized rate of occurrence (ARO)

B. Single loss expectancy (SLE)

C. Exposure factor (EF)

D. Annual loss expectancy (ALE)

32. There are different roles pertaining to security within an organization. Security professionals perform all of the following tasks except_____.

A. Updating firewall configurations

B. Implementing intrusion detection mechanisms

C. Testing access control mechanisms

D. Monitoring employee keystrokes for performance evaluation

33. A policy written solely to educate and not to enforce action is what type of policy?

A. Education

B. Advisory

C. Informative

D. Regulatory

34. Who performs periodic reviews of a company's security policy, procedures, and tools?

A. Data custodian

B. Security accountant

C. Security auditor

D. Senior Management

35. A company can use different types of policies: system-specific, organizational, and issue-specific. Which of the following is an example of an issue-specific policy?

A. Procedures on dialing in remotely to the company's VPN

B. Employee ID badge policy

C. Operating guidelines for a customer provisioning system

D. Company shared drive network standards

36. Ultimate responsibility for the success of company security falls on whose shoulders?

A. Security professional

B. Everyone in the company

C. IT organization

D. Senior management

37. There are many reasons why a company should carry out security awareness training for its employees. Security awareness can provide all of the following benefits except?

A. Stopping attack attempts

B. Informing users of standards and procedures to follow

C. Modifying employees' attitudes and behaviors

D. Improving emergency response time

38. Which of the following data classifications provides the lowest level of protection?

A. Confidential

B. Sensitive

C. Private

D. Public

39. A security control often initiated by human resources which involves a new employee or outside party signing a document stating they will not share company information is called a _____.

A. Employment-at-will doctrine

B. Nondisclosure agreement (NDA)

C. Offer letter

D. Trade secret

40. Management can choose to deal with risks that have been identified and calculated in different ways. Which of the following is not a responsible way of dealing with risk?

A. Accept

B. Reduce

C. Transfer or assign

D. Ignore

41. Which of the following statements best describes the difference between end users and data owners?

A. End users are data owners and can dictate which subjects can access the resources.

B. End users use resources and company information to carry out their tasks and data owners dictate access to those resources and information.

C. Data owners use resources and company information to carry out their tasks and end users dictate access to those resources and information.

D. Senior management is always the data owner and end users are never data owners.

42. Controls and safeguards can be put into place to mitigate identified business risks. Which of the following best describes this practice?

A. Accepting risk through due diligence

B. Transferring risk to a third party to mitigate the total risk

C. Return on investment pertaining to the implementation of controls

D. Rejecting the risks by practicing due care in a responsible manner

43. The Computer Fraud and Abuse Act is one of the most commonly used laws when prosecuting computer criminals. Which of the following actions does the Act address?

A. Conflicts of interest

B. Disrupting the use of the Internet

C. Trafficking of passwords

D. Telephone fraud

44. Hackers use several fallacies to rationalize their activities. One of them is that the systems they compromise and use are idle and not being used to their full capacity. Which of the following best describes the flaw in this logic?

A. This is true. Some systems are not being fully used.

B. The constant use of the systems can damage them, even if this is not the hacker’s intent.

C. The systems are not to be used for general purposes for unintended users.

D. The owner of the system is paying for its activity.

45. If a computer intrusion is identified, then specific steps should be followed. Which of the

following best describes the proper steps?

A. Detect, contain, dump memory, image the disk, notify management

B. Detect, evaluate, notify, contain, eradicate

C. Detect, evaluate, notify, contain, deploy

D. Detect, deploy, notify, contain, eradicate

46. Which of the following best describes why evidence must be properly collected and stored?

A. The individual and agency responsible for these activities may be held liable and the items may not be admissible in court.

B. The individual and agency responsible for these activities may be held liable and the items may be admissible in court.

C. The individual and agency responsible for these activities may be held liable and the items may not be admissible in court because the Prudent Person Rule is being followed.

D. The individual and agency responsible for these activities may be held liable and the items may not be admissible in court because the Computer Fraud and Abuse Act is not being followed.

47. Since there are not necessarily many laws specifically addressing computer crimes and because technology changes more quickly than the laws, what traditional laws are used to prosecute computer criminals?

A. Conspiracy and embezzlement

B. Espionage and fraud

C. Embezzlement, fraud, and wiretapping

D. Wiretapping and eavesdropping

48. Information warfare is becoming more and more important and recognized. Which of the following best describes Information warfare?

A. Signal monitoring, interception, and intelligence

B. Carrying out attacks on a nation's information infrastructure

C. Developing and spreading propaganda materials to a nation

D. Social engineering tactics during wartime

49. Three main categories fall under Common Law. Which of the following is not one of them?

A. Administrative law

B. Civil law

C. Criminal law

D. Union law

50. A common legal concept is the "Prudent Person Rule" which is implemented through different types of laws. Which of the following best describes this rule?

A. A person is expected to react and carry out specific duties that a responsible and prudent person would do in similar circumstances.

B. A person is expected to react and carry out specific duties that a responsible and prudent person would not do in similar circumstances.

C. A person is expected to react and carry out specific duties that an imprudent person would do in similar circumstances.

D. A person is expected to react and carry out specific duties that a responsible and prudent person would do in dissimilar circumstances.

51. If senior executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

A. Criminal

B. International

C. Civil

D. Common

52. Which of the following describes the difference between civil and criminal law?

A. Criminal law has a stricter burden of proof and uses imprisonment as a punishment.

B. Civil law has a stricter burden of proof and does not use imprisonment as a punishment.

C. Civil law has a stricter burden of proof and uses imprisonment as a punishment.

D. Criminal law has a less strict burden of proof and uses imprisonment as a punishment.

53. Which of the following is addressed in the Federal Sentencing Guidelines?

A. Senior executives are not responsible for the computer and information security decisions they make and what actually takes place within their organizations.

B. Senior executives are responsible for the computer and information security decisions they make and what actually takes place within their organizations.

C. This act provides the necessary structure when dealing with espionage and further defines trade secrets to be technical, business, engineering, scientific, or financial.

D. This act requires federal agencies to identify computer systems that will contain sensitive information.

54. In many cases traditional laws do not adequately approach computer crimes and their ramifications. Which of the following is one way legal systems have changed to better allow these established rules to be used?

A. The definition of property has been expanded to include intangible property, as in hard drives.

B. The definition of property has been expanded to include intangible property, as in electronic information.

C. The definition of property has been expanded to include tangible property, as in electronic information.

D. The definition of property has been expanded to include tangible property, as in secondary storage devices.

55. HIPAA is a collection of new regulations that dictate that medical information is sensitive and private and should be treated as such. What is another name for HIPAA?

A. OECD

B. Gramm-Leech-Bliley Act

C. Kennedy-Kassebaum Act

D. Comprehensive Crime Control Act

56. In some situations a law enforcement agent may not need to obtain a warrant if destruction of evidence seems imminent. Which of the following outlines the rules and regulations of this type of activity?

A. Proximate causation

B. Prudent Person Rule

C. Fourth Amendment

D. Exigent circumstances

57. Which of the following is used as a criteria to determine a suspect's involvement in and commission of a crime?

A. Motivation, opportunity, means

B. Motivation, opportunity, methods

C. Motivation, objectives, means

D. Methods, opportunity, means

58. The US Best Evidence Rule indicates that a duplicate or copy of evidence can be accepted during a trial instead of the original under what circumstance?

A. The original evidence was destroyed in the normal course of business.

B. The original evidence was destroyed.

C. The original evidence is written in a different language than what the court uses.

D. It cannot be accepted; only the original will be accepted and admissible as evidence.

59. Monitoring employee e-mail messages may be a useful tool for uncovering malicious activity. Which of the following is not something a company should do if they are going to carry out this type of monitoring?

A. Inform users that this type of monitoring may take place.

B. Explain the ramifications of misuse of this resource to users.

C. Guarantee employee privacy.

D. Monitor all users consistently and fairly.

60. Opinion-based evidence is very important in most cases. Which of the following best describes the difference between expert and non-expert opinion-based evidence requirements?

A. Expert witnesses can give their educated guesses and opinions based on past experience whereas non-expert witnesses can only testify to facts.

B. Non-expert witnesses can give their educated guesses and opinions based on past experience whereas expert witnesses can only testify to facts.

C. Expert witnesses can give their educated guesses specifically on facts whereas non-expert witnesses can only testify to their past experiences.

D. Both types of witnesses are able to give their opinions based on their life experience.

61. The evidence life cycle is best outlined in which of the following answers?

A. Evidence discovery, recording, preservation, transportation, collection, presentation in court, return to owner

B. Evidence discovery, recording, collection, transportation, preservation, presentation in court, return to owner

C. Evidence discovery, transportation, collection, destruction, preservation, presentation in court, return to owner

D. Evidence discovery, recording, collection, transportation, preservation, return to owner, presentation in court

62. Although the words "threat," "vulnerability," "risk," and "exposure" sound similar, which one best describes the probability of a threat materializing?

A. Vulnerability

B. Risk

C. Threat agent

D. Exposure

63. A risk analysis can be carried out through manual or automated processes. Which of the following is the best reason for using an automated risk analysis tool?

A. The tools are built to have easily used interfaces, which greatly simplifies the process for the

team and management.

B. Most of the data that is gathered during a risk analysis cannot be reused, so there is no good reason to put in the effort of gathering it manually.

C. The learning curve for automated risk analysis tools is low. The team can quickly learn how to use the tool for data processing.

D. The amount of information that needs to be gathered will be the same. However, using an automated tool has key advantages because so much information is preconfigured in the tool and the data can be reused.

64. There are different roles within an organization that pertain to security. Thus, it is important that each person fulfilling a role understands their responsibilities. Which of the following is not a responsibility of an information owner?

A. Using preset criteria to determine the classification levels of data that the owner is responsible for.

B. Carrying out regular backups of the data that is owned and periodically testing the validity of the backups.

C. Periodically reviewing classification levels of the data that is owned and modifying classification levels appropriately.

D. Delegating the responsibility of maintaining and protecting the data that is owned to a data custodian.

65. Requiring employees to take their earned vacation time is referred to as mandatory vacations. Which of the following best describes why it is important to enforce mandatory vacations as it pertains to security?

A. Ensures that employees do not get burned out. Statistics show that when employees get tired of their jobs more mistakes and fraudulent activities occur.

B. Enforcing vacation is actually dictated by many little-known industry regulations. A company can be sued successfully if this process is not followed.

C. Allows rotation of another employee into that position. The second employee may be able to uncover fraudulent activities carried out by the first employee.

D. Ensures that morale is kept high and attitudes are not negatively affected.

66. Data classification is an important piece in an organization's security program. It dictates handling procedures of data and the level of protection necessary. When determining the correct classification level for data, which of the following should be considered first?

A. Value

B. Age

C. How badly competitors want access to the data

D. Liability of not properly protecting the data

67. Which of the following best describes the difference between a system owner and a data owner?

A. One system usually has more than one data owner, so it is a one-to-many relationship.

B. The data owner is responsible for defining and implementing security controls.

C. The system owner is responsible for defining the rules for appropriate use of the data among employees.

D. The system usually has one data owner, so they are one and the same.

68. NIST outlines several accepted security self-testing techniques. Which of the following is not

considered one of them?

A. Wardialing

B. Network mapping

C. Log destruction

D. Virus detection

69. A security policy is the crux of a company's overall security program. Which of the following is not true regarding the visibility of the security policy?

A. The security policy should be integrated in all decision-making procedures and should be highly visible only to middle and senior management, since it is senior management's directive.

B. The security policy should be integrated in all decision-making procedures and should not be highly visible to middle and senior management, since it is senior management's directive.

C. The security policy should be integrated in all decision-making procedures and should be highly visible to all employees, since it is senior management's directive.

D. The security policy should be integrated in all decision-making procedures and should not be highly visible to all employees, since it is senior management's directive.

70. Which of the following is an intentional or accidental event that prevents a computer from carrying out its tasks?

A. Computer and resource abuse and misuse and the use of countermeasures

B. Vulnerabilities and risks

C. Compromise

D. Risk assessment

71. To outline a clear direction for a company's security program, a forum can be established. Which of the following is not an activity usually carried out by this forum?

A. Approving of specific security initiatives

B. Outlining security roles within the company and defining those roles' responsibilities

C. Auditing and testing for compliance of security policies that will be put into place

D. Approving and helping to implement the security policy

72. The exercise that carries out qualitative identification of susceptibility that could increase the business or productivity impact of threat events affecting an organization is referred to as_____.

A. Vulnerability assessment

B. Threat assessment

C. Risk mitigation

D. Risk transfer

73. Which of the following classification levels indicates that disclosure outside of the company would not negatively affect the business, its employees, partners, or customers?

A. Confidential

B. Sensitive

C. Public

D. Private

74. Any contractors, vendors, and temporary or permanent employees who use computers and network resources to carry out their tasks are known as which of the following?

A. Data owners

B. Data custodians

C. Information owners

D. End users

75. When carrying out a risk analysis, assets must be identified and assigned values. Vulnerabilities and threats must be identified and the potential loss they could cause must be calculated. Corresponding countermeasures must be chosen and their values calculated. All of these calculations are carried out for which of the following purposes?

A. Cost-benefit analysis

B. Developing a disaster recovery plan

C. Developing and implementing standards and procedures

D. To follow laws and regulations

76. The basic components of a security policy are scope, responsibilities, purpose, and_____.

A. Procedures and standards

B. Compliance and enforcement

C. Provisions and exceptions

D. Vulnerabilities and threats

77. Internal phone books, employee directories, and the company's organization chart should be_____.

A. Available to all customers, vendors, and partners

B. Available to all employees via an intranet and Internet site

C. Unavailable to the public in any form

D. Available to strategically identified employees

78. The main reasons for documenting computer support and operation activities and procedures include all but which of the following?

A. To satisfy and meet auditing requirements based on specific compliance regulations.

B. To ensure consistency of activities, which will provide a more stable environment.

C. To give empolyees detailed instructions on how to carry out different types of tasks.

D. To help ensure that security holes and oversights do not occur.

79. Russ is an entry-level operations technician with limited access permissions. One day when a second-level technician is helping him troubleshoot a problem, Russ watches as the technician types in a password for a restricted diagnostic tool. Which term describes what Russ has done?

A. Sniffing

B. Tapping

C. Shoulder surfing

D. Smurfing

80. Denial-of-service (DoS) attacks are geared at which leg of the AIC triad?

A. Integrity

B. Availability

C. Confidentiality

D. Collision

81. Threats can come in many forms and every company should place high importance on identifying all of its potential threats. Which of the answers below is an accurate example of a potential threat?

A. Unintentional loss of data due to a computer malfunction

B. Unintentional loss of data due to an employee mistake

C. Intentional loss of data due to a disgruntled employee

D. All of the other choices

82. On his last day of work, a disgruntled worker feverishly deletes 100 customer files containing important billing information. The resulting damage is expected to affect the company for several months. What type of loss can a company experience from this kind of action?

A. Residual

B. Delayed

C. Cascading

D. Total

83. Chrissy is performing a risk analysis. To complete one step, she answers these questions: what is the value of the asset to the company, how much does it cost to maintain it, what is its role in the company, how much would it be worth to the competition. What risk analysis step has Chrissy performed?

A. Assigning values to assets

B. Estimating loss per risk

C. Performing a threat analysis

D. Assigning the risk

84. A risk analysis has determined that a knowledge base server has a value of $138,000 and an exposure factor of a specific threat of 45 percent. The annualized rate of occurrence (ARO) for this threat is one in ten years. Based on this information what is the annual loss expectancy (ALE) for the asset?

A. $1800

B. $62,100

C. $140,000

D. $6210

85. In the movie "Office Space," a software programmer writes a program that deducts money from the company's account and deposits it into a personal account. His coworker loads the program onto the mainframe operating system. This type of teamwork is called _____.

A. Separation of duties

B. Collusion

C. Collision

D. Phreaking

86. It has become more and more common for companies to require new employees, contractors, and even vendors to sign nondisclosure agreements (NDAs) as a security control. NDAs protect a company in all but which one of the following ways?

A. Protect senior management from potential lawsuits if due care is not exercised

B. Protect trade secrets

C. Protect public information

D. Protect proprietary network configurations

87. Part of an effective security program is having clear roles and responsibilities within an organization. When dealing with data classification, this is especially important. For example, one person or group of people could have the daily task of backing up data and restoring data from

various media. Which of the following individuals would not typically perform this duty?

A. Data custodian

B. Network administrator

C. System administrator

D. Data owner

88. All companies have instituted some level of data classification to protect information. Military organizations have more rigid parameters than commercial organizations, but each entity has a purpose in mind when employing data security levels and each can provide a unique set of data classifications. So, if a publicly held mortgage fund company has a data classification of "public," which of the following would most likely fit into this category?

A. Internal risk assessment figures

B. Operating system code

C. Quarterly financial report

D. Internal phone directory

89. Because of the varying philosophies that senior managers incorporate into their business structure, there are always different ways to accomplish the same thing. Risk analysis is no different. Qualitative Risk Analysis and Quantitative Risk Analysis are very different from one another but both represent a way of managing risk. Which of the following actions is not a characteristic of Qualitative Risk Analysis?

A. Instituting an employee survey to gather results based upon their opinions

B. Department heads-only meeting to brainstorm ideas

C. Soliciting data from several departments in order to assign an accurate monetary value to an asset

D. Constructing and using a rating system

90. A policy is written and communicated in order to instruct individuals on what to do or what not to do. Nearly everyone at one time or another has been given a stated policy to follow. For example, Judi is a pharmaceutical representative who works with customers and insurance providers. One of her stated policies reads, "Under no circumstances can you divulge a customer's medical information without completing a three-step identification process. Divulging this information improperly will result in swift termination procedures and potential legal action." What type of policy is this?

A. Advisory

B. Ramification

C. Informative

D. Regulatory

91. When classifying data, proper procedures should be followed. Which of the following sequences of action is the correct order for classifying data?

A. Data custodian classifies data by using predefined criteria, data owner is delegated daily operations, data custodian puts necessary controls in place and maintains them.

B. Data owner classifies data by using predefined criteria, data custodian is delegated daily operations, data custodian puts necessary controls in place and maintains them.

C. Data owner classifies data by generating new, unique criteria, data custodian is delegated daily operations, data custodian puts necessary controls in place and maintains them.

D. Data owner classifies data by using predefined criteria, data custodian is delegated daily

operations, data owner puts necessary controls in place and maintains them.

92. What are cascading errors and how can they be damaging to a company?

A. When an error is made at the beginning of a computation or process and that error is carried over in the following processes. This can result in correct results that are believed to be incorrect.

B. When an error is made at the beginning of a computation or process and that error causes the application to fail. This can result in incorrect results that are believed to be correct.

C. When an error is made at the beginning of a computation or process and that error is carried over in the following processes. This can result in incorrect results that are believed to be correct.

D. When an error is made at the beginning of a computation or process and that error is carried over in the following processes. This can result in correct results that are believed to be invalid.

93. Peter is a senior-level account executive who has come under scrutiny by upper management for possibly revealing proprietary company information to customers. Peter's superiors have put several controls in place in order to learn more about his behavior. Which of the actions below is not a viable and ethical option for them?

A. Inform all employees that monitoring can take place before actually monitoring Peter's activities.

B. Place monitoring devices on Peter's computer and phone without notifying him.

C. Place him on probation while the matter is under investigation.

D. Institute the job rotation principle by allowing his coworker Jason to take over the account.

94. A company needs to make sure that purchasing and implementing specific countermeasures are good business decisions. Which of the following best describes the steps that should take place?

A. The total loss before a countermeasure is implemented needs to be calculated. Then the total loss after a countermeasure is implemented needs to be calculated. The second value is subtracted from the first value. Then the annual cost of the safeguard needs to be added to this remaining value.

B. The total loss before a countermeasure is implemented needs to be calculated. Then the total loss after a countermeasure is implemented needs to be calculated. The second value is added to the first value. Then the annual cost of the safeguard needs to be subtracted from this remaining value.

C. The delayed loss before a countermeasure is implemented needs to be calculated. Then the total loss after a countermeasure is implemented needs to be calculated. The second value is subtracted from the first value. Then the annual cost of the safeguard needs to be subtracted from this remaining value.

D. The total loss before a countermeasure is implemented needs to be calculated. Then the total loss after a countermeasure is implemented needs to be calculated. The second value is subtracted from the first value. Then the annual cost of the safeguard needs to be subtracted from this remaining value.

95. An organization can choose to implement informative and\or advisory policies, which are put in place for different reasons. Which of the following best describes the difference between these types of policies?

A. An informative policy outlines behavior expectations and possible ramifications for noncompliance. An advisory policy is not an enforceable policy, but one intended to teach individuals about specific issues relevant to the company.

B. An advisory policy outlines behavior expectations and possible ramifications for noncompliance. An informative policy is not an enforceable policy, but one intended to teach individuals about specific issues relevant to the company.

C. A regulatory policy outlines behavior expectations and possible ramifications for noncompliance. An informative policy is not an enforceable policy, but one intended to teach individuals about specific issues relevant to the company.

D. An advisory policy outlines behavior expectations and possible ramifications for noncompliance. An informative policy is an enforceable policy and one intended to teach individuals about specific issues relevant to the company.

96. Choosing a countermeasure can be an overwhelming task for a security professional because there are so many factors to consider. Which of the following countermeasure traits would not be favorable?

A. Distinct access between user and administrative roles

B. Dependent upon many other components

C. Modular in nature

D. Defaults to no access

97. Bob is a security professional in charge of enforcing security policies within his company. For the last 18 months he has recommended acquiring a closed-circuit TV monitoring system for their general office buildings in order to prevent and detect employee theft. Finally, after countless cost-benefit debates and thousands of dollars lost to theft, the senior leadership team agrees and instructs Bob to purchase the system. The leadership team has done what?

A. Transferred the risk

B. Reduced the risk

C. Accepted the risk

D. Rejected the risk

98. Audit trails are a valuable tool used by security professionals. They can uncover access control violations, improper operating procedures, employee mistakes, and a host of other useful data. Which one of the following control types do audit trails fall under?

A. Physical

B. Corrective

C. Accountability

D. Administrative

99. When a company intends to achieve data confidentiality it must account for several types of attacks. One popular attack is social engineering. Which of the following is not an example of social engineering?

A. An attacker posing as an employee of the company when calling the customer support line

B. An attacker intercepting e-mail messages between two employees

C. An attacker gaining entrance to the facility and telling the receptionist that she is the CEO's friend

D. An attacker pretending to be a vendor in order to steal company information

100. Joe's boss assigns him three projects:

1) Reconfigure the network into a centrally controlled environment;
2) Make sure changes in the projects do not affect production;
3) Convert the entire network to a public key infrastructure (PKI) environment.

Each project can be associated with a security goal type. Which of the project numbers below has the correct goal assigned to it?

A. 1) Tactical 2) Operational 3) Strategic
B. 1) Operational 2) Strategic 3) Tactical
C. 1) Operational 2) Tactical 3) Strategic
D. 1) Daily 2) Functional 3) Tactical

101. Which of the following is not an example of due care?

A. Providing security awareness training to all employees
B. Requiring employees to sign nondisclosure agreements
C. Implementing mandatory vacations for all employees
D. Allowing a key job function to be completed by one highly qualified employee

102. Risk should not be handled in which one of the following ways?

A. Reduce risk
B. Accept risk
C. Transfer risk
D. Reject risk

103. Why is it important to make safeguards highly visible?

A. To improve auditing capabilities
B. To promote employee awareness
C. To justify their cost
D. To deter attackers

104. A software, hardware, or procedural weakness that may give an attacker an open door is called a _____.

A. Vulnerability
B. Capability
C. Asset
D. Countermeasure

105. How is the single loss expectancy (SLE) calculated?

A. Annualized rate of occurrence (ARO) × asset value
B. Annualized rate of occurrence (ARO) × exposure factor
C. Asset value × exposure factor (EF)
D. Asset value × annual loss expectancy (ALE)

106. Which qualitative analysis technique allows individuals to submit their opinions anonymously?

A. Quantitative
B. One-on-one
C. Delphi
D. Qualitative

107. Which of the following is an example of shoulder surfing?

A. Browsing through a file cabinet for data

B. Dumpster diving

C. Social engineering

D. Recording screen shots of another user's computer wth a video recorder

108. If a company wants to protect its intellectual property, which of the following should take place?

A. Employee should agree to a trans-border agreement.

B. Employee should sign a nondisclosure agreement.

C. Employees should be aware of countermeasures in place.

D. Employees should implement and configure their own controls.

109. What does the annualized rate of occurrence (ARO) value represent?

A. Frequency of threat

B. Percentage of damage

C. Risk probability

D. Loss potential

110. If an individual in your organization continually ignores management directives outlined in the organization's security policy, what should you do?

A. Nothing. This is not your job.

B. Disable their account until the matter is cleared up.

C. Change the user's password.

D. Inform their supervisor.

111. The purpose of a security awareness program is:

A. To gain management’s approval of a security program.

B. To modify the attitude of employees about sensitive data.

C. To change corporate attitudes about protecting data.

D. To modify employee’s attitudes and behaviors.

112. Which group causes the most computer crime losses?

A. Management

B. Hackers

C. Employees

D. Contractors

113. Which of the following best describes the differences between regulatory, advisory, and informational policies?

A. Regulatory provides guidance and is not enforceable, and informational is industry specific.

B. Informational is industry specific, and advisory is for information purposes only.

C. Regulatory is industry specific, and informational is not enforceable.

D. Advisory is industry specific, and regulatory is for information purposes only.

114. Which of the following is not a necessary step in setting up a classification system?

A. Identifying the data custodian who will be responsible for maintaining data and its security level.

B. Specifying the criteria that will determine how data is classified.

C. The data owner must indicate the classification of the data she is responsible for.

D. Showing users how to classify and declassify data on their own.

115. Which of the following has an incorrect definition of a specific security role within an organization?

A. Senior manager — Examines security practices and mechanisms within the organization

B. Security professional — Functionally responsible for security and carries out senior manager’s directives

C. Data owner — Determines data classification of information within the organization

D. Data custodian — Maintains data in ways to preserve and protect its confidentiality, integrity, and availability

116. Your company's security officer has requested that the IT department implement an authentication and authorization system based on biometrics. Which type of control will you be implementing?

A. Administrative

B. Technical

C. Physical

D. Detective

117. What are the three fundamental principles that serve as a security program's objectives?

A. Confidentiality, integrity, authenticity

B. Confusion, ignorance, annoyance

C. Confidentiality, integrity, availability

D. Security, privacy, authorization

118. Which of the following defines a countermeasure?

A. A procedure that can eliminate the threat agent

B. A software configuration that can completely prevent a threat

C. A software configuration, hardware, or procedure that can mitigate risk

D. A procedure that fixes the destruction caused by an exposure

119. When implementing a security program, which direction should be taken for proper support and direction?

A. A top-down approach should be implemented, meaning that the implementation and support should come from the IT management and work its way down.

B. A bottom-up approach should be implemented, meaning that the implementation and support should come from the company top management and work its way up to the IT management and staff members.

C. A top-down approach should be implemented, meaning that the implementation and support should come from the company’s top management and work its way through middle management and then to staff members.

D. A bottom-up approach should be undertaken by the IT department by developing a security program and implementing it in order to provide the necessary support and direction..

120. Which statement describes the proper relationship of the words "threat," "exposure," and "risk?"

A. An exposure gives rise to a threat which exploits a risk and leads to a vulnerability.

B. A risk causes a vulnerability that leads to a threat and causes an exposure.

C. An exposure allows a weakness that leads to a threat creating an exposure.

D. A threat is that a threat agent will exploit a vulnerability. The probability of this happening is the risk. Once the vulnerability is exploited there is an exposure.

121. Security models have many layers and different types of goals to accomplish in different time frames. Which of the following accurately describes the goals and their relationship?

A. Tactical goals or daily goals, operational goals or mid-term goals, strategic goals or long-term goals. This approach to planning is called a planning horizon.

B. Strategic goals or long-term goals, tactical goals or mid-term goals, operational goals or daily goals. This approach to planning is called the top-down approach.

C. Tactical goals or daily goals, operational goals or mid-term goals, strategic goals or long-term goals. This approach to planning is called a bottom-up approach.

D. Strategic goals or long-term goals, tactical goals or mid-term goals, operational goals or daily goals. This approach to planning is called a planning horizon.

122. You are trying to justify the security safeguards that you want to implement. What would be your first step?

A. Perform a counter analysis

B. Perform a risk analysis

C. Perform a top-down analysis

D. Perform a bottom-up analysis

123. Organize the following government data classification from most sensitive to least sensitive.

1. Confidential
2. Secret
3. Sensitive but unclassified (SBU)
4. Unclassified
5. Top secret

A. 4,3,1,2,5

B. 5,2,1,3,4

C. 1,2,3,5,4

D. 5.2,3.1.4

124. Once you have established the risk and the potential loss, you purchase insurance to reduce the risk. Which of the answers describes this act?

A. Risk assessment

B. Risk transfer

C. Risk rejecting

D. The game of Risk

125. Which one of the following describes the fundamental differences between procedures, guidelines, policies, and standards?

A. A policy is the senior management statement that dictates what type of role security plays. Procedures are a complete set of instructions. Guidelines are recommendations, and standards are rules.

B. Procedures are managerial statements that dictate the policies for security and the standards and guidelines to be implemented.

C. Standards are the policies that IT dictates to help formulate the procedures to implement for security.

D. Standards are recommended guidelines. Procedures are directly implemented as a consequence of the security policy dictated by senior management.

126. Continually educating the entire organization on security awareness has which one of the following outcomes?

A. The network will operate at an increased level and efficiency.

B. The network users will be able to detect another network user’ s abuses.

C. The IT staff will have the added knowledge of how to hack into their competitors' networks.

D. It broadens the company's perspective on its own security and the protection of its systems and resources.

127. What is the main difference between the data custodian and the data owner?

A. The data custodian decides upon the classification of the data itself and delegates the day-to-day management of the data to the data owner.

B. The data owner decides upon the classification of the data itself and delegates day-to-day management of the data to the data custodian.

C. The data owner defines the classification of the data after the data custodian has secured the data.

D. The data custodian is usually a salaried employee working under the data owner.

128. Which of the following should be done upon the hiring of personnel?

A. All personnel should sign the form 2163 according to HIPAA.

B. All personnel should be made to sign a nondisclosure agreement.

C. Coworkers should have the opportunity to perform interviews to confirm personality compatibility.

D. Extensive physical, emotional, and psychological evaluations should be performed.

129. What would be an appropriate difference between a qualitative and a quantitative risk analysis?

A. Qualitative would be a subjective observation, while a quantitative approach defines statistical costs associated with a threat.

B. Quantitative approach would be a subjective observation, while a qualitative approach defines statistical costs associated with a threat.

C. Qualitative defines the overall appeal of a target or a resource, while quantitative is defined as (threats × vulnerability × asset value) × control gap.

D. Quantitative approach indicates the total cost of security implemented for protection. Qualitative identifies the expected acceptance of the security policy from the organization.

130. If an employee alters a program so that it takes a few pennies from every customer's bank account each month, what is this called?

A. Salami attack

B. Social engineering

C. Spoofing

D. Dumpster diving

131. Which of the following outlines the proper life cycle of evidence?

A. Collection, storage, presentation in court, return to owner

B. Collection, presentation in court, transportation, return to owner

C. Collection, transportation, storage, return to owner

D. Collection, storage, presentation in court, destroy

132. What does a copyright protect?

A. The trade secrets of a company

B. An invention

C. An expression of an idea

D. Distinguishing colors, characters, and words

133. What is administrative law?

A. Deals with violations of regulatory standards

B. Deals with violent violation of individuals

C. Deals with laws developed to protect the public

D. Deals with commerce laws across borders

134. Which of the following is not part of the Code of Ethics developed by the (ISC)2?

A. Share answers of the exam with CISSP prospects.

B. Observe and abide by all contracts, expressed or implied, and give prudent advice.

C. Encourage the growth of research—teach, mentor, and value the certification.

D. Act honestly, justly, responsibly, and legally, and protect society.

135. What type of attack is wiretapping?

A. Active

B. Aggressive

C. Masquerading

D. Passive

136. According to the(ISC)2 Code of Ethics, conflicts should be resolved in what order?

A. Duty to public safety, principles, individuals, and profession

B. Duty to individuals, profession, principles, and public safety

C. Duty to profession, public safety, individuals, and principles

D. Duty to principles, profession, public safety, and individuals

137. Tricking an intruder into accessing confidential information in order to prosecute him is an example of what?

A. Enticement

B. Interrogation

C. Entrapment

D. Salami attack

138. What is the main purpose for interrogating an employee?

A. To evaluate the protection of the security policy

B. To obtain evidence for trial

C. To force the employee to resign

D. To intimidate the employee

139. In computer crime, what does the term MOM refer to?

A. Malice, obstruction, means

B. Motive, opportunity, means

C. Methods, opposition, means

D. Methods, opportunity, means

140. Laws that typically enforce jail time as punishment and were created by the government to protect society are called what?

A. Civil

B. Tort

C. Criminal

D. Administrative

141. A cashier who enters incorrect values in the cash register and keeps the remaining money

has committed what kind of crime?

A. Sniffing

B. Dumpster diving

C. Masquerading

D. Data diddling

142. Which statement is not true regarding computer crimes involving foreign countries?

A. All nations agree on evidence collection methods.

B. Governments are not always willing to cooperate with one another.

C. There are different interpretations of crimes within different countries.

D. The seriousness of computer crime is viewed differently by individual nations.

143. The SBA and BSA were formed to protect what type of organization?

A. Import/export companies

B. Accused cybercriminals

C. Encryption technology manufacturers

D. Software vendors

144. Which of the following must be met so that evidence is legally admissible in court?

A. Modified computer files

B. Lawful search and seizure

C. Forced confession

D. Entrapment evidence

145. Which action is not imperative when investigating a computer crime scene?

A. Dump data from memory.

B. Contact a judge immediately.

C. Follow a proper chain of custody.

D. Image the computer disk drive.

146. Which of the following is a personnel attack?

A. Masquerading

B. Data diddling

C. Wiretapping

D. Dumpster diving

147. Blue Boxing was used in what type of attack?

A. Data diddling

B. Salami

C. Phone fraud

D. Masquerading

148. Extranets, VANs, and shared networks with external entities create what legal concern?

A. Downstream liability

B. Increased SLAs

C. Human resource issues

D. Network configuration complexity

149. A party that can prove that damage was caused and that the damage was the company's fault has proven what?

A. Due care

B. Legally recognized obligation

C. Proximate causation

D. Due diligence

150. Which of the following laws addresses wiretapping?

A. Computer Fraud and Abuse Act of 1986

B. Electronic Communications Privacy Act of 1986

C. HIPPA

D. Privacy Act of 1974

151. Which law pertains to government agencies collecting and maintaining data on individuals?

A. Privacy Act of 1974

B. Gramm-Leech-Bliley Act of 1999

C. HIPPA

D. Comprehensive Crime Control Act of 1984

152. Which of the following items is addressed in the (ISC)2 Code of Ethics?

A. Avoid conflicts of interest.

B. Avoid conducting penetration tests.

C. Protect national security.

D. Protect individual rights.

153. If you are having a computer crime investigated by law enforcement agents, what should you do to ensure that the evidence that is confiscated does not hurt your company's production activities and productivity?

A. Offer backup copies kept in an offsite facility to agents.

B. Do not allow any evidence to be gathered.

C. Only allow certain systems and data to be obtained.

D. Identify critical systems and data and ask the agents for copies.

154. What is the first step when investigating a computer crime?

A. Photograph the area, computer, and contents on the screen.

B. Advise individuals in the area of their rights before evidence is collected.

C. Quickly look for planted logic bombs and Trojan horses to ensure damage cannot be done.

D. Issue a statement to release all necessary evidence.

155. A company takes on the task of repairing any damage caused by an event and having in place a set of steps to prevent the spread of further damage. Which of the following describes this procedure?

A. Due care

B. Due diligence

C. Incident handling program

D. Operations security

156. There are several canons to the (ISC)2 Code of Ethics. Which of the following actions is not one of them?

A. Act responsibly and protect the infrastructure.

B. Maintain a current knowledge of known security issues.

C. Attempt to perform jobs to the best of your ability even if you are not qualified.

D. Avoid acting in a disreputable manner toward the profession.

157. What would be a correct statement regarding ethics and laws?

A. Ethics are always drawn from laws.

B. If something isn't illegal, then it is probably ethical.

C. Most laws are drawn from ethics.

D. Laws apply to everything in society that is right and wrong.

158. Which of the following is an accurate statement regarding computer crime?

A. Most computer crime is reported and documented.

B. Fighting computer crime has a known set of rules that are static.

C. Many computer crimes actually go unreported.

D. The ease of capturing computer criminals has made networks less susceptible to computer crime.

159. An incident response team should contain which set of people?

A. The team needs to contain a security advisor internal to the company as well as an outside consultant.

B. The team needs to contain a security advisor internal to the company, an outside consultant, and occasional contact with upper management.

C. The team needs to contain someone from senior management, the network administrator, security officer, maybe a programmer, and a public liaison.

D. The team should have someone from every department in the company, plus two outside consultants.

160. Which of the following statements regarding trade secrets, copyright, patents, and trademark law is accurate?

A. All countries follow a uniform standard for these areas.

B. A vendor within a country should follow their own country’s standards in these areas as the appropriate method to conduct their business.

C. Any vendor that is interested in doing business in a country outside of theirs should be aware of the differences in these specific areas, and take the necessary steps to properly protect their product.

D. A vendor can choose between his country’ s laws and practices or the foreign country in which they do business.

161. In the United States, which of the following was extended to cover computer crimes and hold senior executives personally responsible if their company did not comply with the laws set out for them?

A. HIPAA

B. Federal Sentencing Guidelines

C. Computer Fraud and Abuse Act

D. Federal Privacy Act of 1974

162. To protect a specific word, symbol, or name, a company would acquire which of the following?

A. Trademark

B. Copyright

C. Patent

D. Trade secret

163. The invention of a new gizmo is revolutionary. You wish to protect this idea. Which of the following is used to protect the new gizmo?

A. Patent

B. Trademark

C. Copyright

D. Trade secret

164. Which of the following acts was created to protect the privacy of medical information?

A. US Federal Privacy Act of 1974

B. Computer Fraud and Abuse Act

C. HIPAA

D. Graham-Leech-Bliley Act of 1999

165. During a trial, a company introduces documents that were created during the course of the trial to show new evidence of wrongdoing. These documents would be classified as what type of evidence?

A. Direct

B. Conclusive

C. Hearsay

D. Corroborative

166. Which of the following is a true statement regarding warrants and seizure of an individual's property?

A. Police do not have to have a warrant for most cases of property seizure.

B. A manager falls under the same restrictions as law enforcement agents if she received direction from a law enforcement agent.

C. A manager without a warrant can seize the information on a computer at a company that contains suspected child pornography information if the manager was directed by a police officer to obtain this information.

D. If law enforcement has a warrant for a home computer in a case of suspected child pornography, they can also confiscate the computers at the homeowner's office.

167. Which of the following is the most common security issue for most companies?

A. IP spoofing

B. Dumpster diving

C. Excessive privileges

D. Denial of service

168. Which of the following answers uses the security terms ' ‘vulnerability," "threat," " ‘risk," and "countermeasure" correctly?

A. There can be a threat, but unless your company has the corresponding vulnerability the company is not exposed and it is not a vulnerability. If the vulnerability does reside in the environment, then a countermeasure is applied to reduce the risk.

B. There can be a vulnerability, but unless your company has the corresponding risk the company is not exposed and it is not a vulnerability. If the vulnerability does reside in the environment, then a countermeasure is applied to reduce the risk.

C. There can be a risk, but unless your company has the corresponding threat the company is not exposed and it is not a vulnerability. If the vulnerability does reside in the environment, then a countermeasure is applied to reduce the risk.

D. There can be a threat, but unless your company has the corresponding vulnerability the company is not exposed and it is not a vulnerability. If the vulnerability does reside in the environment, then a countermeasure is applied to increase the risk.

169. Which of the following best describes ISO 17799 and BS 7799?

A. Nationally recognized Information Security Management Standards that provides high-level, conceptual recommendations on enterprise security.

B. BS 7799 was derived from ISO 17799 and provides guidance on how to set up and maintain security programs.

C. ISO 17799 is the internationally recognized Information Security Management Standard that provides high-level, conceptual recommendations on enterprise security. It was derived from BS 7799.

D. The most commonly used standard is the BS 7799 which was derived from the de facto standard ISO 17799. It is an internationally recognized Information Security Management Standard that provides high-level, conceptual recommendations on enterprise security.

170. The ISO 17799 is broken into ten different sections. Which of the following answers contains all of the proper sections?

A. Information security policy, creation of security infrastructure, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, system lifecycle and repair, business continuity management, compliance

B. Information security policy, creation of security infrastructure, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, system development and maintenance, laws and regulations, compliance

C. Information security policy, creation of security infrastructure, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, system development and maintenance, business continuity management, compliance

D. Information security picy, creation of security infrastructure, asset classification and control, telecommunication security, physical and environmental security, communications and operations management, access control, system development and maintenance, business continuity management Compliance

171. What is the main purpose of information risk management (IRM)?

A. It is the process of identifying, assessing, and reducing the risk to an acceptable level.

B. It is the process of implementing the right mechanisms to maintain an acceptable level of risk.

C. It is the process of obtaining funding, assessing the environment, and implementing government policies.

D. It is the process of identifying, assessing, and increasing the risk to an acceptable level and implementing the right mechanisms to maintain that level of risk.

172. What is the purpose of an information risk management (IRM) policy?

A. It outlines the infrastructure for a company’s risk management processes and procedures.

B. It provides direction for how the IRM team works with government agencies.

C. It is the necessary key for properly detecting administrative, physical, and technical threats.

D. It replaces a company’s security policy because it is more expansive and far reaching.

173. Who sets the acceptable risk level for an organization?

A. Government agencies that create regulations

B. Senior management

C. Auditors

D. Security analyst

174. A proper risk analysis has specific steps and objectives that it needs to accomplish. Which of the following lists these items?

A. Identify assets and their values, identify vulnerabilities and threats, quantify the probability and business impact of these potential threats, and provide non-economical countermeasure recommendations.

B. Identify assets and their values, identify vulnerabilities and threats, quantify the probability and business impact of these potential threats, and provide economical countermeasure recommendations.

C. Identify assets, identify vulnerabilities and threats, quantify the probability and business impact of these potential threats, and provide economical countermeasure recommendation.

D. Identify assets and their values, identify fraud and collusion, quantify the probability and business impact of these potential threats, and provide economical countermeasure recommendation.

175. Sam and David have not carried out proper project sizing and they are halfway through their risk analysis. What is the danger of not doing this?

A. This step outlines the steps for mapping regulations and laws to an organization's risk profile. The team will not be able to assess if the correct level of risk acceptance has been applied.

B. The team will not know if they have secured funding for this project and may put the company into debt.

C. The right team members have not been gathered for the risk analysis project and the team must start all over.

D. The scope of the project is not defined, so the project may run out of money and still not meet its objectives.

176. Why is it important to get the right level of employee involved in a risk analysis?

A. Lower levels may not have adequate knowledge or a thorough enough understanding of the processes.

B. Decision makers need to be involved in this process because of how critical it is to the company.

C. Lower and higher levels of individuals need to be involved to ensure that it is a fair assessment.

D. The level does not matter; the team just needs to have one person per department involved.

177. In risk assessments and analyses, the frequency of a threat needs to be estimated. The value that is used is usually the annualized rate of occurrence (ARO). Which of the following is incorrect pertaining to this value?

A. Once in 100 years is a value of 0.01.

B. It is based on 12-month intervals.

C. Once in 1000 years is a value of 0.0001.

D. It is commonly multiplied by the single loss expectancy (SLE) value.

178. What does it mean that a risk should be accepted based on cost, pain, and visibility?

A. A company should choose to accept a risk if it is an economical decision, it can live with the vulnerability, and it won't be viewed as irresponsible in the industry.

B. A company should choose to accept a risk if it is an emotional decision, it can live with the vulnerability, and it won’t be viewed as irresponsible in the industry.

C. A company should choose to accept a risk if it is an economical decision, it can live with the vulnerability, and it won’t be viewed as responsible in the industry.

D. A company should choose to accept a risk if it is an economical decision, it can live with the vulnerability, and it will be viewed as irresponsible in the industry.

179. ACME's storage facility has been valued at $400,000 and it is estimated that if a flood occurred it would damage 35 percent of the facility. The local government's statistics indicate that a flood has the probability of happening once in ten years. What are the single loss expectancy (SLE) and annual loss expectancy (ALE) values?

A. SLE = $140,000 ALE = $14,000

B. SLE = $35,000 ALE = $3500

C. SLE = $14,000 ALE = $140,000

D. SLE = $3500 ALE = $35,000

180. What do uncertainty values have to do with risk values and calculations?

A. It is a critical component in the cost-benefit formula.

B. It is used to calculate residual risk and total risk.

C. It is a value based on 12-month intervals and is plugged into the cost-benefit formula.

D. It is a confidence level in the data that has been gathered.

181. What is the difference between the modified and consensus Delphi methods?

A. Modified is for brainstorming and consensus is for solving problems.

B. Consensus is for brainstorming and modified is for solving problems.

C. Modified is anonymous and consensus is not anonymous.

D. Modified is not anonymous and consensus is anonymous.

182. Kevin and David are carrying out a risk assessment and they need to perform a cost-benefit analysis on a specific countermeasure to determine if it is a good choice for the company. The potential loss to the company without the control is $200,000. The annualized loss expectancy (ALE) with the control is $75,500. They figure that the annual cost of the safeguard is $55,400. What is the value of this safeguard to the company?

A. $220,100

B. －$69,100

C. $69,100

D. $124,500

183. Which of the following is not an important aspect of an organizational security policy?

A. The policy should dictate business objectives.

B. It should be developed and used to integrate security into all business functions and processes.

C. Each iteration of the policy should be dated and under version control.

D. It should be reviewed and modified as a company changes.

184. Which of the following has an incorrect definition assigned to the term?

A. Baseline = minimum amount of security that is require

B. Guideline = recommended actions and operational guides for users, IT staff, operations staff

C. Procedures = detailed, step-by-step tasks that should be performed to achieve a certain goal

D. Standards = rules that have to be followed by the executive staff only

185. Which of the following statements explains the benefit of having a broad range of classifications to work with in a company's information classification program?

A. It does not provide a benefit.

B. It allows for overlapping classifications.

C. It allows applications and data to be classified.

D. It allows for concise control.

186. Implementation of a security program can help to reinforce all of the following except:

A. Integrity of the data

B. Training and education of authorized users

C. Accuracy of data

D. Protection of corporate assets

187. What is the best description for COBIT?

A. Framework of controls

B. Security controls used to ensure compliance with COSO

C. Security controls developed by (ISC)2

D. IT security governance roadmap

188. Why was the COSO framework developed?

A. To be a guideline for IT security auditors to follow to ensure compliance

B. To deal with fraudulent financial activities and reporting

C. To help organizations install, implement, and maintain COBIT controls

D. To deal with regulatory requirements pertaining to protecting sensitive health information

189. Which of the following best describes the difference between COBIT and COSO?

A. COSO is used to govern the operational level of an organization, while COBIT is used for the strategic level.

B. COSO is used to govern the strategic level of an organization, while COBIT is used for the operational level.

C. COBIT deals with corporate governance, and COSO deals with IT governance.

D. COBIT deals with the full organization, while COSO deals with just the technical side of the organization.

190. Which of the following is a true statement pertaining to ISO standards?

A. ISO 27001 is based on BS 7799 Part 2.

B. ISO 27002 is based on BS 7799 Parts 1 and 2.

C. ISO 27005 lays out measurements to use for security management.

D. ISO 27006 lays out how to protect sensitive health information.

191. Which best describes why the Information Technology Infrastructure Library (ITIL) was created?

A. Because of the increased dependence on IT security controls

B. Because of the lack of integrity of the financial information that was reported to investors

C. Because of the increased dependence upon IT within organizations

D. Because of the lack of confidentiality that was being practiced pertaining to sensitive personal information

192. The reasons for the development of COBIT, COSO, and ITIL are clearly different. What is the

difference between these frameworks?

A. COBIT and COSO provide the "what is to be achieved," but not the "how to achieve it."

B. COBIT and COSO provide the "how to achieve it," whereas ITIL provides the "what to achieve."

C. COBIT and COSO deal with the financial controls, and ITIL deals with the IT controls.

D. ITIL deals with the financial controls, and COBIT and COSO deal with the IT controls.

193. Who are usually considered the customers within the ITIL model?

A. External-facing partners

B. Internal departments

C. Business units

D. Executives

194. Most regulatory compliance requirements are based on COBIT, but there is a specific industry that bases its regulatory requirements on another standard. What industry and standard is this?

A. The financial industry is based on Sarbanes-Oxley (SOX) controls.

B. Health care is based on National Institute of Standard and Technology (NIST) controls.

C. The auto industry is based on ISO 27001 controls.

D. Government is based on COSO controls.

195. Facilitated Risk Analysis Process (FRAP) is a risk assessment methodology. Which of the following best describes the purpose of this approach?

A. Performing qualitative risk assessments based on threat analysis tests

B. Performing quantitative risk assessments based on threat analysis tests

C. Determining functions, identifying functional failures, and assessing the causes of failure

D. Determining functions, identifying functional failures, and assessing the causes of security breaches

196. Christine has been asked to research and identify a risk assessment methodology that will help her company pinpoint potential vulnerabilities. Her boss wants her team to be able to better identify where failures can occur in the company steps and processes. Which approach would best fit this need?

A. Failure Modes and Effect Analysis

B. Failure Modes and Function Analysis

C. OCTAVE

D. NIST 800-60

197. Bill is asked to identify a more statistically oriented approach than the Total Quality Management (TQM) provided back in the 1980s. Which of the following would be the best choice for Bill?

A. ITIL

B. Six Sigma

C. TQL

D. TQS

198. Wayne is in the position of bringing on new partners in Europe. What framework would be best for Wayne to understand before starting business with these companies?

A. COSO

B. ITIL

C. Six Sigma

D. Safe Harbor

199. Chris has been asked to create a charter for the company's new security steering committee. Which of the following would be the best description for Chris to use?

A. The group is responsible for making decisions on tactical and operational security issues within the enterprise as a whole.

B. The group is responsible for making decisions on tactical and strategic security issues within the enterprise as a whole.

C. The group is responsible for making decisions on the risk methodology and metrics that should be used and implemented.

D. The group is responsible for making decisions on operational and strategic security issues within the enterprise as a whole.

200. A threat to a computer system cannot exist without a:

A. Countermeasure

B. Threat agent

C. Risk

D. Vulnerability

201. What are the three main principles in all security programs?

A. Awareness, Information, and Compliance

B. Availability, Integrity, and Confidentiality

C. Authenticity, Importance, and Concealment

D. Administration, Incomparable, and Consecutively

202. Jill is sitting in a coffee shop doing some work on her laptop. As she logs into her company's network, she can't help but notice the man behind her has become very interested in what she is typing. Jill immediately logs off and shuts down her computer. What should Jill be concerned about?

A. The man behind her may be "shoulder surfing."

B. The Internet connection is unsafe.

C. She doesn't like to be watched and decides to call it quits for the day.

D. Nothing, the man is just curious.

203. Denial-of-service (DoS) attacks affect which principle of the AIC Triad?

A. Availability

B. Integrity

C. Confidentiality

D. None of the other choices

204. Which of the following is not the best way to ensure the integrity of a system is maintained?

A. System-critical files should be restricted from the users' view and access.

B. Databases should let only authorized individuals modify data, and data in transit should be protected by encryption or other mechanisms.

C. Systems should be protected from environmental issues like heat, cold, humidity, static electricity, and contaminants.

D. Applications should provide mechanisms that check for valid and reasonable input values.

205. What is the ISO 17799?

A. It outlines the components that should make up organizational security programs.

B. It is an internationally recognized Information Security Management Standard that provides high-level, conceptual recommendations on enterprise security.

C. Both A and B.

D. Neither A nor B.

206. What are the differences between administrative controls, technical controls, and physical controls?

A. Administrative controls include the development and publication of policies, technical controls consist of access control mechanisms, and physical controls entail controlling individual access to both the facility and different departments.

B. Administrative controls include the screening of personnel, technical controls include identification and authentication methods, and physical controls consist of protecting the facility's perimeter.

C. Administrative controls consist of security awareness training, technical controls include locking systems and removing unnecessary USB or CD-ROM drives, and physical controls consist of monitoring for intrusion.

D. All of the other choices

207. A social engineer, a hacker, a shoulder surfer, and even an employee making an unintentional mistake that could expose confidential information are all types of what?

A. Cybercriminals

B. Threat agents

C. Phishers

D. DoS attackers

208. Which of the following is an argument against the validity of "security through obscurity"?

A. "The enemy knows the system."

B. If a system's security depends solely or primarily on keeping an exploitable weakness hidden, then, clearly, if that weakness is discovered, the security is easily compromised.

C. A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that the flaws are not known and that attackers are unlikely to find them.

D. All of the other choices

209. What is meant by confidentiality when used in the AIC Triad?

A. Keeping information regarding a network breach secret

B. Preventing unauthorized modification

C. Ensuring the necessary level of secrecy is enforced at each junction of data processing and preventing unauthorized disclosure

D. Ensuring the ability to recover from disruptions in a secure and quick manner

210. What is meant by open standards?

A. Networks that are not protected correctly and, therefore, are "open"

B. Standards that are subject to debate

C. Publicly available specifications for achieving a specific task

D. No licenses to patent rights are needed to use the standard

211. The ideal risk analysis team is made up of:

A. Individuals who are experts when it comes to technology risks

B. Individuals from all the different areas of a company

C. Individuals who are hired specifically for risk analysis

D. None of the other choices

212. Which of the following is not a main goal of risk analysis?

A. Identify assets and their values.

B. Provide an economic balance between the impact of the threat and the cost of the countermeasure.

C. Educate employees on proper security practices.

D. Identify vulnerabilities and threats.

213. An estimation of the frequency or chance of a threat happening is known as:

A. Vulnerability assessment

B. Consequence analysis

C. Likelihood assessment

D. Safeguard analysis

214. The method that examines potential failures in products or processes and that may be used to evaluate risk management priorities for mitigating known threat vulnerabilities is known as:

A. FMEA

B. FEMA

C. MFAE

D. AFME

215. Joe and Ed are part of a risk analysis team for their company. They are looking at all possible risk scenarios based on their own knowledge and how they feel fellow employees will behave. They then give each scenario a rating. By doing this, they hope to identify all the potential threats to their company. What is this type of research known as?

A. Investigative

B. Quantitative

C. Comprehensive

D. Qualitative

216. The percentage of loss a realized threat could have on a certain asset is known as:

A. Asset value

B. Single loss expectancy

C. Exposure factor

D. Threat value

217. What does ARO = 0.2 mean?

A. Annualized rate of occurrence is equal to once in five years.

B. Annualized rate of occurrence is equal to once in two years.

C. Annualized rate of occurrence is equal to twice a year.

D. None of the above

218. If a flood in a company’s warehouse is estimated to damage 30 percent of the $275,000 asset value, what is the SLE?

A. $91,667

B. $82,500

C. $9,167

D. $8,250

219. Which of the following is an example of delayed loss?

A. Cost of repairing damages

B. Loss in revenue

C. Loss of potential customers

D. Loss in production

220. Running antivirus software on each workstation, web server, and mail server and applying content filtering via a proxy server is considered what type of security?

A. Multiple step security

B. Layered approach security

C. Technical security

D. Controlled security

221. Which of the following is an enterprise security framework?

A. NIST

B. GLBA

C. OCTAVE

D. SABSA

222. The ISO/IEC 27000 standard follows which of the following iterative process frameworks commonly used for business process quality programs?

A. Plan – Do – Check – Act

B. Prepare – Do – Check – Act

C. Plan – Implement – Check – Act

D. Plan – Do – Test – Act

223. Which of the following enterprise frameworks is commonly used to develop business, data, applications, and technology architectures?

A. SABSA

B. TOGAF

C. CMMI

D. MODAF

224. Organizations and companies need to set up security practices internally to ensure that information security strategy consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally. Which of the following is a comprehensive and rigorous method for describing the structure and behavior of all the components that make up a holistic information security management system (ISMS)?

A. Information security management system framework

B. Enterprise security architecture

C. ISMS enterprise architecture

D. BS 7799 standard

225. Which of the following is the de facto standard of best practices for IT service management?

A. Six Sigma

B. Information Technology Infrastructure Library (ITIL)

C. Business Model for Information Security (BMIS)

D. COBIT

226. Information risk management (IRM) is the process of identifying and _____ risk, _____ it to an acceptable level, and _____ the right mechanisms to maintain that level.

A. qualifying, reducing, implementing

B. qualifying, reducing, implementing

C. assessing, increasing, deploying

D. qualifying, increasing, deploying

227. Risk assessments and risk analysis should be carried out with specific goals in mind. Which of the following is the least important pertaining to risk assessments and analysis?

A. Use a defined method of identifying vulnerabilities and threats and assessing the possible impacts.

B. Ensure that security is cost effective, relevant, timely, and responsive to threats.

C. Provide the ability to prioritize risks and show management the amount of resources that should be applied to protecting against those risks in a sensible manner.

D. Implement and fully test the identified countermeasures to ensure that the organization's acceptable risk level is being honored.

228. Which of the following is an incorrect definition or characteristic of the NIST SP 800-30 standard?

A. Named a "Risk Management Guide for Information Technology Systems"

B. A U.S. federal government standard

C. It is specific to IT threats and how they relate to information security risks.

D. International standard

229. _____ is an international standard for how risk management should be carried out in the framework of an information security management system (ISMS).

A. ISO/IEC 27002

B. ISO/IEC 27003

C. ISO/IEC 27001

D. ISO/IEC 27005

230. Which of the following is the second step in a Failure Modes and Effect Analysis?

i. Start with a block diagram of a system or control.

Ii. Draw up a table in which failures are paired with their effects and an evaluation of the effects.

Iii. Correct the design of the system, and adjust the table until the system is not known to have unacceptable problems.

Iv. Consider what happens if each block of the diagram fails

A. iv.

B. ii.

C. iii.

D. i.

231. A _____ proves to be a useful approach to identifying failures that can take place within complex environments and systems. In this method, each situation that has the potential to cause a negative effect is added to the structure as a series of logic expressions.

A. Failure Modes and Effect Analysis

B. fault tree analysis

C. failure modes and criticality analysis

D. fault tree and modes analysis

232. Which of the following best describes the differences between vulnerability assessments and risk assessments?

A. Vulnerability assessments are used to identify the risks. A risk assessment calculates the

probability of the risks being exploited and the associated business impact.

B. Vulnerability assessments are used to identify the threats. A risk assessment calculates the probability of the vulnerabilities being exploited and the associated business impact.

C. Vulnerability assessments are used to identify the vulnerabilities. A risk assessment calculates the probability of the vulnerabilities being exploited and the associated business impact.

D. Vulnerability assessments are used to identify the vulnerabilities and threats. A risk assessment calculates the certainty of the vulnerabilities being exploited and the associated business impact.

233. Risk analysis can be carried out through qualitative and quantitative methods. Each has its own pros and cons. Which of the following is the least important item pertaining to the downfalls of qualitative analysis approaches?

A. The assessments and results are subjective and opinion based.

B. Eliminates the opportunity to create a dollar value for cost/benefit discussions.

C. Hard to develop a security budget from the results because monetary values are not used.

D. Standards are not available. Each vendor has its own way of interpreting the processes and their results.

234. There are four main ways that management can choose to deal with the risks identified within their company. If insurance is purchased, this is an example of _____. If nothing is done, this is considered _____. If a countermeasure is implemented, this is an example of _____. And if terminating the risk-based activity is carried out, this is considered _____.

A. transference. mitigation. acceptance. avoidance.

B. transference. acceptance. mitigation. ignoring.

C. transference. mitigation. reduction. avoidance.

D. transference. acceptance. mitigation. avoidance.

235. It is important for a company to develop baselines in its security program. Which of the following best describes why baselines are used?

A. Provides direction for policy compliance.

B. Provides a consistent reference point.

C. Provides instructions on how to complete specific tasks.

D. Provides metrics to use for governance requirements.

236. ISO\IEC 27001 defines an information security management system (ISMS) as which of the following?

A. An IT structure developed and deployed to protect the organization’s identified assets

B. An enterprise framework that is created to manage an organization’s risk and protect its assets

C. A coherent set of policies, processes, and systems to manage risks to information assets

D. A set of standards and guidelines that are followed by all levels of an organization to ensure compliancy and asset protection

237. Security has _____ requirements, which define the expected behavior from a product or system, and _____requirements, which establish confidence in the implemented products or systems overall.

A. functional, security

B. assurance, security

C. compliance, testing

D. functional, assurance

238. Which of the following could be considered the opposite of privacy?

A. Data security

B. Data sharing

C. Data restriction

D. Data breach

239. All of the following should be examined for risk when acquired from external vendors, except:

A. Hardware

B. Software

C. Services

D. Processes

240. Which of the following best describes a best practice for control implementation?

A. Controls should not be implemented unless the annualized cost of loss exceeds the annualized cost of the control itself.

B. All possible controls should be implemented, regardless of their cost, in order to protect assets.

C. Controls should be implemented based solely upon he threat actor or threatto the asset.

D. Controls should not be implemented for data with low sensitivity.

241. During which of the following phases of risk management does implementation begin?

A. Risk assessment

B. Risk framing

C. Risk response

D. Risk monitoring

242. Which of the following is a traditional tool used in business for reporting performance metrics?

A. Pert chart

B. Venn diagram

C. Balanced scorecard

D. Compliance import

243. Which of the following is monitored after a risk response has been implemented?

A. The cost of maintaining controls

B. The continuing effectiveness of controls to protect assets

C. Incidences resulting from low threats

D. Asset value

244. Which of the following is an accepted international standard that is not focused specifically on information system risk, but is applied more broadly to an organization?

A. NIST RMF (SP 800-37r1)

B. ISO 31000:2009

C. ISACA Risk IT

D. ISO/IEC 27001:2005

245. All of the following are considerations during the continuous improvement process of risk

management, except:

A. Changes in threat

B. Changes in vulnerabilities

C. Environmental or system change

D. Cost of risk management program controls

246. Which of the following is the first step in threat modeling?

A. Determine who would want to exploit a given vulnerability

B. Determine if a given threat source has the means to exploit a vulnerability

C. Determine vulnerabilities

D. Identify assets

247. Which of the following terms is used to describe the process of identifying feasible adverse effects on our assets caused by threat sources?

A. Vulnerability assessment

B. Impact assessment

C. Threat modeling

D. Risk assessment

248. During reduction analysis of potential threats and attacks, which two of the following are goals? Choose two.

A. Reducing the threats

B. Reducing the assets

C. Reducing the vulnerabilities

D. Reducing the number of viableattacks

249. Which of the following terms describes a diagram that represents the attack pattern, by presenting decision points, specific conditions required for an attack, and end points for the attack?

A. Attack tree

B. Cause-and-effect diagram

C. Venn diagram

D. Vulnerability mapping

250. When performing risk management in the acquisition processes, all of the following are sound practices, except:

A. Minimum security requirements for all required software and hardware

B. Service level agreements

C. Third-party assessment, monitoring, and validation of products

D. Accepting product risk assessment results performed by the developing organization as the security baseline

251. As a general rule for mitigating attacks using attack trees and reduction analysis techniques, which of the following is true?

A. The closer you are to the root of the attack tree when you implement a mitigation technique, the more leaf conditions you will defeat with that particular mitigation or control.

B. The farther you are away from the root of the attack tree when you implement a mitigation technique, the more leaf conditions you will defeat with that particular mitigation or control.

C. The closer you are to the leaf nodes of the attack tree when you implement a mitigation technique, the more leaf conditions you will defeat with that particular mitigation or control.

D. The closer you are to the root of the attack tree when you implement a mitigation technique, the fewer leaf conditions you will defeat with that particular mitigation or control.

252. What is the most important reason training should be given at periodic intervals?

A. To meet compliance requirements

B. To respond to the constantly changing threat environment and vulnerabilities

C. To ensure employee training records are up to date

D. To ensure employees cannot say that they were not aware of security policies

253. For which of the following audiences are organizational security training programs created?

A. Management, staff, and customers

B. Technical employees, staff, and customers

C. Management, staff, and technical employees

D. Customers, contractors, and staff

254. Which of the following risk management frameworks is imposed on U.S. federal government agencies?

A. ISO 31000:2009

B. NIST RMF (SP 800-37r1)

C. ISACA Risk IT

D. COSO Enterprise Risk Management – Integrated Framework

255. Which of the following terms is used for the process that involves identifying threats?

A. Vulnerability assessment

B. Asset identification and valuation

C. Threat assessment

D. Threat modeling

第一章答案

1、 B .Copyright law protects the expression of an idea such as a book, song, painting, or even software code. Original work of authors cannot be copied or distributed without permission from the owner.

While the Software Protection Association (SPA) works hard to protect software vendors from piracy, it is an organization not a law.

Trade secrets protect resources that are proprietary and absolutely necessary for survival.

Trademarks are symbols, words, or pictures that uniquely identify something.

2、 D .The Internet Architecture Board (IAB) is an independent committee comprised of a wide variety of professionals. The board is divided into two specialized groups: the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF).

The IAB supports the belief that the Internet is a privilege and should be treated and used with

respect.

3、 A .The G8 is an annual economic and political summit meeting of the heads of government with international officials. One of the topics that is covered by this group is cybercrime.

4、 A .Trademarks can exist in a variety of forms—a word, shape, graphic, or phrase. The determining factor is whether or not that trademark alone represents the larger organization in the eyes of the public. McDonald's, for example, is known worldwide for its golden arches. This symbol is an identifier of the restaurant, and thus, falls under trademark law.

5、 C .Because laws were not addressing white collar crimes related to technology, the Federal Sentencing Guidelines were developed. These guidelines targeted the assumed responsibilities of senior executives and imposed maximum fines of $290 million per instance. However, these fines could be avoided if companies could prove due diligence and due care and the existence of company-wide security policies.

6、 B .Corroborative evidence cannot stand alone, but instead is used as supporting information in a trial. It is often testimony indirectly related to the case that offers enough correlation to augment the lawyer's argument.

The other choices are all types of evidence that can stand alone.

7、 A .Tort, or civil, law deals only with financial restitution or community service as punishments. Typically, civil lawsuits do not require the degree of burden of proof that criminal cases require.

Administrative law deals with government-imposed regulations on large organizations and companies in order to protect the safety and best interest of their employees and customers.

8、 C .Wiretapping is the act of intercepting electronic signals. It is illegal under the US Federal Wiretap Law without a court order. The most common example of wiretapping is with law enforcement agencies. In order for these organizations to legally "tap" into a suspect's line, there must be a court-approved order allowing it.

9、 C .A trade secret can be many things, but the cardinal rule is that it must provide the company with a competitive advantage. A restaurant's secret sauce would qualify as a trade secret, which means it could prosecute the waiter for violating the law.

10、 B .The (ISC)2 demands that its members follow four main canons of ethics. The canons listed on their web site (www.isc2.org) are:

- Protect society, the commonwealth, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

Visit www.isc2.org and read YOUR code of ethics in detail. There will most likely be questions related to the code of ethics on the exam.

11、 B .Secondary evidence is not a reliable form of evidence. Typically, oral evidence like testimonies, are placed in this category. Also, copies of documents are considered secondary in nature.

The other choices are all types of evidence that can stand alone.

12、 A .The Federal Sentencing Guidelines were developed to establish more detail on what is expected of executives within companies. The regulation promotes consistent due diligence and due care by the management team. If the executive can prove that proper due diligence and due care were practiced, then it is conceivable that he would not be liable in the suit.

13、 C .Even though it is the duty of every CISSP to report software piracy, disgruntled employees report the activity most often.

14、 D .The Internet Architecture Board (IAB) is an independent board made up of researchers, engineers, executives, and other technical personnel with experience and interest in the Internet industry.

The IAB does not have a government affiliation, so an FCC representative would not be appointed to the group.

15、 C .The concern with computer-generated files is that they can be fabricated after the fact simply for use in court. However, these types of files are usually critical in cybercrime cases, so a ruling was established to allow them in court. Thanks to the ruling in the Rosenberg vs. Collins case, computer files are admissible in court if they are generated during normal business hours.

16、 A .A good way to investigate cybercrime is with the acronym—MOM. It stands for motivations, opportunities, and means. Motivations are the "who" and "why" of a crime. Opportunities are the "where" and "when," and means involves the capabilities of criminals.

17、 A .Blue Boxing was the first major case of telephone fraud. In 1961, it was discovered that hackers were using an automated tone simulator that telephone switches perceived to be authorization for long distance charges. Other attacks followed including Red Boxes and Black Boxes.

18、 B .A crime scene investigator should use a notebook to compile evidence and establish a proper chain of custody. During a trial, the investigator can use the notebook as a personal resource, however it cannot be used as actual evidence.

19、 B .Enticement is a legal and ethical approach to fighting crime. Often companies will place

honeypot systems in the network that appear like functional systems to an attacker. It is legal for a company to record an attacker attempting to access this device.

Entrapment is illegal and unethical. It involves tricking a would-be attacker into a committing a crime. For example, if a company presents an opportunity to an attacker that appears to be innocent in nature, but when acted on, takes the intruder to unauthorized areas, this is entrapment.

20、 C .Real evidence is tangible and able to stand alone without the need for supplementary evidence. Usually real evidence consists of physical things that were captured from the crime scene. A videotape showing the suspect would be a good example of real evidence.

21、 B .The Gramm-Leech-Bliley Act of 1999 imposes many regulations on financial institutions. It starts with the requirement to notify customers of their privacy rights. In addition, the Act requires senior executives to be accountable for security issues and to provide training to all employees on related security procedures.

22、 C .Patents give full ownership to the inventor for a specified amount of time after it is granted. Patents are used on inventions that are novel, useful, and nonobvious. During the this time period, outside parties wishing to use the invention must pay a fee, however after this window of time, anyone can use it free of charge.

23、 B .In the Qualitative Risk Analysis approach, the Delphi technique is used to achieve honest results by directing individuals to submit their opinions anonymously. The technique is designed to allow participants to express their views without being influenced by others.

24、 A .System-specific policies are technical directives devised by management to protect individual systems. They can outline how a system should be accessed or how users should be trained on a specific system.

25、 C .Security awareness is a vital part of a successful security program. As the name implies, the goal is to make employees aware of the components of the security program. Employees can be informed in a variety of ways, such as e-mail, regular meetings, training classes, or by including security-related tasks in their performance plans.

Access control lists (ACLs) are security controls but do not contribute to security awareness.

26、 B .Risk management plays a key role in the overall security program. Managing risk is a daunting task because there are so many risks to contend with.

27、 A .Single loss expectancy (SLE) is a technique used in Quantitative Risk Analysis. SLE is a formula that helps a company assign financial value to a specific event. The calculation is:

Asset value × exposure factor (EF)

Exposure factor is the percentage of loss placed on an asset each time a threat is realized.

28、 B .Baselines are used to help companies and people understand the lowest level of security that must be provided. Baselines can be applied to individual systems, departments, firewalls, or human errors.

29、 C .Residual risk is the amount of risk remaining after the countermeasure has been implemented. To figure out the actual residual risk the team must identify and calculate total risk, which is threats × vulnerability × asset value. Then, the team must calculate the control gap, which is what the countermeasure cannot provide protection for. The result is residual risk. A company must decide if the residual risk falls within their acceptable level of risk. If it does, and a cost-benefit analysis has been carried out, then the countermeasure can be purchased and installed.

30、 B .Data custodians are typically system administrators. They are responsible for implementing and maintaining security controls, but not for choosing them or enforcing user activity. Their tasks can also include:

- Implementing access controls
- Updating software
- Backing up data
- Maintaining hardware and software
- Dealing with system errors

31、 A .Annualized rate of occurrence (ARO) is a measurement used in Quantitative Risk Analysis. The technique places a value on a threat based upon how many times it is likely to occur. This is an annualized value, so threats that will never happen are given a value of 0.0, while threats that will happen in a one year time span are 1.0. If a threat is estimated to happen once in ten years, the ARO value is 0.1, once in 100 years is 0.01.

32、 D .Security professionals perform a wide variety of tasks in maintaining a security program for a company. Although monitoring employees can fall under a security policy and thereby become the task of a security professional, the event must be relevant to security issues. Monitoring an employee for performance issues would be the responsibility of the employee's manager or human resources.

33、 C .Informative policies are meant to educate employees about events, new developments, or changes within a company. The messages are purely one-way, meaning employees are not responsible for doing anything after reading the document. An example would be a company-wide e-mail that details a recent reorganization of the board of directors.

34、 C .Security auditors are not members of the security team but outside parties that review the program to determine its effectiveness. Auditing procedures are required in many

organizations, particularly in government and financial institutions, where strict standards must be met.

35、 B .A policy providing information and rules about the use of ID badges when entering a facility is an example of an issue-specific policy. This differs from an organizational security policy, which is more general in nature.

36、 D .Although it is everyone's responsibility to abide by security policies and it is the responsibility of security professionals and IT groups to provide critical security functions, ultimate responsibility lies with senior management. This is why they make the big bucks! Senior management personnel are liable for properly protecting the company against threats and must demonstrate due diligence and due care.

37、 A .Security awareness has a host of benefits. Primarily, it serves to educate employees on the potential dangers and how to handle situations if they occur. However, no amount of training or security protection can stop an attack attempt. Attempts will happen, but it is the security program and awareness training that will help to reduce the effect the attempts will have on the company.

38、 D .Data that is deemed "public" has no security mechanisms placed upon it. It is freely available to anyone. There are many different classification levels that companies use today. Military organizations often have many more data classification levels than commercial companies.

39、 B .Nondisclosure agreements (NDAs) have become a common threat countermeasure in the world of business. A signed NDA prohibits an individual from sharing company information with outside parties. Failure to abide by the agreement has legal ramifications.

40、 D .Denying that a risk exists is not practicing due care and the company can be held liable if they take this approach.

The following are ways that risk should/can be dealt with:

- Risk reduction
  - Install security control
- Risk transfer
  - Buy insurance
- Risk acceptance
  - Live with the risks and spend no money on protection

41、 B .This types of question confuses many people in regard to what the CISSP exam is looking for. Data owners make decisions about which subjects can access the resources they own and are responsible for.

End users may or may not be the owners of their data. If a user creates a directory full of her own files and shares the directory out to the environment, she is the data owner and dictates who can access this information. However, she is not the data owner of the company’s financial reports, thus cannot dictate access to this information.

42、 C .Controls and safeguards put into place to mitigate risks need to carry out their intended protection activities and actually reduce the risk the company would face without them. If the controls do these things properly, they provide a return on investment, meaning the company benefits from the investment it made. If incorrect controls were purchased and implemented or the controls did not provide adequate protection, the company has no real return on investment.

43、 C .The Computer Fraud and Abuse Act was amended in 1996 to develop efforts to create a federal law for use in the growing instances of computer crime. It clarified the 1984 law and added three new crimes.

1. Using a federal computer in a fraudulent activity.
2. Modifying or damaging a federal computer or preventing use of the computer or information that causes a loss of $1000 or more.
3. Trafficking computer passwords that affects interstate or foreign commerce or allows unauthorized access to government computers.

44、 C .It does not matter if systems are used to their full capacity or not if they are not yours. Often attackers will use idle systems for their processing power in cracking passwords, cryptographic keys, or during distributed attacks. These systems are private property, not a resource to be used by the open community.

45、 B .The incident must be detected and then properly evaluated by the proper personnel. Evaluation needs to take place to ensure that a true intrusion took place and that it is not a result of misconfiguration or user error. Management needs to be notified of the incident because they will dictate what activities take place next. Management may want the issue contained and the vulnerability fixed or they may want data collected for evidence.

The intrusion needs to be contained and properly eradicated from the system(s).

46、 A .A chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented as evidence in court. Individuals and agencies responsible for ensuring these steps are followed can be seen as liable if the chain of custody is broken. Also, the evidence may not be admissible for the court case.

47、 C .A majority of the computer crimes that take place fall within the general labels of embezzlement, fraud, and wiretapping. There are several established laws in place to prosecute these types of crimes.

48、 B .While the other three answers could be examples of information warfare tactics, the

correct answer is the term's actual definition. Information warfare is action of attacking another nation's infrastructure to gain military advances through information gathering and intelligence, and carrying out active attacks to manipulate and possibly destroy systems and networks.

49、 D .The Common Law system is made up of criminal, civil, and administrative (or regulatory) law. Union law is just a distracter.

50、 A .Laws can be seen as subjective when making determinations between "right" and "wrong" and determining guilt and liability. But they are built upon society's expectations of activities in different situations. So a level of conduct is basically drawn in the sand and is used to judge others and their actions.

51、 C .Civil cases have to do with determining liability more than determining guilt, which applies to criminal law. Criminal laws are set up to protect society and are developed and enforced by the government. Civil law has to do with wrongdoings of individuals or companies that have caused some type of damage.

52、 A .Criminal law is used when an individual's conduct violates government laws which have been developed to protect the public. Jail sentences are commonly the punishment for criminal law cases versus civil law cases where the punishment is usually an amount of money that the guilty individual has to pay to the victim.

Criminal law has more strict requirements on proving one's guilt than civil law.

53、 B .In 1991, US Federal Sentencing Guidelines were developed and passed down to provide judges with courses of action when overseeing white collar crimes within organizations. These guidelines deal with antitrust, federal securities, mail and wire fraud, bribery, contracts, and money laundering. They provide ways that companies and law enforcement should prevent, detect, and report computer crimes. It outlines how senior executives are responsible for the computer and information security decisions they make and what actually takes place within their organizations and it sets a maximum fine of $290 million dollars.

54、 B .Many traditional laws address the abuse of another's property, but the laws always treated property as something physical and tangible. The definition of property has been expanded to include intangible property, as in electronic information.

55、C .The Health Insurance Portability and Accountability Act (HIPAA) is a new federal regulation, which has been mandated to provide national standards and procedures for the storage, use, and transmission of personal medical information and healthcare data.

56、 D .There are circumstances that could allow a law enforcement agent to seize evidence not included in the warrant, such as if a suspect tries to destroy the evidence. This is referred to as exigent circumstances, and a judge will later decide if this was carried out properly and legally so that the evidence can be admitted.

57、A .Motivations are the "who" and "why" of a crime. These motivations can either be induced by internal or external conditions. Opportunities are the "where" and "when" of a crime. Opportunities usually arise when certain vulnerabilities or weaknesses are present. Means pertains to the capabilities a criminal would need to be successful.

58、 A .If it can be proven that the evidence was not destroyed because someone may be trying to hide something and that other similar types of documents were destroyed as a regular business routine, then a copy of the evidence may be accepted.

59、 C .The company should explain to users that this type of monitoring may take place. Users can be informed through awareness training, login banners, and employee handbooks. This is done to explicitly tell employees they should not expect total privacy and that their actions can be monitored as well as their e-mail messages.

Monitoring should be done consistently across the board, meaning that monitoring should not happen only to specific people.

60、 A .Expert witnesses are used to explain complex topics to the judge and jury. They are deemed experts in their field, thus their opinions, educated guesses, and past experience are given a lot of credit. Non-expert witnesses are presented in court only to testify to what they saw or did not see or what they know about a specific crime, but not to their opinions about the activities of the crime.

61、 B .Evidence has its own life cycle and it is important that the individuals involved with the investigation understand the life cycle's different phases and properly follow them. The life cycle of evidence includes:

- Collection and identification
- Storage, preservation, and transportation
- Presentation in court
- Return to victim or owner

62、 B .A risk is the likelihood of a threat agent taking advantage of a vulnerability. A risk is the loss potential, or possibility and probability, that a threat agent will exploit a vulnerability. If a firewall has several ports open, there is a higher risk that an intruder will use one to access the network.

63、 D .The reason for using an automated tool is to reduce the amount of manual work. The tool already has a lot of data ported into it which means the team doesn't have to gather as much data. Plus, the data can be used for future risk assessments, making an automated tool an organized and efficient way of maintaining it.

The other answers are not necessarily wrong (except for the statement that the data would not

be reused), but D is the best answer because the tool reduces the amount of work involved.

64、 B .The data or information owner has the following responsibilities:

- Using predetermined criteria to classify the information.

- Identifying the data custodian who will be responsible for maintaining data and its security level.

65、 C .Although mandatory vacations may sound odd at first, they can be important for uncovering fraudulent activities. Employees carrying out fraud at their companies are less likely to take vacations for fear that someone might find out about their actions.

66、 A .The value of the data to the company is the most critical piece to calculate when determining classification levels. The value actually encompasses the other three answers.

The following issues should be considered when assigning value to information and assets:

- Cost to acquire or develop the asset
- Cost to maintain and protect the asset
- Value of the asset to owners and users
- Value of the asset to adversaries
- Value of intellectual property
- Price others are willing to pay for the asset
- Cost to replace the asset if lost
- Operational and productivity that is affected if the asset is unavailable
- Liability issues if the asset is compromised
- Usefulness of the asset

67、 A .The system owner is responsible for implementing and configuring the security controls. The data owner is responsible for outlining the security level required for the data and the appropriate use of the data.

A system can hold different types of data that may have different owners.

68、 C .The common methods used to test the security level of an environment are:

- War dialing
- Log review
- Password cracking
- Penetration testing
- Vulnerability testing
- Network mapping

These are the activities a hacker will most likely carry out, so they should be performed by the organization to determine the actual level of protection that is currently employed.

69、 C .Since the security policy is the crux of a security program it should be accessible to all employees in the company.

70、 C .When an activity is carried out and it disrupts a computer—either intentionally or accidentally—it can be referred to as a compromise.

71、 C .The forum should address the information in the other three answers and much more. Forum members are brought together to develop and oversee the implementation of a security program. This group does not usually address auditing and compliance—that task is for another group. Auditing is a tool to ensure the forum is on the right track and practicing due care.

72、 A .I know this question is confusing, but it is very representative of what you may encounter on the CISSP exam.

What the question is really asking is which of the following is conducted to find out how susceptible a company is to threats and compromises that can negatively affect it. That is the goal of a vulnerability assessment.

73、 C .When data is assigned a public classification, it means that it can be available to anyone inside or outside the company and not cause a risk.

74、 D .The user is considered any individual who routinely uses the data for work-related tasks. The user must have the necessary level of access to the data to perform the duties within her position and is responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others.

Information and data owners are the same.

75、 A .Risk analysis provides a cost-benefit comparison between the annualized cost of safeguards to protect against threats and the expected cost of loss. A safeguard, in most cases, should not be implemented unless the annualized cost of loss exceeds the annualized cost of the safeguard itself. This means that if a facility is worth $100,000, it does not make sense to spend $150,000 trying to protect it.

There maybe industry-specific regulations and laws that dictate that certain levels of protection must be provided, but a cost\benefit analysis is done so that the company can make good business decisions about different countermeasures.

76、 B .A security policy should state its purpose, the scope of the policy and security program, responsibilities that are assigned to specific roles in the company, and ramifications for noncompliance with the outlined directives.

77、 C .A lot of company data does not seem sensitive or secret at first. But in fact, this data can give potential attackers information that can be used against the company, especially in social engineering attacks. Thus, this data should only be available and used in-house.

78、 A .The reason companies should document these types of activities is to ensure that everyone follows the same procedures on different tasks. This action helps prevent new security vulnerabilities from being introduced with changes to the environment.

Although some organizations may have this as one of the things that is checked during auditing activities, not all companies do and passing an audit is not the reason documentation should be generated.

79、 C .Shoulder surfing is a common way that employees violate confidentiality policies. This happens when one person watches as another enters data into a computer or writes something down.

80、 B .Denial-of-service attacks overwhelm their victims with traffic, negatively affecting a computer or using an environment's bandwidth. When a system freezes, crashes, or reboots, it can become unavailable.

81、 D .It is impossible to list all of the threats to a company—there can be millions. One common misconception is that threats are only intentional in nature. This is inaccurate. Intentional and unintentional actions can cause harm to a company. Even the everyday mistakes of employees constitute a threat and thus, must be dealt with.

82、 B .Delayed loss can be exceptionally damaging to a company as their negative effects are experienced over a long period of time. As in this example, deleting customer billing information can cause a host of problems including the inability to invoice for past services or products received by customers, invoicing delays and thus delay in receiving payments, and delay due to billing disputes with customers.

83、 A .Risk analysis is a multistep process that requires research and planning. Assigning values to company assets is the first step. The steps that make up this procedure follow:

1. Identify assets and assign values to them.
2. Perform a threat analysis.
3. Derive an overall loss potential per threat.
4. Develop remedial measures to counteract each threat.

84、 D .Annual loss expectancy (ALE) determines the loss a company can incur if a specific threat is realized. In this example, the single loss expectancy (SLE) for the knowledge base server is $62,100. The annualized rate of occurrence (ARO) is 0.1.

SLE × ARO = ALE
$62,200 × 0.1 = $6200

85、 B .Collusion is the act of more than one individual working together to carry out fraudulent activities. Controls such as job rotation and separation of duties help to prevent and identify collusion attempts.

86、 C .NDAs are an effective mechanism for protecting internal information from leaking to the general public. If an individual who signed an NDA divulges protected information, she could be held liable for damages. However, NDAs are not intended to protect public information. By its nature, public information is accessible to people outside of the company.

87、 D .A data custodian is a broad term that includes system and network administrators and possibly media librarians. These individuals work to maintain and protect a company's assets, such as systems, networks, and data. A data owner, on the other hand, is a high-level employee who has the responsibility of classifying the data and delegating the daily operations to others.

A system administrator has the focus and responsibility of individual computers, where the network administrator has the focus and responsibility of the whole network. In smaller organizations these roles can be one and the same.

88、 C .A public data classification is the least secure in any organization. It can be compared to the military's "unclassified" level. Because the financial results of public companies are open to anyone, this type of data does not need security controls as strict as those for more sensitive information.

Internal phone directories should not be available because they can be used for social engineering and war dialing attacks.

While the question does not indicate that financial reports should not be protected, this is the best answer because the other answers are comprised of more sensitive data.

89、 C .A major theme in Qualitative Risk Analysis is that it includes opinions based on people's experience and knowledge. While this is typically true, the underlying difference between qualitative and quantitative is that qualitative categorizes threats and losses and quantitative places actual numeric and monetary value on them.

90、 A .A regulatory policy is regulated by law and is written to ensure that the organization is following standards set by a specific industry. This policy is detailed in nature and specific to a type of industry. Regulatory policies are used in financial institutions, health care facilities, and public utilities.

An advisory policy is written to strongly suggest that certain types of behaviors and activities should take place within the organization. It also outlines possible ramifications for

noncompliance. This is used for handling medical information, financial transactions, and processing confidential information.

An informative policy is written to inform employees on certain topics. It is not an enforceable policy, but one intended to teach individuals about specific issues relevant to the company. It could explain how the company interacts with partners, about the company’s goals and mission, or give a general reporting structure in different situations.

91、 B .Without strictly followed procedures, data classification can become loose and meaningless. The sequence of procedures is:

1. Specify classification criteria.
2. Data owner classifies data.
3. Identify data custodian and delegate responsibilities.
4. Data custodian puts controls in place and maintains them.
5. Incorporate into security awareness.

92、 C .A cascading error is when invalid results are passed on to another process. This type of problem can lie within an application's code and is very hard to identify.

93、 B .This is a dicey situation for companies. Extreme care and due care must be taken to ensure that the company is not later held liable for invading someone's privacy. In this example, the only action that could get the company into trouble is monitoring Peter's activity without notice. Most companies avoid this problem by issuing a company-wide notification that all employees are subject to monitoring. In this example though, the company would be in violation of Peter's privacy if his computer and telephone activity were suddenly monitored without him first being warned of the possibility.

94、 D .When determining if a specific countermeasure is a good business decision the following formula can be used:
Annual loss expectancy (ALE) before implementing safeguard – ALE after implementing safeguard – annual cost of safeguard = value of safeguard to the company

95、 B .A regulatory policy is regulated by law and is written to ensure that the organization is following standards set by a specific industry. This policy is detailed in nature and specific to a type of industry. Regulatory policies are used in financial institutions, health care facilities, and public utilities.

An advisory policy is written to strongly suggest that certain types of behaviors and activities should take place within the organization. It also outlines possible ramifications for noncompliance. This is used for handling medical information, financial transactions, and processing confidential information.

An informative policy is written to inform employees on certain topics. It is not an enforceable

policy, but one intended to teach individuals about specific issues relevant to the company. It could explain how the company interacts with partners, about the company’s goals and mission, or give a general reporting structure in different situations.

96、 B .Good countermeasures are independent components. The more a security control has to depend on other components, the more vulnerable it can be. If one of these other components fails, the security control could be disabled in some way.

97、 B .Reducing the risk is the act of employing a countermeasure in order to mitigate the risk. This example is common in companies. They try to live with the threat until it becomes too expensive. Then, a countermeasure is put into place to reduce the expense and risk.

98、 C .With all the different types of controls and all the different ways companies use them, it sometimes seems that every security measure can fall under all of the control types. They can get confusing. However, in this example, there is only one possible answer— accountability. Auditing tools cannot be physical, corrective, or administrative controls. If detective had been listed, it would have been another valid choice when referring to audit trails.

In order to enforce true individual accountability, audit logs should capture unique user identification information.

99、 B .Social engineering is a serious concern for companies trying to protect its assets and sensitive information. It involves one person tricking another person into revealing restricted and useful information. Intercepting e-mail messages is not the correct answer is because it does not necessarily involve trickery or pretending to be someone else.

100、 A .Operational goals are daily tasks carried out to ensure that production is not negatively affected. Tactical goals are short term in nature but may require several steps or phases in order to complete. Strategic goals are long term in nature and involve forward thinking. Whenever you look at all three goals, it is referred to as the "planning horizon."

In most cases, a network needs to be centrally controlled (possibly implementing domain controllers) before a PKI can be incorporated.

101、 D .The separation of duties ensures that no one individual carries out critical tasks alone, thus helping to limit opportunities for fraud. A company can be considered negligent if one individual is allowed to perform a critical task that can negatively impact the company as a whole.

102、 D .Rejecting risk and threat potential is a violation of the due care responsibility that each company's management team is held liable for. Rejecting risk means ignoring it exists and neglecting to take any steps to mitigate the risk.

103、 D .Announcing or displaying safeguards makes it less appealing for attackers because they see it is more likely they will be caught or their tasks made more complicated. But there is still a

fine line. The existence of controls should be known, but the actual configurations and detailed information should not be easily accessed so that users and attackers cannot disable them.

104、 A .Part of security management is identifying vulnerabilities within systems, networks, and companies. A vulnerability is a weakness in a control (or an absence of a control) that can be capitalized on by a threat agent. A threat is a threat agent uncovering the vulnerability and using it.

105、 C .The single loss expectancy (SLE) is calculated by multiplying the asset value by the exposure factor (EF). The SLE is the estimate of loss for a particular asset if a specific threat became true, meaning that there was an actual exposure. The SLE is inputted into the annual loss expectancy (ALE) formula to determine how much money can be spent to protect against that threat.

106、 C .The Delphi technique uses each person's honest opinion in a group setting to get a wide range of ideas on how to address an issue. It allows people to submit their opinions anonymously to ensure that they are not intimidated or bullied by others who might sway them from giving their honest feelings on a specific subject.

107、 D .Shoulder surfing is a type of attack where someone looks over another's shoulder and views information not intended for him. A video recorder can be used for this purpose, thus is an example of a shoulder surfing attack.

108、 B .Companies should ensure that their employees sign a nondisclosure agreement, which states that they are not to give or share any of the company's intellectual property. Employees should be asked to review this document, and possibly sign it again, upon termination.

109、A .The annualized rate of occurrence (ARO) is a value used in calculating the annualized loss expectancy value (ALE). ARO is how many times a threat is expected to take place. If it is estimated that a threat will exploit a vulnerability once in ten years, the ARO value is 0.1. If it is estimated to take place once in 100 years, the ARO is 0.01.

110、D .If an individual is not abiding by the company's policy and security standards, you should tell management or that person's supervisor. You should not take matters into your own hands or approach the individual yourself.

111、 D .The goal of security awareness training is to change employees' attitudes toward security. If they are informed and involved, there is a greater likelihood of them helping, not hindering, the process.

112、 C .Internal employees have a wide range of access to company assets. Damages can be caused by mistakes, misconfigurations, or misdeeds.

113、 C .Regulatory policy is regulated by law and is written to ensure that the organization is

following standards set by a specific industry. It is detailed in nature and specific to a type of industry.

Advisory policy is written to strongly suggest certain types of behaviors and activities that should take place within the organization. It also outlines possible ramifications for noncompliance.

Informative is written to inform employees of certain topics. It is not an enforceable policy, but is intended to teach individuals about specific issues relevant to the company.

114、 D .Users should not classify and declassify data on their own. The data owner determines the classification of data and when it should be declassified. The following are the steps of classification:
1. Identify data custodian who will be responsible for maintaining data and its security level.
2. Specify the criteria that will determine how data is classified.
3. Data owner must indicate the classification of the data she is responsible for.
4. Indicate the security controls that are required for each classification level.
5. Document any exceptions to the previous classification issues.
6. Indicate the methods that can be used to transfer custody of the information to a different data owner.
7. Indicate termination procedures for declassifying the data.
8. Integrate these issues into the security awareness program so that all employees understand how to handle data at different classification levels.

115、 A .Senior management is responsible for driving security, but not carrying out specific implementation or auditing tasks. The following describes the different security roles within a company:

Senior manager — Ultimately responsible for organization's security and the protection of its assets

Security professional — Functionally responsible for security and carries out senior manager's directives

Data owner — Determines classification of data within the organization

Data custodian — Maintains data in ways to preserve and protect its confidentiality, integrity, and availability

User — Uses data for data-processing tasks

Auditor — Examines security practices and mechanisms within the organization

116、 B .Biometric authentication systems fall under the category of technical controls. Technical controls are defined as logical controls that are put into place to protect assets. They can be

access controls, encryption, security devices, and identification and authentication systems.

117、 C .The AIC triad refers to availability, integrity, and confidentiality. A company needs to be concerned with each of these aspects for each of its assets.

118、 C .A countermeasure is put into place to reduce, or mitigate, risk. The countermeasure can be software products, new configurations of current software, new devices, or new procedures. Each of these is put into place to protect against specific threats.

119、 C .Senior management should be the initiators of a security program. With buy-in from the top, a successful top-down approach can begin. This means the program will get more attention, funds, and enforcement compared to a bottom-up approach.

120、 D .A company may identify a vulnerability, which is a weakness or a lack of a safeguard. Then they need to identify the threat agent that could capitalize on this vulnerability. The threat lies in the possibility that someone would exploit this vulnerability. The probability of this taking place is the risk, which has to be calculated.

121、 D .In defining a planning horizon, you will need to define your strategic goals, which are your long-term goals, your tactical goals or mid-term goals, and your operational goals, which are your daily goals.

122、 B .Performing a risk analysis will provide a means to justify the expense and the countermeasures that must be implemented. It will outline the possible threats and current weaknesses, which is necessary in building a case for purchasing and implementing a countermeasure.

123、 B .The following government data classifications are organized from most sensitive to least sensitive: top secret, secret, confidential, sensitive but unclassified, unclassified.

124、 B .Purchasing insurance to help mitigate risk is a means of transferring that risk to a third party, making the remaining risk acceptable.

125、 A .Security policies are statements that originate with senior management. Standards are drawn up to provide uniform ways of carrying out the directives of the security policies and are considered rules. Guidelines are recommendations. Procedures are detailed step-by-step actions.

126、 D .The correct answer is the only answer that pertains to the company as a whole concerning security from an organizational view. The ultimate goal is to educate users about security so that they can be part of the solution and not part of the problem.

127、 B .The data owner is the one who decides on the classification of the data. The data custodian is the one assigned by the owner to manage and maintain the data.

128、 B .The only answer which pertains to a reasonable (and possible) employment request is the mandatory signing of a nondisclosure agreement (NDA). The NDA is put into place to tell the employee the company's expectations of him pertaining to the treatment and handling of sensitive information. It also gives the company a legal basis for carrying out ramifications if the expectations are not met.

129、 A .A quantitative approach employs calculations using statistics of probabilities and ratios pertaining to the possibilities of specific threats. A qualitative approach is more subjective, using opinion polls and other subjective means to identify the priority of threats that pose possible risks.

130、A .A salami attack is when several small crimes are committed with the hope that the larger crime will not be noticed. Taking a few pennies from several accounts is just one example, but it is one of the more common types of salami attack.

131、 A .The life cycle of evidence encompasses collection and identification, storage, preservation, transportation, presentation in court, and return to victim or owner.

132、 C .Copyright law protects the expression of ideas instead of the ideas themselves. This book is protected by copyright law which restricts others from copying and distributing it without the owner's permission. The law does not mean that the data cannot be used as a reference somewhere else, but the way the author expresses the data cannot be copied.

133、 A .Administrative law deals with the standards and regulations that companies and organizations must abide by and follow.

134、 A .CISSPs must know and abide by the Code of Ethics and can be subject to a peer review panel if any of the guidelines are violated. Giving answers related to the CISSP exam is a violation of the Code of Ethics considering that all students have signed a nondisclosure agreement (NDA) before the exam. For further information, please go to www.isc2.org.

135、 D .Because an attacker is not actually "doing something," wiretapping is considered a passive attack. However, wiretapping is illegal and unethical, unless there is a specific court order.

136、 A .Despite what many may think, a CISSP's first duty is not to his or her profession, but to public safety, principles, and individuals.

137、 C .Entrapment is when an attacker is misled into doing wrong and it is considered illegal. Enticement is luring a person to something, but not tricking him. A honeypot system is a sacrificial computer put up so that attackers will attack it instead of critical production systems. This is an example of enticement.

138、 B .Interrogations should be well thought out in order to obtain the most useful information that can be submitted and used in trial.

139、 B .Motive is the "who" and "why" of a crime. Opportunity is the "where" and "when" of a crime. Means are the capabilities of criminals to commit crimes.

140、 C .Criminal laws protect society and see all of society as a victim when one of these laws is broken. The reprimands can be in the form of jail time, whereas civil cases do not use jail time as a possible punishment.

141、 D .Data diddling means altering data before it goes into a system or as soon as it comes out. In this example, the customer can order three tacos, but the cashier only enters one taco and still charges the customer for three. The cashier then keeps the money that the customer gave him for the other two tacos.

142、 A .Thorough research should be done when handling business internationally because each country has different ways of dealing with computer technologies and the crimes associated with these issues.

143、 D .The Software Protection Association (SPA) and Business Software Alliance (BSA) were formed to protect software vendors and their licenses against piracy.

144、 B .Law enforcement agents must perform a legal search and seizure of evidence for it to be admissible into court. Private citizens do not fall under all the same restrictions as law enforcement agents.

145、 B .Collecting evidence does not involve the courts at the beginning of an investigation, unless law enforcement agents are involved and need a search warrant. The other items are important to complete in any computer crime investigation.

146、 A .Masquerading is when someone pretends to be someone else and is a type of personnel attack. Data diddling and wiretapping are seen as operational attacks, and dumpster diving is a physical security attack.

147、 C .Blue Boxing was the process of simulating a frequency tone, which allowed attackers to gain free long distance phone service. This tone was interpreted by the telephone company's equipment as a valid command. Phreakers developed or purchased devices that made this tone to obtain free long distance calls.

148、 A .Companies that share network access with outside parties have a downstream liability to contend with. Downstream liability means that a company can be legally responsible if they put partners at risk by not practicing due care procedures.

149、 C .In order for a company to be liable, proximate causation must be proven. This means that it can be proven that the company was actually at fault and responsible for a negative activity that took place.

150、 B .The Electronics Communications Privacy Act of 1986 outlined the procedures law enforcement agents had to complete before they could eavesdrop on individuals. It dealt mainly with wiretapping, but as more communications happened through computers, networks, and e-mail, the act was extended to encompass those technologies, too.

151、 A .The Privacy Act of 1974 protects individuals' personal information that is held in federal databases. Data can only be used for the purpose that it was collected. It cannot be shared with third party entities without the individual's consent, and the individual should be able to submit changes if the collected information is incorrect.

152、 A .The (ISC)2’s Code of Ethics touches on several items, one of them being that a security professional should not participate in an activity that clearly shows a conflict of interest.

153、 D .In most cases, law enforcement agents will work with a company that reported a computer crime so that the investigation does not negatively affect the company. Critical systems and data should be identified and a request of copying the data for future use should be made. Backup copies will not be acceptable to the agents for investigation. Companies will not have the freedom of telling the agents what they can and cannot obtain during the investigation.

154、 A .The most important piece in investigating any crime is the collection of evidence. The evidence must be properly collected and controlled to ensure that it is not compromised in any way. Before actually touching the computer, peripheral devices, or cables, the area and system should be photographed. This can be used later in court to prove what the environment looked like before any forensics work took place.

155、 C .The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage.

156、 C .This answer violates several of the stipulations in the code, specifically the one dealing with taking on only the jobs you are qualified to perform. To protect the reputation of the CISSP certification, no one with this credential should accept jobs that he/she is not qualified for.

157、 C .Most laws are drawn from ethics and are put in place to ensure that others act in an ethical manner.

158、 C .Many computer crimes are not discovered by a company. They also tend to go unreported when discovered due to embarrassment or fear that it will negatively affect the company's reputation.

159、 C .These are the people a company should have on its incident response team to cover any issues arising from an incident. It may not be necessary to involve each of these individuals with every incident, but the members of the team should be selected and understand their responsibility if called upon.

160、 C .Each country has its own set of laws and practices, and they need to be followed and understood.

161、 B .The Federal Sentencing Guidelines were extended to cover computer crimes. They specified that senior corporate officers could be held personally responsible and forced to pay up to $290 million in fines if their company did not comply with the laws set out for them.

162、 A .A trademark is used to protect a word, name, symbol, sound, shape, color, device, or combination of these. A company would trademark these because they represent their company to the world.

163、 A .Patents are given to individuals or companies to grant them legal ownership and enable them to exclude others from using or copying the invention covered by the patent.

164、 C .HIPAA was specifically designed to provide protection and privacy of an individual's medical information.

165、 C .In order for documents to be admissible in court as evidence other than hearsay, they would have to have been created during the normal course of operations.

166、 B .An individual who is not acting as an agent for the police in many cases can seize property for legal prosecution. Private citizens are not subject to protecting the Fourth Amendment rights of others unless they are acting as police agents.

167、C .Permissions and rights are usually continually given and not taken away from individuals. Employees can usually cause the most damage because of the privileged access they already have to assets. Many times these employees do not need the level of access they have to company resources.

168、 A .There can be a threat, but unless your company has the corresponding vulnerability the company is not exposed and it is not a vulnerability. If the vulnerability does reside in the environment, then a countermeasure is applied to reduce the risk. A vulnerability is a weakness, the threat is that someone can exploit it. The risk is the probability and business impact of this and a countermeasure is a control used to reduce the risk.

169、C .The most commonly used standard is the ISO 17799 which was derived from the de facto standard British Standard 7799 (BS 7799). It is an internationally recognized Information Security Management Standard that provides high-level, conceptual recommendations on enterprise security. These are commonly recognized as best practices and organizations can be certified against them.

170、 C .The sections of ISO 17799 follow:

A. Information security policy

i. Addresses mapping of business objectives to security, management's support, security goals, and responsibilities.

B. Creation of security infrastructure

i. Create and maintain an organizational security structure through the use of security forum, security officer, defining security responsibilities, authorization process, outsourcing, and independent review.

C. Asset classification and control

i. Develop a security infrastructure to protect organizational assets through accountability and inventory, classification, and handling procedures.

D. Personnel security

i. Ability to reduce risk that is inherent with human interaction through employee screening, defining roles and responsibilities, training, and ramifications of not meeting expectations.

E. Physical and environmental security

i. Protect an organization's assets through proper facility location, erecting and maintaining a security perimeter, implementing access control, and equipment protection.

F. Communications and operations management

i. Carry out operations security through operational procedures, proper change control, incident handling, separation of duties, capacity planning, network management, and media handling.

G. Access control

i. Control access to assets based on business requirements, user management, authentication methods, and monitoring.

H. System development and maintenance

i. Implementing security in all phases of a system's lifetime through development of security requirements, cryptography, integrity, and software development procedures.

I. Business continuity management

i. Counter disruptions to normal operations by using continuity planning and testing.

J. Compliance

i. Be in compliance with regulatory, contractual, and statutory requirements with the use of technical controls, system audits, legal awareness.

171、A .Information risk management (IRM) is the process of identifying, assessing, and reducing risk to an acceptable level and implementing the right mechanisms to maintain that level of risk.

172、 A .This policy provides the infrastructure for the organization's risk management processes and procedures and should address all issues of information security, from personnel screening and the insider threat to physical security and firewalls. It should provide direction on how the IRM team should relay information on company risks to senior management and how to properly execute management's decisions on risk mitigation tasks.

173、 B .An organization's acceptable risk level needs to be set by the people ultimately responsible—senior management. Often they will work with a security analyst to help them understand their current risk level, government regulation requirements, and other items which all factor into establishing it. But senior management has to "sign off" on the level, thus they are

ultimately the ones who set it.

174、 B .A risk analysis has four main goals: identify assets and their values, identify vulnerabilities and threats, quantify the probability and business impact of these potential threats, and provide an economic balance between the impact of the threat and the cost of the countermeasure. Risk analysis provides a cost-benefit comparison where the annualized cost of safeguards is compared with the potential cost of loss.

175、 D .It is important to determine the scope of a project before beginning—anyone who has worked on a project without a properly defined scope can attest to this. Before starting an assessment and analysis, the team needs to carry out project sizing. This means understanding what assets and risks are to be evaluated.

176、 A .Managers will tend to delegate any sort of risk analysis task to lower levels within the department. However, these lower levels may not have adequate knowledge or a thorough enough understanding of the processes that the risk analysis team may need to deal with.

177、 C .ARO is an annual value that is used in the calculation of the annual loss expectancy (ALE), so it is multiplied by the single loss expectancy (SLE) value. The range can be from 0.0 (never) to 1.0 (at least once a year), to greater than one (several times a year) and anywhere in between. Once in 1000 years is 0.001.

178、 A .When a company decides to accept a risk it should be a decision based on cost (countermeasure costs more than potential loss) and pain (company can live with the vulnerability and threat). But the company must also understand that accepting a specific risk is a visibility decision in that it may impact their industry reputation.

179、 A .SLE = asset value × exposure factor, so $140,000 = $400,000 × 0.35

ALE = SLE × ARO, so $14,000 = $140,000 × 0.1

SLE = $140,000 ALE = $14,000

180、 D .Uncertainty refers to the degree of a lack of confidence. This value is expressed as a percentage figure, from 0.0 to 100 percent. If one has a 30 percent confidence level in something, then it could be said that they have a 70 percent uncertainty level. Capturing the degree of uncertainty when carrying out a risk analysis is important because it will indicate the level of confidence the team and management should have in the resulting figures.

181、 A .The consensus Delphi method, when used in risk analysis, helps identify the highest priority security issues and corresponding countermeasures. Another Delphi method, the modified Delphi technique, is a silent form of brainstorming. Participants develop ideas individually and silently with no group interaction. The ideas are submitted to a group of decision makers for consideration and action.

182、 C .The formula for calculating the value of a countermeasure is (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the company.

183、 A .The security policy has several important characteristics that need to be understood and implemented:

- Business objectives should drive the policy's creation, implementation, and enforcement. The policy should not dictate business objectives.
- It should be an easily understood document that is used as a reference point for all employees and management.
- It should be developed and used to integrate security into all business functions and processes.
- It should be derived from and support all necessary legislation and regulation applicable to the company.
- It should be reviewed and modified as a company changes through adopting of new business models, merging with another company, or being purchased.
- Each iteration of the policy should be dated and under version control.

184、 D .All other definitions are correct. Standards affect all employees, not just the executive staff.

185、 A .Trick question. Having a lot of classifications can cause confusion and frustration for the individuals who use the system. The classifications should not be too restrictive and detail-oriented because many types of data may need to be classified. Each classification should be unique and separate from the others and not have any overlapping effects.

186、 C .A security program is put into place to protect the company’s assets, but cannot ensure or improve the accuracy of data.

187、 A .COBIT is a framework developed by the Information Systems Audit and Control Association (ISACA). It provides a comprehensive framework that assists enterprises in achieving their goals and delivering value through effective governance and management of enterprise IT COBIT.

188、 B .The COSO framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission in 1985 for providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.

189、 B .COBIT provides a comprehensive framework that assists enterprises in achieving their goals and delivering value through effective governance and management of enterprise IT. COSO is a model for corporate governance, and COBIT is a model for IT governance and management. COSO deals more at the strategic level, while COBIT focuses more at the operational level. You can think of COBIT as a way to meet many of the COSO objectives, but only from the IT perspective. COSO deals with non-IT items also, as in company culture, financial accounting

principles, board of director responsibility, and internal communication structures.

190、 A .The following indicates what the different ISO 27000 series standards cover:

- ISO/IEC 27001: Based on British Standard (BS) 7799 Part 2, which is establishment, implementation, control, and improvement of the Information Security Management System
- ISO/IEC 27002: Code of practice providing best practices advice on ISMS (previously known as ISO 17799, which is itself based on BS 7799 Part 1, last revised in 2005 and renumbered ISO/IEC 27002:2005)
- ISO/IEC 27004: A standard for information security management measurements
- ISO/IEC 27005: Designed to assist in the satisfactory implementation of information security based on a risk management approach
- ISO/IEC 27006: A guide to the certification/registration process
- ISO/IEC 27799: A guide to illustrate how to protect personal health information

191、 C .The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management. ITIL was created because of the increased dependence on information technology to meet business needs.

192、 A .COBIT and COSO provide the “what is to be achieved,” but not the “how to achieve it.” This is where the ITIL and ISO\IEC 27000 series come in. Where COBIT defines IT goals, ITIL provides the steps at the process level on how to achieve those goals.

193、 B .ITIL’s focus is internal service level agreements (SLAs) between the IT department and the “customers” it serves. The customers are usually internal departments. ITIL was created because of the increased dependence on information technology to meet business needs.

194、 B .NIST SP 800-30 and 800-66 are methodologies that can be used by the general public, but their initial creation was designed to be implemented in the healthcare field or other regulated industries. They were designed to be used by Health Insurance Portability and Accountability Act (HIPAA) clients.

195、 A .FRAP is designed with the intention of exploring a qualitative risk assessment process in a manner that allows for tests to be conducted on different aspects and variations of the methodology. The intent of this methodology is to provide an organization with the means of deciding what course of action must be taken in specific circumstances to deal with various issues.

196、 A .Failure Modes and Effect Analysis (FMEA) is a method for determining failures, identifying functional failures, and assessing the causes of failure and their effects through a structured process. The application of this process to a chronic failure enables one to determine where exactly the failure is most likely to occur.

197、 B .Six Sigma is a process improvement methodology. It is the “new and improved” Total Quality Management (TQM) that hit the business sector in the 1980s. Its goal is to improve

process quality by using statistical methods of measuring operational efficiency and reducing variation, defects, and waste.

198、 D .The “Safe Harbor” framework outlines how any entity that is going to move privacy data to and from Europe must go about protecting it. U.S. companies that deal with European entities can become certified against this rule base so that data transfer can happen more quickly and easily.

199、 B .A security steering committee is responsible for making decisions on tactical and strategic security issues within the enterprise as a whole and should not be tied to one or more business units. The group should be made up of people from all over the organization so they can view risks and the effects of security decisions on individual departments and the organization.

200、 D .A threat to a company does not exist without a vulnerability. A vulnerability characterizes the absence or weakness of a safeguard that could be exploited and, if identified by someone or something, then becomes a threat.

201、 B .Availability, Integrity, and Confidentiality are referred to as the AIC Triad. Availability means the systems and networks should provide adequate capacity in order to perform in a predictable manner with an acceptable level of performance. Integrity is upheld when the assurance of accuracy and reliability of information and systems are provided, and unauthorized modification is prevented. Confidentiality ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure.

202、 A .Shoulder surfing is when a person looks over another person’s shoulder and views data that he is not authorized to view.

203、 A .DoS attacks are popular methods for hackers to disrupt a company’s system availability and productivity. These attacks are mounted to reduce the ability of users to access system resources and information. To protect against these types of attacks, only the necessary services and ports should be available on systems, and intrusion detection systems should monitor the network traffic and host activities. Certain firewall and router configurations can also reduce the threat of DoS attacks and possibly stop them from occurring.

204、 C .By protecting against environmental issues, one is ensuring that the system remains available. Integrity is upheld when the assurance of accuracy and reliability of information and systems are provided and unauthorized modification is prevented.

205、 C .ISO 17799 was the de facto standard and the most commonly used standard for organizational security programs before the development of the ISO/IEC 27000 series. It consists of two parts. Part 1 is an implementation guide with guidelines on how to build a comprehensive information security infrastructure. Part 2 is an auditing guide based on requirements that must be met for an organization to be deemed compliant with ISO 17799. It is the benchmark used to indicate a “correct security infrastructure.”

206、 D .Administrative controls (“soft” controls) include policies, procedures, standards, and guidelines; employee management; testing and drills; risk management and analysis; information classification; and awareness training. Technical controls (logical controls) include firewalls, intrusion detection systems (IDSs), encryption, protocols, authentication mechanisms, auditing, and access control technologies. Physical controls consist of doors, windows, and walls; security guards and dogs; fencing and lighting; locks; environmental controls; and monitoring for intruders.

207、 B .A threat agent is an entity that takes advantage of a vulnerability. It could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy, a tornado wiping out a facility, or an employee making an unintentional mistake that could expose confidential information or destroy a file’s integrity.

208、 D .Security through obscurity is not implementing true security controls, but rather attempting to hide the fact that an asset is vulnerable in the hope that an attacker will not notice. Security through obscurity is an approach to try and fool a potential attacker, which is a poor way of practicing security. Vulnerabilities should be identified and fixed, not hidden.

209、 C .Confidentiality should prevail while data reside on systems and devices within the network, as they are transmitted, and once they reach the destination. Confidentiality can be provided by encrypting data as they are stored and transmitted; by using network traffic padding, strict access control, and data classification; and by training personnel on the proper procedures.

210、 C .Open standards are publicly available specifications for achieving a specific task. By allowing anyone to use the standard, compatibility is increased between various hardware and software components, since anyone with technical know-how and the necessary equipment to implement solutions can build something that works together with those of other vendors.

211、 B .The risk analysis team is made up of members from various departments. If this is not possible, the team should make sure to interview people in each department so that all risks are fully understood and quantified. The risk analysis team also needs to be made up of people who understand the processes that are part of their individual departments.

212、 C .A risk analysis has four main goals: identify assets and their values, identify vulnerabilities and threats, quantify the probability and business impact of these potential threats, and provide an economic balance between the impact of the threat and the cost of the countermeasure. The results of the risk analysis are provided to help management take the necessary steps for security.

213、 C .A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the effectiveness of safeguards. In general, the greater the likelihood of a threat occurring, the greater the risk.

214、 A .Failure Modes and Effects Analysis (FMEA) helps select remedial actions that reduce cumulative impacts of life-cycle consequences (risks) from a systems failure (fault). By adapting hazard tree analysis to facilitate visual learning, this method illustrates connections between multiple contributing causes and cumulative (life cycle) consequences. The basic process is to take a description of the parts of a system and list the consequences if each part fails.

215、 D .: Qualitative research is one of the two major approaches to research methodology in social sciences. Qualitative research involves an in-depth understanding of human behavior and the reasons that govern it. Unlike quantitative research, qualitative research relies on reasons behind various aspects of behavior. Simply put, it investigates the why and how of decision making, as compared to the what, where, and when of quantitative research. Hence, the need is for smaller but focused samples rather than large random samples. Qualitative research categorizes data from these samples into patterns as the primary basis for organizing and reporting results.

216、 C .The exposure factor (EF) represents the percentage of loss a realized threat could have on a certain asset. So, for example, if a data warehouse has an asset value of $150,000, it might be estimated that if a fire were to occur, 25 percent (EF) of the warehouse would be damaged, in which case the single loss expectancy would be $37,500.

217、 A .Annualized rate of occurrence (ARO) is equal to once in five years (1 / 5 = 0.2). The ARO is the value that represents the estimated frequency of a specific threat taking place within a one-year timeframe. ARO range can be anywhere between 0 and infinity.

218、 B .Asset value (AV) × exposure factor (EF) = SLE, so $275,000 × 30% = $82,500.

219、 C .A risk can have delayed loss and/or delayed damages, meaning that losses can be experienced over time or damages can be experienced at a later date.

220、 B .A layered approach presents layers of barriers that an attacker must go through and compromise to get to the sought-after resource.

221、 D .The Sherwood Applied Business Security Architecture (SABSA) slices an enterprise into different layers so that security can be more focused and precise. The model is made up of six layers. Each layer represents a different view of the organization and the types of security controls that need to be put into place.

222、 A .ISO follows the Plan – Do – Check – Act (PDCA) cycle, which is an iterative process that is commonly used in business process quality control programs.

223、 B .TOGAF is a framework that can be used to develop the following architecture types:

- Business architecture
- Data architecture
- Applications architecture

- Technology architecture

224、 B .An enterprise security architecture is a subset of an enterprise architecture and defines the information security strategy that consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally. It is a comprehensive and rigorous method for describing the structure and behavior of all the components that make up a holistic information security management system (ISMS). The main reason to develop an enterprise security architecture is to ensure that security efforts align with business practices in a standardized and cost-effective manner. The architecture works at an abstraction level and provides a frame of reference. Besides security, this type of architecture allows organizations to better achieve interoperability, integration, ease of use, standardization, and governance.

225、 B .The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management. ITIL was created because of the increased dependence on information technology to meet business needs.

226、 B .Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.

227、 D .Controls are not implemented and tested during these phases. Risk assessments and analysis can help identify the necessary controls, but they are not implemented during these processes. A risk assessment is a method of identifying vulnerabilities and threats, and assessing the possible impacts to determine where to implement security controls. A risk assessment is carried out, and the results are analyzed. Risk analysis is used to ensure that security is cost effective, relevant, timely, and responsive to threats. Risk analysis helps companies prioritize their risks and shows management the amount of resources that should be applied to protecting against those risks in a sensible manner.

228、 D .This NIST methodology is named a “Risk Management Guide for Information Technology Systems” and is considered a U.S. federal government standard. It is specific to IT threats and how they relate to information security risks. It is not considered an international standard.

229、 D .ISO/IEC 27005 is an international standard for how risk management should be carried out in the framework of an information security management system (ISMS).

230、 A .The correct steps for Failure Modes and Effect Analysis are as follows:

1. Start with a block diagram of a system or control.
2. Consider what happens if each block of the diagram fails.
3. Draw up a table in which failures are paired with their effects and an evaluation of the effects.
4. Correct the design of the system, and adjust the table until the system is not known to have unacceptable problems

231、 B .A fault tree analysis usually proves to be a useful approach to identifying failures that can take place within more complex environments and systems. Fault tree analysis follows this general process. First, an undesired effect is taken as the root or top event of a tree of logic. Then, each situation that has the potential to cause that effect is added to the tree as a series of logic expressions. Fault trees are then labeled with actual numbers pertaining to failure probabilities.

232、 C .Vulnerability assessments are used to identify the vulnerabilities. A risk assessment calculates the probability of the vulnerabilities being exploited and the associated business impact.

233、 D .There are no real standards for qualitative or quantitative approaches. The most critical element of any risk analysis is that the correct data are used for the best business decisions to be made.

234、 D .If a company decides the total risk is too high to gamble with, it can purchase insurance, which would transfer the risk to the insurance company. If a company decides to terminate the activity that is introducing the risk, this is known as risk avoidance. Another approach is risk mitigation, where the risk is reduced to a level considered acceptable enough to continue conducting business. The last approach is to accept the risk, which means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure.

235、 B .A baseline refers to a point in time that is used as a comparison for future changes. Once risks have been mitigated and security put in place, a baseline is formally reviewed and agreed upon, after which all further comparisons and development are measured against it. A baseline results in a consistent reference point.

236、 C .An information security management system (ISMS) is a coherent set of policies, processes, and systems to manage risks to information assets as outlined in ISO\IEC 27001.

237、 D .Security has functional requirements, which define the expected behavior from a product or system, and assurance requirements, which establish confidence in the implemented products or systems overall.

238、 D .Data breaches can be thought of as the opposite of privacy: data owners lose control of who has the ability to access their data.

239、 D .Processes are typically developed internally by the organization, and employs various hardware, software, and services that could be provided by an external party. Those externally provided items must undergo a risk assessment, and preferably should be validated by an external third party.

240、 A .A control, in most cases, should not be implemented unless the annualized cost of loss

exceeds the annualized cost of the control itself. For example, if an asset costs $10,000, then it makes no sense to spend $50,000 to protect it.

241、 C .Implementation begins after risk has been framed and assessed, and begins with risk response and continues through risk monitoring.

242、C .The balanced scorecard is a traditional strategic tool used for performance measurement in the business world. The goal is to present the most relevant information quickly and easily. Measurements are compared with set target values so that if performance deviates from expectations, that deviation can be conveyed in a simplistic and straightforward manner.

243、 B .After a risk response has been implemented, the continuing effectiveness of controls to protect assets is carefully monitored, to ensure that they maintain their protection, in the face of a changing threat environment.

244、 B .ISO 31000:2009 acknowledges that there are things outside our control and that these can have negative (e.g., financial loss) or positive (e.g., business opportunity) consequences. Unlike the NIST RMF, this framework is not focused on information systems, but can be applied more broadly to an organization.

245、 D .The costs of the risk management program controls is not relevant to the continuous improvement process of risk management. Regardless of cost, improvements must be made. They are made by continually monitoring and adjusting to environmental or system changes, changing threats, and new vulnerabilities.

246、 C .The first step in threat modeling is to determine asset vulnerabilities , followed by determining which threats could exploit against those vulnerabilities.

247、 C .Threat modeling is the process of describing feasible adverse effects on our assets caused by threat sources.

248、A D .Through reduction analysis you can either reduce the number of attacks to consider, or reduce the threat posed by the attacks.

249、 A .Attack tree describes a diagram that represents the attack pattern, by presenting decision points, specific conditions required for an attack, and end points for the attack, represented by branches and leaf nodes to illustrate the various decision points and conditions.

250、 D .Accepting product risk assessment results performed by the developing organization as the security baseline is not a sound practice, simply because the risk assessment is not independent and does not validate true security posture of the acquired product. Third-party validation should be used whenever possible.

251、 A .In general, when implementing mitigation techniques using attack trees and reduction

analysis, the closer you are to the root of the attack tree when you implement a mitigation technique, the more leaf conditions you will defeat with that particular mitigation or control.

252、 B .Threats and vulnerabilities change constantly, so users at all levels must be aware of new threats and vulnerabilities that could affect the organization and its resources.

253、 C .Organizational security training programs are created and targeted to three specific audiences: managers, staff members, and technical employees. Each group receives the type of awareness training that best fits their responsibilities and roles within the organization. While an organization may also optionally provide training to contractors and customers, this is not typically part of the core security awareness and training the organization requires.

254、 B .NIST RMF (SP 800-37r1)is a risk management framework that has been imposed as mandatory for use on .S. federal government systems, within all government agencies.

255、 C .During a threat assessment, which is only a component of threat modeling, threats and threat actors are identified.

第二章题目

1. Which of the following is an example of an ultimate data owner?
   A. Frontline employee
   B. A customer accessing information via the extranet
   C. IT administrator
   D. Chief information officer (CIO)
2. Which of the following is not a primary process of the information life cycle?
   A. Archival
   B. Disposal
   C. Use
   D. Storage
3. When data is no longer regularly used, which phase of the information life cycle does it enter?
   A. Disposal
   B. Archival
   C. Use
   D. Acquisition
4. Which of the following is true about data classification?
   A. Eliminates risk
   B. Saves resources, such as money
   C. Allows the organization to expend resources to secure information at the level it requires
   D. Is performed only to ensure compliance with regulations and governance
5. All of the following are examples of data that can be considered at the sensitivity level of private, except:
   A. Personal information for use within a company

B. Salary information

C. Protected health information

D. Budget expenditures by a particular individual

6. In this U.S. government classification of data, if this data were disclosed it could cause grave damage to national security.

A. Secret

B. Sensitive but unclassified

C. Confidential

D. Top secret

7. All of the following factors are used to determine the sensitivity of data, except:

A. Value of data

B. Cost to back up the data

C. Regulatory governance

D. Effects to the organization if the data were disclosed to unauthorized persons

8. Which of the following should be used to protect data during transmission to prevent unauthorized access?

A. Encryption and authentication

B. Permissions

C. Physical security

D. Policies and procedures

9. What step should the organization take to ensure that the classification levels assigned to data are current and relevant?

A. Periodic reviews

B. Reclassification

C. Data destruction

D. Data archival

10. Which of the following is the first step the organization should take in developing the data sensitivity program?

A. Identify data owners who will be responsible for classifying data

B. Identify security controls required for sensitive data

C. Specify the criteria that will be used to determine how data is classified

D. Define classification levels

11. Who has the ultimate responsibility for data in the organization?

A. Data owner

B. Data custodian

C. Senior management

D. Data user

12. Who is responsible for the strategic use and management of information systems and technology within the organization?

A. CIO

B. CFO

C. CEO

D. CISO

13. In an organization such as a hospital, which role would be responsible for protecting health

and personal information?

A. Chief information officer

B. Chief executive officer

C. Chief information security officer

D. Chief privacy officer

14. How is privacy different from security?

A. Security indicates the amount of control an individual should be able to have and expect as it relates to the release of their own sensitive information.

B. Privacy is the mechanisms that can be put into place to provide the level of control a person needs to safeguard information.

C. Privacy indicates the amount of control an individual should be able to have and expect as it relates to the release of their own sensitive information

D. Privacy and security are the same thing.

15. Who decides upon the classification of the data she is responsible for and alters that classification if the business need arises?

A. Data user

B. Data owner

C. Data custodian

D. CISO

16. Who is responsible for maintaining and protecting the data?

A. Data custodian

B. Data owner

C. Data user

D. System owner

17. Who is responsible for integrating security considerations into application and system purchasing decisions and development projects?

A. Data owner

B. Data user

C. Data custodian

D. System owner

18. What is the most important aspect of data retention?

A. Ensure that your organization has and follows a documented data retention policy

B. Ensure that your organization is following the law

C. Ensure that data is destroyed immediately when it is no longer being processed or used

D. Ensure that data is retained for a minimum of five years

19. Which of the following is NOT one of the considerations for a data retention policy?

A. What type of data is kept

B. How much it will cost to store the data

C. How long the data is kept

D. Where the data is stored

20. What is the process of producing for a court or external attorney all electronically stored information (ESI) pertinent to a legal proceeding called?

A. Computer forensics

B. Due diligence

C. e-discovery

D. Due care

21. When data has been deleted or erased, what is the metadata, or remaining fragments of the data called?

A. Data remanence

B. Loss clusters

C. Lost sectors

D. Inodes

22. How do most file systems "delete" data?

A. Overwriting data with 1's and 0's

B. Marking the data as deleted without wiping the original data

C. Degaussing

D. Encrypting the file so it can no longer be accessed, and marking it as free space

23. Which of the following terms refers to data that is in storage?

A. Data in transit

B. Data in use

C. Data at rest

D. Inactive data

24. Which of the following terms refers to data that is being transmitted over a network?

A. Data at rest

B. Data in transit

C. Inactive data

D. Data in use

25. Which of the following terms refers to data that is being processed?

A. Data in use

B. Data at rest

C. Data in transit

D. Interactive data

26. Which of the following algorithms is typically not used to encrypt data in transit?

A. SSL

B. TLS

C. MD5

D. IPsec

27. What does TLS rely on to verify the identity of one or both endpoints in a transmission?

A. Digital certificates

B. MD5 hash algorithm

C. AES symmetric algorithm

D. Usernames and passwords

28. Which of the following data states is difficult to encrypt?

A. Data in transit

B. Data at rest

C. Data in storage

D. Data in use

29. A _____ attack exploits information that is being leaked by a cryptosystem.

A. Side-channel attack

B. Brute-force attack

C. Dictionary attack

D. Man-in-the-middle attack

30. Which of the following is a very recent famous example of how failure to perform secure programming practices, including checking boundaries, can have a severe detrimental effect on security worldwide?

A. Nimda

B. The "ILoveYou" virus

C. The Melissa virus

D. Heartbleed

31. Which of the following is an example of a physical media control?

A. Encrypting data on backup media

B. Locking up backup tapes in a secure area

C. Creating a security policy for backup media

D. Assigning backup operator privileges to only specified individuals in charge of performing backups

32. If an organization has a formal media library, which individual is responsible for the overall security and protection of the media included in the library?

A. CISO

B. CIO

C. Media librarian

D. Data owner

33. All of the following are aspects of media control, except:

A. Properly marked

B. Verified integrity

C. Properly stored

D. Kept attached to the processing system when not in use

34. What should be done to media that is no longer required for use and is to be disposed of?

A. It should be sanitized.

B. The data on the media should be encrypted.

C. Nothing; since the data is obsolete, it is of no value to anyone.

D. It should be reviewed for data sensitivity classification.

35. Which of the following methods does NOT ensure that data cannot be accessed by unauthorized persons after the media it resides on has been disposed of?

A. Degaussing

B. Purging

C. Deleting

D. Overwriting

36. Which of the following is the term for residual information on media?

A. Fragmented files

B. Free space

C. Data remanence

D. Slack space

37. When sanitizing or destroying data, which of the following drives the choice of method and the required level of reassurance that the data cannot be accessed by unauthorized persons?

A. Data sensitivity

B. Cost of sanitization method

C. Number of personnel trained on sanitization methods

D. Cost of the media

38. Which of the following tasks performed during media management activities is focused on determining who has custody of each piece of media at any given moment?

A. Documenting media change history

B. Tracking media

C. Implementing environmental controls

D. Ensuring media integrity

39. Which of the following might be considered obsolete media?

A. DVD discs

B. Blu-ray Disks

C. USB thumb drives

D. Zip disks

40. What is the most common cause of data breaches for businesses?

A. Lack of administrative controls

B. Lack of technical controls

C. Lack of awareness and discipline among employees

D. Lack of physical controls

41. What causes an overwhelmingly large majority of all data leak breaches?

A. Negligence

B. Lack of encryption

C. Lack of secure storage

D. Inadequate network perimeter controls

42. Which term describes the collective actions that organizations take to prevent unauthorized external parties gaining access to sensitive data?

A. Data leakage prevention

B. Cryptography

C. Policies and procedures

D. Physical and operational controls

43. Which of the following is the first step in preventing data loss or leakage?

A. Develop a data leakage policy

B. Determine data flows

C. Develop a data protection strategy

D. Conduct a data inventory

44. What is a significant issue in protecting data during the data life cycle?

A. Access creep

B. Lack of encryption

C. Securing the data as it transitions from one stage of the life cycle to another

D. Lack of authentication

45. When evaluating DLP technical solutions, all of the following are critical factors, except:

A. Sensitive data awareness
B. Policy engine
C. Accuracy
D. Volume of data

46. Which of the following is a critical element in ensuring the DLP solution works correctly?
A. Data flows
B. Authorization
C. Encryption
D. Content

47. Which of the following describes threat actors and the actions they may perform on systems or data?
A. Use case
B. Misuse case
C. Vulnerability
D. Risk

48. Which of the following is a critical element of both security and DLP, and concerns the ability to deal with challenges, damage, and crises, and return to normal conditions quickly?
A. Business continuity
B. Disaster preparedness
C. Flexibility
D. Resiliency

49. Which type of DLP technology applies data protection policies to data in motion?
A. Network DLP
B. Endpoint DLP
C. Enterprise DLP
D. SSL interception

50. Which type of DLP solution is primarily concerned with both data at rest and data in use?
A. Network DLP
B. Endpoint DLP
C. Enterprise DLP
D. Stand-alone DLP

51. Which of the following is an example of how endpoint DLP (EDLP) is effective in preventing data leakage or loss?
A. Preventing sensitive data from traveling from the internal network to the external network
B. Encrypting all sensitive network traffic
C. Preventing users from copying data to non-networked devices and external media
D. Preventing users from copying data to trusted file shares

52. Which of the following is the most complex type of DLP technology?
A. Network DLP
B. Hybrid DLP
C. Endpoint DLP
D. Host DLP

53. What is the greatest threat to sensitive data on mobile devices?
A. Device wipe

B. Data loss due to device malfunction

C. Mobile device theft

D. Mobile device hacking

54. All of the following are security measures that can be easily implemented on a mobile device, except:

A. Device wipe

B. Data encryption

C. Device tracking and location services

D. Restricting the mobile device to a specific office location

55. Data in what type of media is better controlled using physical and operational security measures and procedures than technological ones?

A. Paper records

B. Backup tapes

C. Thumb drives

D. Hard disk drives

56. A safe that has the capability to detect when someone attempts to tamper with it, and upon detection engages extra internal bolts to ensure that it cannot be compromised, has a(n)_____.

A. Thermal relocking function

B. Passive relocking function

C. Active relocking function

D. Intrusion detection alarm

57. The concept of determining sensitive information by piecing together smaller pieces of nonsensitive information is called _____.

A. Data synthesis

B. Inference

C. Data aggregation

D. Data reduction

58. What is the primary factor that drives information classification?

A. The value of the information to the organization

B. The cost to protect the information

C. The cost of recovering the information if it is lost

D. The value of the information to a competitor

59. Which of the following is the most valuable asset an organization has?

A. Equipment

B. Facilities

C. Information

D. Reputation

60. Which of the following is a true statement about the difference between data backups and data archives?

A. An archive is a copy of a data set currently in use that is made for the purpose of recovering from the loss of the original data.

B. An archive is a copy of a data set that is no longer in use, but which is kept in case it is needed at some future point.

C. A backup is a copy of a data set that is no longer in use, but which is kept in case it is needed at some future point.

D. A backup and an archive are the same thing.

61. Which of the following is true about the data classification level?

A. Classification level is determined by data sensitivity.

B. Classification level depends upon how much it will cost to protect the data.

C. Classification level depends upon how valuable the data is to an outside organization.

D. Classification level depends upon the level of liability the organization would incur if the data were lost.

62. All of the following are security controls that should be implemented to ensure adequate protection of data, except:

A. Encryption of data while stored and while in transmission

B. Separation of duties

C. Assignment of data permissions based upon an individual's seniority in the organization

D. Auditingnd monitoring

63. All of the following statements about data retention policies are true, except:

A. The data retention policy must consider legal, regulatory, and operational requirements.

B. The data retention policy should address what data is to be retained, where, how, and for how long.

C. The data retention policy must assign roles and responsibilities.

D. The data retention policy must be independent of data sensitivity and classification.

64. Which of the following entails replacing the 1's and 0's that represent data on storage media with random or fixed patterns of 1's and 0's in order to render the original data unrecoverable?

A. Degaussing

B. Overwriting

C. File deletion

D. Disk formatting

65. Which of the following is the process of removing or reducing the magnetic field patterns on conventional disk drives or tapes?

A. Overwriting

B. Degaussing

C. Shredding

D. Formatting

66. Which of the following is a best practice regarding collection of personal and private data by organizations?

A. Organizations should collect the least amount of private personal data required for the performance of their business functions.

B. Organizations should collect the most amount of private personal data possible for the performance of their business functions.

C. Organizations should not collect any amount of private personal data to assist in the performance of their business functions.

D. Organizations should collect any private personal data they feel is required for the performance of their business functions.

67. Which of the following statemnts about the information life cycle is true?

A. The information lifecycle beginwith its creation and ends with its use.

B. Most information must be retaind only in accordance with existing laws, regulations, and business needs.

C. Only sensitive information requires classification.

D. Data sensitivity is not based upon its value to the organization.

68. Which of the following are commonly used as government data classification levels?

A. Public, Releasable, and Secret

B. Proprietary, Company Sensitive, and Private

C. Unclassified, Secret, and Top Secret

D. Sensitive but unclassified, Proprietary, Public

69. Information will typically be archived when _____.

A. it is no longer needed in the present, but may be needed at some point in the future

B. it is to be used to restore data from backup

C. it is to be used to comply with data destruction requirements

D. it is to be used in the event of a disaster

70. If a user accesses information that is of a classification higher than the user requires for the performance of their duties, which of the following should the organization do?

A. Increase the user's clearance level

B. Increase the security controls on information

C. Decrease the security controls on information

D. Decrease the user's security clearance level

第二章答案

1、 D .The key here is the word "ultimate." Employees and administrators can be data owners in some situations, but senior management is ultimately the owner of business-oriented data. Data owners are legally bound to protect data within a company. Because of this responsibility, data owners should be members of senior management. These individuals must practice due care with data classifications and associated security policies.

2、 D .Storage is part of the use phase of the information life cycle.

3、 B .Often, governance requires that you archive information for a specified period of time. Additionally, you may want to keep information for a period of time for later review. Only after your archival requirements have been met, would you dispose of the information.

4、 C .Data classification allows the organization to expend resources to protect information at the level it requires, and ensures that it is handled appropriately throughout its life cycle.

5、 D .Any organizational budget expenditures by a particular individual would be considered organizational data, possibly proprietary data, but not directly related to an individual's personal data.

6、 D .Top secret is the highest classification of data within the U.S. government. If this type of information is disclosed, it could cause grave damage to the national security of the United States.

7、 B .The cost to back up the data should not be a factor in determining data sensitivity. The value of data, regulatory governance, and effects to the organization if the data were lost would affect how you might rate its sensitivity. If it is highly sensitive, then it is probably worth the cost it would take to protect it, including backing it up.

8、 A .Encryption and authentication are two of the most important measures to consider when protecting data during transmission. While the other factors listed are also used to protect data, they may be used to protect data in different ways, such as during storage or use.

9、 A .Periodic reviews, where the organization reviews classification levels, and the data and programs that adhere to them, are used to ensure the classification levels are still in alignment with business needs; data or applications may also need to be reclassified or declassified, depending upon the situation as time goes by.

10、 D .First, the organization should define classification levels based on the type of data the organization produces, and its level of sensitivity. It should develop an idea of how valuable its data is to it, and the consequences if the data were lost or stolen. This will drive the classification level.

11、 C .Senior management always carries the ultimate responsibility for the organization.

12、 A .The chief information officer, or CIO, oversees and is responsible for the day-to-day technology operations of the company. The CIO may work for either the chief executive officer (CEO) or the chief financial officer (CFO), and the chief information security officer (CISO), who is responsible for information security, typically reports to the CIO.

13、 D .The chief privacy officer is responsible for protecting health and personal information in a healthcare organization.

14、 C .Privacy is different from security. Privacy indicates the amount of control an individual should be able to have and expect as it relates to the release of their own sensitive information. Security is the mechanisms that can be put into place to provide this level of control.

15、 B .The data owner has due care responsibilities and thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data she is responsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and

defining user access criteria.

16、 A .The data custodian (information custodian) is responsible for maintaining and protecting the data. This role is usually filled by the IT or security department, and the duties include implementing and maintaining security controls; performing regular backups of the data; periodically validating the integrity of the data; restoring data from backup media; retaining records of activity; and fulfilling the requirements specified in the company’s security policy, standards, and guidelines that pertain to information security and data protection.

17、 D .The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure the systems are properly assessed for vulnerabilities and must report any incidents to the incident response team and data owner.

18、 A .The most important aspect of data retention is to ensure that your organization has and follows a documented data retention policy, and that it is being followed and audited. A secondary aspect is to ensure the policy is designed to comply with any relevant governance. This policy may have requirements for archiving for specified periods of time, or specific data destruction instructions.

19、 B .How much it will cost to store the data directly depends upon the data sensitivity, not the data retention policy, so cost should not be a consideration when creating the data retention policy.

20、 C .Discovery of electronically stored information (ESI), or e-discovery, is the process of producing for a court or external attorney all ESI pertinent to a legal proceeding.

21、 A .Data remanence is any data that remains after it has been erased or deleted using conventional means. Data remanence could be metadata, or data fragments, in the form of file fragments or used clusters.

22、 B .Most file systems don't actually wipe the data as part of their normal deletion process. Rather, the normal process simply marks the data as deleted, without deleting it. It is usually marked as deleted in the file system's file tables. However, the data remains unless it is overwritten or degaussed.

23、 C .Data at rest refers to stored data on any medium not currently being processed by software. These media could be hard disks, DVDs, or tapes.

24、 B .Data in transit, sometimes referred to as data in motion, is data that is moving between computing nodes over a data network such as the Internet.

25、 A .Data in use is the term applied to data that is in active memory and being processed by the CPU or an application. It is neither in storage nor in transit.

26、 C .Typically, data in transit is encrypted by one of several encryption algorithms. These include Secure Sockets Layer (SSL), Transport Layer Security (TLS), SSH, and Internet Protocol Security (IPsec). MD5 is a hashing algorithm, not a true encryption algorithm.

27、 A .Transport Layer Security (TLS) uses digital certificates to verify the identity of both or either parties to a transmission.

28、 D .While data at rest and data in transit are fairly easy to encrypt, data in use is very difficult to encrypt. This is because many applications don't understand data in its encrypted form, nor do operating systems. While not impossible to encrypt data in use, it is generally very difficult and not generally done.

29、 A .A side-channel attack focuses on information leaked by a cryptosystem, as a byproduct of that system. This type of attack is effective when direct attacks on the cryptosystem, its algorithms, the key, the plaintext, or the ciphertext are ineffective.

30、 D .The infamous Heartbleed bug of 2014 is a very recent famous example of how failure to perform secure programming practices (in this case, bounds checking) can have a severe detrimental effect to security worldwide. In this bug, which affected OpenSSL implementations, the main issue was that anyone communicating with the server could request an arbitrarily long heartbeat management message from it, including those that might be composed of hundreds of characters, enabling an attacker to access sensitive data. Heartbeat messages are typically short strings that let the other end know that an endpoint is still there and wanting to communicate.

31、 B .Locking up backup tapes in a secure area, where only a limited number of authorized people have access to them, is an example of a physical media control.

32、C .If an organization has a formal media library, the role of media librarian is usually assigned to someone who has overall supervisory authority over the media library. This person supervises the media library, and is in charge of security for all the media that reside in it.

33、 D .When media is not in use, it should be disconnected or removed from the system it supports, and properly stored. This ensures that unauthorized personnel are unable to steal or access the media or the data that resides on it.

34、 A .Before disposing of media, it should be erased (cleared of its contents), or sanitized.

35、 C .Simply erasing data by deleting it does not actually destroy the data or erase it from the media. Deleted files can actually be recovered quite easily, using simple forensic techniques.

36、 C .Data remanence is the physical representation of information that was saved and then erased in some fashion, but not completely removed from the media. Data remanence presents a security risk, because it may mean that the data can be recovered through various forensic techniques.

37、 A .Data sensitivity drives the method of sanitization, and the level of reassurance that the organization requires that the data cannot be accessed by unauthorized persons after media sanitization.

38、 B .Tracking who has custody of each piece of media at any given moment is essentially auditing the activities involved with media creation, storage, use, movement, and destruction.

39、D .Zip disks, produced by Iomega, stored a maximum of 256 MB on each 3.5-inch disk. This is extremely low capacity compared to the storage media routinely in use today. ZIP disks are not made any longer, and the drives used to read them are difficult to locate. All of the other choices are popular media storage commonly used in today's computing world.

40、 C .Lack of awareness and discipline among employees is the most common cause of data breaches for businesses. The human factor is the most difficult aspect of a business to control.

41、 A .Negligence by employees is one of the highest occurring causes of data leaks.

42、 A .Data leakage prevention (sometimes referred to as Data loss prevention), or DLP, is the collective actions that organizations take to prevent unauthorized external parties gaining access to sensitive data. This includes policies, procedures, technologies, physical controls, and so on.

43、 D .Conducting a data inventory is the very first step in preventing data loss or leakage. I you don't know what data you have, how it's classified in terms of sensitivity, and where it is located then you can't effectively prevent its loss or leakage.

44、 C .Securing data as it transitions from one stage of the data life cycle to another is a significant issue that affects adequately protecting data. An example of this would be the lack of protections enforced on data that is no longer actively used, as it is retired or archived before disposal.

45、 D .The volume of data the organization processes is usually not a consideration when selecting a DLP technical solution. Regardless of volume, the DLP solution should work. Volume of data is more of a factor that affects the size and efficiency of the solution.

46、 A .Data flows within your organization is a critical element, since data should be allowed to flow to the individuals and departments who need it, and prevented from flowing to those who do not, particularly outside of the organization.

47、 B .A misuse case describes threat actors and the actions they may perform on systems or data - typically actions that have negative consequences. This is the opposite of the use case, which is used by system analysts to document the actions that authorized persons perform with systems or data.

48、 D .Resiliency is the ability of the system to deal with challenges, damage, and negative actions, and return to a normal state of operation quickly, with minimum impact to the organization.

49、 A .Network data leak prevention (NDLP) applies data protection policies and technologies to data in transit, over networks. Network DLP is usually implemented as appliances deployed at the perimeter of an organization's network.

50、 B .Endpoint DLP (EDLP) is primarily concerned with both data at rest and data in use, typically on protected hosts, such as servers and workstations. Typically a software agent runs on the host, and reports back to a central EDLP server.

51、 C .EDLP can prevent data loss by preventing users from copying sensitive data to non-networked devices, as well as storage devices, such as thumb drives and external hard drives. It can also prevent writing sensitive data to media such as DVD or CD-ROM.

52、 B .A hybrid data leak prevention (DLP) solution uses both network DLP (NDLP) and endpoint DLP (EDLP) across entire enterprise. Such a solution is very costly and complex, but it can cover both data in transit and data at rest.

53、 C .Theft of a mobile device is one of the greatest threats to data. If the mobile devices is in the hands of an unauthorized person, and adequate security protections are not in effect on the device, then the person possessing the device could have access to a great deal of sensitive data, including e-mails, files, secure websites, and so on.

54、 D .Restricting a mobile device to a very small, specific location is contrary to what mobile devices were invented for. These devices are designed to be mobile, providing convenience and ease of data access when an employee is away from the company premises.

55、 A .Paper records can't be easily protected with technical controls, such as encryption and authentication measures. They are better controlled using physical security measures and operational procedures.

56、 B .A safe with a passive relocking function can detect when someone attempts to tamper with it and then engage extra internal bolts that will fall in place to ensure that the safe can't be compromised.

57、 C .Data aggregation is the process of combining smaller pieces of nonsensitive information to determine a larger picture or concept of sensitive information from it. Inference is the goal of

aggregation.

58、 A .The value of information to the organization is what drives the classification of that information. The more valuable the information is to the organization, the higher the data sensitivity and classification will be. This also drives the level of protection data requires. The more valuable the information is, and the more sensitive it is, the more protection it will require.

59、 C .Information is the most valuable asset an organization has, simply because it can help create revenue and make the organization competitive in the market. Reputation is a difficult asset to place a dollar value on, and facilities and equipment have finite values, which can depreciate over time.

60、 B .An archive is a copy of a data set that is no longer in use, but which is kept in case it is needed at some future point. A backup is a copy of a data set currently in use that is made for the purpose of recovering from the loss of the original data. Backup data normally becomes less useful as time goes on.

61、 A .Classification level determines how much protection an asset, such as equipment, facilities, information, and so on, gets. Classification level is directly determined by data sensitivity.

62、 C .Assignment of data permissions based upon an individual's position in the organization does not take into account the individual's duties and need-to-know for access to data.

63、 D .The data retention policy cannot be independent of data sensitivity and classification; data is retained based upon data sensitivity, as well as legal and governance requirements.

64、 B .Overwriting is the process of replacing all of the 1's and 0's that represent data on a storage medium, with patterns of 1's and 0's to completely obliterate the existing data.

65、 B .Degaussing removes and reduces the magnetic field patterns on magnetic media, such as disk drives and tapes. This effectively obliterates the data on those media, and can destroy the media as well, rendering it useless and unreadable.

66、 A .Organizations should collect the least amount of private personal data required for the performance of their business functions, to minimize the risk of unauthorized data disclosure and limit the amount of data they are required to protect.

67、B .Most information must be retained only in accordance with existing laws, regulations, and business needs, and destroyed when no longer required.

68、 C .Standard levels of classification for government information are Unclassified, Secret, and Top Secret.

69、 A .Information will typically be archived when it is no longer needed in the present, but may be needed at some point in the future.

70、 B .In the event of an unauthorized access to information, the organization should consider increasing the security controls on that information, to avoid future disclosures.

第三章题目

1. Which activity typically follows the process of developing a system architecture?
   A. Development
   B. Gathering requirements
   C. Design
   D. Implementation
2. Which of the following is the international standard that is used as the basis for the evaluation of security properties of products under the CC framework?
   A. ISO/IEC15408
   B. ISO/IEC 42010
   C. ISO/IEC 27001
   D. ISO 31000:2009
3. Which of the following statements best describes why a system goes through the evaluation process for its trusted computing base (TCB)?
   A. To identify the architecture, security services, and assurance mechanisms that make up the TCB, and how they protect the system
   B. To ensure that it can be certified and accredited
   C. To find all of its potential vulnerabilities and exploit them
   D. To perform a cost-benefit analysis for assigning controls
4. When should security considerations be included in the overall systems security engineering lifecycle?
   A. Development and implementation
   B. Architecture and design
   C. All phases of the lifecycle
   D. Requirements gathering only
5. Database security measures are implemented to prevent all of the following security weaknesses, except:
   A. Inference
   B. Data analytics
   C. Buffer overflows
   D. Aggregation
6. What is the primary reason for developing security controls for, and assigning them to, a system that has been evaluated under a trusted computing base criteria?
   A. To ensure the system can be accredited
   B. To lower costs required to develop controls for the system
   C. To reduce the overall risk to the system

D. To ensure that controls are aligned with the protection mechanisms found inside the systems

7. Which of the following term refers to computing technologies embedded into automated systems, that usually control utilities, communications, and so forth?

A. Embedded systems

B. Smart grids

C. Standalone systems

D. Isolated systems

8. Parallel computing can happen at one of three possible levels. Which of the following accurately describes those levels?

A. CPU, workstation, or server

B. Bit, instruction, or task

C. User mode, kernel mode, or OS level

D. Register, memory, or CPU

9. All of the following are potential issues with mobile devices in the enterprise, except:

A. Lack of encryption

B. Loss or theft

C. Internet access through means that are not company controlled

D. Workstation compromise

10. Which of the following terms refers to input validation that is done before the input is sent back to the server to process?

A. Server-side includes

B. Cross-site scripting

C. Client-side validation

D. Parameter validation

11. Which of the following terms refers to access control technologies commonly used to protect copyright material?

A. Encryption

B. Steganography

C. Digital rights management

D. Authentication

12. All of the following are issues regarding Internet of Things (IoT) embedded devices, except:

A. Lack of connection to the outside world

B. Lack of authentication

C. Lack of encryption

D. Inability to update devices

13. All the following are areas where digital media, data, and information systems could be located and therefore need to be protected, except:

A. Wiring closets

B. Media storage facilities

C. Evidence storage areas

D. Employee break rooms

14. Julius Caesar constructed his own encryption method to hide data during transmission or while being stored. The Caesar Cipher works in which of the following ways?

A. Each letter in the alphabet is replaced with a letter three places beyond it.

B. Letters are randomly scrambled.

C. The message itself consists of clues to recover from different places in the physical world.

D. Replaces letters of the alphabet with letters 13 characters beyond it.

15. PKI and PGP can provide similar functionality, but a PKI provides an actual framework for an environment to work within. They also use different trust structures. Which of the following best describes PGP's trust structure?

A. Certificate authorities

B. Web of trust

C. PACs

D. Hierarchical

16. Secure Sockets Layer (SSL) is the most common protocol for secure Internet transactions. Which of the following is not a characteristic of SSL?

A. Originally developed by Netscape

B. Protects both the message and communication channel over the Internet via VPN service

C. Provides encryption, message integrity, and server authentication

D. Uses public key encryption

17. In a 64-bit Data Encryption Algorithm (DEA) key, how many bits make up the true key and how many bits make up parity?

A. 16 + 48 for parity

B. 48 + 16 for parity

C. 64 and no parity

D. 56 + 8 for parity

18. DES has gone through different generations, DES, Double-DES, and Triple-DES (3DES). 3DES is how much stronger than DES?

A. 2 exponent 56

B. 2 exponent 3

C. 3

D. 192

19. Which is not true of Advanced Encryption Standard (AES)?

A. It was developed to replace DES.

B. Uses key sizes of 64, 128, and 192.

C. It is a block symmetric cipher.

D. Uses the algorithm Rijndael.

20. Different types of algorithms use different types of mathematics. The more complex the mathematics, the more resources that are required for computation. Which asymmetric algorithm is the most efficient requiring the fewest resources?

A. RSA

B. ECC

C. Blowfish

D. IDEA

21. The Clipper Chip was a proposed hardware encryption chip that was intended for all American-made communication devices. What size key was the Clipper Chip to employ?

A. 16

B. 80

C. 64

D. 56

22. Which of the following is the 128-bit algorithm that was accepted for the DES?

A. Skipjack

B. Data Encryption Algorithm

C. Lucifer

D. RSA

23. Which of the following is not true of RSA?

A. Was accepted as the new AES in the late 1990s

B. Can be used for encryption and digital signatures

C. Can be used for key exchange

D. Developed at MIT by Ron Rivest, Adi Shamir, and Leonard Adleman

24. Which of the following algorithms was not considered by NIST when determining what algorithm to adopt for the new AES in 1997?

A. MARS

B. Rinjdael

C. El Gamal

D. Twofish

25. An attacker who has access to a large section of ciphertext, determines which part of it is to be decrypted, and ultimately has access to the resulting plaintext has performed what type of attack?

A. Chosen-ciphertext

B. Known-plaintext

C. Chosen-plaintext

D. Ciphertext-only

26. In 1976, Diffie and Hellman introduced what cryptography technology?

A. Electronic key distribution

B. Digital signatures

C. Symmetric key encryption

D. 256-bit key encryption capabilities

27. A secret key that is used for data encryption only one time is called a _____.

A. Public key

B. Asymmetric key

C. Key exchange

D. Session key

28. Which key knows the trapdoor, allowing for decryption to take place?

A. Session key

B. Public key

C. Private key

D. Asymmetric key

29. A fixed-length value used as a message fingerprint is called a _____.

A. MAC

B. Hash value

C. Message value

D. Digital signature

30. What is a chosen-plaintext attack defined as?

A. An attacker chooses the ciphertext for encryption and has access to the decrypted plaintext.

B. An attacker has both plaintext and ciphertext of multiple messages.

C. An attacker has plaintext and can choose which part of the plaintext gets encrypted and then has access to the generated ciphertext.

D. An attacker has ciphertext from several messages.

31. The two main types of symmetric ciphers are block and stream. Block ciphers perform substitution by which of the following?

A. Keystream generators

B. S-boxes

C. XOR functionality

D. Initialization vectors

32. An encryption mode that inputs the previous block of ciphertext to the current block being encrypted as a way of reducing the existence of patterns is _____.

A. ECB

B. CBC

C. CFB

D. OFB

33. Which of the following is the science of studying and breaking encryption algorithms and cryptosystems?

A. Cryptography

B. Encryption

C. Monoalphabetic substitution

D. Cryptanalysis

34. Which of the following statements pertaining to International Data Encryption Algorithm (IDEA) is false?

A. IDEA uses a 128-bit key.

B. IDEA is often used in PGP encryption software.

C. IDEA was not the successor to DES because it was not publicly tested.

D. Data blocks are put through eight rounds of mathematical functions.

35. An algorithm that produces the same hash value for two different messages causes what?

A. Pad

B. Collision

C. One-way function

D. MAC

36. Cryptography can be used for several different reasons. What is the overall realistic goal of cryptography?

A. To hide information from authorized individuals

B. To make it so time-intensive that an attacker will stop trying to break it

C. To improve the cryptoanalysis techniques

D. To make data transmissions more efficient

37. Which of the following hashing algorithms produces a 160-bit hash value?

A. MD4

B. MD5

C. Haval

D. SHA

38. Which of the following is not true about asymmetric cryptography systems?

A. Faster than symmetric cryptography

B. Uses a variable-length key

C. Provides authentication and nonrepudiation

D. One side uses a public key and the other uses a private key.

39. Sometimes basic fencing does not provide the level of protection a company requires. Which of the following combines the functions of intrusion detection systems and fencing?

A. PIDAS

B. PERIMETER

C. Closed-circuit TV

D. Acoustical-seismic detection system

40. A physical security mechanism consisting of a small area with two doors used to "hold" an individual until his identity can be verified is called a _____.

A. Turnstile

B. Holding area

C. Mantrap

D. Man-in-the-middle

41. Different organizations have different physical security protection requirements, thus they need different types of controls and countermeasures. Which of the following is not a legitimate justification for using security guards at a facility?

A. They are one of the best deterents for potential intruders.

B. They are flexible and can be positioned randomly.

C. They provide judgement and understanding of different situations.

D. They are cheaper than most automated detection systems.

42. An organization can be faced with many different types of fire. If a fire was ignited by an electrical wire short in a dropped ceiling, what fire class would this fall within?

A. Class A

B. Class B

C. Class C

D. Class D

43. Which physical security mechanism is used because it can provide "discriminating judgment?"

A. Security guards

B. Security dogs

C. Photometric intrusion detection system

D. PIDAS

44. Smoke detector placement is important for ensuring that all types of fires in different parts of the building can be quickly identified. Which location is not necessarily a good place for a smoke detector?

A. Raised flooring

B. Dropped ceiling

C. Exterior rear doorway

D. Air ducts or vents

45. The different classes of fires indicate what type of material is burning. The classes also require specific suppression agents. Which of the following is the best description of the Halon and FM-200 suppression agents?

A. CO2

B. A gas suppressant

C. Water

D. Soda acid

46. Which one of the following security controls doesn't belong with the other three?

A. Host-based intrusion detection system

B. Photoelectric system

C. Acoustical-seismic detection system

D. Passive infrared system

47. Which one of the following characteristics is not true of an ideal data processing room?

A. Humidity level of 50 percent

B. Carpeting

C. Room temperature around 72° F

D. Independent HVAC and ventilation systems

48. A security system that uses changes in heat waves in a particular area to identify possible intruders is called a _____.

A. Proximity detection system

B. Passive infrared system

C. Acoustical-seismic detection system

D. Photometric

49. The Montreal Protocol has declared that Halon should no longer be used because of its negative effects on the ozone and human beings. Which is not a replacement for Halon?

A. NAF-S-III

B. DD3-410

C. Water

D. CEA-410

50. Doors configured in fail-safe mode assume what position in the event of a power failure?

A. Open and locked

B. Closed and locked

C. Closed and unlocked

D. Open

51. Which of the following fire suppressing agents should not be used in an operations center containing employees?

A. Gas

B. Soda acid

C. Water

D. CO2

52. Piggybacking can be best prevented by which physical control?

A. Turnstile

B. Mantrap

C. Badge reader

D. Fail-safe door

53. Different water suppression systems exist for different purposes and regions. Which sprinkler system's pipes are filled with water all the time?

A. Wet pipe

B. Preaction

C. System pipe

D. Dry pipe

54. The current that moves through power lines and cables can be negatively affected by its environment. Line noise created by lightning or electrical motors can cause what?

A. Electronagnetic interference (EMI)

B. Radio modulation interference (RMI)

C. Radio frequency interference (RFI)

D. Energy fluctuation interference (EFI)

55. A secured computing room should have all of the following characteristics except _____.

A. No more than two doorways

B. Walls that extend from the true flooring to the true ceiling

C. Many comfortable sitting areas around workstations

D. Strict physical access controls

56. A control center that operates mission critical systems would most likely have which of the following power arrangements?

A. Primary power source, UPS, and generator

B. Just a primary power source because most data systems have their own power sources

C. Primary power source and UPS

D. Stand-alone generator

57. Which type of lock uses programmable keypads to restrict access?

A. Device

B. Cipher

C. Preset

D. Complex

58. Which of the following is a reason for a company to use physical locks to secure devices?

A. Locks are the most secure physical control.

B. Locks are convenient for employees.

C. Locks are inexpensive.

D. Locks are difficult to break.

59. Proper lighting in critical areas is important to deterring potential intruders and protecting employees and customers. Lighting is an example of what type of control?

A. Technical

B. Physical

C. Environmental

D. Access

60. Which is not a characteristic or name of a system sensing proximity card reader?

A. Transponder

B. User activated

C. Passive device

D. Field-powered

61. Several types of fire detectors are available on the market. Which of the following detects a fire by identifying changes in a stream of light waves?

A. Optical detector

B. Thermometer detector

C. Heat-activated detector

D. Flame-activated detector

62. What is the name of a water sprinkler system that keeps pipes empty and doesn't release water until a certain temperature is met and a "delay mechanism" instituted?

A. Wet

B. Preaction

C. Delayed

D. Dry

63. Cipher locks have four general features that can be configured. Of the following answers, which is not one of the features?

A. Hostage alarm

B. Key override

C. Voice activated

D. Master keying

64. Which TCSEC publication addresses computer operating systems for government and military use?

A. Red Book

B. Brown Book

C. Green Book

D. Orange Book

65. A processor and operating system can work in different modes depending upon the privilege of the process that made a request. If a process is able to communicate directly to hardware, what state is the processor and system running in?

A. Problem state

B. Wait state

C. Run state

D. Supervisory state

66. What is it called when two or more processes commit resources, but cannot carry out their tasks because the other required resources are currently committed?

A. Stalemate

B. Deadlock

C. Buffer overflow

D. Crash

67. There are different types of security models, such as Bell-LaPadula, Biba, and State Machine. Which of the following is the correct definition of "security model?"

A. A framework that outlines the requirements necessary to support a security policy

B. A beta version operating system

C. Strict guidelines at a company level based on procedures to follow regarding computer security and access controls

D. Identifying, assessing, and reducing security risks

68. A multithreading computer can do what?

A. Run multiple processes at one time.

B. Run and process multiple requests at one time.

C. Run multiple programs at one time.

D. Run multiple tasks at one time.

69. A product that has been evaluated as providing discretionary protection according to the TCSEC would have what classification rating?

A. A

B. B

C. C

D. D

70. Products that pass through the Trusted Products Evaluation Program (TPEP) are published in what?

A. Orange Book

B. List of evaluated products

C. National Accreditation Report

D. Computing Society Product Evaluation Report

71. What are the distinguishing factors between a product with a TCSEC rating of A1 and one with a rating of B3?

A. Architecture features

B. Protection features

C. Verified protection

D. Security policies

72. Using a path that is not intended for communication transmissions to send and receive information is an example of a _____.

A. Covert channel

B. Salami attack

C. Piggybacking attack

D. Buffer overflow

73. Which term refers to a hidden set of software instructions created by the developer as a matter of convenience?

A. Covert channel

B. Software patch

C. Maintenance hook

D. GUI

74. Which of the following is not a requirement of a B3 TCSEC Rating?

A. Security administrator role defined.

B. Monitors events and notifies appropriate personnel.

C. Exhibits trusted recovery.

D. Uses formal methods and procedures.

75. The Orange Book was developed in the 1970s for the purpose of evaluating specific items. There have been many criticisms of it because it is not overly robust and is very focused in nature. Which is not true about the Orange Book?

A. Places trust in the computer operating system.

B. Does not address integrity and availability.

C. Works with protection rankings, which is well suited for the commercial industry.

D. Uses a small number of ratings that are not very flexible.

76. Which of the terms below is best described as a simulated environment for applications to run in?

A. TCB

B. Virtual machine

C. Protection rings

D. Execution domains

77. Which of the following is a way for one process to communicate to another by modulating the use of the system's resources?

A. Covert timing channel

B. Covert storage channel

C. Maintenance hook

D. TOC/TOU

78. Companies should follow certain steps in selecting and implementing a new computer product. Which of the following sequences is ordered correctly?

A. Evaluation, accreditation, certification

B. Evaluation, certification, accreditation

C. Certification, evaluation, accreditation

D. Certification, accreditation, evaluation

79. Which of the following security models allows for dynamically changing access controls that protect against conflicts of interest?

A. Bell-LaPadula

B. Graham-Denning

C. Brewer-Nash

D. Clark-Wilson

80. Which is not true of the Clark-Wilson model?

A. Was developed to provide confidentiality.

B. Incorporates the "separation of duties" principle.

C. Addresses all three goals of integrity.

D. Is suited for the commerical industry.

81. What is the result of combining RAM and secondary storage?

A. Virtual storage

B. Real storage

C. Primary storage

D. Combo storage

82. Software held in a nonvolatile storage area that is difficult to alter is called _____.

A. Cache memory

B. Firmware

C. ROM

D. EPROM

83. A space on the hard drive saved for faults when the main memory's capacity is full is called what?

A. Cache storage

B. Swap space

C. Secondary storage

D. Primary storage

84. The Bell-LaPadula model possesses all of the following characteristics except?

A. Incorporates a state machine model.

B. Used primarily in the commercial industries.

C. Based on the fundamentals of the information flow model.

D. Was the first mathematical access control State Machine model used for confidentiality.

85. When an operating system allows two or more classification levels to be processed at one time, it is operating in what mode?

A. Multiuser mode

B. Dedicated security mode

C. Multilevel security mode

D. System high mode

86. A protection domain is also called a security domain or an execution domain. Which of the following is a correct definition?

A. The system resources that are available to a subject.

B. The system resources that fall outside of the security perimter.

C. The system resources that work within the trusted computing base.

D. The system resources that work in protection ring 1 and 3.

87. There are many types of high-level languages, then there is assembly code and machine language. Which is not true of machine language?

A. Expressed in binary format

B. Understood by processors

C. Referred to as "source code"

D. Uses ones and zeros

88. Which security model incorporates the star integrity axiom and the simple integrity axiom?

A. Brewer-Nash

B. Goguen and Meseguer

C. Clark-Wilson

D. Biba

89. What is the term that defines when senior management initiates and sponsors a company's security program?

A. Bottom-up approach

B. Top-down approach

C. Steering committee

D. Middle-driven approach

90. Which of the following would not be part of an organizational security policy?

A. Security program goals

B. E-mail security policy

C. Responsibilities assignments

D. Enforcement information

91. Which of the following terms is a recommendation to an employee on how to act?

A. Baseline

B. Rule

C. Guideline

D. Standard

92. An operating system that can execute two or more applications with different classification levels simultaneously without threatening the security of the applications or the system is referred to as what?

A. Multiprocessing

B. Multistate

C. Multiprogramming

D. Multitasking

93. The Clark-Wilson model is based on which of the following components to provide data and application integrity?

A. Star integrity axiom and simple integrity axiom

B. Separation of duties and data classifications

C. Separation of duties, internal and external consistency, and access triple

D. Internal and external consistency, star security and simple security rules

94. There are several types of components that fall within the trusted computing base (TCB). Which of the following would not be within the security perimeter?

A. Firmware on motherboard

B. Applications

C. Protective hardware components

D. Reference monitor and security kernel

95. Computer systems can use secondary and primary storage areas. Which of the following best describes the difference between these different storage medias?

A. Primary storage is collectively the memory that is available to applications and the operating system itself. Secondary storage is nonvolatile devices that may supplement the system's primary storage.

B. Primary storage is collectively the memory that is available to applications and the operating system itself. Secondary storage is volatile devices that may supplement the system’s primary storage.

C. Primary storage is collectively the memory that is available to applications and the operating system itself. Secondary storage is nonvolatile devices that include the system’s RAM and registers.

D. Primary storage is collectively the nonvolatile memory that is available to only applications and not the operating system itself. Secondary storage is volatile devices that may supplement the system’s primary storage.

96. Walls built to create sensitive rooms should have which of the following characteristics?

A. Extend from the real floor to the real ceiling.

B. Have a one-hour fire rating.

C. Be monitored via closed-circuit TV.

D. Be constructed of steel.

97. How should personnel documentation, employee directories, and internal telephone information be protected?

A. Kept in fireproof safes

B. Not be available or accessible to external entities

C. Catalogued and labeled

D. Encrypted and protected with access controls

98. DEA is the algorithm that is used within DES. Which of the following is a DES attribute?

A. DES is a block cipher.

B. DES is a public key algorithm.

C. DES is a stream cipher.

D. DES is a one-time pad.

99. There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term that describes when two pieces of data result in the same value is _____.

A. Polymorphism

B. Collusion

C. Escrow

D. Collision

100. Which of the following best describes the most secure way of transmitting a file?

A. Encrypting the file before transmission

B. Digitally signing the message

C. Transmitting a file using FTP

D. Passing the file though a hashing algorithm before transmitting it

101. Cryptography has different components: hashing, MAC, asymmetric and symmetric algorithms, and digital signatures. A digital signature is used to provide which one of the following services?

A. To ensure the receiver cannot deny receiving a message

B. To ensure that the message is properly protected during transmission

C. To ensure that the sender’s identity is provided and to prevent repudiation

D. To ensure repudiation is provided

102. El Gamal has which of the following characteristics?

A. A symmetric algorithm

B. A hashing algorithm

C. A message authentication code algorithm

D. A public key algorithm

103. Some cryptographic components can provide nonrepudiation. What does nonrepudiation do?

A. System or data origin authentication of a message

B. Ensures that someone cannot deny a previous action

C. Ensures the integrity of the message and provides a way of key exchange

D. Incorporated in most key recovery procedures to enforce dual control

104. Cryptanalysis is an important piece to cryptography as a whole. Which best describes the purpose of cryptanalysis?

A. Assurance of securely transmitting data over public and hostile environments

B. The science of hiding the meaning of communication

C. A system that provides encryption and decryption and can be created through hardware components or program code in an application

D. Science of studying and breaking the secrecy of encryption algorithms and their necessary pieces

105. Which of the following is not a component of a public key infrastructure (PKI)?

A. CRL

B. RA

C. PGP

D. CA

106. IPsec includes which of the following characteristics?

A. Support for encrypting and tunneling through non-IP networks

B. Integrity and system authentication

C. Support for timestamping and message playback

D. Integrity and user authentication

107. IPsec's main protocols are AH and ESP. Which of the following services does AH provide?

A. Confidentiality and authentication

B. Confidentiality and availability

C. Integrity and accessibility

D. Integrity and authentication

108. Crackers and hackers are words that are used interchangeably in the field, but really have their own specific definition. Crackers are defined as which of the following?

A. Tools dedicated to decrypt protected passwords

B. Vulnerability tools used to identify holes in an environment

C. People who carry out malicious activities for personal or financial gain

D. Tools used in penetration testing

109. Some mantraps today actually use a biometric system to weigh the individuals that enter it. What is the purpose of this?

A. To ensure that more than one person did not enter the mantrap. This is done to prevent piggybacking and tailgating.

B. To ensure that more than one person entered the mantrap. This is done to prevent piggybacking and tailgating.

C. An enrollment period weighs different people and builds a biometric reference file. When the person attempts to authenticate, the system compares the current weight with what is held in the reference file.

D. An enrollment period weighs different people and builds a biometric reference file. When the person attempts to authenticate, the system compares the current weight with another individual's reference file.

110. There are different types of water suppression systems. Which of the following answers best describes the difference between a deluge and a preaction system?

A. A deluge system provides a delaying mechanism that allows someone to deactivate the

system in case of a false alarm or if the fire can be extinguished by other means. A preaction system provides similar functionality but has wide open sprinkler heads that allow a lot of water to be dispersed quickly.

B. A preaction system provides a delaying mechanism that allows someone to deactivate the system in case of a false alarm or if the fire can be extinguished by other means. A deluge system has wide open sprinkler heads that allow a lot of water to be dispersed quickly.

C. A dry pipe system provides a delaying mechanism that allows someone to deactivate the system in case of a false alarm or if the fire can be extinguished by other means. A deluge system has wide open sprinkler heads that allow a lot of water to be dispersed quickly.

D. A preaction system provides a delaying mechanism that allows someone to deactivate the system in case of a false alarm or if the fire can be extinguished by other means. A deluge system provides similar functionality but has wide open sprinkler heads that allow a lot of water to be dispersed quickly..

111. If an encryption algorithm is poorly designed it may carry out the following scenario: Message A is encrypted with key 1 and comes up with ciphertext ABC. Message B is encrypted with key 1 and comes up with ciphertext ABC. Which of the following terms is used to describe this issue?

A. Collision

B. Key clustering

C. Key mastering

D. Birthday attack

112. Which list best describes the functionality provided by MAC, hashing algorithms, digital signatures, and symmetric keys?

A. System authentication and integrity, integrity, authenticity and integrity, confidentiality and integrity

B. User authentication and integrity, integrity, authenticity and integrity, confidentiality

C. System authentication and integrity, integrity, authenticity and integrity, confidentiality

D. System authentication and integrity, integrity and confidentiality, authenticity and integrity, confidentiality

113. If Marge uses her private key to create a digital signature on a message she is sending to George, but she does not show or share her private key with George, what is it an example of?

A. Key clustering

B. Avoiding a birthday attack

C. Providing data confidentiality

D. Zero knowledge proof

114. Because the CPU is the brain of a computer, it and the operating system have multiple layers of self-protection. One mechanism they use is protection rings to separate critical components through boundaries of security controls. Which of the following computer components would be placed in the outermost ring?

A. Applications and programs

B. I/O drivers and utilities

C. Operating system kernel

D. Remaining parts of the operating system

115. The ability for a computer to perform I/O functions is the key factor in its effectiveness.

When proper I/O levels cannot be maintained, a system may malfunction and operations freeze. Which one of the core security principals does this affect most?

A. Integrity

B. Availability

C. Confidentiality

D. Consistency

116. The Bell-LaPadula model enforces confidentiality by establishing security levels for both subjects and objects. It also ensures that the state of the operating system remains secure at all times. It operates under the premise that if the system starts up secure, allows only secure state transitions, and shuts down securely, the system will remain secure. What is the name of this concept?

A. Simple security rule

B. * - property rule

C. Least privilege

D. Basic Security Theorem

117. Several evaluation criteria have been developed and used all over the world to assign assurance ratings to products. What is the evaluation process referred to when using the TCSEC criterion?

A. EPL

B. TPEP

C. Orange Book

D. NCSC

118. Most operating systems are able to interact with other systems even though they use different protocols, function in different manners, and have different requirements. This is possible because vendors use standard interfaces and protocols. Systems that work on this type of architecture are referred to as what?

A. Open systems

B. Universal systems

C. Closed systems

D. Interoperable systems

119. All of the users within a department have the necessary clearance to the data on a specific server, but not all of them have the need to know. What type of mode does the system run in?

A. Dedicated

B. System-high

C. System-secure

D. System-low

120. The CPU is responsible for processing instructions on a computer. This vital component is made up of different pieces. What piece carries out the logic functions and mathematical computations?

A. ALU

B. Control unit

C. Primary storage

D. Registers

121. Computers have many methods for protecting themselves. One security measure is an

abstract machine that ensures all subjects have adequate permission to access objects. This concept ensures objects will not be harmed by untrusted subjects. What is this security control called?

A. Security kernel

B. Trusted computer base

C. Reference monitor

D. Security domain

122. A public relations executive is writing a press release regarding a major bug discovered in a software program. As he is finishing, he realizes he needs more technical details. Unable to get information from the engineering department head, he accesses their shared network drive and finds the information in one of the staff's personal folders. The shared drive has a lower integrity level than his program does. He has just violated the "no read down" rule stated in what security model?

A. Biba

B. Clark-Wilson

C. Bell-LaPadula

D. Brewer-Nash

123. Computer security evaluations have gone through many phases. First, TCSEC was used but it was considered too narrow. Next, ITSEC was developed to be flexible but in the process became extremely complicated. Now, products are evaluated with a new program. What is this program called?

A. International Evaluation Criteria System

B. Universal Evaluation Standards

C. Common Criteria

D. National Security Standards

124. Data is stored in a variety of ways. Sometimes it is stored based on convenience and sometimes on necessity. Sequential storage means that data saved on a medium must be accessed in the same order in which it was saved. Which of the media types below is a sequential storage device?

A. CD-ROM

B. Floppy disk

C. Magnetic tape

D. Hard drive

125. Companies going through the evaluation, certification, and accreditation process must account for the many steps and different avenues that can be taken. Which of the following characteristics of the process is not true?

A. The order of the process should be evaluation, certification, accreditation.

B. Certification and accreditation only take place once, when the product is initially purchased.

C. Accreditation is the formal acceptance of a product by management.

D. Evaluation can be provided by TCSEC, ITSEC, or Common Criteria.

126. If a product receives a TCSEC C1 assurance rating, what would be the equivalent rating in ITSEC?

A. F1 + E1

B. F3 + E3

C. F5 + E6

D. E0

127. Operating systems have ways to increase their own memory. One method involves storing data on the hard drive when the main memory fills up. When the operating system needs to use this data now stored on the hard drive, it recalls it back into the main memory. This recall process is referred to as _____.

A. Page mapping

B. Page fault

C. Memory mapping

D. Supervisory state

128. In an operations group, users must have access to a key billing system to enter specific codes. However, these users input their data into an external program that then communicates with the billing system's database. Use of an external program to provide communication between subjects and objects is part of what security model?

A. Bell-LaPadula

B. Chinese Wall

C. Clark-Wilson

D. Brewer-Nash

129. A company makes routers and bridges for use in local area and wide area networks. Which book in the Rainbow Series would be used as the evaluation criteria?

A. Orange Book

B. Red Book

C. Network components are not evaluated by TCSEC

D. Brown Book

130. Computer evaluations help the consumer make more educated purchase decisions. Rating the security mechanisms of a system gives the customer confidence that it will perform accurately and consistently in different situations. What is this referred to as?

A. Availability

B. Assurance

C. Confidentiality

D. Integrity

131. Some systems allow two or more classifications of information to be processed at one time even if the subjects do not have the same clearance levels. Information flows in a direction that does not negate the system's security policy. The information is passed by a component called a pump. What type of system does this describe?

A. System-high mode computers

B. Dedicated security mode computers

C. Multilevel security mode computers

D. Complex security mode computers

132. Don is a senior manager of an architectural firm. He has just found out that a key contract was renewed, allowing the company to continue developing an operating system that was idle for several months. Excited to get started, Don begins work in the operating system privately, but cannot tell his staff until the news is announced publicly in a few days. However, as Don begins making changes in the software, various staff members notice changes in their connected

systems, even though they work in a lower-security level. What kind of model could be used to ensure this does not happen?

A. Biba

B. Bell-LaPadula

C. Noninterference

D. Clark-Wilson

133. Many of the security architecture models (Bell-LaPadula, Biba, Clark-Wilson) are very high-level constructs and provide abstracts for software designers to use as a map to meet specific security goals. Which of the following models address more granular activities, as in how subjects and objects should be created securely?

A. Harrison-Ruzzo-Ullman model

B. Brewer-Nash

C. Information Flow

D. Graham-Denning model

134. A company has performed the following steps when buying a new operating system: 1) Analyzed Common Criteria evaluation report on the product; 2) Purchased the product after comparing other alternatives; and 3) Properly certified the product within the internal network. What is the next step that needs to happen before the process is complete?

A. Software debugging

B. Contigency planning

C. Accreditation

D. Establish access control policies

135. Which security model enforces the principle that the security levels of an object should never change and is known as the "strong tranquility" property?

A. Biba

B. Bell-LaPadula

C. Brewer-Nash

D. Noninterference

136. Denise is a newly hired executive brought on specifically to implement improved physical security controls. In her first staff meeting with her team, she asks the group to outline how data flows through the company. The critical assets necessary to keep data flowing and existing redundant paths. What is the name of the process Denise has just delegated?

A. Critical path analysis

B. Risk reduction

C. Planning horizon

D. Policy planning

137. What does a company need to investigate to ensure that the availability of production systems are not negatively affected for a long period of time if a new system goes down?

A. NDA and MTTR

B. SLAs and MTTR

C. MTBF and NDA

D. MTTR and TSCEC

138. Companies that offer mission critical services to their customers have to make contingencies for potential power failures. An uninterruptible power supply (UPS) is a common alternative that

companies select. In situations where even one second of power interruption is unacceptable, the UPS can take over the load as soon as power is lost. These UPS types have primary power continually running through them and are activated immediately if the primary source fails. What are these systems called?

A. Standby UPS

B. Online UPS

C. Ghost UPS

D. Generator

139. A company with highly combustible materials is trying to determine which sprinkler system type to purchase. They are not concerned with false alarms, but instead are insistent that the system be effective at extinguishing large and rapidly growing fires extremely fast. Which would be the best sprinkler system for this company?

A. Wet pipe

B. Deluge

C. Dry pipe

D. Preaction

140. Jonathan's workstation is overloaded with electrical connections into a small number of outlets. He is daisy-chaining power strips in order to service all of his equipment. One problem that always remains is excessive line noise and power fluctuation. He needs to address the problem but does not have a great deal of money budgeted for it. Which of the solutions below would be least favorable for this specific issue?

A. Surge protector

B. Line conditioners

C. Redistribute cords to other outlets

D. UPS

141. When discussing the risks associated with fire, it's important to consider fire's "four legs." The four legs are heat, oxygen, fuel, and chemical reaction. Which of the statements below is true about fire suppression?

A. Heat should be reduced; fuel and oxygen should be removed; and chemical reactions should be disrupted.

B. Heat and oxygen should be reduced; fuel should be added; and chemical reactions should be disrupted.

C. Heat should be reduced; and fuel, oxygen, and chemical reactions should be increased.

D. Heat, oxygen, fuel, and chemical reactions should be combined.

142. A storage company has just acquired operational space in a high-rise building located downtown. They will have access to the bottom two floors of the building and intend to use the space for individual customer storage lockers. Customers range from residents with furniture and boxes to construction companies with heavy equipment. Of the following considerations, which would be the lowest priority?

A. Load bearing of walls, ceilings, and floors

B. Combustibility of the materials in the facility

C. Intrusion detection systems

D. The existence of ultraviolet-protected windows

143. Mike and Lisa are business managers who must negotiate a renewal maintenance contract

with a vendor. In order to optimize redundancy while reducing cost, they had to evaluate the situation based upon MTBF and MTTR values. MTBF is the mean time between failure. What does MTTR mean?

A. Maximum time to respond

B. Maximum time to recover

C. Mean time to repair

D. Minimum time to repair

144. There are many environmental issues to consider when securing a facility and its assets. One issue is maintaining proper temperatures to avoid damage to devices. What is the threshold temperature at which computer devices will become damaged?

A. 98° F

B. 110° F

C. 175° F

D. 350° F

145. Due to some recent after-hours altercations in a nearby parking lot, Jim's company is installing new lights at the location to improve security. Jim is in charge of physical security and has done the research on lighting requirements in critical areas. One of the requirements Jim found was something called two foot-candles. What does this mean?

A. Lights must be placed 2 feet apart.

B. The area being lit must be illuminated 2 feet high and 2 feet out.

C. This is an illumination metric used for lighting.

D. Each lit area must be within 2 feet of the next lit area.

146. Craig is handling all the details of a move into a new building his company has just purchased. While walking with the inspector on the facility tour, the inspector comments, "You need positive drains throughout this place." What does the inspector mean by this?

A. There always needs to be more drain outlet points than incoming source points.

B. Each floor must have a positive number of drains.

C. Drainage systems must be installed at positive angles.

D. Contents should flow out of buildings, not into them.

147. The classes of fire are determined by their level of combustibility. Of the materials below, which does not have a Class A rating.

A. Wood

B. Rubber

C. Oil-based paint

D. Paper

148. Max is in charge of security for his company. The engineering group has recently purchased a mockup prototype of their new product currently in research and development. The prototype was built to scale and thus was a very costly outsourcing expense. To protect this asset, Max has installed a new mechanism that emits an electromagnetic field around the object. Detectors are used to sense disruptions in this field. What type of security mechanism has Max implemented?

A. Photometric detector

B. Proximity detector

C. Wave detector

D. Passive infrared detector

149. Companies can choose to protect their entire premises with tall stone fences that portray a fortress-type image. They can also choose smaller scale barriers such as 3- to 4-foot high fences. What type of control would these smaller fences be considered?

A. Corrective

B. Deterrent

C. Technical

D. Administrative

150. Which of the following is not a fire-related requirement in computer rooms?

A. Detectors should be placed in raised flooring spaces.

B. Class C suppressing agents should be present.

C. Deluge sprinkler systems are most common.

D. Humidity should not be too high.

151. Patrice arrives home one evening and plays the messages in her voice mail. One says, "This is a message from the power company. Several thousand customers in your area experienced service disruption today. This region suffered a brownout due to capacity issues with our systems. The situation has been restored and you should no longer suffer any adverse effects. Thank you for your understanding." What exactly did the region suffer?

A. Prolonged power supply that is below normal

B. Momentary low voltage

C. Prolonged loss of power

D. Momentary power outage

152. Low levels of humidity result in static electricity. High levels of humidity create a host of problems as well. Which of the following issues pertaining to high levels of humidity is the most concerning to a security professional?

A. Excessive moisture in the air is not an optimum condition for employees who spend their days in a computer room.

B. High humidty levels put strain on HVAC systems, which can cause security concerns.

C. High humidty levels can damage or destroy computer parts.

D. High humidity levels make the possibility of fire more likely.

153. Because environmental changes can dramatically affect the performance of computing devices, it is important to consistently monitor levels. What would a person be measuring if he were using a hygrometer?

A. Temperature changes over time

B. Humidity levels

C. Dust contaminants

D. Combustibility of materials

154. An often-forgotten consequence of fire is the damaging effects that smoke can cause. Smoke can create many problems in data centers. Which of the following is not true regarding smoke?

A. Power should be turned off immediately when smoke is present.

B. Smoke is more damaging over time than first realized.

C. The major damage done is by smoke in the air, which causes circuit boards to malfunction.

D. Smoke detectors should be in dropped ceilings and under raised flooring.

155. Scott, a senior network engineer with exceptional knowledge of the existing security controls protecting the company's network, is terminated. He is immediately escorted from the

building by security guards. Although Scott's permissions were cleared, his employee ID swipe card was not retrieved when he was let go. Later that night, he returns to the facility and sabotages the network. Which of the following security controls failed in this example?

A. Door locks

B. The decision to escort Scott off the premises immediately

C. Employee termination procedures

D. Enforcement of need to know

156. Bob became interested in security after working on several physical IDS mechanisms with his company. He has worked on systems with advanced capabilities such as infrared detection, photometrics, and seismic detectors. Which type of IDS is sensitive to sound?

A. Infrared

B. Photometric

C. Seismic

D. Proximity

157. Not all fire suppressing agents can be used in all situations. For example, a particular agent could be used in an unmanned facility but should not be used in a typical office building with employees. Which of the following suppressing agents is the most harmful to people?

A. FM-200

B. CO2

C. Soda acid

D. Argonite

158. The Bell-LaPadula model has three main rules: 1) Simple Security Property; and 2) Star Property. What is the third rule and what does it state?

A. Strong Star Property means that a subject that has read and write capabilities can only perform those functions at its own security level.

B. Strong Star Property means that a subject that has read and write capabilities can only perform those functions to objects at a higher security level.

C. Strong Star Property means that a subject that has read and write capabilities can only perform those functions to the objects at a lower security level.

D. Strong Star Property means that a subject that has read and write capabilities can only perform those functions to the subjects at a higher security level.

159. Operating systems that provide multilevel security and mandatory access control are based on which model?

A. Brewer-Nash

B. Biba

C. Clark-Wilson

D. Bell-LaPadula

160. Which security model incorporates the "no write up" and "no read down" rules?

A. Biba

B. Bell-LaPadula

C. Information Flow

D. Clark-Wilson

161. The Common Criteria uses which of the following to describe specific security solution needs?

A. EPL

B. EAP

C. Protection profiles

D. Security targets

162. What book in the Rainbow Series focuses on network security?

A. Blue Book

B. Tan Book

C. Red Book

D. Aqua Book

163. Which rating offers the highest level of assurance?

A. B1

B. C2

C. B3

D. C1

164. TCSEC classification A offers what characteristic that classification B does not?

A. Testing is less detailed in A.

B. A requires fewer TCB components.

C. More formal methods of evaluation are used in A.

D. Security mechanisms are under less scrutiny in A.

165. What type of attack would alter a configuration file after the system looked to see if it had that specific file?

A. Covert channel

B. Back door

C. Fraggle

D. TOC/TOU

166. The concept that dictates that once an object is used it must be stripped of all of its data remnants is called _____.

A. Layering

B. Object reuse

C. Multiuse

D. Polymorphism

167. What type of computer memory improves system performance by acting as a special storage area for information that is retrieved often?

A. Primary

B. Virtual

C. RAM

D. Cache

168. The reference monitor ensures what?

A. Only authorized subjects access objects.

B. Information flows from a low security level to a high security level.

C. The CPU does not access memory directly

D. Subjects do not write down to lower objects

169. The concepts within the TCSEC, ITSEC, CTCPEC, and the Federal Criteria were used to create what?

A. Orange Book

B. Rainbow Series

C. Common Criteria

D. Red Book

170. A computer's hard drive, floppy disks, or CD-ROM is called _____.

A. Primary storage

B. Virtual memory

C. Real storage

D. Secondary storage

171. Which of the following computer components dictates when data is processed by the system's processor?

A. Control unit

B. Registers

C. ALU

D. Ring 0

172. A CPU that can handle more than one process at a time is considered what type of system?

A. Multithreading

B. Multitasking

C. Multiprogramming

D. Multifunctioning

173. Which organization developed the TCSEC?

A. ISO

B. DoD

C. FBI

D. ITSEC

174. Using a communication path in an unintended way in order to do harm is called _____.

A. Timing attack

B. Asynchronous attack

C. Buffer overflow

D. Covert channel

175. Which of the following will not lose data when power is lost?

A. Registers

B. RAM

C. Storage devices

D. Buffers

176. Which of the following advances to microprocessor architecture has increased some vulnerabilities?

A. Distributed environments

B. Network connectivity

C. Increased circuits, cache memory, and multiprogramming

D. Increases in processing power

177. Which of the following best describes TCSEC?

A. A criteria to validate the security and assurance provided in products

B. The Red Book

C. European assurance evaluation criteria

D. A penetration testing method

178. Which of the following is referred to when management states that it understands the level of protection that a system will provide in its current environment and the security risks associated with installing this system?

A. Certification

B. Accreditation

C. Open system

D. Closed system

179. Which of the following tasks takes place before the accreditation phase?

A. Certification

B. Accreditation

C. Disposal

D. Closing a system

180. Traditional systems, as opposed to modern systems, exhibited which type of environment?

A. Certified

B. Accredited

C. Open

D. Closed

181. Which of the following statements about trusted computing base (TCB) is accurate?

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 addresses the level of significance each mechanism of a system portrays in a secure environment.

182. Which of the following is an accurate description of the relationship between the security kernel and the reference monitor and their requirements?

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 is an abstract machine or component that is invoked by the security kernel for every access attempt and is sometimes possible to bypass in extreme situations. The security kernel is testable and can be verified.

C. The reference monitor is a piece of software that allows the security kernel to run on top of its services. The reference monitor is accessed by every security access attempt and cannot be circumvented. The security kernel is small enough to be tested and verified.

D. The reference monitor is an abstract machine that is invoked by the security kernel for all access attempts. It should be impossible to circumvent the reference monitor, and the security kernel can be tested and verified. The security kernel enforces the reference monitor concept.

183. This model incorporates the idea of "separation of duties" and requires that access to data and objects be done through programs. Which of the following models incorporates these ideas

and concepts?

A. State Machine

B. Bell-LaPadula

C. Clark-Wilson

D. Biba

184. Which classification in the TCSEC specifies "discretionary protection?"

A. Division D

B. Division C

C. Division B

D. Division A

185. Which security model specifies that commands and activities performed at one security level should not be seen or affect subjects or objects at a different security level?

A. Biba model

B. Information flow model

C. Security separation model

D. Noninterference model

186. What does a lattice provide within a system?

A. An upper bound and lower bound of authorized access

B. A rule indicating the flow of data within the system

C. A rule indicating what subjects can write to a higher level

D. An upper bound and lower bound on user accessibility to network resources

187. Which of the following provides the highest security when it comes to memory?

A. Memory mapping

B. Hardware segmentation

C. Virtual machines

D. Protection rings

188. What is the main reason why an application would be developed using the Brewer-Nash model?

A. To provide varying degrees of confidentiality and integrity

B. To ensure that unauthorized subjects cannot make modifications

C. To ensure conflicts of interests are minimized through dynamic access control

D. To ensure that the integrity of an object at a higher level is not compromised

189. The interleaved execution of two or more programs by a CPU is called what?

A. Multiprogramming

B. Multitasking

C. Multiprocessing

D. Multithreading

190. What is the purpose of a virtual machine within an operating system?

A. To implement hardware and logical separation of memory segments

B. To implement the different protection rings and domains of resources

C. To ensure that the reference monitor is invoked for every access attempt

D. To provide a container and environment for applications

191. The ITSEC criteria uses which of the following ratings?

A. E – F

B. EAP

C. EPL

D. A – D

192. Water and gas lines should have shutoff values and positive drains. What is a positive drain?

A. Water does not go into the drain until a fire has been detected.

B. This characteristic ensures that the pipe is unbreakable.

C. Water and gas flow out instead of in.

D. Water and gas flow in instead of out.

193. How does water suppress a fire?

A. Modifies the chemical combustion elements

B. Reduces the fuel

C. Reduces the temperature

D. Reduces the oxygen

194. How does an acoustical-seismic device detect an intruder?

A. Change in vibration

B. Change in magnetic field

C. Change in microwaves within room

D. Breakage of foil strip in window

195. Which of the following does not describe proper use of a fire extinguisher?

A. Must be in an area with electrical equipment

B. Must be visible

C. Must be inspected yearly

D. Must contain fire suppression agent appropriate for area

196. Which one of the following has the correct definitions?

A. A spike is a period of prolonged high voltage, and a fault is a momentary power outage.

B. A brownout is a prolonged low voltage period, and a surge is a prolonged high voltage period.

C. A fault is a prolonged power loss, and a spike is a prolonged high voltage period.

D. A sag is a prolonged power loss, and a brownout is a period of momentary high voltage.

197. Which of the following properly describes a dry pipe system?

A. Water is always in pipe.

B. Water is kept in pipe, and a link has to melt before water is released.

C. Water is in pipe, and the head is always open.

D. Water is not in pipe, and system should be used in colder areas.

198. When looking at facility construction, which of the following items is not as important as the others?

A. The load that the floors, ceilings, or walls need to hold

B. The fire rating of the walls and doors

C. The combustion rate of the materials used

D. Using photoelectric material

199. Which of the following items is not considered a preventive physical control?

A. Fencing

B. Access logs

C. Security guards

D. Security dogs

200. If a company has two extinguishers that were filled with Halon and they need to be refilled, what does the company need to do?

A. Refill them with Halon.

B. Throw the extinguishers away. They can no longer be used as outlined in the Montreal Protocol.

C. Refill them with FM-300.

D. Refill them with FM-200.

201. Which of the following water sprinkler systems sounds an alarm and delays water release?

A. Wet pipe system

B. Preaction system

C. Deluge system

D. Dry pipe system

202. How far should portable fire extinguishers be located from electrical equipment?

A. 100 feet

B. 50 feet

C. 40 feet

D. 20 feet

203. Which of the following should be used to suppress a Class A fire?

A. Water

B. Gas

C. CO2

D. FM-200

204. A momentary level of high voltage is referred to as a _____.

A. Sag

B. Surge

C. Spike

D. Strike

205. Internal partitions should not be used in which of the following instances?

A. To provide protection of a sensitive area

B. To create storage rooms for nonsensitive materials

C. To create different work areas

D. To create barriers between areas

206. The estimated lifetime of a device or the estimated timeframe until a component within a device gives out is called _____.

A. UPS

B. MTTB

C. MTTR

D. MTBF

207. Power levels that do not fluctuate are referred to as _____.

A. Safe

B. Clean

C. Surge

D. Ground

208. Which is true of how CO2 works to control a fire?

A. Removes or displaces the oxygen

B. Adds fuel

C. Interferes with the chemical reaction

D. Reduces the temperature

209. What is plenum space?

A. Open space above dropped ceilings and below raised floors

B. The screened subnet area within the DMZ

C. The unprotected area around the security perimeter fence

D. A VPN tunnel

210. What is a hygrometer used to monitor?

A. Noise reduction for acoustical sensors

B. Power reduction to allow for clean power supplies

C. Humidity in an environment

D. Static electricity in an environment

211. Any of the following actions can be taken to prevent static electricity except which one?

A. Install carpet

B. Use anti-static bands when working in computer systems

C. Install anti-static flooring

D. Ensure proper grounding

212. Sprinkler systems that allow the release of large volumes of water in a short time are called _____.

A. Wet pipe

B. Deluge

C. Preaction

D. Dry pipe

213. Which of the following lock types prevents the removal of I/O devices by passing cables through a lockable unit?

A. Table lock

B. Port control

C. Switch control

D. Cable trap

214. Using special key combinations with cipher locks during emergency situations is called _____.

A. Switch controls

B. Key override

C. Door delay

D. Master keying

215. When an intruder follows an authorized individual through the entrance without authenticating to the access control system, it is called _____.

A. Forced entry

B. Piggybacking

C. Disguising

D. Wiretapping

216. In physical security, what are electronic access control (EAC) tokens used for?

A. To authenticate subjects

B. To control the amount of radiation that escapes from control rooms

C. To lock down a facility or system after an intrusion has been detected

D. To authenticate objects

217. CCTV mechanisms are best when used with which of the following?

A. Penetration testing software

B. Other controls in a synergistic way

C. Fire suppression and detection controls

D. Encryption and key recovery implementations

218. Physical security components combat all of the following main risks except _____.

A. SYN flood

B. Physical damage

C. Theft

D. Loss of availability

219. What is the most prevalent cause of computer center fires?

A. AC equipment

B. Electrical systems

C. Heating systems

D. Natural causes

220. The vulnerability of a facility to damage or attack may be assessed by reviewing all of the following except _____.

A. Inspection

B. History of losses

C. Security controls

D. Security budget

221. Which of the following is currently the most recommended water system for a computer room?

A. Preaction

B. Wet pipe

C. Dry pipe

D. Deluge

222. Which of the following should be used to suppress the fuel supply of a fire of common combustibles?

A. Soda acid

B. CO2

C. Halon

D. Air

223. What is the last line of defense in a physical security sense?

A. People

B. Interior barriers

C. Exterior barriers

D. Perimeter barriers

224. Which of the following uses a photoelectric device to trigger an alert?

A. Automatic dial-up alarms

B. Heat-activated fire detectors

C. Flame-activated fire detectors

D. Smoke-activated fire detectors

225. Which class of fire can involve petroleum products and coolants?

A. Class A

B. Class B

C. Class C

D. Class D

226. Four-foot fences can be used to _____.

A. Deter casual trespassers.

B. Provide reasonable defense from external intrusion.

C. Discourage a determined intruder.

D. Slow down a determined intruder.

227. Which of the following is not a characteristic of Digital Signature Algorithm (DSA)?

A. Can be used for key exchange

B. Developed by the NSA

C. Part of the DSS

D. Uses a secure hash algorithm to condense the message before signing it

228. One-way hashed passwords are most vulnerable to which of the following attack types?

A. Plaintext attack

B. Fraggle attack

C. Dictionary attack

D. Smurf attack

229. What size of message digest does Secure Hash Algorithm (SHA) produce?

A. 128-bit

B. 160-bit

C. 64-bit

D. 120-bit

230. Which of the following is the science of studying and breaking the secrecy of cryptosystems and their necessary pieces?

A. Cryptosystem

B. Brute force

C. Kerchoff

D. Cryptanalysis

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

A. DEA

B. Rijndael

C. Twofish

D. IDEA

232. A cipher that scrambles letters into different positions is referred to as what?

A. Substitution

B. Stream

C. Running key

D. Transposition

233. Which of the following DES modes is typically used when small amounts of data are encrypted, such as in ATM PIN numbers?

A. OFB

B. ECB

C. CFB

D. CBC

234. What function does the symmetric key in hybrid cryptography provide?

A. Key storage

B. Key generation

C. Key distribution

D. Message encryption

235. The HAVAL algorithm performs what function?

A. Hashing

B. Key distribution

C. Digital signature

D. Encryption

236. A function that takes a variable-length string and creates a fixed-length value is called_____.

A. Key

B. Digital signature

C. One-way hash

D. Encryption

237. What was the algorithm that was accepted as the Data Encryption Standard (DES)?

A. El Gamal

B. IDEA

C. RC5

D. Lucifer

238. Random and unreadable text messages are called_____.

A. Cleartext

B. Ciphertext

C. Plaintext

D. Cryptotext

239. What was the size of the key used in the Clipper Chip?

A. 80-bit

B. 64-bit

C. 128-bit

D. 160-bit

240. Which of the following is considered the perfect encryption scheme and is unbreakable?

A. RSA

B. IDEA

C. PKI

D. One-time pad

241. Hiding messages within the text of this question would be considered what type of encryption method?

A. Steganography

B. Running key cipher

C. Concealment cipher

D. Frequency analysis

242. Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Security

B. Speed

C. Scalability

D. Key distribution

243. Which of the following is a symmetric key algorithm?

A. Diffie-Hellman

B. ECC

C. El Gamal

D. Blowfish

244. Which protocol protects the communications channel and the messages between a client and a server?

A. S/MIME

B. RPC

C. S-HTTP

D. HTTPS

245. Block ciphers use which of the following to perform mathematical functions, substitution, and permutations on message bits?

A. S-boxes

B. Certificates

C. Keystream

D. Initialization vectors

246. A keystream generator is used in what type of cipher?

A. Block

B. Stream

C. Concealment

D. DES

247. Which of the following is not a characteristic of a strong stream cipher?

A. Unbiased keystream

B. Long periods of unrepeated patterns within keystream

C. Best used in software implementations

D. Statistically unpredictable

248. Rivest, Shamir, and Adleman developed what algorithm?

A. Rijndael

B. RSA

C. DES

D. IDEA

249. Which statement is not true of a good one-way hashing function?

A. It is computed on a portion of the message.

B. It is resistant to birthday attacks.

C. It is impossible to compute another message with the same hash value.

D. Messages are not disclosed by their digests.

250. Which IPsec protocol provides confidentiality and integrity?

A. ESP

B. AH

C. ISAKMP

D. IKE

251. What function does the Diffie-Hellman algorithm perform?

A. Encryption

B. Key exchange

C. Digital signature

D. Hashing

252. If an attacker intercepts a public key and forwards his own key to the receiver, what kind of attack is this?

A. Replay

B. Smurf

C. Dictionary

D. Man-in-the-middle

253. What technology is used when all the data in a communication path is encrypted, including the header, trailer, and routing information?

A. Data hiding

B. Link encryption

C. End-to-end encryption

D. S/MIME

254. Which protocol is used for setting up secured channels between two devices, typically in VPNs?

A. IPSec

B. PPP

C. PEM

D. SET

255. Which one of the following asymmetric algorithms is often used in web browsers with SSL?

A. DES

B. ECC

C. RSA

D. Twofish

256. The standard used for encrypting and digitally signing e-mail that contains attachments is called _____.

A. SET

B. MIME

C. S/MIME

D. MSP

257. The act of hiding data within another medium is called _____.

A. Steganography

B. Transposition

C. Substitution

D. Permutation

258. Which is not true of PGP?

A. It uses a hierarchical trust model.

B. It uses a web of trust between users.

C. Public keys are kept in key ring files.

D. Users can determine how much they trust one another.

259. Which statement is true about stream ciphers?

A. Messages are divided into blocks and encrypted.

B. They are better used in software compared with block ciphers.

C. They use a keystream generator to produce a stream of bits.

D. They carry out 16 rounds of computation.

260. What is not true of asymmetric cryptography?

A. Can provide nonrepudiation and authentication

B. Better scalability than symmetric cryptography

C. Better key distribution than symmetric cryptography

D. Faster than symmetric cryptography

261. What is it called when an algorithm produces the same hash values for two different messages?

A. Key cluster

B. Collision

C. Brute force attack

D. Birthday attack

262. Which of the following was developed by Visa and MasterCard as a way of securing credit card transactions?

A. IPSec

B. SSH

C. SSL

D. SET

263. When a sender cannot deny sending a message to the receiver, what is this called?

A. Authenticity

B. Nonrepudiation

C. Integrity

D. Data origin authentication

264. MD2 produces what size of hash value?

A. 128-bit

B. 150-bit

C. 160-bit

D. 64-bit

265. Which one of the following items falls under the responsibility of key management?

A. Access control and user identification
B. Key length and algorithm correctness
C. Access control and encryption integrity
D. Key generation and destruction

266. Which security services do digital signatures provide?
A. Confidentiality and availability
B. Integrity and accountability
C. Integrity and accessibility
D. Confidentiality and integrity

267. What is the standard used for PKI certificates?
A. X.400
B. X.500
C. X.509
D. LDAP

268. Which of the following is required for cryptanalysis?
A. Access to plaintext
B. Access to plaintext and ciphertext
C. Access to algorithm source
D. Access to ciphertext and algorithm source

269. SSL requires which of the following?
A. PKI
B. KDC
C. S/MIME
D. MIME

270. A brute force attack is launched to obtain which of the following?
A. Encryption keys
B. A public algorithm
C. A public key
D. Ciphertext

271. Which of the following is the most important type of protection when dealing with passwords?
A. Encrypting them where they are stored centrally
B. Using non-dictionary words
C. Ensuring they are at least six characters long
D. Sending in cleartext

272. Which of the following provides the best protection for a network's traffic?
A. Link encryption because it does not encrypt headers and trailers
B. Link encryption, which encrypts everything but data link messaging
C. End-to-end encryption because it encrypts all headers and trailers
D. End-to-end encryption because headers have to be decrypted at each intermediate device

273. What does AES accomplish?
A. Key recovery
B. Symmetric key distribution
C. Bulk data encryption

D. Message integrity

274. Which of the following is a cryptosystem that uses a session key?
   A. IDEA
   B. PGP
   C. DES
   D. Blowfish
275. Which of the following is not a true 3DES mode?
   A. DES-EEE1 uses one key.
   B. DES-EEE2 uses two keys.
   C. DES-EEE3 uses three keys.
   D. DES-EDE2 uses two keys.
276. What does AES use S-boxes for during the encryption process?
   A. Chaining
   B. Key exchange
   C. Substitution
   D. Key generation
277. Which of the following is a true weakness of DES?
   A. S-box usage
   B. Secrecy of the algorithm
   C. Incompatible with AES
   D. Key size
278. Which of the following is a proper characteristic of SKIP and ISAKMP?
   A. They work at the application layer.
   B. They work at the transport layer.
   C. They work at the data link layer.
   D. They work at the network layer.
279. Which of the following best describes a characteristic of IPsec?
   A. Provides system authentication
   B. Provides content filtering
   C. Works as a proxy
   D. Provides application layer protection
280. What is the purpose of a public key?
   A. To authenticate a network interface
   B. To encrypt a private key
   C. To authenticate a private key
   D. To be encrypted by a private key
281. Which of the following best describes what takes place in an SSL connection?
   A. The client creates a session key and encrypts it with a public key.
   B. The client creates a session key and encrypts it with a private key.
   C. The server creates a session key and encrypts it with a public key.
   D. The server creates a session key and encrypts it with a private key.
282. Which one of the following is an accepted practice for providing strong encryption services?
   A. Maintaining the secrecy of the hashing algorithm
   B. Use of a large keyspace to provide a greater variety of keys

C. Use of a smaller keyspace to provide the ability to choose a strong key

D. Making sure the plaintext itself is not hard to guess

283. Which of the following statements about symmetric and asymmetric cryptography is true?

A. Asymmetric encryption performs faster, is slower to implement, and uses only one key.

B. Asymmetric encryption is slower than symmetric, encrypts keys, and uses a key pair.

C. Symmetric encryption uses in-band key exchange, performs faster, and uses a single key.

D. Symmetric encryption performs faster, is slower to implement, and uses a key pair.

284. Which statement is true regarding digital signatures?

A. Confidentiality is assured due to the use of the sender’s private key for encryption.

B. Confidentiality is assured due to the use of the receiver’s private key for encryption.

C. Authentication is assured due to the use of the sender’s private key.

D. Authentication is assured due to the use of the receiver’s public key.

285. Which type of cipher works at the bit level and is more suitable for hardware implementations?

A. Stream cipher

B. Block cipher

C. Chunking cipher

D. CDC cipher

286. Which of the following is a proper description of DES?

A. DES encryption employs an asymmetric key using a stream cipher and a 56-bit key for encryption.

B. DES encryption employs a symmetric key using a block cipher and a 56-bit key for encryption.

C. DES encryption employs a block cipher using a 128-bit key for encryption.

D. DES encryption employs a block cipher using a true key length of 64 bits for encryption.

287. Which one of the following is a hybrid system employing asymmetric and symmetric encryption services?

A. 3DES

B. PKI

C. RSA

D. Diffie-Hellman

288. Which service in a PKI will vouch for the identity of an individual or company?

A. KDC

B. CBC

C. CA

D. CR

289. Which asymmetric algorithm would be ideal to employ within cell phones?

A. 3DES

B. Diffie-Hellman

C. RSA

D. ECC

290. A typical PKI infrastructure would have which of the following transactions?

1. Receiver decrypts and obtains session key.

2. Sender requests receiver’ s public key.

3. Public key is sent from a public directory.

4. Sender sends a session key encrypted with receiver's public key.

A. 4, 3, 2, 1

B. 2, 1, 3, 4

C. 2, 3, 4, 1

D. 2, 4, 3, 1

291. A user would like to send a message and allow only one other person to verify the integrity of the message. The user would need to implement what function?

A. One-way hash

B. Message digest

C. Message authentication code

D. Trapdoor one-way function

292. Which one of the following is not a hashing algorithm used for message integrity?

A. SHA

B. MD5

C. Diffie-Hellman

D. HAVAL

293. Which type of encryption would be considered the more secured encryption method across a single link?

A. End-to-end encryption

B. Tunnel encryption

C. Transport encryption

D. Link encryption

294. An appropriate encryption method when encrypting only individual messages between two computers is _____.

A. HTTPS

B. SSL

C. IPSec

D. S-HTTP

295. You are trying to provide a secure method of terminal access to a remote computer. Which protocol should you use?

A. Telnet

B. rlogin

C. SSH

D. rsh

296. The method of IPsec encryption that secures the payload as well as the routing and header information is _____.

A. Security association

B. Tunnel mode

C. Transport mode

D. Security parameter index (SPI)

297. What is the equation to calculate the number of symmetric keys needed and how many keys are required if ten people need to communicate using symmetric keys?

A. N(N + 1)/3 and 40 keys are needed.

B. N(N – 1)/2 and 45 keys are needed.

C. N(N/2) – 1 and 35 keys are needed.

D. N(N + 1) and 25 keys are needed.

298. Knapsack is what type of algorithm?

A. Asymmetric

B. Hashing

C. Symmetric

D. Hybrid

299. Which of the following is a true statement about the Caesar algorithm?

A. The algorithm is an alphabet and the key is the number of shifts.

B. The algorithm is the number of shifts in an algorithm and the key is the algorithm.

C. It uses a secret word for polyalphabetic encryption.

D. It is another name for the scytale method.

300. The Vigenere cipher was developed in the 16th century in France. Which of the following is a correct characteristic of this algorithm?

A. It uses one-time pads.

B. It uses a secret word as the key.

C. It requires a messenger to take the right size rod to the destination.

D. It was used in World War II.

301. How is it possible that anyone can know how a specific algorithm works and it can still provide protection through secrecy?

A. The source code is not provided.

B. The S-boxes are continually changed through the use of initialization vectors.

C. No one has access to the keystream.

D. Cryptovariable provides the secrecy.

302. If a cryptosystem is using a key size of 8, what is the keyspace size?

A. 64

B. 32

C. 256

D. 16

303. What is Kerckhoff’s principle and why is it relevant?

A. One-time pads should be just as long as the message, otherwise patterns will be shown.

B. A public key needs to associated with an individual’s identity for true nonrepudiation.

C. The only secret portion to a cryptosystem should be the key so that the algorithms can be stronger.

D. More than one alphabet should be used in substitution ciphers to increase the workfactor.

304. Which of the following is a requirement for a secure Vernam cipher?

A. The pad must be used just one time.

B. A symmetric key must be encrypted with an asymmetric key.

C. The private key must only be known to the owner.

D. It needs to hide the existence of a message.

305. There are different binary mathematical functions. Which of the following is a true rule of the exclusive OR function?

A. Same value XOR same value equals one

B. 1 XOR 1 = 1

C. 0 XOR 0 = 1

D. 1 XOR 0 = 1

306. Which of the following is not a requirement of a secure one-time pad implementation?

A. Pad must be distributed securely.

B. Pad must be at least as long as the message.

C. Pad must be used only two times.

D. Pad must be made up of truly random values.

307. Which of the following is not addressed in the Wassenaar Arrangement?

A. Symmetric algorithms

B. Asymmetric algorithms

C. Intangibles that could be downloaded from the Internet

D. Products exported to terrorist countries

308. Which of the following is a true difference between an asymmetric and symmetric algorithm?

A. Symmetric algorithms are faster because they use substitution and transposition.

B. Asymmetric algorithms are slower because they use substitution and transposition.

C. Asymmetric algorithms are best implemented in hardware and symmetric in software.

D. Asymmetric algorithms are more vulnerable to frequency analysis attacks.

309. A symmetric algorithm must have certain characteristics to be considered strong. Which of the following is not correct pertaining to these types of characteristics?

A. Confusion is carried out through transposition and diffusion is carried out through diffusion.

B. Confusion is carried out through substitution and diffusion is carried out through transposition.

C. Confusion and diffusion are both used to increase the workfactor.

D. The randomness of the key and functions in the algorithm correlate with the level of confusion and diffusion that is provided.

310. How are a one-time pad and a stream cipher similar?

A. They are both asymmetric algorithms.

B. They are both vulnerable to linear frequency cryptanalysis attacks.

C. They both use XOR bits for their encryption process.

D. They are both block ciphers.

311. Both block and stream algorithms use initialization vectors. Which of the following is not a reason that they are used?

A. They are used to add randomness to the encryption process.

B. They ensure that two identical plaintext values result in different ciphertext values when encrypted with the same key.

C. They provide extra protection in case an implementation is using the same symmetric key more than one time.

D. They are XORed to the plaintext after encryption to ensure more randomness to the process.

312. Which of the following is not a necessary characteristic to ensure a strong symmetric algorithm?

A. The bits that are generated from the keystream generator cannot be predicted.

B. If someone figures out the keystream values, it does not mean that she knows the key value.

C. Long periods of repeating patterns within keystream values.

D. There should be no dominance in the number of 0s or 1s in the keystream.

313. How are symmetric and asymmetric keys used together?

A. An asymmetric key encrypts the symmetric key.

B. An asymmetric key encrypts bulk and symmetric keys encrypt a small amount of data.

C. An asymmetric key is used and then encrypted with a symmetric key.

D. A symmetric key encrypts the data and then the asymmetric key encrypts both of them.

314. Which of the following security services are provided if a sender encrypts data with her private key?

A. Integrity

B. Confidentiality

C. Authentication

D. Corruption

315. Which of the following security services are provided if a sender encrypts data with the receiver's public key?

A. Integrity

B. Confidentiality

C. Authentication

D. Corruption

316. DEA uses how many rounds and parity bits?

A. 16 rounds and 8 bits

B. 8 rounds and 24 bits

C. 56 bits and 16 rounds

D. 72 rounds and 36 bits

317. What flaw creates buffer overflow vulnerabilities?

A. An application executing in privileged mode

B. Inadequate memory segmentation

C. Inadequate protection ring use

D. Insufficient bounds checking

318. The operating system performs all except which of the following tasks?

A. Memory allocation

B. Input and output tasks

C. Resource allocation

D. User access to database views

319. If an operating system allows sequential use of an object without refreshing it, what security issue can arise?

A. Disclosure of residual data

B. Unauthorized access to privileged processes

C. Data leakage through covert channels

D. Compromise of the execution domain

320. What is the final step in authorizing a system for use in an environment?

A. Certification

B. Security evaluation and rating

C. Accreditation

D. Verification

321. What feature enables code to be executed without the usual security checks?

A. Temporal isolation

B. Maintenance hook

C. Race conditions

D. Process multiplexing

322. If a component fails, a system should be designed to do which of the following?

A. Change to a protected execution domain

B. Change to a problem state

C. Change to a more secure state

D. Release all data held in volatile memory

323. What security advantage does firmware have over software?

A. It is difficult to modify without physical access.

B. It requires a smaller memory segment.

C. It does not need to enforce the security policy.

D. It is easier to reprogram.

324. The Information Technology Security Evaluation Criteria was developed for which of the following?

A. International use

B. U.S. use

C. European use

D. Global use

325. A security kernel contains which of the following?

A. Software, hardware, and firmware

B. Software, hardware, and system design

C. Security policy, protection mechanisms, and software

D. Security policy, protection mechanisms, and system design

326. What is the purpose of base and limit registers?

A. Countermeasure buffer overflows

B. Time sharing of system resources, mainly the CPU

C. Process isolation

D. TCB enforcement

327. A guard is commonly used with a classified system. What is the main purpose of implementing and using a guard?

A. Ensure that less trusted systems only receive acknowledgements and not messages

B. Ensure proper information flow within the operating system

C. Ensure that less trusted and more trusted systems have open architectures and interoperability

D. Allow systems at different classification levels to communicate

328. What is the imaginary boundary that separates components that maintain and enforce security with an operating system from components that are not security related?

A. Reference monitor

B. Security kernel

C. Security perimeter

D. Security policy

329. Which model deals only with confidentiality?

A. Bell-LaPadula

B. Clark-Wilson

C. Biba

D. Reference monitor

330. When is system security most effective and economical?

A. When it is designed and implemented from the beginning of the development of the system

B. When it is designed and implemented as a secure and trusted front end

C. When it is customized to fight specific types of attacks

D. When the system is optimized before security is added

331. In secure computing systems, why is a logical form of separation used between processes?

A. Processes are contained within their own security domains so that each does not make unauthorized access to other processes or their resources.

B. Processes are contained within their own security perimeter so that they can only access protection levels above them.

C. Processes are contained within their own security perimeter so that they can only access protection levels equal to them.

D. The separation is hardware and not logical in nature.

332. What type of attack is taking place when a higher-level subject writes data to a storage area and a lower-level subject reads them?

A. TOC/TOU

B. Covert storage attack

C. Covert timing attack

D. Buffer overflow

333. What type of rating system is used within the Common Criteria structure?

A. PP

B. EPL

C. EAL

D. A – D

334. Which best describes the *-integrity axiom?

A. No write up in the Biba model

B. No read down in the Biba model

C. No write down in the Bell-LaPadula model

D. No read up in the Bell-LaPadula model

335. Which best describes the simple security rule?

A. No write up in the Biba model

B. No read down in the Biba model

C. No write down in the Bell-LaPadula model

D. No read up in the Bell-LaPadula model

336. Which of the following was the first mathematical model of a multilevel security policy used to define the concepts of a security state and mode of access and to outline rules of access?

A. Biba

B. Bell-LaPadula

C. Clark-Wilson

D. State machine

337. Which of the following is a true statement pertaining to memory addressing?

A. The CPU uses absolute addresses. Applications use logical addresses. Relative addresses are based on a known address and an offset value.

B. The CPU uses logical addresses. Applications use absolute addresses. Relative addresses are based on a known address and an offset value.

C. The CPU uses absolute addresses. Applications use relative addresses. Logical addresses are based on a known address and an offset value.

D. The CPU uses absolute addresses. Applications use logical addresses. Absolute addresses are based on a known address and an offset value.

338. What are the distinguishing factors between a product with a TCSEC rating of A1 and one with a rating of B3?

A. Architecture features

B. Protection features

C. Verified protection

D. Security policies

339. Using a path that is not intended for communication transmissions to send and receive information is an example of a _____.

A. Covert channel

B. Salami attack

C. Piggybacking attack

D. Buffer overflow

340. Which of the following terms is best described as a simulated environment for applications to run in?

A. TCB

B. Virtual machine

C. Protection rings

D. Execution domains

341. Companies should follow certain steps in selecting and implementing a new computer product. Which of the following sequences is ordered correctly?

A. Evaluation, accreditation, certification

B. Evaluation, certification, accreditation

C. Certification, evaluation, accreditation

D. Certification, accreditation, evaluation

342. What is the result of combining RAM and secondary storage?

A. Virtual storage

B. Real storage

C. Primary storage

D. Combo storage

343. A space on the hard drive saved for faults when the main memory’s capacity is full is called what?

A. Cache storage

B. Swap space

C. Secondary storage

D. Primary storage

344. The Bell-LaPadula model possesses all of the following characteristics except?

A. Incorporates a state machine model

B. Used primarily in the commercial industries

C. Based on the fundamentals of the information flow model

D. Was the first mathematical access control state machine model used for confidentiality

345. When an operating system allows two or more classification levels to be processed at one time, it is operating in what mode?

A. Multiuser mode

B. Dedicated security mode

C. Multilevel security mode

D. System high mode

346. There are several types of components that fall within the trusted computing base (TCB). Which of the following would not be within the security perimeter?

A. Firmware on motherboard

B. Applications

C. Protective hardware components

D. Reference monitor and security kernel

347. The CPU is responsible for processing instructions on a computer. This vital component is made up of different pieces. What piece carries out the logic functions and mathematical computations?

A. ALU

B. Control unit

C. Primary storage

D. Registers

348. Companies going through the evaluation, certification, and accreditation process must account for the many steps and different avenues that can be taken. Which of the following characteristics of the process is not true?

A. The order of the process should be evaluation, certification, and accreditation.

B. Certification and accreditation only take place once, when the product is initially purchased.

C. Accreditation is the formal acceptance of a product by management.

D. Evaluation can be provided by TCSEC, ITSEC, or Common Criteria.

349. The concept that dictates that once an object is used it must be stripped of all of its data remnants is called _____.

A. Layering

B. Object reuse

C. Multiuse

D. Polymorphism

350. What type of computer memory improves system performance by acting as a special storage area for information that is retrieved often?

A. Primary

B. Virtual

C. RAM

D. Cache

351. Which of the following statements about trusted computing base (TCB) is accurate?

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 addresses the level of significance each mechanism of a system portrays in a secure environment.

352. An _____is a formal description and representation of a system, the components that make it up, the interactions and interdependencies between those components, and the relationship to the environment.

A. Architecture description

B. Architecture framework

C. Architecture structure

D. Architecture system

353. Which of the following best describes the ISO/IEC 42010 standard?

A. International standard on system design to allow for better quality, interoperability, extensibility, portability, and security

B. International standard on system security to allow for better threat modeling

C. International standard on system architecture to allow for better quality, interoperability, extensibility, portability, and security

D. International standard on system architecture to allow for better quality, extensibility, portability, and security

354. The _____ for a system are the users, operators, maintainers, developers, and suppliers. Each stakeholder has his own _____ pertaining to the system. The system architecture expresses system data, which is done through _____.

A. Stakeholders, developers, views

B. Users, concerns, reviews

C. Stakeholders, concerns, views

D. Users, requirements, views

355. The _____ is the component that fetches the code, interprets the code, and oversees the execution of the different instruction sets.

A. CPU

B. Control unit

C. Register

D. Processor

356. A CPU has different types of registers it uses to carry out its tasks. Which of the following is not a function type used with special registers (aka dedicated registers)?

A. Program counter

B. Stack pointer

C. Program status word

D. Control condition allocation

357. After a CPU completes its steps in executing instructions and data requested by a specific application, how does the CPU get the resulting values back to the requesting application?

A. Control unit sends the requesting program’s address down the address bus and sends the new results down the data bus with the command “write”

B. CPU sends the requesting program’s address down the address bus and sends the new results down the data bus with the command “write”

C. CPU sends the requesting program’s address down the data bus and sends the new results down the address bus with the command “write”

D. CPU sends the requesting program’s address down the register bus and sends the new results down the data bus with the command “write”

358. Process-to-process communication commonly takes place through the use of memory stacks. A memory stack allows processes to read and write data back and forth to each other. Which of the following best describes how the data are put onto the stack by the initiating process and taken off by the receiving process?

A. Stepwise in a prenumbered sequence

B. Last in, first out

C. Stepwise as configured in the special register

D. First out, last out

359. If a piece of software is carrying out process isolation through encapsulation, how is this implementing data hiding?

A. A process does not need to interact with the interior code of another process but only communicate to the process’s interface.

B. A process must provide the correct cryptographic key to be able to interact with the other process’s internal code.

C. A process enforces object boundaries through temporal access control.

D. A process executes in a virtual environment so that its internal code is not accessible to unauthorized entities.

360. If an application is developed improperly and does not carry out proper process isolation through encapsulation, which of the following is the most likely security concern?

A. Scripting attacks

B. Man-in-the-middle attacks

C. Invalid input values

D. Macro viruses

361. Which of the following memory types is most commonly used in USB drives and solid-state hard drives?

A. ROM

B. Flash memory

C. RAM

D. EPROM

362. Sam is a security engineer at an automobile company. He has found out that many of the critical applications have been developed in the C programming language and has asked for these applications to be reviewed for a specific class of security vulnerabilities. Which of the following is Sam most likely concerned with in this situation?

A. Injection attacks

B. Memory leaks

C. Buffer overflows

D. Browsing attacks

363. Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

A. A page fault is occurring, which forces the operating system to write data from the hard drive to RAM.

B. A race condition is being exploited, and the operating system is containing the malicious process.

C. Malicious code is attempting to execute instructions in a nonexecutable memory region.

D. Malware is executing in either ROM or a cache memory area.

364. A _____ is software that runs an algorithm to identify unused committed memory and then tells the operating system to mark that memory as "available."

A. Memory allocator

B. Garbage collector

C. Application memory tool

D. Process allocator

365. Which of the following best describes Phase Alternative Line (PAL)?

A. It provides specific requirements for monitors used with closed-circuit TVs (CCTVs).

B. It is another name for the National Television Systems Committee (NTSC).

C. It provides specific requirements for cabling and review protocols used with CCTVs.

D. It provides specific requirements for monitors used with CCTVs within the United States.

366. When should a Class C fire extinguisher be used instead of a Class A fire extinguisher?

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

367. How does Halon fight fires?

A. It reduces the fire's fuel intake.

B. It reduces the temperature of the area and cools the fire out.

C. It disrupts the chemical reactions of a fire.

D. It reduces the oxygen in the area.

368. What is a mantrap?

A. A trusted security domain

B. A logical access control mechanism

C. A double-door facility used for physical access control

D. A fire suppression device

369. What is a common problem with vibration-detection devices used for perimeter security?

A. They can be defeated by emitting the right electrical signals in the protected area.

B. The power source is easily disabled.

C. They cause false alarms.

D. They interfere with computing devices.

370. Which problems may be caused by humidity in an area with electrical devices?

A. High humidity causes excess electricity, and low humidity causes corrosion.

B. High humidity causes corrosion, and low humidity causes static electricity.

C. High humidity causes power fluctuations, and low humidity causes static electricity.

D. High humidity causes corrosion, and low humidity causes power fluctuations.

371. Different organizations have different physical security protection requirements, thus they need different types of controls and countermeasures. Which of the following is not a legitimate justification for using security guards at a facility?

A. They are one of the best deterrents for potential intruders.

B. They are flexible and can be positioned randomly.

C. They provide judgment and understanding of different situations.

D. They are cheaper than most automated detection systems.

372. Smoke detector placement is important for ensuring that all types of fires in different parts of the building can be quickly identified. Which location is not necessarily a good place for a smoke detector?

A. Raised flooring

B. Dropped ceiling

C. Exterior rear doorway

D. Air ducts or vents

373. Which one of the following security controls doesn’t belong with the other three?

A. Host-based intrusion detection system

B. Photoelectric system

C. Acoustical-seismic detection system

D. Passive infrared system

374. Which one of the following characteristics is not true of an ideal data-processing room?

A. Humidity level of 50 percent

B. Carpeting

C. Room temperature around 72 degrees Fahrenheit

D. Independent HVAC and ventilation systems

375. A security system that uses changes in heat waves in a particular area to identify possible intruders is called a _____.

A. Proximity detection system

B. Passive infrared system

C. Acoustical-seismic detection system

D. Photometric

376. The Montreal Protocol has declared that Halon should no longer be used because of its negative effects on the ozone and human beings. Which is not a replacement for Halon?

A. NAF-S-III

B. DD3-410

C. Water

D. CEA-410

377. Which of the following fire-suppressing agents should not be used in an operations center containing employees?

A. Gas

B. Soda acid

C. Water

D. CO2

378. Piggybacking can be best prevented by which physical control?

A. Turnstile

B. Mantrap

C. Badge reader

D. Fail-safe door

379. Different water suppression systems exist for different purposes and regions. Which sprinkler system’s pipes are filled with water all the time?

A. Wet pipe

B. Preaction

C. System pipe

D. Dry pipe

380. The current that moves through power lines and cables can be negatively affected by its environment. Line noise created by lightning or electrical motors can cause what?

A. Electromagnetic interference (EMI)

B. Radio modulation interference (RMI)

C. Radio frequency interference (RFI)

D. Energy fluctuation interference (EFI)

381. A secured computing room should have all of the following characteristics except _____.

A. No more than two doorways

B. Walls that extend from the true flooring to the true ceiling

C. Many comfortable sitting areas around workstations

D. Strict physical access controls

382. A control center that operates mission-critical systems would most likely have which of the following power arrangements?

A. Primary power source, UPS, and generator

B. Primary power source because most data systems have their own power sources

C. Primary power source and UPS

D. Stand-alone generator

383. Which of the following is a reason for a company to use physical locks to secure devices?

A. Locks are the most secure physical control.

B. Locks are convenient for employees.

C. Locks are inexpensive.

D. Locks are difficult to break.

384. Proper lighting in critical areas is important to deterring potential intruders and protecting employees and customers. Lighting is an example of what type of control?

A. Technical

B. Physical

C. Environmental

D. Access

385. Which is not a characteristic or name of a system-sensing proximity card reader?

A. Transponder

B. User activated

C. Passive device

D. Field powered

386. Cipher locks have four general features that can be configured. Of the following answers, which is not one of the features?

A. Hostage alarm

B. Key override

C. Voice activated

D. Master keying

387. Walls built to create sensitive rooms should have which of the following characteristics?

A. Extend from the real floor to the real ceiling

B. Have a one-hour fire rating

C. Be monitored via closed-circuit TV

D. Be constructed of steel

388. Some mantraps today actually use a biometric system to weigh the individuals that enter it. What is the purpose of this?

A. To ensure that more than one person did not enter the mantrap. This is done to prevent piggybacking and tailgating.

B. To ensure that more than one person entered the mantrap. This is done to prevent piggybacking and tailgating.

C. An enrollment period weighs different people and builds a biometric reference file. When the person attempts to authenticate, the system compares the current weight with what is held in the reference file.

D. An enrollment period weighs different people and builds a biometric reference file. When the person attempts to authenticate, the system compares the current weight with another individual’s reference file.

389. Denise is a newly hired executive brought on specifically to implement improved physical security controls. In her first staff meeting with her team, she asks the group to outline how data flow through the company. The critical assets that are necessary to keep data flowing need to be identified along with existing redundant paths. What is the name of the process Denise has just delegated?

A. Critical path analysis

B. Risk reduction

C. Planning horizon

D. Policy planning

390. What does a company need to investigate to ensure that the availability of production systems are not negatively affected for a long period of time if a new system goes down?

A. NDA and MTTR

B. SLAs and MTTR

C. MTBF and NDA

D. MTTR and TSCEC

391. Companies that offer mission-critical services to their customers have to make contingencies for potential power failures. An uninterruptible power supply (UPS) is a common alternative that companies select. In situations where even one second of power interruption is unacceptable,

the UPS can take over the load as soon as power is lost. These UPS types have primary power continually running through them and are activated immediately if the primary source fails. What are these systems called?

A. Standby UPS

B. Online UPS

C. Ghost UPS

D. Generator

392. A company with highly combustible materials is trying to determine which sprinkler system type to purchase. They are not concerned with false alarms, but instead are insistent that the system be effective at extinguishing large and rapidly growing fires extremely fast. Which would be the best sprinkler system for this company?

A. Wet pipe

B. Deluge

C. Dry pipe

D. Preaction

393. Jonathan’s workstation is overloaded with electrical connections into a small number of outlets. He is daisy-chaining power strips in order to service all of his equipment. One problem that always remains is excessive line noise and power fluctuation. He needs to address the problem but does not have a great deal of money budgeted for it. Which of the following solutions would be least favorable for this specific issue?

A. Surge protector

B. Line conditioners

C. Redistribute cords to other outlets

D. UPS

394. When discussing the risks associated with fire, it’s important to consider fire’s “four legs.” The four legs are heat, oxygen, fuel, and chemical reaction. Which of the following statements is true about fire suppression?

A. Heat should be reduced, fuel and oxygen should be removed, and chemical reactions should be disrupted.

B. Heat and oxygen should be reduced; fuel should be added; and chemical reactions should be disrupted.

C. Heat should be reduced; and fuel, oxygen, and chemical reactions should be increased.

D. Heat, oxygen, fuel, and chemical reactions should be combined.

395. A storage company has just acquired operational space in a high-rise building located downtown. They will have access to the bottom two floors of the building and intend to use the space for individual customer storage lockers. Customers range from residents with furniture and boxes to construction companies with heavy equipment. Of the following considerations, which would be the lowest priority?

A. Load bearing of walls, ceilings, and floors

B. Combustibility of the materials in the facility

C. Intrusion detection systems

D. The existence of ultraviolet-protected windows

396. Mike and Lisa are business managers who must negotiate a renewal maintenance contract with a vendor. In order to optimize redundancy while reducing cost, they had to evaluate the

situation based upon MTBF and MTTR values. MTBF is the mean time between failures. What does MTTR mean?

A. Maximum time to respond

B. Maximum time to recover

C. Mean time to repair

D. Minimum time to repair

397. There are many environmental issues to consider when securing a facility and its assets. One issue is maintaining proper temperatures to avoid damage to devices. What is the threshold temperature at which computer devices will become damaged?

A. 98 degrees Fahrenheit

B. 110 degrees Fahrenheit

C. 175 degrees Fahrenheit

D. 350 degrees Fahrenheit

398. Craig is handling all the details of a move into a new building his company has just purchased. While walking with the inspector on the facility tour, the inspector comments, "You need positive drains throughout this place." What does the inspector mean by this?

A. There always needs to be more drain outlet points than incoming source points.

B. Each floor must have a positive number of drains.

C. Drainage systems must be installed at positive angles.

D. Contents should flow out of buildings, not into them.

399. Ventilation ducts and utility tunnels can also be used by intruders and thus must be properly protected with _____ and _____ mechanisms.

A. Sensors, access control

B. IDS, CCTV

C. IPS, CCTV

D. Monitors, fire suppression

400. There are common cloud computing service models. _____ usually requires companies to deploy their own operating systems, applications, and software onto the provided infrastructure. _____ is the software environment that runs on top of the infrastructure. In the _____ model the provider commonly gives the customers network-based access to a single copy of an application.

A. Platform as a Service, Infrastructure as a Service, Software as a Service

B. Platform as a Service, Service as a Platform, Application as a Service

C. Infrastructure as a Service, Application as a Service, Software as a Service

D. Infrastructure as a Service, Platform as a Service, Software as a Service

401. A concealment cipher is a message within a message. It is a way to hide a secret message within something familiar. What is another name for a concealment cipher?

A. Null cipher

B. Running key cipher

C. Asymmetric cipher

D. Session cipher

402. Which of the following is not a required component of steganography?

A. Carrier file

B. Payload

C. Stego-medium

D. Graphic file

403. Lee is told to modify the least significant bit (LSB) in the graphic file he is inserting a secret message within. What is the LSB?

A. The leftmost bit position

B. The first bit in a byte

C. The leftmost bit in a 24-bit graphic

D. The rightmost bit position

404. What is the role of the least significant bit (LSB) in steganography?

A. It allows for the injection of bytes into a message.

B. It allows for the injection of bytes into an encryption process.

C. It does not cause noticeable distortion.

D. It increases file size after byte injection.

405. How are steganography and digital watermarking different?

A. Steganography protects copyright material.

B. Digital watermarking is reversible.

C. Steganography is a component of Digital Rights Management.

D. Steganography is used for secret messages.

406. What are Key Derivation Functions (KDFs)?

A. Session keys created from each other

B. Algorithms that generate keys from a master key

C. Master keys that are replaced regularly during a short period

D. Master keys that are generated from a session key

407. Company X is implementing several encryption schemes in order to support their new security policies. Rich, a security administrator at Company X, is responsible for key management. Which of the following is the most important item that Rich needs to consider when implementing key management?

A. Key life cycle

B. Public key

C. Private key

D. PKI

408. The process of changing plaintext to ciphertext is known as?

A. Hashing

B. Encrypting

C. Steganography

D. Decrypting

409. Rich, a security administrator at Company X, has decided to change jobs. Rich creates his letter of resignation in an e-mail, creates a hash of that e-mail, and attaches it to the e-mail before sending it. What is Rich ensuring?

A. Availability

B. Integrity

C. Confidentiality

D. Nonrepudiation

410. What is a substitution cipher?

A. A cipher that rearranges all the plaintext characters

B. A cipher that hides all the characters in a picture

C. A cipher that replaces characters with different characters or symbols

D. A cipher that uses a one-way operation to create unreadable text

411. What is a transposition cipher?

A. A cipher that hides all the characters in a picture

B. A cipher that rearranges all the plaintext characters

C. A cipher that replaces characters with different characters or symbols

D. A cipher that uses a one-way operation to create unreadable text

412. Hashing provides which of the following?

A. Confidentiality

B. Integrity

C. Availability

D. All of the other choices

413. Secure Sockets Layer (SSL) is the most common protocol for secure Internet transactions. Which of the following is not a characteristic of SSL?

A. Originally developed by Netscape

B. Protects transmissions at the data link layer

C. Provides encryption, message integrity, and server authentication

D. Uses public key encryption

414. Which is not true of Advanced Encryption Standard (AES)?

A. It was developed to replace DES.

B. It uses key sizes of 64, 128, and 192.

C. It is a block symmetric cipher.

D. It uses the Rijndael algorithm.

415. Which of the following is the 128-bit algorithm that was accepted for the DES?

A. SkipJack

B. Data Encryption Algorithm

C. Lucifer

D. RSA

416. An attacker who has access to a large section of ciphertext, determines which part of it is to be decrypted, and ultimately has access to the resulting plaintext has performed what type of attack?

A. Chosen-ciphertext

B. Known-plaintext

C. Chosen-plaintext

D. Ciphertext-only

417. In 1976, Diffie and Hellman introduced what cryptography technology?

A. Electronic key distribution

B. Digital signatures

C. Symmetric key encryption

D. 256-bit key encryption capabilities

418. Which key knows the trapdoor, allowing for decryption to take place?

A. Session key

B. Public key

C. Private key

D. Asymmetric key

419. What is a chosen-plaintext attack?

A. An attacker chooses the ciphertext for encryption and has access to the decrypted plaintext.

B. An attacker has both plaintext and ciphertext of multiple messages.

C. An attacker has plaintext and can choose which part of the plaintext is encrypted and then has access to the generated ciphertext.

D. An attacker has ciphertext from several messages.

420. The two main types of symmetric ciphers are block and stream. Block ciphers perform substitution by using which of the following?

A. Keystream generators

B. S-boxes

C. XOR functionality

D. Initialization vectors

421. Which of the following is the science of studying and breaking encryption algorithms and cryptosystems?

A. Cryptography

B. Encryption

C. Monoalphabetic substitution

D. Cryptanalysis

422. An algorithm that produces the same hash value for two different messages causes what?

A. Pad

B. Collision

C. One-way function

D. MAC

423. Which of the following is not true about asymmetric cryptography systems?

A. They are faster than symmetric cryptography.

B. They use a variable-length key.

C. They provide authentication and nonrepudiation.

D. One side uses a public key and the other uses a private key.

424. There are several ways to gain insight on how a cryptosystem works, with the goal of reverse-engineering the process. A term that describes when two pieces of data result in the same value is _____.

A. Polymorphism

B. Collusion

C. Escrow

D. Collision

425. Some cryptographic components can provide nonrepudiation. What does nonrepudiation do?

A. Provides system or data origin authentication of a message

B. Ensures that someone cannot deny a previous action

C. Ensures the integrity of the message and provides a way of key exchange

D. Is incorporated in most key recovery procedures to enforce dual control

426. Which of the following is not a component of a public key infrastructure (PKI)?

A. CRL

B. RA

C. PGP

D. CA

427. If Marge uses her private key to create a digital signature on a message she is sending to George, but she does not show or share her private key with George, what is it an example of?

A. Key clustering

B. Avoiding a birthday attack

C. Providing data confidentiality

D. Zero-knowledge proof

428. What function does the symmetric key in hybrid cryptography provide?

A. Key storage

B. Key generation

C. Key distribution

D. Message encryption

429. A function that takes a variable-length string and creates a fixed-length value is called_____.

A. Key

B. Digital signature

C. One-way hash

D. Encryption

430. Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Security

B. Speed

C. Scalability

D. Key distribution

431. Rivest, Shamir, and Adleman developed what algorithm?

A. Rijndael

B. RSA

C. DES

D. IDEA

432. What technology is used when all the data in a communication path are encrypted, including the header, trailer, and routing information?

A. Data hiding

B. Link encryption

C. End-to-end encryption

D. S/MIME

433. Which one of the following items falls under the responsibility of key management?

A. Access control and user identification

B. Key length and algorithm correctness

C. Access control and encryption integrity

D. Key generation and destruction

434. What is the standard used for PKI certificates?

A. X.400

B. X.500

C. X.509

D. LDAP

435. Which of the following is the most important type of protection when dealing with passwords?

A. Encrypting them where they are stored centrally

B. Using nondictionary words

C. Ensuring they are at least six characters long

D. Sending in cleartext

436. How are symmetric and asymmetric algorithms and keys used together?

A. An asymmetric key encrypts the symmetric key.

B. An asymmetric key encrypts bulk data, and symmetric keys encrypt a small amount of data.

C. An asymmetric key is used and then encrypted with a symmetric key.

D. A symmetric key encrypts the data, and then the asymmetric key encrypts both of them.

437. How is a key used in encryption?

A. A key is used to determine which algorithm should be used.

B. A key is used to determine the final length of the information.

C. A key is used to provide randomness.

D. A key is used to unlock S-boxes.

438. What needs to be considered with key management?

A. How to securely store the keys

B. How to securely transport the keys

C. How to securely destroy the keys

D. All of the other choices

439. Which of the following is a symmetric cipher?

A. AES

B. DSA

C. Diffie-Hellman

D. All of the other choices

440. Windows Vista and Server 2008 allow for whole-disk encryption through BitLocker drive encryption. Which of the following is needed in order to run BitLocker drive encryption?

A. TPM

B. HTTPS

C. PKI

D. IPSec

441. What is the name of the principle that argues the reverse of “security by obscurity”?

A. Kipling’s principle

B. Kerckhoffs’ principle

C. Principle of security

D. Shannon’s principle

442. Sally has been concerned about cryptographic keys and digital certificates being held and maintained on workstations in semiprotected software solutions. Which of the following would

be the best solution Sally should look at implementing?

A. Hardware cryptographic render

B. Trusted platform module

C. Key store

D. PKI registrar database

443. A trusted platform module (TPM) has two types of internal memory used for specific purposes. Which of the following best describes how these two memory types are used?

A. Persistent memory is static in nature and contains the endorsement key and the storage root key. Versatile memory is dynamic and contains the attestation identity key, platform configuration register hashes, and storage keys.

B. Persistent memory is versatile in nature and contains the storage keys and the storage root key. Versatile memory is static and contains the attestation identity key, platform configuration register hashes, and endorsement key.

C. Persistent memory is versatile in nature and contains the attestation identity key and the storage root key. Versatile memory is static and contains the platform configuration register hashes and endorsement key.

D. Persistent memory is static in nature and contains the platform configuration register hashes and the storage root key. Versatile memory is dynamic and contains the attestation identity key, endorsement key, and storage keys.

444. What cryptographic attack type carries out a mathematical analysis by trying to break a math problem from the beginning and the end of the mathematical formula?

A. Known plaintext

B. Adaptive ciphertext

C. Known ciphertext

D. Meet-in-the-middle

第三章答案

1、 C .The design process usually follows the process of developing the system architecture. The design process is very detailed, and produces a solid design that can be used for development or acquisition purposes.

2、 A .ISO/IEC 15408 is the international standard that is used as the basis for the evaluation of security properties of products under the CC framework

3、 A .The reason that a system goes through the evaluation process for its TCB is to identify the architecture, security services, and assurance mechanisms that make up the TCB, and how they protect the system.

4、 C .Security considerations should be included in all phases of the system security engineering lifecycle.

5、 C .Buffer overflows are application security weaknesses, not commonly database security weaknesses.

6、 D .Security controls are assigned to an evaluated system based upon the TCB, and the protection mechanisms it offers. Controls often are developed to supplement protections offered by the TCB, and may depend upon the environment it is deployed in and not part of its design.

7、 B .Smart grids are computer systems and networks that are embedded into grids of large pieces of infrastructure, such as power production, communications networks, and so forth.

8、 B .Parallelism can take place at one of three levels: bit, instruction, or task. All of these levels of information are fed into the computer, and are then processed.

9、 D .Workstation compromise is not an issue with mobile devices in the enterprise. Mobile devices are subject to loss and theft, download of malicious software, Internet access through communications lines that are not controlled by the company, and lack of encryption on the device, among other issues.

10、 .In client-side validation, input validation is done on the client before the input is even sent back to the server to process.

11、 C .Digital rights management refers to any of the access control technologies that are commonly used to protect copyrighted materials, such as digital media and software.

12、 A .The entire purpose of having Internet of Things (IoT) embedded devices is to be able to connect to and control these devices over the Internet or from remote networks.

13、 D .As they are unlikely to house critical digital assets and information systems, employee break rooms probably do not need to be protected at the same level as other areas where information systems are located.

14、 A .Julius Caesar created one of the earliest forms of encryption. The Caesar Cipher shifts letters of the alphabet three spaces forward, thus disguising the original message into an unrecognizable text string. Although this type of encryption technique is simplistic compared to today's cryptography, during Caesar's time many people could not read in the first place.

ROT-13 is a cipher that shifts letters of the alphabet 13 places forward.

Transposition ciphers scramble text and a running key cipher uses clues in the outside world.

15、 B .Pretty Good Privacy (PGP) is a security program focused on protecting e-mail messages. It uses public key encryption by implementing a "web of trust" among users. In contrast to certificate authorities, which control the levels of trust, PGP allows users to sign each others' public keys, thus developing a trusted network.

PKI uses a hierarchical trust structure instead of a horizontal structure.

16、 B .Secure Sockets Layer (SSL) provides data encryption over the Internet. Although it provides encryption while the message is being sent, it does not secure the data once it is received and decrypted. Also it does not provide a true VPN service by protecting header information.

SSL uses public key encryption and was developed originally by Netscape. Along with encryption and message integrity, SSL also ensures server authentication and optional client authentication.

17、 D .Data Encryption Standard (DES) uses a 64-bit key. The true key consists of 56 bits and parity accounts for 8 bits. DES is a block symmetric algorithm that has four distinct operating modes: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB).

DES is really a standard and not an algorithm, although we commonly refer to the algorithm as DES. The algorithm used in DES is DEA, thus has the same characteristics as DES.

18、 A .Triple-DES (3DES) improves upon both DES and Double-DES. DES uses a true key size of 56 bit, and Double-DES uses a 112-bit key. Both have the same work factor necessity to break them.

3DES, on the other hand, uses 48 rounds of computation and is 2 to the 56th power stronger than DES, meaning that three rounds of encryption are used. It is highly resistant to attacks but requires significantly more overhead than its predecessors.

Some 3DES use two keys instead of three, but this is the best answer of the four.

19、 B .AES was developed to improve upon DES's security and flexibility. It uses 128, 192, and 256-bit keys. Rijndael, a block symmetric cipher created by Vincent Rijmen and Joan Daemen, was selected as the new AES algorithm.

20、 B .Elliptic curve cryptosystems (ECC) is the most efficient of the asymmetric algorithms. It uses elliptic curve properties to combine group and rule information, requiring fewer resources than the other methods.

21、 B .The Clipper Chip was a short-lived encryption device initiated by the US government in the early 1990s. The chip was a hardware encryption device that was to be implemented in all communication-related devices, however it had too many weaknesses and was ultimately abandoned. Some of the issues included an 80-bit key that was weak, the 16-bit checksum could be broken easily, and the SkipJack algorithm was kept private and was not a trusted encryption technology in the industry.

22、 C .In 1974 IBM created Lucifer, which would eventually become the Data Encryption

Standard (DES). DES absorbed significant controversy over speculation that the NSA weakened the algorithm in order to have more control over breaking the code. However, it remained the primary encryption standard for many years until it was cracked in the late 1990s. This led to the creation of the Advanced Encryption Standard (AES).

Lucifer was accepted and the key size was reduced from 128 to 64 and renamed the Data Encryption Algorithm (DEA).

23、 A .RSA is the de facto standard and most widely used asymmetric algorithm today. The strength of RSA comes from factoring large numbers into their original prime numbers. It performs encryption, digital signatures, and key exchange. It works well in web browsers with the Secure Sockets Layer (SSL) protocol.

RSA is named after its MIT inventors— Ron Rivest, Adi Shamir, and Leonard Adelman.

The Advanced Encryption Standard (AES) algorithm uses Rijndael, a symmetric encryption system.

24、 C .The Advanced Encryption Standard (AES) uses a symmetric block algorithm. El Gamal is a public key (asymmetric) encryption system, and thus was not considered for the advanced standard. El Gamal is similar to RSA, however it utilizes discrete logarithms in a finite field.

25、 A .Chosen-ciphertext attacks have the highest probability of the encryption being cracked. In this type of attack, the intruder must capture a large portion of the ciphertext and then must be able to choose which parts of it are decrypted. That section of text is transformed into plaintext. The translation is then analyzed in an attempt to identify the key that was used in the encryption process.

26、 A .The Diffie-Hellman key exchange was created as a way of exchanging public keys and generating a session key without needing to set up a prior relationship. This technology does not handle any form of data encryption, rather it is simply a method of exchanging keys.

Diffie and Hellman created the first asymmetric algorithm.

27、 D .A session key improves security because it is used only once per transmission. If a session key was not used, then users would use the same symmetric key for every message sent. Over time, attackers would be more likely to uncover this key. However, new session keys are generated each time a transmission is initiated, which provides a higher level of protection.

28、 C .A trapdoor one-way function applies the concept of factoring numbers into their original prime numbers. Public keys encrypt a message with a built-in, one-way function. This function is referred to as one-way because it is relatively simple to encrypt, but much more difficult to decrypt without knowing the correct trapdoor. A private key, however, knows the code of the trapdoor, and is able decrypt the message.

29、 B .A one-way hash is a function that changes a variable length text string into a fixed length value, or hash value. This process creates a fingerprint of the message, which in turn is used to ensure the integrity of the message.

One-way hashing does not use keys. If the message being sent needs confidentiality, a key would be needed to encrypt the message itself.

If a symmetric key was not going to be used for encryption, but instead for data origin authentication, this is referred to as a MAC.

This is also called a message digest.

30、 C .Chosen-plaintext attackers have access to plaintext and the ciphertext that is generated. The attacker chooses which piece of plaintext is encrypted. The goal is to use the resulting ciphertext to uncover the key that was used in the encryption process.

31、 B .Substitution boxes, or S-boxes, are used within block ciphers. They use lookup tables to determine how a block is encrypted or decrypted. The key is used to decide which S-box to utilize with each block.

32、 B .In a sense, Cipher Block Chaining (CBC), chains blocks of messages together so that the encryption process will look different each time. Without CBC, if a message were encrypted and decrypted over and over, patterns would begin to surface. However, CBC attaches previous blocks onto the current block, which means that the result will always be different.

This is a way of adding more randomness to the process of encryption.

33、 D .Cryptanalysis is studied by different types of audiences. The science of breaking encryption algorithms and cryptosystems is an area of interest in both academic and commercial settings (ethical) and by curious or devious hackers (unethical).

34、 C .International Data Encryption Algorithm (IDEA) is a block cipher that uses a 128-bit key. It uses a 64-bit block that is broken down into 16 subblocks and then sent through eight rounds of permutations.

IDEA was actually thought to be the next DES algorithm but because it was patented and required licensing fees, it was not adopted.

35、 B .A collision occurs when two separate messages have the same hash value. This creates an opportunity for a potential hacker. Taking advantage of a collision is done through a "birthday attack."

36、 B .The ultimate goal of cryptography is to hide information from unauthorized individuals.

Because hacking will always exist, it is unlikely that a full-proof encryption scheme will ever truly be developed. However, the realistic goal of cryptography is to make it so difficult and time consuming that a potential hacker will give up trying or not attempt it in the first place.

37、 D .Secure Hash Algorithm (SHA) is a hashing algorithm that improves upon MD5 by producing a larger hash value of 160 bits. SHA does additional math functions in order to get the larger message digest. This makes more powerful against birthday attacks.

38、 A .Asymmetric cryptography, also referred to as public key cryptography, uses both public and private keys. It is used for key encryption and key distribution. Variable-length keys are used and algorithms are much more complex than symmetric cryptography. However, due to the complexity, asymmetric algorithms are slower than symmetric key encryption. While symmetric encryption provides only confidentiality and system authentication, asymmetric cryptography has added capabilities such as user authentication and nonrepudiation.

39、 A .Perimeter Intrusion Detection and Assessment Systems (PIDAS) consist of boundary fencing with motion detectors. This mechanism is good for facilities that require a higher level of protection. When using PIDAS, if an intruder comes close to the fence or even begins to climb it, alarms would alert security personnel.

40、C .Mantraps are used to control individuals attempting to access facilities or sensitive rooms. Typically, a person enters through a door into a small room that has a second door. Once inside this "mantrap," both doors are locked. The individual's identity must then be authenticated before the second door unlocks and she is allowed inside. If she is unable to prove her identification, she must wait in this area to be questioned by security.

Turnstiles are the revolving doors so often seen at corporate high-rise buildings or in hotels. These can be used as physical security mechanisms as well.

41、 D .The use of security guards comes with a host of advantages, however their expense is not one of them. Salaries, benefits, vacations, insurance, and background checks are all factors that must be considered when employing reliable, productive security guards.

42、 C .Fires are classified according to the kind of material burning. Below are definitions for all four classes:

Class A — Common combustibles such as wood or paper

Class B — Liquid such as fuels and oils

Class C — Electrical such as wiring and equipment

Class D — Combustible metals such as magnesium or sodium

43、 A .One of the greatest advantages of security guards, and what separates them from automated security systems, is their ability to use "discriminating judgment." Over time, unusual or suspicious activities are bound to occur and the ability of a security guard to react to the situation is a valuable tool for a company to have.

44、 C .Smoke detectors should be placed strategically throughout a facility. Raised floors and dropped ceilings are good places for detectors because these areas are common places for electrical wiring. Air ducts and vents are good places because in the event of a fire, air travels fluidly through these devices.

A detector would not be necessary around doorways, rather, inside the building.

45、 B .These types of gases interfere with the chemical reactions in a fire and act as effective suppressing agents for class B and C fires. Halon is a gas that has been used in fire extinguishers for years and still exists in some older units. However, the EPA recently found that Halon is harmful to the ozone and potentially harmful to humans. Several replacement agents, including FM-200, are just as effective on fires as Halon and are being used in new units.

46、 A .Host-based intrusion detection system doesn't belong with this physical intrusion detection group. This control pertains to an individual computer and not to detecting unauthorized people who may try to enter a facility.

47、 B .An ideal computing environment, or data center, would use anti-static flooring, not carpeting. If carpeting is absolutely necessary, then it should be specialized anti-static carpeting.

Other ideal characteristics are:

- Proper humidity and temperature levels
- Raised flooring or dropped ceilings for wiring
- Independent HVAC systems

48、 B .A passive infrared system measures changes in heat waves for a specified area by using a series of beams. If the temperature in a specific area where one of the beams terminates suddenly increases, it is possible that a person has entered the area.

49、 B .Because Halon has been deemed dangerous to both humans and the environment, an acceptable replacement list was created by the EPA:

FM-200
NAF-S-III
CEA-410
FE-13
Water
Inergen

Argon
Argonite

50、 C .A company must decide how to handle physical access control in the event of a power failure. In fail-safe mode, doorways are automatically unlocked. This is usually dictated by fire codes to ensure that people do not get stuck inside of a burning building.

Fail-secure means that the door will default to lock.

51、 D .CO2 is a dangerous gas that removes or displaces oxygen from the air. It should not be used in areas where humans are present. Instead, a Halon substitute, water or soda acid, should be used.

CO2 is often used in unattended facilities or when absolutely necessary, and it is usually used with a delay mechanism that gives individuals a warning before it is dispersed.

52、 B .A mantrap offers the best control for piggybacking because the intruder has to be identified and authenticated before entering a building or area. Piggybacking is difficult to accomplish and seldom attempted in this scenario.

Although a badge reader is an effective method of physical access control, it is common for an intruder to lurk in the shadows of an authorized employee and then sneak in through a closing door after the employee has entered the building.

53、 A .The wet pipe system, as its name implies, has water in the pipes at all times. When a fire detector initiates the system, water is released through the sprinkler heads.

A dry pipe holds the water in a reserve tank, not in the pipes. When the temperature threshold is achieved, the water releases, fills the pipes, and then sprays from the sprinkler heads.

A preaction system can be a wet pipe or dry pipe system.

54、 A .Electromagnetic interference (EMI) is a type of power line interference. Along with lightning and electrical motors, EMI is also caused by the difference between positive, negative, and neutral wires.

55、C .Secured computer rooms should have no more than two doorways and should be isolated from public areas, such as restrooms and main hallways. These parameters reduce traffic levels and limit the potential for unauthorized access. In addition, a highly secured computer room should not have comfortable areas for individuals to gather in or loiter.

56、 A .Control centers typically cannot afford to have any downtime, not even for a few seconds. As a result, the best power scheme would be a primary power source (a feeder coming in from a substation), uninterruptible power supply (UPS), and a generator. The UPS can be a type of

short-term alternate power supply unit that detects failures in the primary power supply. In the event of a failure, the UPS unit turns on immediately. The limitation of UPS units are their longevity— they are temporary power supplies. For a mission critical control center, contingencies should be planned in the event of a long-term outage. A generator can provide this alternative or a second feeder from a different power substation.

57、 B .Cipher locks provide more flexibility and functionality than other types of locks. Users enter an assigned combination into the keypad in order to gain admittance. Flexibility comes from the fact that the combinations can be changed as often as needed and different functionality can be added. Cipher locks are usually more expensive than standard locks and keys.

58、 C .Locks are used for a variety of purposes, including securing laptops, storage rooms, and file cabinets. Their number one advantage is that they are very inexpensive and simple to implement. However, physical locks also have many drawbacks. They can be easily broken or picked, keys are easily lost, and combinations easily forgotten.

Locks are seen only as delaying devices because a determined intruders can get through them.

59、 B .Just as perimeter fences, intrusion detection systems, and guard dogs are important to protecting a facility from intruders—lighting plays an important role in physical security as well. Search lights, flood lights, street lights, and spot lights are all types of lighting that a company may choose to install.

60、 B .Wireless proximity readers are different from user activated systems. With a user activated system the user must insert a card into the reader and then a set of credentials must be given to the system to properly authenticate the user. In wireless proximity systems, such as system sensing readers, the readers "sense" the presence of an object and transmit signals to a proximity card to obtain the access control credentials held on the card.

61、 A .Optical detectors send out a beam of light to a receiver within the detector itself. If that beam is obstructed by anything, the detector assumes it is smoke and an alarm will sound, signaling that a fire could have started.

62、 B .A link must melt before the water will pass through the sprinkler heads which creates the delay in water release. This type of suppression system is best in data processing environments because it allows time to deactivate the system if there is a false alarm.

63、 C .Cipher locks are programmable keypad locking devices that have four different feature sets:

Door delay — If a door is held open for a certain amount of time, an alarm will sound.

Key override — An easy-to-remember emergency code can be programmed into the keypad.

Master keying — Allows authorized individuals to change key codes.

Hostage alarms — A specialty combination for those in duress to use.

64、 D .The Trusted Computer System Evaluation Criteria (TCSEC) was developed by the Department of Defense to evaluate their own computer systems.

The Orange Book evaluates security features within operating systems, devices, and applications and uses TCSEC's assurance levels as its measurements.

65、 D .The main modes a processor and operating system works in are user mode and privileged mode. Privileged mode is also called supervisor or supervisory mode. If a process of lower privilege makes a request, the request will be fulfilled in user mode. If a process has the privilege level to carry out something critical, like communicating directly with hardware, then the processor and operating system will carry out its request in privileged mode.

66、 B .The way operating systems handle the input and output of system resources is critical. When resources are not released properly, it can lead to a "deadlock" situation. This means that there are not enough resources for other programs to execute because too many are tied up with already-running applications.

A true deadlock situation is when process 1 has committed resource A and requires resource B to finish its task. But process 2 has committed resource B and requires resource A. Neither process can finish its work until the other releases the necessary resource. So they are both suspended or "hung."

67、 A .Security models are used to help implement security policies. While policies state specific objectives that must be accomplished, the security model will detail how to achieve those particular objectives. Basically, models explain how a system should control subject and object relationships and interactivity.

68、 B .Computers have many capabilities. Some are capable of multithreading, multiprocessing, and multitasking. The definition of these capabilities follow:

Multithreading — Processing more than one request or thread at one time

Multitasking — Processing more than one task, or process, at one time

Multiprocessing — Has multiple CPUs and can process separate instructions in parallel

69、 C .The Trusted Computer System Evaluation Criteria (TCSEC) has four classification rankings:

A = Verified protection
B = Mandatory protection

C= Discretionary protection
D= Minimal security

Each class has subrankings that provide more detail on the security criteria the product was evaluated against.

70、 B .After successful evaluation, products are published in the "List of evaluated products." Similar to Consumer Reports, the list is a publication that consumers can use to gain information about products, their rankings, and their features. You can find the list at the following URL: www.commoncriteriaportal.org/public/consumer/index.php?menu=4

71、 C .The major difference between Class A-ranked products and Class B-ranked products is the formality of design, development, documentation, testing, and implementation. Most of the security features are similar.

If a system is going to receive an A assurance rating, the evaluation team will go through every piece of that system's lifecycle in a granular and detailed manner.

72、 A .Covert channels can be used because the operating system is not anticipating this type of activity and thus does not protect against it. The use of covert channels violates the system's security policy. Systems with many covert channels typically have lower assurance ratings than systems with few covert channels.

A covert channel is using resources for communication purposes in a way that they were not designed for. An overt channel is using resources that were developed specifically for communication purposes.

73、 C .It is common for software developers to create "backdoors" into their applications. This is done during the development stage to give them quick access into the program to make changes or run tests. It is important that these hidden access points are removed before software is implemented.

Backdoors that are implemented within programming code for this type of access is most accurately referred to as maintenance hooks.

74、 D .Class B3 requires all of the listed features except the use of formal methods and procedures. Only Class A products require a system's design, development, implementation, and documentation to be formalized.

A Class A-rated product would exhibit all of the answers shown in this question.

75、 C .The Orange Book was the first publication of the TCSEC evaluation criteria, however it has been the victim of many criticisms.

Its classification scheme is built well for government and military organizations rather than the commercial industry. To be fair, it was developed for the DoD so this makes sense. We have used it to evaluate products for the commercial sector instead of developing a separate evaluation criteria.

The Common Criteria is the Orange Book's replacement and deals with military and commercial sectors more effectively.

76、 B .Virtual machines act as an operating and holding area for different programs to run in. This serves as a protection mechanism for the operating system. The operating system communicates with the virtual machine, thus it never has to interface directly with the untrusted program code.

Virtual machines can manage the program code in a controlled manner.

77、 A .A covert timing channel modulates the operating system's resources, which allows for communication between two processes. This is an example of a covert communication channel.

78、 B .The first step is evaluation. Evaluation involves reviewing the product's protection functionality and assurance ratings. The next phase is certification. Certification involves testing the newly purchased product within the company's environment. The final stage is accreditation, which is management's formal approval.

79、 C .The goal of the Brewer-Nash model is to protect against conflicts of interest by tracking previous access requests before future access attempts are allowed. If a user accesses data set A, then data set B is now unavailable to her.

80、 A .The Clark-Wilson model is a full-scale integrity model, however it does not address confidentiality. This is the main reason it is more suited for the commercial industry than the Bell-LaPadula model, which is a confidentiality model.

The Clark-Wilson model enforces the following integrity goals:

1. Prevent unauthorized users from changing data

2. Internal and external consistency

3. Prevent authorized users from changing data improperly

81、 A .Secondary storage can be a computer's hard drive, floppy disks, or CD-ROM. Virtual storage is when a computer extends its memory by using these types of secondary storages devices, specifically the hard drive.

Virtual storage is a way for the operating system to trick itself into thinking it has more memory

than it does. A system with 128-bit RAM chip could actually have up to 2GB or 4GB of memory because of these techniques.

82、 B .Firmware is loaded onto read-only memory (ROM) chips, a nonvolatile storage area. Nonvolatile means that when the computer is turned off, the data is not lost.

Erasable/programmable ROM is a storage place, not the software that is stored.

83、 B .When the main memory of a computer is full, it uses secondary storage placeholders, called swap spaces. When data is passed to this area, it is called "swapping." This combination of main memory and secondary storage is called virtual memory.

84、 B .The Bell-LaPadula was the first mathematical access control state machine model used to control access to data that held different classification levels. Since it uses data classification levels, this model is well-suited for government and military organizations.

The model also uses the concepts of the information flow model, which dictates how data flows based on set security policies.

85、 C .Multilevel security mode means that an operating system can make access decisions based on data classification, user clearance, and need to know.

The system can house and maintain different classification levels (e.g., top secret, secret, confidential, public) and understand different clearance levels.

86、 A .A domain is the collection of resources that are available to a subject, whether it is a user, network device, or process.

Within an operating system it is referred to as a protection, security, or execution domain because the process requires these resources to carry out its tasks. Its resources need to be properly protected from other processes.

87、 C .Processors need instructions in 1s and 0s, or binary code. This is called "machine language." Binary code is very difficult for programmers and developers to work in, so they use assembly language or higher languages to write their source code. The source code is then compiled or interpreted into machine code for the processor to understand and work with.

88、 D .The Biba model was created after the Bell-LaPadula to address integrity issues. It is based on two properties:

- Integrity Star Property — No write up
- Simple Integrity Property — No read down

89、 B .A top-down approach to security management is the ideal method because it is typically

more successful than the bottom-up approach. A top-down approach means that management is driving a project and bottom-up means that a lower level employee is driving a project. The most important factor in security management is obtaining the support of upper management.

90、 B .An organizational security policy covers the entire program at a high level. Typically this will cover how the program is set up, goals and objectives, who is responsible for what, and how to enforce the policy.

E-mail security is an issue-specific policy.

91、 C .Guidelines are used to provide employees with recommendations on how to perform specific tasks. This is different than a standard, which is a rule that must be followed, and a baseline, which is a minimal level of security.

92、 B .A system is operating as a multistate system (also referred to as multilevel-security mode) when it permits two or more classification levels of information to be processed at the same time. This does not mean, however, all the users have clearance or formal approval to access all the information being processed by the system.

93、 C .The Clark-Wilson model is an integrity model that dictates that critical tasks should be split up between users (separation of duties) and that a subject should only be able to access and modify an object by using an application (access triple). The model also dictates that internal and external consistency should be in place.

94、 B .The trusted computing base (TCB) is a term that originated in the Orange Book. It describes the components that are used to provide protection for the system or product and what components will be evaluated under the Orange Book criteria. The TCB is made up of hardware, software, and firmware components. The reference monitor and security kernel reside in ring 0 and are components of the TCB. Applications lie within ring 3 and are not considered system-wide protection mechanisms.

95、 A .Secondary storage is considered nonvolatile storage media, which can be the computer's hard drive, floppy disks, or CD-ROM. It can supplement the system's primary memory, as in when a hard drive is used during paging data from RAM to the drive. A system's primary storage is a combination of the RAM and cache that is directly accessible to the CPU and indirectly accessible to programs.

96、 A .Security barriers and walls that surround sensitive areas should go from the true floor to the true ceiling. This means that the walls do not stop at a dropped ceiling or at the raised floor because those could be circumvented and used as entry points into the sensitive area.

97、 B .Information that offers insight into a company's organization and personnel directories should not be available to anyone outside of the company who does not require it. This kind of material can be very useful to outsiders and is often used in social engineering attacks. Only

authorized employees should be able to access it.

98、 A .DES (Data Encryption Standard) is a standard that outlines the use of Data Encryption Algorithm (DEA) for encrypting sensitive but unclassified data. Although DES is actually a standard, in the industry the term is used to describe DEA. It is a block cipher that uses 64-bit blocks, 16 rounds, and a true key size of 56 bit.

99、 D .A collision is when two items have the same value but were not supposed to. In this domain it pertains to when two different messages end up having the same message digest values. Two messages being passed through a hashing algorithm should result in different message digest values. The birthday attack takes advantage of the occurrence of these two values being the same. Hashing algorithms that have longer message digest values are less vulnerable to a birthday attack because they have more possible message digest values.

100、 A .Encrypting a file before transmission provides the most security. FTP does not provide any encryption protection and moves files in clear text, thus it is not protected. Passing a file though a hashing algorithm just produces a message digest value and does not encrypt or protect the file. This is the same for a digital signature.

101、 C .A digital signature is used to provide authenticity of the sender to the receiver. It is also used to prevent repudiation. Repudiation means that someone denies doing something that they, indeed, did carry out. A digital signature provides nonrepudiation, meaning the sender cannot deny sending a message.

102、 D .El Gamal is an asymmetric algorithm, which is also called a public key algorithm. It can be used for digital signatures, encryption, and key exchange. It is not based on the difficulty of factoring large numbers, but is based on calculating discrete logarithms in a finite field.

103、 B .Nonrepudiation means that someone cannot deny carrying out some type of activity once it has been completed. A private key is used to generate digital signatures to provide the receiver with a high level of assurance of the authenticity of the message and makes sure the sender cannot deny sending the message later. It works this way because the private key is bound to the individual's identity and it is that individual's responsibility to ensure that no one else obtains that private key.

104、 D .Cryptanalysis is a science of studying and breaking cryptosystems and their necessary pieces. It is performed in academic settings by cryptographers and by curious and motivated hackers, either to satisfy their inquisitiveness or use their findings to commit fraud and destruction. When cryptanalysis is carried out through white hat means (the good guys) the goal is to identify weaknesses that should be addressed in the algorithm and cryptosystem.

105、 C .Pretty Good Privacy (PGP) was the first widespread public key encryption program. It is a complete working system that uses cryptographic protection to protect e-mail and files. This application works on a different type of trust model than a PKI environment and uses its own

type of digital certificates. PGP can be integrated within a PKI, but is the best answer because the other three are core components of every PKI implementation.

PGP is considered a cryptosystem and PKI is an infrastructure.

106、 B .IPsec is a suite of protocols used to provide integrity, confidentiality, and system authentication (also called data origin authentication). It does not provide user authentication in that any digital certificates that are used in a PKI environment are tied to the identity of the individual systems providing IPsec functionality, not users.

IPsec can only tunnel through IP networks.

107、 D .IPsec is made up of two main protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides system authentication and integrity, but not confidentiality or availability. ESP provides system authentication, integrity, and confidentiality, but not availability. Nothing within IPsec can ensure the availability of the system it is residing on.

108、 C .A cracker is an individual who does unethical or illegal things to obtain information or assets that do not belong to him or has the goal of disrupting another's environment and productivity.

Hacker and cracker are used interchangeably at times. A cracker is not software or a tool, but a human being.

109、 A .A mantrap can be used with a biometric system to weigh people that enter the room. The goal is to ensure that two or more people are not in the room and trying to get in on just one set of credentials.

110、 B .A preaction system has a link that must be burned through before water is released. This is the mechanism that provides the delay in water release. A deluge system has wide open sprinkler heads that allow a lot of water to be released quickly. It does not have a delaying component.

111、 B .Key clustering means that one key is used to encrypt two different messages and they both end up with the same ciphertext.

112、 C .Message authentication code (MAC) uses a symmetric key and a hashing algorithm and provides system authentication and integrity. Hashing algorithms provide integrity. Digital signatures provide integrity and user authentication, or authenticity. Symmetric keys are used for confidentiality.

113、 D .Zero knowledge proof means that someone can tell you something without telling you more information than you need to know. In cryptography it means to prove that you have a specific key without sharing that key or showing it to anyone.

114、 A .Applications and programs can be written by different vendors and individuals. Because they can contain harmful code, the CPU and operating system's self-protecting rings are used as containers to hold and control them.

115、 B .If the operations of a system are negatively affected, then its availability is negatively affected. While this could also affect the system's integrity and consistency, (although not a core security principle) availability is still the best answer.

116、 D .The Basic Security Theorem is a simple security principle that states that if a system starts in a secured state, all future states remain secure, and the system shuts down securely, then the system will always be in a secure state.

117、 B .In TCSEC, products are submitted to the National Computer Security Center (NCSC) and ultimately published in the Evaluation Product List (EPL). The act of rating a product's security capabilities is called the Trusted Products Evaluation Program (TPEP).

118、 A .Open systems allow customers the flexibility of seamlessly incorporating new products into an established network. A closed system does not interact with other applications or programs as well because it is built on proprietary protocols and does not use standard interfaces.

119、 B .A system is operating in system-high security mode when all users have a security clearance or authorization to access the information but not necessarily a need to know for all the information processed on the system.

120、 A .The CPU is made up of a control unit and an arithmetic logic unit (ALU). The ALU is considered the brain because it performs the mathematical and logical functions needed to process instructions. The control unit acts like a traffic cop by controlling what instructions are processed by the ALU and when. When the instructions are waiting to be processed, pointers to their addresses in memory are held in registers for the CPU.

121、 C .The reference monitor is referred to as an abstract machine that protects a computer's resources. It enforces a simple and cardinal rule in computer security: subjects must have proper authority to access objects.

The reference monitor holds the rules that outline how subjects can access objects and the security kernel enforces these rules.

122、 A .The Biba model enforces data integrity, which makes it very suitable for commercial organizations. The no read down rule exists to ensure that data of lower integrity is not used by subjects that have higher integrity. In this example, a subject (public relations executive) accesses data at a lower integrity level (engineering staff member).

By only accessing data at an equal or higher integrity level, the executive can ensure that the information is correct and has high integrity.

This model actually controls how subjects and objects communicate within an application. This question was really just a way to conceptually walk you through the concepts of the model.

123、C .The Common Criteria was created by several organizations in different countries as a way of combining the best parts of TCSEC and ITSEC and other criteria into a more useful measure. The Common Criteria has been accepted globally.

124、 C .Magnetic tape is often used out of convenience. Backing up large chunks of data for contingency planning is a good example of a use for magnetic tape. However, it offers minimal security because if a user needs to access a file on a tape, he has access to all other information stored there, too.

125、 B .A common mistake is abandoning the certification and accreditation process after the product is accepted and implemented. The problem occurs when changes to the network or the system take place. Networks are upgraded, products reconfigured, and many other types of changes can take place in an environment. So, the product should be recertified and reaccredited if a major change takes place.

126、 A .ITSEC separates functionality and assurance ratings while TCSEC combines the two into one rating. A C1 TCSEC-rated product would have the functionality rating of F1 and an assurance rating of E1 in ITSEC.

127、 B .Data is sent from the main memory to the secondary memory (hard drive) in pages and coincidently is called "paging." When the data is returned to the main memory, the process is called "page fault."

128、 C .The Clark-Wilson model enforces data integrity by ensuring that the data is not intentionally or unintentionally modified. This is done by adding a third piece or middleman (the application) between subjects and objects.

The program controls what the subjects can and cannot do with the objects (data) held in the database. This is also referred to as access triple.

129、 B .The Red Book was designed to address network components and products. This was done as a follow-up to the Orange Book focusing on stand-alone operating systems and not networking issues.

130、 B .The trust level tells the customer how much he can expect out of the system, what level of security it will provide, and gives assurance that the system will act in a correct and predictable manner in each and every computing situation.

131、 C .A system is operating in multilevel security mode when it permits two or more classification levels of information to be processed at the same time and all the users do not have the clearance or formal approval to access all the information being processed by the system.

132、 C .In this example, lower-ranked staffers could have deduced that the contract had been renewed by paying attention to the changes in their systems. The noninterference model addresses this specifically by dictating that no action or state in higher levels can impact or be visible to lower levels.

In this example, the staff could learn something indirectly or infer something that they do not have a right to know yet.

The model mainly addresses mainframe operating systems and centralized server software, but this question walks you through the ideas of the model conceptually.

133、 A .The Harrison-Ruzzo-Ullman model outlines how access rights can be changed and how subjects and objects should be created and deleted. This newer model provides more granularity and direction for vendors on how to actually meet the goals outlined in the earlier models.

134、 C .Immediately following certification, the formal acceptance and sign-off on a product by senior management is necessary. This formally closes the process and is referred to as accreditation.

135、 B .Bell-LaPadula models have rigid security policies that are built to ensure confidentiality. The "strong tranquility" property is an inflexible mechanism that enforces the consistent security classification of an object.

136、 A .This task is identifying the critical path, which is defined as the path that is critical for business functionality. It should be shown in detail with all supporting mechanisms required for critical data flow. Redundant paths should be shown and there should be at least one redundant path for every critical path.

The critical path analysis lists all pieces of an environment and how they interact and are interdependent. Diagrams should be developed that show the devices and their place and relevance to a facility. The diagrams should include power, data, water, and sewer lines. Air conditioners, generators, and storm drains may also be included to provide a full description and understanding.

137、 B .The mean time to repair (MTTR) value is used to estimate how long it will take to repair the device and get it back into production.

Service level agreements (SLAs) are legally binding guarantees that state a vendor will fix or replace a system within a specific time period.

138、 B .Online UPS systems respond more quickly than standby systems. This is because the primary source is connected to the online UPS keeping its battery charged to its maximum level. When the primary source fails, the online system activates with a strong enough battery to maintain the same level of energy as the primary power source for a period of time.

139、 B .A deluge sprinkler system offers the best solution to this company. It has open sprinkler heads, which allow for very large volumes of water to be released quickly.

140、 D .A UPS is a temporary power source intended to be a backup supply in the event of a power failure, thus does not address Jonathan's ongoing problem of line noise.

A surge protector can extract extra line voltages to protect his system and data. A line conditioner uses a tap to look for lows and highs in voltage and compensates for them.

What he really needs to do is move the cords and cables to other outlets to reduce line noise and the threat of fire.

141、 A .Different suppression agents affect the four legs of fire in various ways. Fuel and oxygen help feed fires and should be removed in order to successfully extinguish them with soda acid or CO2. High temperatures should be reduced by using water. Chemical reactions can be the product of fires and should be disrupted by using a type of gas (Halon, FM-200).

Different suppression agents attack one of these legs when combating a fire.

142、 D .Although having ultraviolet-protected windows could be an important consideration when choosing a facility, it is not as critical as the other issues. A storage company would be most concerned with intrusion detection systems to prevent theft and the combustibility of materials to prevent fire. Also, since this company stores heavy construction equipment, they need to account for the load bearings of floors, ceilings, and walls.

143、 C .Each device has a mean time between failure (MTBF) and a mean time to repair (MTTR). The MTBF estimate is used to determine the expected lifetime of a device or when an element within that device is expected to give out.

The MTTR value is used to estimate the amount of time it will take to repair the device and get it back into production. These estimates can be used to calculate the risk of utility failure and evaluate other devices that may have better MTBF or MTTR values.

144、 C .Although some computers react differently, most will experience major damage when a temperature of 175° F is reached. Some will have significant performance issues at lower temperatures but will not necessarily experience actual damage.

145、 C .The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated 8 feet high and use two

foot-candles, which is a unit that represents the illumination power of an individual light.

146、 D .The idea is that the material should flow out of the building and not into it. The positive drain principle is a protection mechanism.

147、 C .Class A materials include wood, paper, cloth, rubber, plastics, and other ordinary combustibles. All of these materials possess the same level of combustibility.

148、 B .A proximity detector, or capacitance detector, emits a measurable magnetic field while in use. The detector monitors this electrical field and an alarm sounds if the field is disrupted. These devices are usually used to protect specific objects (e.g., artwork, cabinets, safe) as opposed to a whole room or area.

149、 B .Fencing, in any form, is a deterrent to a potential intruder. While a small 3-foot fence is less intimidating than an 8-foot fence, its mere existence helps to dissuade criminals from trespassing. Many times a fence will create a perception that an area is secure, even if no other mechanisms exist.

150、 C .The incorrect answer is the deluge sprinkler system. This is the worst of the four sprinkler options for protecting computer rooms. Because of its open sprinkler head design, it releases more water than the other systems.

151、 A .Brownouts have become more and more common in large cities. Overpopulation results in increased power usage and power companies have had a difficult time providing the necessary power supply. A brownout is a reduction in voltage below normal levels for a prolonged period of time.

152、 C .The first priority of a security professional when dealing with humidity is protecting the equipment. Excessive moisture can cause damage and performance issues with computers.

153、 B .A hygrometer is used to measure humidity levels. High humidity levels create too much moisture which can damage computers. Low humidity levels cause static electricity, which also causes problems to computers.

154、 C .The major damage done by smoke to equipment happens over time. After the smoke has cleared, particles fall and can build up on computer components. This can damage or destroy circuit boards, transistors, and other metal contacts.

155、 C .The employee termination procedures were not followed completely. Scott's ID badge was not retrieved when he was escorted from the building. This is an administrative control.

156、 C .This type of system is sensitive to sounds and vibrations and detects noise level changes in the area it is placed in. These devices do not emit any waves, they only listen for sounds within an area and are considered passive devices.

157、 B .CO2 can be a fatal gas to humans. It rapidly removes or displaces the oxygen from the air and because of this should not be used in locations with employees present.

158、 A .The third rule, the Strong Star Property, states that a subject that has read and write capabilities can only perform those functions at the same security level, nothing higher and nothing lower. The Simple Security, Star Property, and Strong Star property rules indicate what states the system can use to control access to objects.

159、 D .This model gets hit hard on the CISSP exam, so it is important that you know all of the necessary information pertaining to it.

160、A .The Biba model focuses on protecting the integrity of the data rather than confidentiality, as in the Bell-LaPadula model. The "no write up" rule ensures that a subject at a lower level of integrity cannot corrupt or negatively affect the higher integrity object. The "no read down" rule ensures that the higher integrity level subject cannot degrade its integrity by obtaining data from an object of lower integrity.

161、 C .Protection profiles outline a specific security solution that is needed to fulfill a specific requirement. Many types of people and organizations can write a protection profile explaining what they need in a product. A vendor may choose to build a product to meet the need described in a particular protection profile.

162、 C .The Orange Book looks at operating systems and not networking issues. The Red Book was created to evaluate the level of protection provided by different networking devices, software, and configurations.

163、 C .TCSEC has four classifications, with A being the best and D providing the least amount of protection. Within each classification are divisions of ratings, with the higher numbers being the best and the lower numbers providing lower protection. So C2 would provide more protection than a system that achieved a C1 rating and a B2 would provide more protection than a B1 rating.

164、 C .The biggest difference between classifications A and B is the existence of more formalized methods of evaluation. The system's design, coding practices, documentation, testing procedures, and even product delivery are highly scrutinized.

165、 D .Time-of-check versus time-of-use (TOC/TOU) attacks take advantage of timing differences between when a system checks for files and when it actually executes the files. It is an asynchronous attack.

166、 B .Object reuse means that a different subject will use the same media. If it contains sensitive information, that data should be properly erased before another subject can have access to it.

167、 D .Cache memory is a type of RAM that holds specific information that is accessed often.

168、 A .The reference monitor is an abstract machine that contains the system's access control security policy. The security kernel enforces the reference monitor and its configurations. Subjects cannot directly access objects without the security kernel and reference monitor allowing it.

169、 C .These are all different evaluation criteria used to evaluate the functionality, assurance, and security provided by operating systems, devices, and software products. None of them were used globally, but within individual countries. The Common Criteria took the best of all of these criteria and was developed to be used globally.

170、 D .Secondary storage is not volatile, meaning that data stored on these types of devices will not be lost if power is lost. Virtual storage is the use of RAM and secondary storage to extend a computer's memory capabilities.

171、 A .The control unit determines when data instructions can be sent on to the CPU for processing. Data is held in registers until its turn to have access to the CPU. The ALU is a component of the CPU that performs mathematical and logical operations.

172、 B .Multitasking systems can process many tasks and processes at one time. A CPU and operating system have to be specially developed to perform multitasking functionality.

173、 B .The US Department of Defense (DoD) developed the Trusted Computer System Evaluation Criteria (TCSEC) to evaluate the security and assurance operating systems provide. It is also referred to as the Orange Book and is in the Rainbow Series.

174、 D .Covert channels are ways of communicating that were not envisioned by the developer of the system or application. There are two types: timing and storage.

175、 C .Storage devices are hard drives, CD-ROMs, zip drives, floppy drives, and tape drives. They are not volatile, meaning they will not lose data when power is lost. The other listed items are volatile memory types, which will lose the data held within them when the power is lost.

176、 D .As processing power increases in the microprocessors within systems today, attackers can perform more powerful brute force attacks. Brute force attacks try all possible combinations of something (e.g., passwords, cryptographic key values, credential sets), and the more power one has to do this, the more combinations that can be enumerated within a shorter period of time. Multiprogramming is an older architecture of operating systems. We do not use it any longer and it is not an advancement in microprocessor design.

177、 A .The TCSEC (Trusted Computer System Evaluation Criteria), alias the Orange Book, is an evaluation criteria used to rate the assurance and security provided by mainly operating systems. ITSEC is a European assurance evaluation criteria, and the Red Book is used for evaluating

network components.

178、 B .Accreditation is the formal acceptance of the adequacy of a system's overall security by management. Management reviews the findings from the certification process to make its decision. When they have accepted the new system, they are also stating that they are accepting the risk that comes along with it.

179、 A .Certification is a technical evaluation to determine if the system or product provides the necessary functionality and security required by a specific environment.

180、 D .Traditional systems exhibited a more closed network environment. These are mainly mainframe environments that did not provide the distributed and open environments we experience today. Closed environments and systems do not allow for as much interoperability as open systems and environments and are more proprietary in nature.

181、 C .Trusted computing base (TCB) is a term used in the Orange Book to refer to the protection mechanisms in a system. The mechanisms can be hardware, software, and firmware, and these are the components that will be evaluated and tested when the product is submitted for an assurance rating.

182、 D .Specific ideals of the reference monitor and the security kernel (not necessarily a complete listing):

- The reference monitor is an abstract machine which mediates all access to objects.
- The security kernel is made up of mechanisms that enforce the reference monitor concept.
- The processes carrying out the reference monitor concept and security kernel must be isolated.
- The reference monitor must be invoked for all access attempts and impossible to circumvent.
- The security kernel must be small enough to be tested and verified.

183、 C .The Clark-Wilson model specifies that all data modification must be done through programs. It is an integrity model that also enforces the separation of duties concept.

184、 B .Division C specifies discretionary protection versus mandatory protection, which is addressed in the B classifications. Classification A provides formal and verified protection. Classification D provides minimal protection.

185、 D .The question is a direct definition of the noninterference model. Activities that are carried out by subjects at one level should not affect the environment of any other subjects, especially at lower levels. Biba is an integrity model. Information flow is a model used for restricting the flow of data to ensure the security policy is enforced.

186、 A .A lattice is an access control model that provides bounds outlining what a subject can and cannot do pertaining to individual objects.

187、 B .All other protection controls are logical, meaning they take place in software and are easier to get around and circumvent than actually segmenting the pieces of memory physically.

188、 C .The Brewer-Nash model is different from the other models in that it allows for dynamically changing access controls. It uses context-based control, meaning the application will make access decisions based on the previous activities of the subjects. This is done to ensure that conflicts of interest do not arise within the application itself by controlling what a subject can and cannot access.

189、 A .Multiprogramming is when an operating system and CPU can execute more than one program at a time. It is different from multiprocessing in the way the operating system controls the processes and the way they control and use resources. In a multiprogramming environment, the processes can commit a resource and the operating system has less control over when the process releases the resource than in multiprocessing environments.

190、 D .Virtual machines are logical containers for applications to work within. They provide a simulated environment for applications and protect the operating system from rogue applications that may attempt to access system resources in an inappropriate and unsafe manner.

191、 A .The ITSEC criteria rates functionality and assurance separately. They have an E rating for the assurance level of the product and an F rating for the functionality rating. This provides a more accurate and granular approach to product evaluation. The Orange Book uses A – D ratings, and the Common Criteria uses EAL packages.

192、C .Positive drain means that contents flow out instead of in. If the surrounding area flooded for some reason, a company wants to ensure that outside water and other substances are not allowed to flow back into their facility through pipes.

193、 C .Fire suppressing agents attack a fire in different ways. Water reduces the temperature of a fire. Gases modify the chemical combustion elements, and CO2 can reduce the oxygen.

194、 A .Acoustical-seismic devices detect vibration changes within a given area and can easily cause false alarms if they are very sensitive.

A proximity device monitors an electronic field and an electromechanical detection device detects a break in foil strips.

195、 C .Fire extinguishers should be inspected quarterly, not yearly.

196、 B .The following are definitions of the different terms:

Spike — Momentary high voltage
Surge — Prolonged high voltage power loss

Fault — Momentary power outage
Blackout — Prolonged loss of power

197、 D .Dry pipe systems do not hold water in the pipes but release it when a fire is detected. They are a better choice in colder climates so that pipes will not break when the water freezes.

198、 D .When looking at the construction of a facility, the other three items are very important to consider and perform risk analysis on. Photoelectric has to do with types of fire detectors and intrusion detection systems.

199、 B .Physical controls are a big part of physical security and include things like fencing, locks, lighting, and construction materials. Lighting is used as a preventive control and should be in places where employees walk or intruders may try to slip in. Access logs are detective controls because they are reviewed "after the fact."

200、 D .Halon extinguishers are federally restricted due to the dangers they cause. Companies are not required to replace old units, but they must refill them with another approved substance when the extinguisher is depleted. Several EPA-approved chemicals can be used to replace Halon —FM-200 is one of them.

201、 B .Preaction systems release water into the pipes after a certain temperature is met and then delay the release until a link mechanism melts. These systems are the most popular for data processing environments because they give people time to put the fire out themselves, if it is small enough. This is good because releasing water into a data processing environment can be damaging to the computers. It also allows people to react and turn off the system if it is a false alarm.

202、 B .Portable extinguishers should be placed within 50 feet of electrical equipment.

203、 A .Class A fires include the burning of wood, paper, or laminates and should be suppressed with water or soda acid.

204、C .Spikes in power can cause noise and line interference for users and can damage sensitive components. Surge protectors and line conditioners should be put in place to ensure a constant, steady stream of power.

205、A .Internal partitions only go up to the dropped ceiling and not to the real ceiling. Someone can easily go through the dropped ceiling, climb over the partition, and enter the sensitive area.

206、 D .Mean time before failure (MTBF) is used to prepare for hardware failures and the expected cost of replacing it. The mean time to repair (MTTR) is the time needed to get the device fixed and back into production.

207、 B .A "clean" power supply means there is no interference or fluctuation in voltage levels.

208、 A .CO2 is a potentially dangerous fire suppression method because it removes oxygen from the area. This can be deadly if people are nearby.

209、 A .Plenum space is used for wiring and cabling. This is a place where fires can easily start. Wires and cables in this area must be plenum cables, meaning that their coating is made out of chemicals that are not hazardous when they burn.

210、 C .Hygrometers monitor humidity levels, which can affect system performance. High humidity can cause corrosion of electrical components and low humidity can cause static electricity.

211、 A .Carpeting should not be present in data centers and around computer systems because it creates static electricity. If carpet is used, it should be static-free carpet. Static electricity can introduce electricity damaging to electrical components.

212、 B .Deluge systems are much like dry pipe systems, however, their sprinkler heads are open to allow more water to release more quickly. Dry pipes do not hold water in the pipes, but in a water storage area. When a fire detection mechanism sounds an alarm, the water is released into the pipe. Deluge systems should not be used in data processing environments. Preaction systems should be used instead because they provide a delayed reaction.

213、 D .Cable traps are device locks intended to protect hardware from theft. They are used for mobile devices and lock them to a secure feature of an environment.

214、 B .Key override can be used during emergency situations or with authorized personnel to gain immediate access. Master keying has to do with the capability of reconfiguring the lock, as in resetting the access code. Door delay is a control that sets off an alarm if a door is open for an extended period.

215、 B .Piggybacking can be prevented by increasing security at each entrance and by educating employees. It has a more basic definition of an entity using another entity's legitimate credentials for access which means that a piggybacking attack is not limited to physical security issues.

216、 A .Electronic access control (EAC) tokens are used in physical security to authenticate subjects. They can be proximity readers, programmable locks, or biometric systems that identify and authenticate users before allowing them entrance.

217、 B .Closed-circuit television (CCTV) systems are monitoring devices that allow a security guard to watch several areas from one centralized location. CCTVs are great physical security tools, but best when not totally depended upon as the only tool. Companies need at least one security guard to view the monitor screen and then can also use motion detectors and/or intrusion detection systems to provide complete protection of a facility or department.

218、 A .The main risks that physical security components combat are theft, interruptions to services, physical damage, compromised system integrity, and unauthorized disclosure of information.

219、 B .Electrical fires are the most common cause of fires in computing centers.

220、 D .The security budget on its own does not affect an assessment of a facility's vulnerabilities. The past security incidents and compromises should be reviewed along with the current security controls in place. A full assessment should be done to understand the level of protection being provided.

221、 A .Preaction combines both the dry and wet pipe systems and allows manual intervention before a full discharge of water occurs.

222、 A .Soda acid suppresses the fuel supply of a fire of common combustibles, Halon disrupts the chemical combustion, and CO2 displaces the oxygen.

223、 A .People are the last line of defense in physical security. Devices and controls are put into place to protect a facility, its contents, and especially the people within it.

224、 D .Smoke-activated detectors use photoelectric optical detectors to detect changes in light intensity. One portion of the detector sends a beam of light to a receiver. If this beam is interrupted, the detector assumes that smoke has caused it and sets off the alarm.

225、 B .Class B refers to liquid fires, which can be suppressed with Halon, CO2, or soda acid.

226、 A .A 4-foot fence most likely will have no effect against a determined intruder, but it is effective in preventing casual trespassers.

227、 A .DSA is only used for digital signatures and cannot perform message encryption or key exchange. The DSS dictates that SHA-1 and DSA (or RSA or ECDSA) are to be used for digital signatures.

228、 C .If an attacker can gain control of the password file or an individual password, he can use a dictionary attack program that has thousands of commonly used dictionary words to uncover the password. Passwords should not be made up of words, but a sequence of letters, symbols, and numbers at least seven characters long.

229、 B .SHA is a hashing algorithm. It is specified to be used in the Digital Signature Standard to create the necessary message digest. This message digest will then be encrypted with a private key to create a digital signature. A hashing algorithm alone only provides data integrity.

230、 D .Cryptanalysis has been used for many years as a way of discovering new and innovative methods of breaking algorithms, keys, and cryptosystems. It can be done with a "black hat"

approach to gain unauthorized access to encrypted information. Or it can be done with a "white hat" approach, which finds flaws or weaknesses in algorithms and cryptosystems so that they can be better developed and improved upon.

231、 B .Rijndael is the algorithm in place today for protecting sensitive but unclassified US government information. DES was finally broken and needed to be replaced by a stronger algorithm that provided larger key sizes.

232、 D .Transposition ciphers use permutation to hide their messages. This is different than substitution which substitutes each character or bit for another. Transposition and substitution are used in many algorithms today.

233、 B .Electronic Code Book (ECB) mode does not use any chaining. This means that the same plaintext will create the same ciphertext every time it is encrypted with the same key. The other DES modes use chaining, which means some of the previously encrypted data is used in the encryption process. These modes do not provide patterns as the ECB mode does.

234、 D .The symmetric key, or secret key, is used to encrypt the actual message, while the asymmetric key is used to encrypt the symmetric key. The key exchange protocol is responsible for the other key management issues.

235、 A .The HAVAL algorithm is a single purpose algorithm that performs one-way hashing functionality. It creates a variable-length message digest, where the other hashing algorithms (MD, SHA) create a specific size message digest. The MD family creates a 128-bit message digest, and SHA creates a 160-bit message digest.

236、 C .One-way hashing creates a fingerprint of the message so the function can more easily identify and monitor the message to see if it has been altered. It takes a variable-length string (the message) and generates a fixed-length value (message digest).

237、 D .IBM's 128-bit algorithm, Lucifer, was accepted as the national standard in 1974. It was altered by NIST and referred to as Digital Encryption Algorithm, which used a 56-bit key.

238、 B .Ciphertext is the result of encryption and is unreadable by human or machine.

239、 A .The Clipper Chip was intended to use the SkipJack algorithm. One of the identified weaknesses was its 80-bit key, which was considered too short to provide the necessary level of protection.

240、 D .One-time pads are considered unbreakable. A pad of random values is created and used to encrypt the message. The pad is at least as long as the message itself. The pad is destroyed after it is used, and a new pad is created if another message must be encrypted.

241、 C .Concealment ciphers disguise messages within the text or body of a message, such as

using every other word in a sentence to form a different message.

242、 B .Symmetric key systems are considerably faster than asymmetric key systems. However, they cannot provide nonrepudiation or authenticity and struggle with proper key distribution and controlling keys as more users need to communicate

243、 D .Blowfish is a symmetric key algorithm that can use a key length up to 448 bits.

244、 D .HTTPS encrypts all data that is passed between two systems, instead of just individual messages. S-HTTP only encrypts individual messages and not the whole communication channel. MIME and S/MIME are e-mail standards.

245、 A .Substitution boxes, or S-boxes, use lookup tables that determine how bits should be scrambled and substituted.

246、 B .Keystream generators are used in stream ciphers to produce a random stream of bits. These bits are XORed to the message, which results in an encrypted message (ciphertext). The keystream generator is similar to the one-time pad concept.

247、 C .For a stream cipher to be strong against cryptanalysis attacks it should contain the other mentioned characteristics. Block ciphers work better in software implementations because they work with blocks of data. Stream ciphers work better within hardware because they work with one bit at a time and are resource intensive.

248、 B .RSA, named after its inventors. It is an asymmetric algorithm that can provide data encryption, key distribution, and digital signatures. It is a de facto standard in many types of products.

249、 A .A good and secure hashing algorithm creates a message digest from the whole message and not just a portion of the message. If it only worked with a portion of the message, the other portion could be modified, and it would not be revealed to the receiver.

250、 A .Encapsulating Security Payload (ESP) is a protocol within IPsec that uses cryptographic mechanisms to provide confidentiality, message integrity, and system authentication. AH provides integrity and system authentication, but not confidentiality.

251、 B .The Diffie-Hellman algorithm was developed in 1976 as the first method for electronic key distribution. It was the first public key algorithm and allowed for a symmetric key to be exchanged securely without a prior relationship being set up.

252、 D .When an attacker intercepts messages and then pretends to be one of the parties involved in the communication, a man-in-the-middle attack has been performed. This is what takes place when an attacker forwards her public key without the receiver's knowledge.

253、 B .Link encryption provides additional security by encrypting all the information. But for traffic to be routed or forwarded, all the routers, switches, and associated equipment must be configured to support this type of service. These intermediate devices need to decrypt a portion of the headers to make decisions on forwarding or routing.

254、 A .IPsec protects data exchange between two devices and can provide authentication, confidentiality, and integrity.

255、 C .RSA is an asymmetric algorithm used to encrypt the session key created by the client. This allows for the session key to be securely transmitted to the web server. The client and server can then set up an SSL connection, which encrypts all data passed back and forth.

256、 C .While MIME specifies how multimedia data and e-mail attachments are transferred over the network, S/MIME provides a standard for encryption and digital signatures of e-mail messages. S/MIME extended the capabilities of the MIME standard.

257、 A .Steganography involves secretly placing a piece of data within another medium. The data could be in a wave file, graphic, or bits that are altered within a document. It involves hiding the existence of the message, not actually encrypting the message.

258、 A .Pretty Good Privacy (PGP) is a freeware e-mail security program that was developed by Phil Zimmerman in 1991. It does not use a hierarchical trust model, as in PKI, but a web of trust. This means individual users determine to what degree they trust each other.

259、 C .Keystream generators produce streams of bits that are then XORed with the plaintext and the result is ciphertext. Block ciphers divide messages into blocks and put each block through rounds of computation. Stream ciphers are best used in hardware implementation.

260、 D .Asymmetric cryptography uses public and private keys. In most cases, the public key is used to encrypt a symmetric key. Asymmetric algorithms use more complex mathematics, making them much slower than symmetric algorithms.

261、 B .Strong hashing algorithms should produce few or no collisions. Two hashes created for two different messages should be different and not the same value. If the same value is produced, there can be patterns and information that an attacker may use to uncover information. Hashing algorithms that create longer digest values are less vulnerable to birthday attacks, which look for collisions.

262、 D .Secure Electronic Transaction (SET) has been a suggested substitution for the way SSL is being used today to provide secure electronic transactions. But the required overhead, added software, and infrastructure have prevented this technology from being fully adopted.

263、 B .Nonrepudiation is a service that ensures that a person cannot deny sending a message at a later time. This service is provided by digital signatures.

264、 A .MD2 is a one-way hashing algorithm that produces a 128-bit hash value. This hash value is also referred to as a message digest. Hashing algorithms are used to ensure the integrity of messages.

265、 D .Key management includes the following: key generation and proper destruction, key storage and transmission, key secrecy, and key length. Most of these activities are taken care of by different protocols, but a security professional who is responsible for implementing and maintaining an encryption system should ensure that these tasks are actually being done properly. Improper key management is one of the biggest downfalls of encryption implementation and the easier target for attackers.

266、 B .Digital signatures are created by using a hashing algorithm to create a message digest, and then a private key is used to encrypt the message digest. Integrity is provided by using the hashing algorithm because the receiver will create another message digest value and compare it with the one that was sent. It provides authentication because when the receiver decrypts the message digest value with the sender's public key she is sure who sent it. Digital signatures provide nonrepudiation, meaning the sender cannot deny sending a message which, in turn, provides accountability.

267、 C .X.509 is a standard that outlines the format of certificates that are used in a public key infrastructure (PKI). This standard dictates the fields and possible values that can be used in these certificates.

268、 D .Cryptanalysis is the process of trying to break a cryptosystem; this usually means uncovering the key that was used for encryption. Cryptanalysis can be performed by "white hats" to uncover flaws and weaknesses in a cryptosystem or by "black hats" to gain unauthorized access to encrypted data. The attacker must at least know the algorithm that was used and capture some ciphertext to run brute force attacks against it.

269、 A .Secure Sockets Layer (SSL) is a protocol that provides authentication, integrity, and confidentiality and is used to encrypt a communication channel between two systems. It is based on public key infrastructure (PKI), meaning that it performs authentication by using certificate authorities and certificates.

270、 A .A brute force attack is when an attacker tries all possible solutions until the correct one is uncovered. This can be trying to find a sequence of characters that represents a valid password or all possible key values within a keyspace to uncover one specific key. Cryptanalysis is a category of hacking that tries to break an encryption system, usually by uncovering the selected keys. Once the key is uncovered, any data encrypted using that key can be deciphered and read.

271、 A .Most passwords in environments are centrally stored for user authentication. Any password that is stored should not be stored in cleartext, rather it should be encrypted or hashed. Passwords that are stored centrally are even more vulnerable because an attacker would try to

access all passwords to an environment. Passwords should be at least seven to eight characters long. They should also be non-dictionary words. Thus, answer D is correct, but answer A is more important when weighing the two. This is why answer A is correct.

272、 B .Link encryption provides encryption at a lower end of the OSI model, working at the data link and physical layers. All information, including header information, is encrypted. End-to-end encryption works at the application and presentation layers and does not encrypt the actual packet headers, but only the packet's data payload. Data link messaging is connection maintenance, error detection, and correction used by the link encryption software. This information is not encrypted. Link encryption provides a higher level of protection by encrypting all data, not just the payload.

273、 C .Advanced Encryption Standard (AES) uses the Rijndael algorithm. It is a symmetric algorithm, which is used to encrypt bulk data. Symmetric keys are not used in key recovery— asymmetric algorithms are used for that purpose. Hashing algorithms are used to create message digests which are used for data integrity.

274、 B .PGP is a free encryption product that uses asymmetric and symmetric algorithms together in a hybrid approach. It allows users to encrypt, digitally sign, and determine how much they trust other users. The other answers are algorithms and not cryptosystems. A cryptosystem is all the necessary software, algorithms, keys, and protocols needed to carry out cryptographic functions.

275、 A .The following are the correct modes for Tripe-DES (3DES): DES-EEE3 uses three keys for encryption; DES-EDE3 uses three keys and encrypts, decrypts, and encrypts data. DES-EEE2 and DES-EDE2 are the same as the previous modes, but the first and third operations use the same key. There is no DES-EEE1 mode using one key. That is a phony answer.

276、 C .S-boxes (substitution boxes) hold the mathematics and logic that will be performed on the different blocks of data. These S-boxes are used by the algorithm to carry out the substitution and transposition functions.

277、 D .Today, a 56-bit key can only provide a few hours of protection. If DES had a larger key size, then it could provide more protection. Because of this weakness, AES was developed using the Rijndael algorithm. AES replaced DES and Rijndael has much larger key sizes than DES.

278、 D .Simple Key management for IP (SKIP) and Internet Security Association and Key Management Protocol (ISAKMP) are both key exchange protocols that can be used by IPsec. The de facto standard for IPsec is to use Internet Key Exchange (IKE), which is a combination of ISAKMP and the OAKLEY protocol. SKIP, ISAKMP, and IPsec work at the network layer.

279、 A .IPsec uses a message authentication code (MAC) function by calculating the Integrity Check Value (ICV) to provide data origin authentication. This means the receiving system knows what system sent the data. However, it does not mean that the actual user is authenticated, only

the system that sent the information. If user authentication is required, credentials would need to be sent and verified, or a digital signature would need to be used. A symmetric key is not bound to an individual's identity as credentials and private keys are.

280、 C .Asymmetric algorithms use public and private keys for key encryption and distribution and digital signatures. When something is encrypted with a private key, only the corresponding public key can decrypt it. If a specific public key can decrypt something, then the user knows that the person with the corresponding private key encrypted it in the first place. So the public key authenticates that the proper private key was used.

281、 A .After a server authenticates to a client, when setting up a SSL connection, the client creates a session key that will be used by both the client and the server for bulk encryption. The client encrypts the session key with the server's public key and sends it. Only the server can decrypt it, because only the server is supposed to have the corresponding private key.

282、 B .The strength of the encryption method comes from the algorithm, secrecy of the key, length of the key, and the key management practices. The larger the keyspace, the more random the actual bits making up the key can be.

283、 B .Asymmetric algorithms use more complex mathematics than symmetric algorithms and thus, are slower. Asymmetric keys can be used to encrypt symmetric keys and use a pair of keys—public and private.

284、 C .Through the use of public key encryption schemes, digital signatures use the private key to encrypt a hash of the message and append that hash to the message. The private key provides authentication and nonrepudiation, and the use of a hashing algorithm provides integrity.

285、 A .Stream ciphers encrypt one bit at a time and work best if implemented in the hardware due to the intensive nature of manipulating each bit and the continual generation of the keystream.

286、 B .DES is a symmetric encryption algorithm that uses a 64-bit key for encryption, but 8 bits of the key are used for parity. Thus, the true key is 56 bits. It is also a block cipher, not a stream cipher.

287、 B .PKI uses an asymmetric process to encrypt a session key for an exchange process and then uses symmetric encryption for bulk encryption.

288、 C .A certificate authority (CA) generates a digital certificate, binding the public key to the individual or company's identity. The CA vouches for the identification of the owner of the certificate.

289、 D .Elliptic curve cryptosystem (EEC) provides similar services as the RSA algorithm, but requires much less processing power. Thus, it is an ideal choice for cell phones and small wireless

electronic devices.

290、 C .The sender would need to first obtain the receiver's public key, which could be from the receiver or a public directory. The sender needs to protect the symmetric session key as it is being sent, so she encrypts it with the receiver's public key. The receiver decrypts the session key with his private key.

291、 C .Message authentication code (MAC) is the use of a symmetric key and a hashing algorithm. The only party that could properly check the integrity of the message is the one that has the other copy of the symmetric key.

292、 C .Diffie-Hellman is not used for message integrity. It is an asymmetric algorithm that was created for the purpose of key exchange only.

293、 D .Link encryption encrypts all data along a physical path between two endpoints and provides higher security and performance for the encryption services. Headers, trailers, data payload, and routing data would all be encrypted.

294、 D .S-HTTP and HTTPS are both used for encryption, but HTTPS is used to encrypt a channel between two systems, and S-HTTP is used to encrypt individual messages.

295、 C .Secure Shell (SSH) is a means of providing a secure tunnel that provides terminal-like access to remote computers.

296、 B .When tunnel mode is used in IPsec it means the data payload and the header information is protected. In transport mode, only the payload is protected.

297、 B .The correct equation for determining how many symmetric keys are needed is N(N － 1)/2. If ten people need to communicate via symmetric encryption processes, then 45 keys are needed.

298、 A .Knapsack is an asymmetric algorithm. It is not widely used anymore because it has been broken.

299、 A .In the Caesar algorithm the alphabet serves as the algorithm and the key is the number of locations that are shifted during the encryption and decryption process. It is not a polyalphabetic algorithm.

300、 B .In this algorithm a Vigenere table is a polyalphabetic algorithm that uses a secret word to encrypt and decrypt a message. Where the Caesar cipher used one shift alphabet (letters were shifted up three places), the Vigenere cipher has 27 shift alphabets where the letters are shifted up one place.

301、 D .The algorithm, the set of rules, dictates how enciphering and deciphering take place.

Many of the mathematical algorithms used in computer systems today are publicly known and are not the secret part of the encryption process. If the internal mechanisms of the algorithm are not a secret, then something must be. The secret piece of using a well-known encryption algorithm is the key. Cryptovariable is another name for a key.

302、 C .The keyspace equals 2 to the 8th power, which is 256. If an algorithm allows a key length of 2 bits, the keyspace for that algorithm would be 4, which indicates the total number of different keys that would be possible. (Remember that we are working in binary and that 2 to the 2nd power equals 4.)

303、 C .Auguste Kerckhoff published a paper in 1883 stating that the only secrecy involved with a cryptography system should be the key. He claimed that the algorithm should be publicly known. Cryptographers in the private and academic sectors agree with Kerckhoff’s principle because making an algorithm publicly available means that many more people can view the source code, test it, and uncover flaws or weaknesses.

304、 A .A one-time pad is a perfect encryption scheme because it is considered unbreakable if implemented properly. One of these requirements is that the pad is used only one time. It was invented by Gilbert Vernam in 1917, thus sometimes referred to as the Vernam cipher.

305、D .XOR is an operation that is applied to two bits and is a function commonly used in binary mathematics and encryption methods. When combining the bits, if both values are the same, the result is zero (1 XOR 1 = 0). If the bits are different from each other, the result is one (1 XOR 0 = 1).

306、 C .One-time pad requirements:

- Pad is made up of truly random values.
- Pad is used only one time.
- Pad is securely distributed to destination.
- Pad is secured at sender and receiver's sites.
- Pad is at least as long as message.

307、C .In 1996 several countries (33 total) came together to control the export of the same type of items to the agreed upon "terrorist countries." Their guidelines are referred to as the Wassenaar Arrangement. These countries (Iran, Iraq, Libya, North Korea, Sudan, Cuba, and Syria) were identified as having connections with terrorist groups and activities. The agreed-upon controls did not apply to products that could be downloaded from the Internet.

308、 A .Symmetric algorithms carry out relatively simplistic mathematical functions on the bits during the encryption and decryption processes. They substitute and scramble (transposition) bits, which is not overly difficult or processor-intensive. The reason that it is hard to break this type of encryption is because they carry out this type of functionality over and over again. Asymmetric algorithms use much more complex mathematics to carry out their functions, which

require more processing time and is why they are slower than symmetric algorithms. Symmetric algorithms are more vulnerable to frequency analysis attacks.

309、 B .Confusion is commonly carried out through substitution, and diffusion is carried out by using transposition. For a cipher to be considered strong it must contain both of these attributes to ensure that reverse engineering is basically impossible. The randomness of the key values and the complexity of the mathematical functions dictate the level of confusion and diffusion involved.

310、 C .The individual bits in the one-time pad are used to encrypt the individual bits of the message through the XOR function. In a stream algorithm the individual bits created by the keystream generator are used to encrypt the bits of the message through XOR also.

311、 D .Initialization vectors (IVs) are random values that are used with symmetric algorithms to ensure that patterns are not created during the encryption process. They are usually used as seeding values or starting points and do not need to be encrypted when being sent to the destination. If IVs were not used, then two identical plaintext values that are encrypted with the same key will create the same ciphertext.

312、 C .The following are requirements to ensure that a stream algorithm is strong:

- Long periods of no repeating patterns within keystream values
  i. Bits that are generated by the keystream must be random.
- Statistically unpredictable keystream
  i. The bits that are generated from the keystream generator cannot be predicted.
- A keystream not linearly related to the key
  i. If someone figures out the keystream values it does not mean that she knows the key value.
- Statistically unbiased keystream (as many 0s as 1s)
  i. There should be no dominance in the number of 0s or 1s in the keystream.

313、 A .A symmetric algorithm creates keys that are used for encrypting bulk data. An asymmetric algorithm creates keys that are used for automated key distribution.

314、C .Authenticity of the sender and nonrepudiation. If the receiver can decrypt the encrypted data with the sender's public key, then she knows that it was encrypted with the sender’s private key.

315、 B .Confidentiality, because only the receiver's private key can be used to decrypt the symmetric key and only the receiver should have access to this private key.

316、 A .DEA is the algorithm that fulfills DES, which is really just a standard. So DES is the standard and DEA is the algorithm, but in the industry we usually just refer to it as DES. So they both use 8 bits in parity for their key and 16 rounds.

317、 D .A buffer overflow takes place when too much data are accepted as input. Programmers should implement the correct security controls to ensure that this does not take place. This means they need to perform bounds checking and parameter checking to ensure that only the allowed amount of data are actually accepted and processed.

318、D .The operating system has a long list of responsibilities, but implementing database views is not one of them. This is the responsibility of the database management software.

319、 A .If an object has confidential data and these data are not properly erased before another subject can access them, this leftover or residual data can be accessible. Disclosing this confidential information can compromise the data and system security. This is true of media (hard drives) and memory segments also.

320、 C .Certification is a technical review of a product, and accreditation is management’s formal approval of the findings of the certification process. This question asked you which step was the final step of authorizing a system before it is to be used in an environment.

321、B .Maintenance hooks get around the system’s or application’s security and access control checks by allowing whoever knows the key sequence to access the application, and most likely its code. Maintenance hooks should be removed from any code before it goes into production.

322、 C .The state machine model dictates that a system should start up securely, carry out secure state transitions, and even fail securely. This means that if the system encounters something it deems unsafe, it should change to a more secure state for self-preservation and protection.

323、 A .Firmware is a type of software that is held in a ROM or EROM chip. It is usually used to allow the computer to communicate with some type of peripheral device. The system’s BIOS instructions are also held in firmware on the motherboard. In most situations, firmware cannot be modified unless someone has physical access to the system. This is different from other types of software that may be modified remotely or through logical means.

324、 C .ITSEC is a criterion that was developed for use by European countries to evaluate and rate their products.

325、 A .The security kernel makes up the main component of the TCB, which is made up of software, hardware, and firmware. The security kernel performs a lot of different activities to protect the system; enforcing the reference monitor’s access rules is just one of those activities.

326、 C .The CPU has base and limit registers that hold the starting and ending memory addresses that a process is allowed to work within. This ensures that the process is isolated from other processes in that it cannot interact with another process’s memory segment.

327、 D .A guard is either a dedicated device or a piece of software that monitors and controls

software between systems of different classification levels. It helps to ensure that sensitive information is not accessible to those who do not have the clearance level to access it.

328、 C .The security perimeter is a boundary between items that are within the trusted computing base (TCB) and items that are outside the TCB. It is just a mark of delineation between these two groups.

329、 A .The Bell-LaPadula model was developed for the U.S. government with the main goal of keeping sensitive data unavailable to those who were not authorized to access and view them. This model was the first mathematical model of a multilevel security policy used to define the concepts of a security state and mode of access and to outline rules of access. The Biba and Clark-Wilson models do not deal with confidentiality, but with integrity.

330、 A .It is difficult to add useful and effective security at the end of product development or to add security as a front end to an existing product. Adding security at the end of a project is usually more expensive because it will break items and the team will need to go back to the drawing board and redesign and recode portions of the product.

331、 A .Processes are assigned their own variables, system resources, and memory segments, which make up their domain. This is done so that they do not corrupt each other’s data or processing activities.

332、 B .A covert channel is being used when something is using a resource for communication purposes and that is not the reason this resource was created. A process can write to some type of shared media or storage place that another process will be able to access. The first process writes to this media, and the second process reads it. This action goes against the security policy of the system.

333、 C .The Common Criteria uses a different assurance rating system than the previously used criteria. It has packages of specifications that must be met for a product to obtain the corresponding rating. These ratings and packages are called Evaluation Assurance Levels (EALs). Once a product achieves any type of rating, customers can view this information on an Evaluated Products List (EPL).

334、 A .The *-integrity axiom (or star integrity axiom) indicates that a subject of a lower integrity level cannot write to an object of a higher integrity level. This rule is put into place to protect the integrity of the data that reside at the higher level.

335、 D .The simple security rule is implemented to ensure that any subject at a lower security level cannot view data that reside at a higher level. The reason this type of rule is put into place is to protect the confidentiality of the data that reside at the higher level. This rule is used in the Bell-LaPadula model. Remember that if you see “simple” in a rule, it pertains to reading; * or “star” pertains to writing.

336、B .“The first mathematical model of a multilevel security policy used to define the concepts of a security state and mode of access and to outline rules of access” is a formal definition of the Bell-LaPadula model, which was created and implemented to protect government and military confidential information.

337、 A .The physical memory addresses that the CPU uses are called absolute addresses. The indexed memory addresses that software uses are referred to as logical addresses. Relative addresses are based on a known address with an offset value applied.

338、 C .The major difference between Class A – ranked products and Class B – ranked products is the formality of design, development, documentation, testing, and implementation. Most of the security features are similar. If a system is going to receive an A assurance rating, the evaluation team will go through every piece of that system’s life cycle in a granular and detailed manner.

339、 A .Covert channels can be used because the operating system is not anticipating this type of activity and thus does not protect against it. The use of covert channels violates the system’s security policy. Systems with many covert channels typically have lower assurance ratings than systems with few covert channels. A covert channel is using resources for communication purposes in a way that they were not designed for. An overt channel is using resources that were developed specifically for communication purposes.

340、 B .Virtual machines act as an operating and holding area for different programs to run in. This serves as a protection mechanism for the operating system. The operating system communicates with the virtual machine; thus, it never has to interface directly with the untrusted program code. Virtual machines can manage the program code in a controlled manner.

341、 B .The first step is evaluation. Evaluation involves reviewing the product’s protection functionality and assurance ratings. The next phase is certification. Certification involves testing the newly purchased product within the company’s environment. The final stage is accreditation, which is management’s formal approval.

342、 A .Secondary storage can be a computer’s hard drive, USB drive, or CD-ROM. Virtual storage is when a computer extends its memory by using these types of secondary storages devices, specifically the hard drive. Virtual storage is a way for the operating system to trick itself into “thinking” it has more memory than it does. A system with 128-bit RAM chip could actually have up to 2GB or 4GB of memory because of these techniques.

343、 B .When the main memory of a computer is full, it uses secondary storage placeholders, called swap spaces. When data are passed to this area, it is called “swapping.” This combination of main memory and secondary storage is called virtual memory.

344、 B .The Bell-LaPadula model was the first mathematical access control state machine model used to control access to data that held different classification levels. Since it uses data

classification levels, this model is well suited for government and military organizations. The model also uses the concepts of the information flow model, which dictates how data flow based on set security policies.

345、 C .Multilevel security mode means that an operating system can make access decisions based on data classification, user clearance, and need to know.
The system can house and maintain different classification levels (e.g., top secret, secret, confidential, public) and understand different clearance levels.

346、 B .The trusted computing base (TCB) is a term that originated in the Orange Book. It describes the components that are used to provide protection for the system or product and what components will be evaluated under the Orange Book criteria. The TCB is made up of hardware, software, and firmware components. The reference monitor and security kernel reside in ring 0 and are components of the TCB. Applications lie within ring 3 and are not considered system-wide protection mechanisms.

347、 A .The CPU is made up of a control unit and an arithmetic logic unit (ALU). The ALU is considered the brain because it performs the mathematical and logical functions needed to process instructions. The control unit acts like a traffic cop by controlling what instructions are processed by the ALU and when. When the instructions are waiting to be processed, pointers to their addresses in memory are held in registers for the CPU.

348、 B .A common mistake is abandoning the certification and accreditation process after the product is accepted and implemented. The problem occurs when changes to the network or the system take place. Networks are upgraded, products reconfigured, and many other types of changes can take place in an environment. So, the product should be recertified and reaccredited if a major change takes place.

349、 B .Object reuse means that a different subject will use the same media. If it contains sensitive information, that data should be properly erased before another subject can have access to them.

350、 D .Cache memory is a type of RAM that holds specific information that is accessed often.

351、 C .Trusted computing base (TCB) is a term used in the Orange Book to refer to the protection mechanisms in a system. The mechanisms can be hardware, software, and firmware, and these are the components that will be evaluated and tested when the product is submitted for an assurance rating.

352、 A .An architecture description is a formal description and representation of a system, the components that make it up, the interactions and interdependencies between those components, and the relationship to the environment.

353、 C .ISO/IEC 42010 has the goal of internationally standardizing how system architecture

takes place instead of product developers coming up with their own proprietary approaches. A disciplined approach to system architecture allows for better quality, interoperability, extensibility, portability, and security.

354、 C .The stakeholders for a system are the users, operators, maintainers, developers, and suppliers. Each stakeholder has his own concern pertaining to the system, which can be performance, functionality, security, maintainability, quality of service, usability, etc. The system architecture needs to express system data pertaining to each concern of each stakeholder, which is done through views. The views of the system can be logical, physical, structural, or behavioral.

355、 B .The control unit is the component that fetches the code, interprets the code, and oversees the execution of the different instruction sets. It manages and synchronizes the system while different applications' code and operating system instructions are being executed.

356、 D .Special registers (dedicated registers) hold information such as the program counter, stack pointer, and program status word (PSW).

357、 B .Once the CPU is done with its computation, it needs to return the results to the requesting program's memory. The CPU sends the requesting program's address down the address bus and sends the new results down the data bus with the command "write." These new data are then written to the requesting program's memory space.

358、 B .Each process has its own stack, which is a data structure in memory that the process can read from and write to in a last in, first out (LIFO) fashion. The process being communicated to takes the last piece of data the requesting process laid down from the top of the stack and works down the stack.

359、 A .When a process is encapsulated, no other process understands or interacts with its internal programming code. Encapsulation provides data hiding, which means that outside software components will not know how a process works and will not be able to manipulate the process's internal code. This is an integrity mechanism and enforces modularity in programming code.

360、 A .If a process is not isolated properly through encapsulation, this means its interface is accepting potentially malicious instructions.

361、 B .Flash memory is a nonvolatile computer storage chip that can be electrically erased and reprogrammed. It is primarily used in memory cards, USB flash drives, solid-state drives, and similar products for general storage and transfer of data.

362、 C .The C programming language is susceptible to buffer overflow attacks because it allows for direct pointer manipulations to take place. Specific commands can provide access to low-level memory addresses without carrying out bounds checking.

363、 C .Data Execution Prevention (DEP) is a security feature included in modern operating systems. It is intended to prevent a process from executing code from a nonexecutable memory region. This helps prevent certain exploits that store code via a buffer overflow, for example. DEP can mark certain memory locations as “off limits” with the goal of reducing the “playing field” for hackers and malware.

364、 B .A garbage collector is software that runs an algorithm to identify unused committed memory and then tells the operating system to mark that memory as “available.” Different types of garbage collectors work with different operating systems and programming languages.

365、 A .National Television Systems Committee (NTSC) and Phase Alternative Line (PAL) are two most widely used video recording and transmission standards. Each provides specific requirements for monitors, recording, transmitting, and receiving equipment used with CCTVs in individual countries. The NTSC standard is used in the United States, most of South America, and Japan. The PAL standard is used in the United Kingdom and several other countries in Europe, Australia, the Middle East, Russia, France, and parts of Africa.

366、 A .A Class C fire is an electrical fire. Thus, an extinguisher with the proper suppression agent should be used.

367、 C .Halon is a type of gas used to interfere with the chemical reactions between the elements of a fire. A fire requires fuel, oxygen, high temperatures, and chemical reactions to burn properly. Different suppressant agents have been developed to attack each aspect of a fire: carbon dioxide displaces the oxygen, water reduces the temperature, and soda acid removes the fuel.

368、 C .A mantrap is a small room with two doors. The first door is locked; a person is identified and authenticated by a security guard, biometric system, smart card reader, or swipe card reader. Once the person is authenticated and access is authorized, the first door opens and allows the person into the mantrap. The first door locks, and the person is trapped. The person must be authenticated again before the second door unlocks and allows him into the facility.

369、 C .This type of system is sensitive to sounds and vibrations, and detects the changes in the noise level of an area it is placed within. This level of sensitivity can cause many false alarms. These devices do not emit any waves; they only listen for sounds within an area and are considered passive devices.

370、 B .High humidity can cause corrosion, and low humidity can cause excessive static electricity. Static electricity can short out devices or cause loss of information.

371、 D .The use of security guards comes with a host of advantages; however, their expense is not one of them. Salaries, benefits, vacations, insurance, and background checks are all factors that must be considered when employing reliable, productive security guards.

372、 C .Smoke detectors should be placed strategically throughout a facility. Raised floors and dropped ceilings are good places for detectors because these areas are common places for electrical wiring. Air ducts and vents are good places because in the event of a fire, air travels fluidly through these devices. A detector would not be necessary around doorways but rather, inside the building.

373、 A .Host-based intrusion detection system doesn’t belong to this physical intrusion detection group. This control pertains to an individual computer and not to detecting unauthorized people who may try to enter a facility.

374、 B .An ideal computing environment, or data center, would use antistatic flooring, not carpeting. If carpeting is absolutely necessary, then it should be specialized antistatic carpeting.
Other ideal characteristics are:

- Proper humidity and temperature levels
- Raised flooring or dropped ceilings for wiring
- Independent HVAC system

375、 B .A passive infrared system measures changes in heat waves for a specified area by using a series of beams. If the temperature in a specific area where one of the beams terminates suddenly increases, it is possible that a person has entered the area.

376、 B .Because Halon has been deemed dangerous to both humans and the environment, an acceptable replacement list was created by the EPA:

- FM-200
- NAF-S-III
- CEA-410
- FE-13
- Water
- Inergen
- Argon
- Argonite

377、 D .CO2 is a dangerous gas that removes or displaces oxygen from the air. It should not be used in areas where humans are present. Instead, a Halon substitute, water, or soda acid should be used. CO2 is often used in unattended facilities or when absolutely necessary, and it is usually used with a delay mechanism that gives individuals a warning before it is dispersed.

378、 B .A mantrap offers the best control for piggybacking because the intruder has to be identified and authenticated before entering a building or area. Although a badge reader is an effective method of physical access control, it is common for an intruder to lurk in the shadows of an authorized employee and then sneak in through a closing door after the employee has entered the building.

379、 A .The wet pipe system, as its name implies, has water in the pipes at all times. When a fire

detector initiates the system, water is released through the sprinkler heads. A dry pipe holds the water in a reserve tank, not in the pipes. When the temperature threshold is achieved, the water releases, fills the pipes, and then sprays from the sprinkler heads. A preaction system contains an additional fire detection device that will recognize a fire before the sprinklers are activated.

380、 A .Electromagnetic interference (EMI) is a type of power line interference. Along with lightning and electrical motors, EMI is also caused by the difference between positive, negative, and neutral wires.

381、 C .Secured computer rooms should have no more than two doorways and should be isolated from public areas, such as restrooms and main hallways. These parameters reduce traffic levels and limit the potential for unauthorized access. In addition, a highly secured computer room should not have comfortable areas for individuals to gather in or loiter.

382、 A .Control centers typically cannot afford to have any downtime, not even for a few seconds. As a result, the best power scheme would be a primary power source (a feeder coming in from a substation), uninterruptible power supply (UPS), and a generator. The UPS can be a type of short-term alternate power supply unit that detects failures in the primary power supply. In the event of a failure, the UPS unit turns on immediately. The limitation of UPS units is their longevity — they are temporary power supplies. For a mission-critical control center, contingencies should be planned in the event of a long-term outage. A generator can provide this alternative or a second feeder from a different power substation.

383、 C .Locks are used for a variety of purposes, including securing laptops, storage rooms, and doors. Their number-one advantage is that they are very inexpensive and simple to implement. However, physical locks also have many drawbacks. They can be easily broken or picked, keys are easily lost, and combinations easily forgotten. Locks are seen only as delaying devices because a determined intruder can get through them.

384、 B .Just as perimeter fences, intrusion detection systems, and guard dogs are important to protecting a facility from intruders—lighting plays an important role in physical security as well. Search lights, flood lights, street lights, and spot lights are all types of lighting that a company may choose to install.

385、 B .Wireless proximity readers are different from user-activated systems. With a user-activated system the user must insert a card into the reader and then a set of credentials must be given to the system to properly authenticate the user. In wireless proximity systems, such as system-sensing readers, the readers “sense” the presence of an object and transmit signals to a proximity card to obtain the access control credentials held on the card.

386、 C .Cipher locks are programmable keypad locking devices that have four different feature sets:

- Door delay — If a door is held open for a certain amount of time, an alarm will sound.
- Key override — An easy-to-remember emergency code can be programmed into the

keypad.

- Master keying — Allows authorized individuals to change key codes.
- Hostage alarms — A specialty combination for those in duress to use.

387、 A .Security barriers and walls that surround sensitive areas should go from the true floor to the true ceiling. This means that the walls do not stop at a dropped ceiling or at the raised floor because those could be circumvented and used as entry points into the sensitive area.

388、 A .A mantrap can be used with a biometric system to weigh people who enter the room. The goal is to ensure that two or more people are not in the room and trying to get in on just one set of credentials.

389、 A .This task is identifying the critical path, which is defined as the path that is critical for business functionality. It should be shown in detail with all supporting mechanisms required for critical data flow. Redundant paths should be shown, and there should be at least one redundant path for every critical path. The critical path analysis lists all pieces of an environment and how they interact and are interdependent. Diagrams should be developed that show the devices and their place and relevance to a facility. The diagrams should include power, data, water, and sewer lines. Air conditioners, generators, and storm drains may also be included to provide a full description and understanding.

390、 B .The mean time to repair (MTTR) value is used to estimate how long it will take to repair the device and get it back into production. Service level agreements (SLAs) are legally binding guarantees that state a vendor will fix or replace a system within a specific time period.

391、 B .Online UPS systems respond more quickly than standby systems. This is because the primary source is connected to the online UPS, keeping its battery charged to its maximum level. When the primary source fails, the online system activates the battery to maintain the same level of energy as the primary power source for a period of time.

392、 B .A deluge sprinkler system offers the best solution for this company. It has open sprinkler heads, which allow for very large volumes of water to be released quickly.

393、 D .A UPS is a temporary power source intended to be a backup supply in the event of a power failure; thus, it does not address Jonathan’s ongoing problem of line noise. A surge protector can extract momentary extra line voltages to protect his system and data. A line conditioner uses a tap to look for lows and highs in voltage and compensates for them. What he really needs to do is move the cords and cables to other outlets to reduce line noise and the threat of fire—this is the least expensive solution.

394、 A .Different suppression agents affect the four legs of fire in various ways. Fuel and oxygen help feed fires and should be removed in order to successfully extinguish them with soda acid or CO2. High temperatures should be reduced by using water. Chemical reactions can be the product of fires and should be disrupted by using a type of gas (Halon, FM-200). Different

suppression agents attack one of these legs when combating a fire.

395、 D .Although having ultraviolet-protected windows could be an important consideration when choosing a facility, it is not as critical as the other issues. A storage company would be most concerned with intrusion detection systems to prevent theft and the combustibility of materials to prevent fire. Also, since this company stores heavy construction equipment, they need to account for the load bearings of floors, ceilings, and walls.

396、 C .Each device has a mean time between failure (MTBF) and a mean time to repair (MTTR). The MTBF estimate is used to determine the expected lifetime of a device or when an element within that device is expected to give out. The MTTR value is used to estimate the amount of time it will take to repair the device and get it back into production. These estimates can be used to calculate the risk of utility failure and evaluate other devices that may have better MTBF or MTTR values.

397、 C .Although some computers react differently, most will experience major damage when a temperature of 175 degrees Fahrenheit is reached. Some will have significant performance issues at lower temperatures but will not necessarily experience actual damage.

398、 D .The idea is that the material should flow out of the building and not into it. The positive drain principle is a protection mechanism.

399、 A .Ventilation ducts and utility tunnels can also be used by intruders and thus must be properly protected with sensors and access control mechanisms.

400、 D .The most common cloud service models are:

- Infrastructure as a Service (IaaS)—Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them.
- Platform as a Service (PaaS)—Cloud providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment. Whereas IaaS is the “raw IT network,” PaaS is the software environment that runs on top of the IT network.
- Software as a Service (SaaS)—Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network-based access to a single copy of an application created specifically for SaaS distribution and use.

401、 A .A concealment cipher, also called a null cipher, is a type of steganography method. Steganography is a way to hide a message, but not through an encryption process. The message is in cleartext and could be hidden in a message, graphic, or other method.

402、 D .The components that are involved with steganography:
The carrier file is a file that has information hidden inside of it.

The stego-medium is the medium in which the information is hidden.
The payload is the information that is to be concealed.
A graphic, document, or any type of file can be used as a carrier.

403、 D .The least significant bit (LSB) is the bit position in a binary integer. The LSB is sometimes referred to as the rightmost bit, due to the convention in positional notation of writing less significant digits further to the right. In the following bits 11111110, the LSB is 0.

404、 C .In the least significant bit (LSB) approach, graphics with a high resolution or an audio file that is of high quality are the best to hide information within. There is usually no noticeable distortion, and the file is usually not increased to a size that can be detected. So after the secret message is broken down into bits, each bit can be stored in the carrier file’s LSB, and it will likely go unnoticed.

405、 D .Instead of there being a secret message within a graphic that is supposed to be invisible to you, digital watermarks are usually visible. These are put into place to work as a deterrent for people so they cannot use some type of material that is not theirs. After you purchase the company’s graphic, for example, they will extract the embedded logo and allow you to use it. This type of steganography is referred to as Digital Rights Management (DRM). The goal is to help restrict the usage of material that is owned by a company or individual.

406、 B .For complex keys to be generated, a master key usually is created and then session keys are generated from it. The algorithm or function that is used for the generation of keys, which is made up of random values, is referred to as the Key Derivation Function (KDF). KDF allows for more complex keys to be generated and used.

407、 A .Rich needs to be concerned with the key life cycle. This includes the generation, distribution, storage, backup, and destruction of a key. If any part of this life cycle is compromised, the whole system could be compromised. While Company X may be using public and private keys, these keys should just follow the key life cycle. Public key infrastructure (PKI) is the infrastructure that is based on public key cryptography. Company X may be building out a PKI, but the keys generated will still follow the key life cycle.

408、 B .The process of changing plaintext to ciphertext is known as encryption. The process of changing ciphertext to plaintext is known as decryption. The process of creating a fixed length of unreadable text is known as hashing. The process of hiding information in a message or picture is known as steganography.

409、 B .Rich is ensuring the integrity of the e-mail. By creating a hash of the message and sending it with the message, the user can re-create the hash to validate the message hasn’t changed. Confidentiality is the process of ensuring that only those people who need to read the e-mail can read it. Availability is the process of ensuring that systems are functioning when people need them. Nonrepudiation is the process of ensuring that someone cannot refute the ownership of an action.

410、 C .A substitution cipher is the process of replacing characters with different characters or symbols. The process of rearranging characters is a transposition cipher. The process of hiding all the characters in a picture or message is steganography. Hashing is the process of using a one-way operation to create unreadable text.

411、 B .A transposition cipher is the process of rearranging the characters. A substitution cipher is the process of replacing characters with different characters or symbols. The process of hiding all the characters in a picture or message is steganography. Hashing is the process of using a one-way operation to create unreadable text.

412、 B .By creating a hash of the message and sending a copy with it, integrity can be provided. Once another user receives the message, he can create a hash of the message and verify it against the one that was sent. If the two hash values match, the message has not been changed. Since the message is not encrypted, it does not provide confidentiality. Hashing does not ensure that the data will be available when the user needs them.

413、 B .Secure Sockets Layer (SSL) provides data encryption over the Internet and works at the transport layer of the OSI model. Although it provides encryption while the message is being sent, it does not secure the data once they are received and decrypted. SSL uses public key encryption and was developed originally by Netscape. Along with encryption and message integrity, SSL ensures server authentication and optional client authentication.

414、B .AES was developed to improve upon DES's security and flexibility. It uses 128-, 192-, and 256-bit keys. Rijndael, a block symmetric cipher created by Vincent Rijmen and Joan Daemen, was selected as the new AES algorithm.

415、 C .In 1974, IBM created Lucifer, which would eventually become the Data Encryption Standard (DES). Lucifer was accepted, and the key size was reduced from 128 to 64 and renamed the Data Encryption Algorithm (DEA).

416、 A .Chosen-ciphertext attacks have the highest probability of the encryption being cracked compared to most other cryptanalysis attacks. In this type of attack, the intruder must capture a large portion of the ciphertext and then must be able to choose which parts of it are decrypted. That section of text is transformed into plaintext. The translation is then analyzed in an attempt to identify the key that was used in the encryption process.

417、 A .The Diffie-Hellman key exchange was created as a way of exchanging public keys and generating a session key without needing to set up a prior relationship. This technology does not handle any form of data encryption; rather, it is simply a method of exchanging keys. Diffie and Hellman created the first asymmetric algorithm.

418、 C .A trapdoor function is a one-way function that applies the concept of finding prime factors of large numbers. Public keys encrypt a message with a built-in, one-way function. This

function is referred to as one-way because it is relatively simple to encrypt, but much more difficult to decrypt without knowing the correct trapdoor. A private key, however, knows the code of the trapdoor, and is able to decrypt the message.

419、 C .Chosen-plaintext attackers have access to plaintext and the ciphertext that is generated. The attacker chooses which piece of plaintext is encrypted. The goal is to use the resulting ciphertext to uncover the key that was used in the encryption process.

420、 B .Substitution boxes, or S-boxes, are used within block ciphers. They use lookup tables to determine how a block of data is encrypted or decrypted. The key is used to decide which S-box to utilize with each block.

421、 D .Cryptanalysis is studied by different types of audiences. The science of breaking encryption algorithms and cryptosystems is an area of interest in both academic and commercial settings (ethical) and by curious or devious hackers (unethical).

422、 B .A collision occurs when two separate messages have the same hash value. This creates an opportunity for a potential hacker. Taking advantage of a collision is done through a “birthday attack.”

423、 A .Asymmetric cryptography, also referred to as public key cryptography, uses both public and private keys. It is used for key encryption and key distribution. Variable-length keys are used, and algorithms are much more complex than with symmetric cryptography. However, due to the complexity, asymmetric algorithms are slower than symmetric key encryption. While symmetric encryption provides only confidentiality and system authentication, asymmetric cryptography has added capabilities, such as user authentication and nonrepudiation.

424、 D .A collision is when two items have the same value but were not supposed to. In this domain, it pertains to when two different messages end up having the same message digest values. Two messages being passed through a hashing algorithm should result in different message digest values. The birthday attack takes advantage of the fact that these two values are the same. Hashing algorithms that have longer message digest values are less vulnerable to a birthday attack because they have more possible message digest values.

425、 B .Nonrepudiation means that someone cannot deny carrying out some type of activity once it has been completed. A private key is used to generate digital signatures to provide the receiver with a high level of assurance of the authenticity of the message and makes sure the sender cannot deny sending the message later. It works this way because the private key is bound to the individual’s identity, and it is that individual’s responsibility to ensure that no one else obtains that private key.

426、 C .Pretty Good Privacy (PGP) was the first widespread public key encryption program. It is a complete working system that uses cryptographic protection to protect e-mail and files. This application works on a different type of trust model than a PKI environment and uses its own

type of digital certificates. PGP can be integrated within a PKI, but is the best answer because the other three are core components of every PKI implementation. PGP is considered a cryptosystem, and PKI is an infrastructure. CA is certification authority, which issues the certificates. CRL is certification revocation list. RA is registration authority.

427、 D .Zero-knowledge proof means that someone can tell you something without telling you more information than you need to know. In cryptography, it means proving that you have a specific key without sharing that key or showing it to anyone.

428、 D .The symmetric key, or secret key, is used to encrypt the actual message, while the asymmetric key is used to encrypt the symmetric key. The key exchange protocol is responsible for the other key management issues.

429、 C .One-way hashing creates a fingerprint of the message so the function can more easily identify and monitor the message to see if it has been altered. It takes a variable-length string (the message) and generates a fixed-length value (message digest).

430、 B .Symmetric key systems are considerably faster than asymmetric key systems. However, they cannot provide nonrepudiation or authenticity and struggle with proper key distribution and controlling keys as more users need to communicate.

431、 B .RSA, named after its inventors. It is an asymmetric algorithm that can provide data encryption, key distribution, and digital signatures. It is a de facto standard in many types of products.

432、 B .Link encryption provides additional security by encrypting all the information. But for traffic to be routed or forwarded, all the routers, switches, and associated equipment must be configured to support this type of service. These intermediate devices need to decrypt a portion of the headers to make decisions on forwarding or routing.

433、 D .Key management includes the following: key generation and proper destruction, key storage and transmission, key secrecy, and key length. Most of these activities are taken care of by different protocols, but a security professional that is responsible for implementing and maintaining an encryption system should ensure that these tasks are actually being done properly. Improper key management is one of the biggest downfalls of encryption implementation and the easier target for attackers.

434、 C .X.509 is a standard that outlines the format of certificates that are used in a public key infrastructure (PKI). This standard dictates the fields and possible values that can be used in these certificates.

435、 A .Most passwords in environments are centrally stored for user authentication. Any password that is stored should not be stored in cleartext; rather, it should be encrypted or hashed. Passwords that are stored centrally are even more vulnerable because an attacker could

try to access all passwords to an environment. Passwords should be at least eight characters long. They should also be nondictionary words.

436、 A .A symmetric algorithm creates keys that are used for encrypting bulk data. When it is necessary to transport this encrypted bulk data and the associated symmetric key together, the symmetric key is encrypted with the receiver’s public key. The receiver decrypts the symmetric key with his private key and uses the symmetric key to decrypt the bulk data.

437、 C .The key allows for randomness in the encryption process. An algorithm is a set of mathematical formulas and logic structures. The algorithm uses the values of the key to integrate randomness in the output of these formulas and logic structures. Determining what you are trying to secure determines what algorithm will be used, not the key. The final length of information is based on more than just the algorithm.

438、 D .All of these need to be considered when implementing key management. If keys are not properly secured in storage and transport, they can fall into the hands of a malicious person, who would then have full access to the sensitive information. In addition, when a user leaves the company, it is important to destroy the key so that the information cannot be accessed at a later date. It is important to keep in mind that these are not the only considerations.

439、 A .AES, Advanced Encryption Standard, is the only symmetric cipher listed. DSA and Diffie-Hellman are common asymmetric ciphers.

440、 A .A TPM, trusted platform module, is needed in order to run BitLocker drive encryption. PKI is the public key infrastructure and is used to distribute certificates. IPsec is the protocol that creates a secure tunnel to send information across an insecure network. HTTPS is the protocol used to secure information on a web server.

441、 B .In cryptography, the reverse of security by obscurity is Kerckhoffs’ principle from the late 1880s, which states that system designers should assume that the entire design of a security system is known to all attackers, with the exception of the cryptographic key: “the security of a cipher resides entirely in the key.”

442、 B .The trusted platform module (TPM) is a microchip installed on the motherboard of modern computers and is dedicated to carrying out security functions that involve the storage and processing of symmetric and asymmetric keys, hashes, and digital certificates. The TPM was devised by the Trusted Computing Group (TCG), an organization that promotes open standards to help strengthen computing platforms against security weaknesses and attacks.

443、 A .TPM’s internal memory is divided into two different segments: persistent (static) and versatile (dynamic) memory modules:

- Persistent memory There are two kinds of keys present in the static memory: endorsement key (EK) and storage root key (SRK):
- The EK is a public/private key pair that is installed in the TPM at the time of manufacture

and cannot be modified. The private key is always present inside the TPM, while the public key is used to verify the authenticity of the TPM itself. The EK, installed in the TPM, is unique to that TPM and its platform.

- The SRK is the master wrapping key used to secure the keys stored in the TPM.
- Versatile memory There are three kinds of keys (or values) present in the versatile memory: attestation identity key (AIK), platform configuration register hashes (PCR), and storage keys:
- The AIK is used for the attestation of the TPM chip itself to service providers. The AIK is linked to the TPM’s identity at the time of development, which in turn is linked to the TPM’s endorsement key. Therefore, the AIK ensures the integrity of the EK.
- The PCR is used to store cryptographic hashes of data used for TPM’s “sealing” functionality.
- The storage keys are used to encrypt the storage media of the computer system.

444、 D .Meet-in-the-middle attack refers to a mathematical analysis used to try and break a math problem from both ends. It is a technique that works on the forward mapping of a function and the inverse of the second function at the same time. The attack works by encrypting from one end and decrypting from the other end, thus meeting in the middle.

第四章题目

1. Trunk lines are used in which one of the following scenarios?
   A. Remote office ISDN wiring for an employee
   B. Communication between two switches at a central office
   C. Internal wiring in a Token Ring architecture
   D. Communication between terminals for different classes of traffic
2. Different types of Internet connection technologies have different characteristics. Which of the following is an "always on" technology?
   A. Basic Rate Interface (BRI)
   B. Primary Rate Interface (PRI)
   C. Dial-up
   D. Digital Subscriber Line (DSL)
3. Which is not true about Trivial File Transfer Protocol (TFTP)?
   A. Has a smaller subset of commands compared to File Transfer Protocol (FTP)
   B. Has less functionality than File Transfer Protocol (FTP)
   C. Could allow any user read and write privileges
   D. Encrypted passwords provide the only form of security
4. Because the Address Resolution Protocol (ARP) does not perform authentication, it is vulnerable to what kind of attacks? (Two answers)
   A. Table poisoning
   B. Masquerading
   C. DoS
   D. Birthday
5. What protocol protects the Internet Protocol (IP) header as well as the upper-layer protocol

headers above IP?

A. Reverse Address Resolution Protocol (RARP)

B. Internet Protocol Security (IPSec)

C. Fiber Distributed Data Interface (FDDI)

D. Serial Line Internet Protocol (SLIP)

6. An IT administrator who secures a communication channel through an untrusted network by configuring firewall software has just implemented a _____.

A. Public-switched telephone network (PSTN)

B. Virtual public network

C. Virtual private network

D. Bastion host

7. When a router modifies an unregistered IP address of a computer into a registered IP address to send out through an external link, it is performing _____.

A. Network address translation

B. Polling

C. Address Resolution Protocol

D. Multiplexing

8. Which polling protocol is used mainly to communicate with IBM mainframe systems?

A. Primary Data Link Control (PDLC)

B. Synchronous Data Link Control (SDLC)

C. Switched MultiMegabits Data Service (SMDS)

D. X.25

9. HDLC improves upon SDLC in what ways? (Choose two answers)

A. Works over asynchronous lines

B. Is bit-oriented

C. Provides a higher throughput

D. Supports full-duplex transmissions

10. A SONET architecture at a large university connecting internal networks in each building is an example of what?

A. WAN

B. LAN

C. MAN

D. Extranet

11. The Internet Protocol (IP) has gone through different generations. IP version 6 is being slowly deployed in the US and more quickly in Asia. IP version 6 has how many address bits?

A. 16

B. 32

C. 64

D. 128

12. A corporate vice president routinely using his office phone for personal international phone calls is an example of what security issue?

A. Telephone fraud

B. Telephone phreaking

C. Winnuke attacking

D. Land attacking

13. All of the following are true statements about bastion hosts except which one?

A. Locked-down systems

B. Often the first device to be tampered with by hackers

C. Contains no third-party applications

D. Protected by the DMZ and has internal user accounts

14. Many types of perimeter devices are critical to protecting a company and its assets. Which of the following is not an example of a firewall?

A. TCP Wrapper

B. A packet-filtering router

C. Proxy server

D. A repeater

15. Internet Protocol Security (IPsec) is actually a suite of protocols. Each protocol within the suite provides different functionality. Collectively IPsec does everything except _____.

A. Encrypt

B. Work at the data link layer

C. Authenticate

D. Protect the payload and the headers

16. A dumb terminal that broadcasts requests to find its network configurations and operating system when booting up is using what protocol?

A. Address Resolution Protocol (ARP)

B. Internet Protocol Security (IPSec)

C. Reverse Address Resolution Protocol (RARP)

D. Layer 2 Tunneling Protocol (L2TP)

17. Which of the following protocol resolves IP addresses to hardware addresses?

A. Address Resolution Protocol (ARP)

B. Reverse Address Resolution Protocol (RARP)

C. BOOTP

D. Polling

18. An Ethernet environment that connects local systems and resources in a small area is a(n) _____.

A. Wide area network

B. Metropolitan area network

C. Local area network

D. Extranet

19. When trying to determine connectivity with a newly installed device, Katie sends out a PING command. What protocol has she utilized?

A. Address Resolution Protocol (ARP)

B. Internet Control Message Protocol (ICMP)

C. Reverse Address Resolution Protocol (RARP)

D. Line Printer Daemon (LPD)

20. Which of the following TCP protocols typically works on ports 20 and 21?

A. Telnet

B. Hypertext Transfer Protocol (HTTP)

C. File Transfer Protocol (FTP)

D. Simple Network Management Protocol (SNMP)

21. Telnet is a commonly used protocol that works at the application layer of the OSI model. Telnet is used in all of the following ways except which one?

A. Network monitoring and polling

B. Remote login capabilities

C. To establish command prompts on remote devices

D. To execute commands on a remote system

22. There are several different types of DSL technologies. Each provides specific characteristics to best fit individual customer needs. Asymmetric DSL means which of the following?

A. The service is comparable to dial-up.

B. Downstream traffic flows faster than upstream traffic.

C. Upstream traffic flows faster than downstream traffic.

D. Both streams of traffic flow at the same speed.

23. A communication medium consisting of interwoven, insulated copper wires is called _____.

A. Twisted pair

B. Coaxial

C. Fiber

D. Ethernet

24. Which of the following is a "best effort" protocol requiring fewer resources than other transport protocols?

A. IP

B. UDP

C. TCP

D. ARP

25. Different network devices work at specific OSI model layers because they carry out different types of functionality. A bridge works on which OSI layer?

A. Physical

B. Application

C. Data link

D. Network

26. More advanced bridges can work at more than one layer at a time to carry out more robust functionality. Which of the following describes the two OSI model layers where a bridge can work?

A. Network and application

B. Physical and data link

C. Data link and network

D. Physical and transport

27. Which protocol is described as a "best effort" protocol?

A. TCP

B. SPX

C. UDP

D. ARP

28. Which of the following best describes TCP versus UDP protocol?

A. TCP provides more services and is more reliable, but UDP provides more security services.

B. TCP provides a best-effort delivery, and UDP sets up a virtual connection with the destination.

C. TCP is reliable and UDP deals with flow control and ACKs.

D. TCP provides more services and is more reliable in data transmission, whereas UDP takes less resources and overhead to transmit data.

29. Which of the following firewall types keeps track of each ongoing dialogue between internal and external systems?

A. Packet filtering

B. Circuit-level proxy

C. Stateful

D. Application-level proxy

30. Thin Net is another name for what type of Ethernet implementation?

A. 10Base-T

B. Gigabyte Ethernet

C. Fiber

D. 10Base2

31. Which of the following tunneling protocols would be used if tunneled communication needed to take place over X.25, ATM, or frame relay?

A. PPTP

B. L2TP

C. IPSec

D. PPP

32. What is the name of the network topology in which all computers are connected together in a non-uniform formation?

A. Mesh

B. Ring

C. Star

D. Bus

33. What architecture type is used when an external router is used to filter traffic before it enters the network and another screening device is used to monitor traffic before it enters the internal network?

A. Screened-host

B. Screened-subnet

C. Dual-homed firewall

D. Dual subnets

34. Which of the following is not true of application-level proxy firewalls?

A. Provides a higher level of protection than circuit-level firewalls.

B. Hides network information from external entities.

C. One proxy per service is needed.

D. Improves network performance.

35. A network segment located between the protected and unprotected network is called what?

A. Honeypot

B. Safe zone

C. DMZ

D. VPN

36. In which of the following areas do application-based proxy firewalls have an advantage over packet-filtering firewalls?

A. Application independence

B. Scalability

C. Security

D. Performance

37. Which of the following protocols replaced SLIP?

A. IPSec

B. L2TP

C. L2F

D. PPP

38. Packets containing routing information within their headers is a technique referred to as what?

A. Broadcasting

B. Source routing

C. Forwarding

D. Poisoning

39. What device works at the physical layer to amplify electrical signals between network segments?

A. Switch

B. Router

C. Repeater

D. Gateway

40. All computers are connected to a central device in which of the following topologies?

A. Star

B. Bus

C. Mesh

D. Tree

41. ARP broadcasts messages on the network to find what?

A. IP address

B. MAC address

C. Router

D. Hostname

42. Which of the following technologies uses fiber-optic rings to connect different networks and is a MAN technology?

A. ATM

B. Token Ring

C. FDDI

D. Frame relay

43. What is the central hub called in a Token Ring network?

A. Star
B. MAU
C. PBX
D. MUA

44. What is the maximum cable length of 10Base2?
A. 500 meters
B. 185 meters
C. 85 meters
D. 100 meters

45. Ethernet uses what type of access method?
A. CSMD
B. Polling
C. CSMA
D. Token passing

46. Which of the following is not true of circuit-switched networks?
A. Acts as a dedicated virtual connection
B. Connection-oriented
C. Usually carries voice traffic
D. Variable delays

47. In which technology do different users share the same network medium?
A. DSL
B. Cable modem
C. Dial-up
D. ISDN

48. How many bearer channels does a BRI ISDN service have?
A. 23
B. 24
C. 2
D. 1

49. A WAN technology that uses 53-byte cells and has low delay levels is called what?
A. ATM
B. Frame relay
C. X.25
D. SMDS

50. The loss of signal strength as it travels is called what?
A. Cross-talk
B. Attenuation
C. Noise
D. Preamble

51. In twisted pair cabling, the tighter the wire is twisted, the more resistant the cable is to what?
A. Attenuation and breaking
B. Causing fire hazards
C. Interference and attenuation
D. Corrosion

52. A telephone switch located on a company's property with a direct connection to the phone company's central office is called _____.

A. Hub

B. PBX

C. Router

D. BPX

53. What is a one-to-many transmission called?

A. Multicast

B. Broadcast

C. Unicast

D. Simplex

54. Router work at which OSI layer?

A. Data link

B. Session

C. Transport

D. Network

55. Backbones that connect businesses to WANs, the Internet, and other businesses usually via SONET networks are called what?

A. MANs

B. WANs

C. VPNs

D. VLANs

56. Which of the following devices typically works at the application layer and acts as a protocol translator for different environments?

A. Switch

B. Gateway

C. Bridge

D. Switch

57. Which of the following hides internal addresses by centralizing them on one router and then forwarding only the source address of that router?

A. DNS

B. CHAP

C. NAT

D. IPSec

58. Which is a physical layer standard for transmitting data over fiber-optic lines?

A. SDD

B. SONET

C. Frame relay

D. X.25

59. Which of the following can provide up to 45 Mbps of bandwidth?

A. BRI

B. T3

C. T1

D. M1

60. A high-speed technology that is "always on" and can provide data rates up to 52 Mbps (using line of 1000 feet or less for high speed) is called what?

A. DSL

B. ISDN

C. Dial-up

D. CHAP

61. Which statement is not true of a dedicated line?

A. More secure than using public networks

B. Connects two locations

C. Inflexible and expensive

D. Uses packet-switching technology

62. Paying for a guaranteed amount of frame relay bandwidth is called what?

A. CIR

B. SVC

C. QoS

D. LIN

63. Which of the following is a real threat in wireless communication?

A. Encryption is not available in wireless technologies.

B. Users cannot be authenticated as they move from one AP to another.

C. No data integrity can be performed as users move from one AP to another.

D. Eavesdropping can uncover traffic analysis, and AP and station location can be uncovered.

64. What cannot be accomplished by a man-in-the-middle attack?

A. Digital signature

B. Masquerading

C. Session hijacking

D. Spoofing

65. How does PPTP provide protection?

A. Through encryption

B. Through encapsulation

C. Through encryption and encapsulation

D. Through CHAP and AEP

66. How does a SOCKS-based firewall provide protection?

A. By providing one proxy per protocol

B. By acting as a proxy

C. By denying any access attempts from internal entities

D. By inspecting protocol commands

67. Which of the following is the best definition of a socket?

A. A session layer link

B. A MAC address and a port number

C. An IP address and a port number

D. An IP address and a MAC address

68. Which firewall makes access decisions based only on addresses and port numbers?

A. Circuit-based proxy

B. Application-based proxy

C. Stateful

D. Dual-homed

69. Which of the following is required for LAN- and WAN-centralized access control technologies?

A. Single point of failure

B. RADIUS and TACAS+

C. System with database of authentication information

D. Connection to ISP

70. Which of the following is a reason companies implement routers and packet filters?

A. To provide content filtering

B. To provide protection that is transparent to users

C. To provide circuit-based proxy protection

D. To provide application-based proxy protection

71. Which of the following best describes the issue of an ARP attack?

A. Proper IP to MAC address translation does not take place, which causes masquerading.

B. Two IP addresses and two MAC addresses are used.

C. A RARP service is poisoned via DNS resource records.

D. An ARP table is completely deleted.

72. Why are network sniffers dangerous to an environment?

A. They can be used to launch active attacks.

B. Their presence can cause many false positives.

C. Their presence and activities are not auditable.

D. They can access sensitive data within applications.

73. Which layer of the OSI reference model deals with providing end-to-end data transmissions between systems?

A. Network

B. Data link

C. Transport

D. Session

74. Which of the following is a good definition of asynchronous communication?

A. Low data transfer rate using only one channel for transmission

B. High data transfer using many channels

C. High-speed transmission controlled by electronic timing signals

D. Sequential data transfer, using bits framed with start and stop bits

75. Which of the following protocols does not map to the transport layer of the OSI model?

A. Transmission Control Protocol

B. Sequenced Packet Exchange

C. User Datagram Protocol

D. Internetwork Packet Exchange

76. Which of the following is a LAN transmission technology that is susceptible to collisions and provides a mechanism for retransmission?

A. Ethernet

B. Token Ring

C. ATM

D. FDDI

77. Which of the following could be considered an advantage of token passing over carrier sensing multiple access (CSMA) media access technologies?

A. Collision increase

B. Collision detection

C. Lack of collisions

D. Primary device coordinates transmission with secondary devices

78. Which of the following does not cause signal attenuation?

A. Asynchronous signals

B. Cable malfunctions

C. Cable breaks

D. Length of the cable

79. Which of the following devices does not pass broadcast information?

A. Repeater

B. Router

C. Switch

D. Bridge

80. What is a function of a state table on a firewall?

A. To provide virus detection

B. To ensure that all requests are acceptable to the security policy

C. To filter based on user identification

D. To improve performance

81. Which one of the following is not a primary component or aspect of firewall systems?

A. Protocol filtering

B. Packet switching

C. Rule enforcement engine

D. Extended logging capability

82. Which of the following is not true about an application-based proxy firewall?

A. Better performance than non-proxy firewalls

B. Can work on all seven OSI layers

C. Obscures the sender's address from the receiver

D. May be on a dual-homed device

83. Which of the following is not true about ISDN?

A. Requires both B and D channels

B. Supports voice, video, and data transmission

C. Sends control information over the B channel

D. Uses the same wires as analog transmission

84. Which of the following is a disadvantage of PPTP?

A. Works only over IP

B. Will not work over a NAT server

C. Does not provide encryption

D. Does not provide for authentication

85. What is the difference between CSMA/CD and CSMA/CA?

A. CA listens to the wire to detect when it would be best to send data.

B. CD sends out a message to all other computers indicating that it is going to send data.

C. CA sends out a message to all other computers indicating that it is going to send data.

D. A computer cannot communicate without a token.

86. Which of the following is not a layer in the TCP/IP model?

A. Application

B. Session

C. Internet

D. Network access

87. What does the "gap in the WAP" problem address?

A. Not requiring a wireless device to prove it has a cryptographic key for authentication

B. The security flaws of WEP

C. Translation between WTLS and SSL

D. Authentication flaws between the wireless devices and the AP

88. What is the difference between the 802.11a and 802.11b standards?

A. 802.11a works in the 5 GHz range and provides a faster data transfer speed than 802.11b.

B. 802.11a works in the 2.4 GHz range and provides a faster data transfer speed than 802.11b.

C. 802.11b works in the 5 GHz range and provides a faster data transfer speed than 802.11a.

D. 802.11b works in the 2.4 GHz range and provides a faster data transfer speed than 802.11a.

89. What is the difference between open system authentication (OSA) and shared key authentication (SKA)?

A. SKA requires the correct SSID value and IP address.

B. OSA requires a WEP encryption key.

C. SKA requires a WEP encryption key.

D. OSA requires a correct MAC and IP address.

90. Which of the following is true about a SSID value?

A. It is a value that can be used to create a VPN connection between the wireless device and the AP.

B. It is a security mechanism that provides strict protection for wireless transmissions.

C. It is a value that the AP uses to authenticate to the gateway.

D. It is a value that the wireless device uses to authenticate to the AP.

91. What does 802.11i represent?

A. A standard that has been developed to allow European countries to use products that work in the 2.4 GHz range

B. Standard that specifies security mechanisms for wireless networks

C. A working group that is currently working on the interoperability between 802.11a and 802.11b

D. A standard that increase data transfer rates to 54 Mbps

92. The application layer in the TCP/IP model equates to what layer in the OSI model?

A. Application

B. Session, transport, application

C. Application, session, presentation

D. Application, session, transport

93. Not every data transmission incorporates the session layer. Which of the following best describes the functionality of the session layer?

A. End-to-end data transmission

B. Application client\server communication mechanism in a distributed environment

C. Application to computer physical communication

D. Provides application with the proper syntax for transmission

94. In the TCP/IP model, where does the SPX protocol reside?

A. Host-to-host

B. Internet

C. Network access

D. Application

95. In the TCP/IP model, where does the BGP protocol reside?

A. Host-to-host

B. Internet

C. Network access

D. Application

96. The OSI data link layer is broken down into two sub-layers. Which of the following are the correct IEEE standards for these sub-layers?

A. 802.1 and 802.2

B. 802.3 and 802.4

C. 802.3 and 802.5

D. 802.2 and 802.3

97. In the TCP/IP model, where does the PPP protocol reside?

A. Host-to-host

B. Internet

C. Network access

D. Application

98. What is the purpose of the Logical Link Control (LLC) layer in the OSI Model?

A. Provides a standard interface for the network layer protocol

B. Provides the framing functionality of the data link layer

C. Provides addressing of the packet during encapsulation

D. Provides the functionality of converting bits into electrical signals

99. What is the port range for "well-known ports?"

A. 0 – 1024

B. 1 – 65,565

C. 1 – 1023

D. 0 – 1023

100. What is the purpose of classless interdomain routing (CIDR)?

A. To allow for the traditional classes to be used more efficiently

B. To extend the IP address space to 128-bit in size

C. To provide more security for the network traffic

D. To all for more efficient routing

101. What is the purpose of a packet Time to Live (TTL)?

A. To protect against source routing

B. To ensure that a packet does not continue to be routed forever

C. To ensure that a packet contains the correct transport header information

D. To protect against Loki attacks

102. Which of the following is not true of IPng?

A. Uses a 128-bit addressing space

B. IPSec is incorporated into the protocol

C. Requires NAT

D. Contains auto-configuration functionality

103. Why is it easier for a repeater to "clean up" a digital signal versus an analog signal?

A. An analog signal can have an infinite number of states.

B. An analog signal discretely represents binary values.

C. The encoding process is legacy.

D. Digital signals are more fragile than analog signals.

104. What is a beaconing functionality in a token passing technology?

A. Ensures that a fault domain never occurs

B. Ensures that only one frame is on the network at a time

C. Allows the computers to communicate to each other through the token

D. Excludes a misbehaving computer from the ring

105. How are FDDI and FDDI-2 different?

A. FDDI-2 provides higher bandwidth.

B. FDDI-2 allows for fixed bandwidth to be assigned.

C. FDDI-2 works over fiber.

D. FDDI-2 is an actual standard, where FDDI is a de facto standard.

106. What is the importance of using plenum-rated cabling in buildings?

A. They are noncombustible.

B. Human safety

C. They increase speed and bandwidth.

D. They are made out of polyvinyl chloride.

107. Claude has been told that he needs to integrate IGMP into the corporation routers. What type of functionality does the company want to allow?

A. Exterior routing

B. Interior routing

C. Instant messaging

D. Multicasting

108. Which of the following is a characteristic of a token passing technology?

A. Chatty

B. Deterministic

C. Collision-oriented

D. Burst-like

109. Kevin has seen an increase in ICMP traffic going towards the company's web server. It has not been a lot of ICMP traffic, so he is not sure if he should be concerned or not. What is a possible attack that could be going on?

A. Fraggle

B. DoS

C. Birthday

D. Loki

110. Which of the following is not a characteristic of a multilayered switch?

A. QoS

B. High-speed routing

C. Can use MPLS

D. Works only at the data link layer

111. Trunk lines are used in which of the following scenarios?

A. Remote office ISDN wiring for an employee

B. Communication between two switches at a central office

C. Internal wiring in a Token Ring architecture

D. Communication between terminals for different classes of traffic

112. There are different types of Internet connection technologies with different characteristics. Which of the following is an "always-on" technology?

A. BRI

B. PRI

C. Dial-up

D. DSL

113. What protocol protects the IP header as well as the upper-layer protocol headers above IP?

A. RARP

B. IPSec

C. FDDI

D. SLIP

114. Which polling protocol is used mainly to communicate with IBM mainframe systems?

A. PDLC

B. SDLC

C. SMDS

D. X.25

115. A Synchronous Optical Networking (SONET) architecture at a large university used to connect internal networks in each building is an example of what?

A. WAN

B. LAN

C. CAN

D. Extranet

116. Which of the following resolves IP addresses to hardware addresses?

A. ARP

B. RARP

C. BOOTP

D. Polling

117. An Ethernet environment that connects local systems and resources in a small area is a(n) _____.

A. Wide area network

B. Metropolitan area network

C. Local area network

D. Extranet

118. When trying to determine connectivity with a newly installed device, Katie sends out a ping command. What protocol has she utilized?

A. ARP

B. ICMP

C. RARP

D. LPD

119. There are several different types of DSL technologies. Each provides specific characteristics to best fit individual customer needs. Asymmetric DSL means which of the following?

A. The service is comparable to dial-up.

B. Downstream traffic flows faster than upstream traffic.

C. Upstream traffic flows faster than downstream traffic.

D. Both streams of traffic flow at the same speed.

120. A communication medium consisting of interwoven, insulated copper wires is called _____.

A. Twisted pair

B. Coaxial

C. Fiber

D. Ethernet

121. Ethernet uses what type of access method?

A. CSMD

B. Polling

C. CSMA

D. Token passing

122. What cannot be accomplished by a man-in-the-middle attack?

A. Digital signature

B. Masquerading

C. Session hijacking

D. Spoofing

123. The application layer in the TCP/IP model equates to what layer in the OSI model?

A. Application

B. Session, transport, application

C. Application, session, presentation

D. Application, session, transport

124. In the TCP/IP model, where does the BGP protocol reside?

A. Host to host

B. Internet

C. Network access

D. Application

125. The OSI data link layer is broken down into two sublayers. Which of the following are the correct IEEE standards for these sublayers?

A. 802.1 and 802.2

B. 802.3 and 802.4

C. 802.3 and 802.5

D. 802.2 and 802.3

126. In the TCP/IP model, where does the PPP protocol reside?

A. Host to host

B. Internet
C. Network access
D. Application

127. What is the port range for “well-known ports”?
A. 0 – 1024
B. 1 – 65,565
C. 1 – 1023
D. 0 – 1023

128. What is the purpose of classless interdomain routing (CIDR)?
A. To allow for the traditional classes to be used more efficiently
B. To extend the IP address space to 128 bits in size
C. To provide more security for the network traffic
D. To allow for more efficient routing

129. What is the purpose of a packet’s time to live (TTL)?
A. To protect against source routing
B. To ensure that a packet does not continue to be routed forever
C. To ensure that a packet contains the correct transport header information
D. To protect against Loki attacks

130. Which of the following is not true of Ipng?
A. Uses a 128-bit addressing space
B. IPSec is incorporated into the protocol
C. Requires NAT
D. Contains auto-configuration functionality

131. Why is it easier for a repeater to “clean up” a digital signal versus an analog signal?
A. An analog signal can have an infinite number of states.
B. An analog signal discretely represents binary values.
C. The encoding process is legacy.
D. Digital signals are more fragile than analog signals.

132. How are FDDI and FDDI-2 different?
A. FDDI-2 provides higher bandwidth.
B. FDDI-2 allows for fixed bandwidth to be assigned.
C. FDDI-2 works over fiber.
D. FDDI-2 is an actual standard, whereas FDDI is a de facto standard.

133. What is the importance of using plenum-rated cabling in buildings?
A. They are noncombustible.
B. Human safety
C. They increase speed and bandwidth.
D. They are made out of polyvinyl chloride.

134. Mark has been told that he needs to integrate IGMP into the corporate routers. What type of functionality does the company want to allow?
A. Exterior routing
B. Interior routing
C. Instant messaging
D. Multicasting

135. Which of the following is a characteristic of a token-passing technology?

A. Chatty

B. Deterministic

C. Collision oriented

D. Burst-like

136. Kevin has seen an increase in ICMP traffic going toward the company’s web server. It has not been a lot of ICMP traffic, so he is not sure if he should be concerned or not. What is a possible attack that could be going on?

A. Fraggle

B. DoS

C. Birthday

D. Loki

137. Which of the following is not a characteristic of a multilayer switch?

A. QoS

B. High-speed routing

C. Can use MPLS

D. Works only at the data link layer

138. Which of the following best describes why classless interdomain routing (CIDR) was created?

A. To allow IPv6 traffic to tunnel through IPv4 networks

B. To allow IPSec to be integrated into IPv4 traffic

C. To allow an address class size to meet an organization’s need

D. To allow IPv6 to tunnel IPSec traffic

139. It is important to have a mechanism in place that ensures that network packets that do not get to a destination system do not transverse networks continuously. Which of the following best describes this mechanism?

A. Time to live

B. Subnet

C. IP address header

D. Trailer

140. The new version of IPv4 provides more scalability control for multicast routing. Which of the following best describes how this functionality is provided?

A. Scope filed

B. Autoconfiguration

C. Increased address space

D. Integrated tunneling

141. In IPv6 the packet payload value has been increased compared to the IPv4 packet payload. Which of the following best describes why this value was increased for the new protocol version?

A. IPv4 limits packets to 65,536, which does not match the new MAN maximum transmission unit requirements.

B. Improve network performance for network links that vary in maximum transmission unit requirements.

C. The maximum transmission unit requirements for wireless transmissions have increased as bandwidth demand has increased.

D. The maximum transmission unit requirements for cellular transmissions have increased as

bandwidth demand has increased.

142. Hanna is a new security manager for a computer consulting company. She has found out that the company has lost intellectual property in the past because malicious employees installed rogue devices on the network, which were used to capture sensitive traffic. Hanna needs to implement a solution that ensures that only authorized devices are allowed access to the company network. Which of the following IEEE standards was developed for this type of protection?

A. IEEE 802.1AR

B. IEEE 802.1AE

C. IEEE 802.1AF

D. IEEE 802.1XR

143. Which of the following best describes a technology that allows for variable-length subnet masking to increase the efficiency of IP address ranges?

A. Subnet addressing

B. Classless interdomain routing

C. Autoconfiguration

D. Max supersubnetting

144. Jacob is a network engineer and needs to ensure that each critical network device that is configured with an IPv6 address can communicate with other devices using IPv6 addresses, even if their traffic has to transverse IPv4 networks. Which of the following best describes what Jacob should configure for this need?

A. IPv4 forwarding

B. 6to4

C. IPv6 routing

D. IP submasking

145. A telecommunication technology can use baseband or broadband transmission techniques. Which of the following best describes the difference between these two transmission types?

A. A broadband technology uses the entire communication channel for its transmission, whereas a baseband technology divides the communication channel into individual and independent channels.

B. Broadband provides a higher level of security at the protocol level, and baseband provides a higher level of performance at the data link level.

C. Baseband provides a higher level of security at the protocol level, and broadband provides a higher level of performance at the data link level.

D. A baseband technology uses the entire communication channel for its transmission, whereas a broadband technology divides the communication channel into individual and independent channels.

146. Elena is a network administrator for a company that monitors international e-commerce transactions. She has found out that someone has been able to install rogue devices on the company’s network for malicious purposes. Which of the following technologies would be best for Elena to install to prevent rogue devices from being able to actively participate in network functionality?

A. Device callback system

B. Public key infrastructure

C. DHCP snooping

D. RADIUS

147. The Simple Network Management Protocol (SNMP) has two main components which provide very specific tasks. Which of the following best describes these two components and their purposes?

A. The manager is the server portion, which polls different devices to check status information and provides a centralized place to hold all network-wide information. The agent has a list of objects that it is to keep track of for a specific device.

B. The agent is the server portion, which polls different devices to check status information and provides a centralized place to hold all network-wide information. The server has a list of objects that it is to keep track of for a specific device.

C. The manager is the server portion, which protects different devices centrally. The agent protects individual devices locally.

D. The manager is the server portion, which protects network-based traffic. The agent protects individual devices locally and maintains a state table.

148. The SNMP uses community string values, which should be properly protected. Which of the following best describes the role of a community string in this context?

A. A subnet mask value used to segregate network devices

B. A password a manager uses to request data from the agent

C. A value used by a session key for randomized network traffic encryption

D. A value used for device-based authentication

149. A DNS resolver can send out a non-recursive query or a recursive query to a specific DNS server. Which of the following best describes the difference between these two query types?

A. A recursive query means that the request just goes to that specified DNS server, and either the answer is returned to the resolver or an error is returned. A non-recursive query means that the request can be passed on from one DNS server to another one until the DNS server with the correct information is identified.

B. A non-recursive query means that the request goes to that specified PKI server, and either the answer is returned to the resolver or an error is returned. A recursive query means that the request can be passed on from one DNS server to another one until the DNS server with the correct information is identified.

C. A non-recursive query means that the request just goes to that specified DNS server, and either the answer is returned to the resolver or an error is returned. A recursive query means that the request can be passed on from one DNS server to another one until the PKI server with the correct information is identified.

D. A non-recursive query means that the request just goes to that specified DNS server, and either the answer is returned to the resolver or an error is returned. A recursive query means that the request can be passed on from one DNS server to another one until the DNS server with the correct information is identified.

150. _____ is the process of replicating the databases containing the DNS data across a set of DNS servers.

A. DNSSEC synchronization

B. DNS zone transfer

C. DNS synchronization

D. DNS replication

151. _____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attack types.

A. Resource records

B. Zone transfer

C. DNSSEC

D. Resource transfer

152. Jack is a network administrator who needs to be able to specify which systems can send e-mail through his company's mail servers. Which of the following best describes the solution that would provide this type of functionality?

A. SMTP authentication

B. TLS within a PKI

C. Sender policy framework

D. SMTP and IMAP authentication framework

153. _____ allows for high performance on telecommunications networks by using short path labels instead of network addresses, thus avoiding the use of complex routing tables.

A. Multiprotocol label switching

B. ARP-based table routing

C. ATM cell switching

D. Frame-based relay routing

154. John has uncovered a rogue system on the company network that emulates a switch. The software on this system is being used by an attacker to modify frame tag values. Which of the following best describes the type of attack that has most likely been taking place?

A. DHCP snooping

B. VLAN hopping

C. Network traffic shaping

D. Network traffic hopping

155. Which of the following best describes the Spanning Tree Protocol?

A. A network protocol that ensures a loop-free topology for any bridged Ethernet LAN

B. A networking technology that directs data from one network node to the next based on short path labels

C. The protocol that carries out core routing decisions on the Internet

D. A routing protocol used in packet-switching networks where each router constructs a map of the connectivity within the network

156. Which of the following best describes why packet-filtering firewalls cannot protect against application-specific attacks?

A. Keeps a state table on each protocol communication dialog

B. Reviews only packet header and trailer data

C. No firewall type can access application-layer data within packets

D. Cannot maintain state data

157. Which of the following best describes the difference between a virtual firewall that works in bridge mode versus one that is embedded into a hypervisor?

A. Bridge-mode virtual firewall allows the firewall to monitor individual traffic links, and hypervisor integration allows the firewall to monitor all activities taking place within a host system.

B. Bridge-mode virtual firewall allows the firewall to monitor individual network links, and hypervisor integration allows the firewall to monitor all activities taking place within a guest system.

C. Bridge-mode virtual firewall allows the firewall to monitor individual traffic links, and hypervisor integration allows the firewall to monitor all activities taking place within a guest system.

D. Bridge-mode virtual firewall allows the firewall to monitor individual guest systems, and hypervisor integration allows the firewall to monitor all activities taking place within a network system.

158. _____ is the combining of server, storage, and network capabilities into a single framework.

A. Super computers

B. Converged infrastructure

C. Enterprise architecture

D. CORBA

159. Metropolitan area network (MAN) architectures are commonly built upon the following layers: access, aggregation/distribution, metro, and core. Which of the following best describes these different layers?

A. Core devices exist at customer’s premises, which connect the customer’s equipment to the service provider’s network. The service provider’s distribution network aggregates the traffic and sends it to the provider’s access network. From there, the traffic is moved to the next aggregation network that is closest to the destination.

B. Access devices exist at customer’s premises, which connect the customer’s equipment to the service provider’s network. The service provider’s distribution network aggregates the traffic and sends it to the provider’s core network. From there, the traffic is moved to the next aggregation network that is closest to the destination.

C. Core devices exist at customer’s premises, which connect the customer’s equipment to the service provider’s network. The service provider’s access network aggregates the traffic and sends it to the provider’s core network. From there, the traffic is moved to the next core network that is closest to the destination.

D. Access devices exist at customer’s premises, which connect the customer’s equipment to the service provider’s network. The service provider’s core network aggregates the traffic and sends it to the provider’s aggregation network. From there, the traffic is moved to the next aggregation network that is closest to the destination.

160. High-speed fiber-optic connections are measured based upon their transmission rates, which are defined by rate of the bit stream of the digital signal. Which of the following best describes the measurement unit used for this purpose?

A. Optical carrier

B. Bits per second

C. Bytes per second

D. Transmission units

161. Which of the following is a type of multiplexing in which two or more bit streams or signals are transferred, apparently simultaneously, as subchannels in one communication channel, but are physically taking turns on the single channel?

A. Time-division multiplexing

B. Wave-division multiplexing

C. Frequency-division multiplexing

D. Statistical time-division multiplexing

162. Greg is a network administrator for a government agency. The agency has deployed several time-sensitive applications that cannot tolerate latency. Which of the following functionalities should Greg ensure the agency’ s new network products provide?

A. Maximum tolerable downtime

B. Traffic shaping

C. Bandwidth throttling

D. Rate limiting

163. The Point-to-Point Protocol (PPP) has a Link Control Protocol (LCP) and a Network Control Protocol (NCP). Which of the following best describes these two subprotocol components?

A. LCP establishes, configures, and maintains the connection, and NCPs are used for network layer protocol configuration and provide user authentication capabilities through PAP, CHAP, and EAP protocols.

B. LCP allows for user authentication capabilities through PAP, CHAP, and EAP protocols, and NCPs establish, configure, and maintain the connection.

C. They both allow for user authentication capabilities through PAP, CHAP, and EAP protocols and network configuration.

D. LCP allows for device authentication capabilities through PAP, CHAP, and EAP protocols, and NCPs establish, configure, and maintain the connection.

164. In traditional telephone networks the Signaling System 7 (SS7) protocol sets up and breaks down call sessions and provide phone-line features, as in generating busy signals, phone dialing, and causing a phone to ring. Which protocol provides this type of functionality in a VoIP network?

A. Voice over Quality of Service

B. Session initiation protocol

C. Session management protocol

D. Voice Quality of Service protocol

165. The U.S. government agencies commonly use an encryption device that is based upon IPsec, which allows for secure end-to-end connectivity in heterogeneous environments. Which of the following best describes this device type?

A. High Assurance Internet Protocol Encryptor

B. High Confidentiality Internet Protocol Device

C. High Assurance Protection Device

D. High Confidentiality and Assurance Protection Device

166. John is a security network administrator who needs to ensure the correct VPN solutions are deployed in the right areas of the network and for the right purposes. Which of the following is an incorrect reason to deploy the associated technology?

A. PPTP is used when a PPP connection needs to be extended through an IP-based network.

B. L2TP is used when a PPP connection needs to be extended through an IP-based network.

C. IPSec is used to protect IP-based traffic and is commonly used in gateway-to-gateway connections.

D. SSL VPN is used when a specific application layer traffic type needs protection.

167. _____ is a digital multicarrier modulation scheme that compacts multiple modulated carriers tightly together and uses a composite of narrow channel bands.

A. Direct sequence spread spectrum

B. Frequency hopping spread spectrum

C. Orthogonal frequency-division multiplexing

D. Wave division multiplexing

168. Sam has found out that all of the company’s mobile devices have Bluetooth enabled by default. Which of the following is the attack type Sam should be most concerned with in this situation?

A. Bluesnarfing

B. Blue backing

C. Blue-based attacks

D. BlueDoS

169. Which of the following terms means the combining of server, storage, and network capabilities into a single framework?

A. Network convergence

B. Multiprotocol Label Switching

C. Voice over Internet Protocol

D. Integrated convergence management

170. Which of the following is NOT considered a spread spectrum technology? (Choose all that apply.)

A. FHSS

B. DSSS

C. OFDM

D. WPA2

171. Which of the following is NOT a deficiency of WEP?

A. Use of static encryption keys

B. Small initialization vectors

C. Lack of packet integrity assurance

D. Use of AES

172. Which of the following standards was incorporated as WPA2?

A. IEEE 802.1X

B. IEEE 802.11i

C. IEEE 802.11b

D. IEEE 802.11g

173. Which of the following IEEE standards provides QoS support of multimedia traffic in wireless transmissions?

A. 802.11a

B. 802.11i

C. 802.11e

D. 802.11ac

174. Which of the following technologies was developed specifically to protect IP traffic?

A. IPsec

B. HTTPS

C. TLS

D. SSH

175. Which of the following is used in VPN implementations when using IPsec?

A. Transport mode

B. Tunnel mode

C. Authenticated mode

D. Encrypted mode

176. Which of the following technologies protects each individual messages sent between two computers, instead of all traffic?

A. IPsec

B. HTTP

C. HTTPS

D. S-HTTP

177. What type of network does a smartphone use?

A. Cellular

B. Ethernet

C. Token ring

D. Star

178. Which of the following is NOT a multiple access technology used for mobile cellular networks?

A. Frequency division multiple access (FDMA)

B. Time division multiple access (TDMA)

C. Direct sequence spread spectrum (DSSS)

D. Code division multiple access (CDMA)

179. During which generation of cellular technology was circuit switching replaced with packet switching?

A. 1G

B. 4G

C. 3G

D. 2G

180. Which of the following consists of multiple servers distributed across a large region, each of which provides content that is optimized for users closest to it?

A. Metropolitan area networks (MAN)

B. Content distribution networks (CDN)

C. Local area networks (LAN)

D. Wide area networks (WAN)

181. Which of the following devices provides only a physical link for multiple hosts, and performs no elimination of collision or broadcast domains?

A. Hub

B. Bridge

C. Switch

D. Router

182. An example of a software-defined network would be a _____.

A. VPN

B. Proxied network

C. DMZ

D. VLAN

183. Which of the following types of attack is typically launched for financial gain, and involves the attacker encrypting the user's data, and refusing to release the encryption key unless the user pays the attacker money?

A. Ransomware

B. Flooding

C. Spyware

D. Adware

第四章答案

1、 B .Trunks are used to connect multiple switches for traffic of the same class. The best example of a trunk is the communication channel between two voice switches at a local phone company's central office. The other answers refer to links or lines that connect endpoints to a larger network.

2、 D .Digital Subscriber Line (DSL) has a continuous connection which offers convenience to a user, but can also cause security concerns as it is "always on" for potential hackers to infiltrate. Basic Rate Interface (BRI) and Primary Rate Interface (PRI) are different flavors of ISDN.

Cable modems also use an "always on" technology.

3、 D .TFTP is an insecure protocol with much less functionality than FTP. It has no encryption or authentication capabilities and exists simply to transfer files. The use of passwords with FTP is insecure as they are sent in clear text.

4、 A B .ARP table poisoning is a type of masquerading attack that takes advantage of the weakness in the ARP protocol. An attacker who successfully "poisons" an ARP table will replace the victim's MAC address with his own. Now the IP address that is mapped to its assigned MAC address is actually being mapped to the attacker's address.

5、 B .Internet Protocol Security (IPsec) can be applied in two distinct ways: transport mode or tunnel mode. Transport mode refers to protecting just the data payload. In tunnel mode, the headers and data payload are protected.

The other protocols do not provide protection and also work at the data link layer.

6、 C .Virtual private networks (VPN) are tunnels through the network made secure by encryption techniques and protocols. It is common to implement VPNs through firewall software, which performs an additional filtering step before passing it through to the internal network.

7、 A .Network address translation (NAT) helps to conserve the use of registered IP addresses. Companies use private addresses to communicate internally and use NAT to change them to public addresses when connecting with the outside world.

8、 B .Synchronous Data Link Control (SDLC) enables secondary devices to communicate with the primary stations or mainframes in an IBM architecture. SDLC is the original IBM proprietary protocol. HDLC provides basically the same functionality and more and is an open protocol.

9、 C D .High-level Data Link Control (HDLC) is based upon the SDLC protocol. Both are bit-oriented and both work over synchronous lines. However, HDLC supports full-duplex connections, and thus can provide a higher throughput. Like SDLC, HDLC provides polling, which enables secondary units to communicate with primary units.

10、 C .A metropolitan area network (MAN) is a backbone network that joins together local area networks (LANs). In this example, each building's network is a LAN. Each of the LANs communicate with one another through the SONET network or MAN.

11、 D .IP version 6, which is slowly replacing the current version 4, offers 128-bit addresses. The additional bits will dramatically increase the number of available addresses, thus solving one of the major limitations of version 4. Other benefits of version 6 include improved quality of service and IPsec.

12、 A .Even high-ranking officials can be guilty of telephone fraud—an extremely common security violation within companies. Personal telephone charges can be costly for companies if not monitored properly. Security policies should be implemented and communicated as a good countermeasure.

13、 D .The demilitarized zone (DMZ) is a buffer zone between two networks. Devices in the area, like the bastion host, are extremely vulnerable to hacking. Because of this, no unnecessary programs, user information, utilities, or subsystems should be placed on them.

Bastion hosts should not have internal user accounts. They should only have the accounts necessary to carry out their tasks.

14、 D .A repeater simply re-amplifies the signal of a connection and cannot perform decision-based functionality regarding access restrictions. However, true examples of firewalls can come in many different forms and can be a single device or combination of devices. Routers, proxy servers, and TCP Wrapper (a firewall program to protect Unix systems) could be accurately characterized as firewalls if they have rules configured to monitor traffic.

15、 B .IPsec is a protocol used to provide VPNs that boast strong encryption and authentication functionality. It can protect in two different modes—tunnel mode (payload and headers are protected) or in transport mode (payload protection only). IPsec works at the network layer, not the data link layer.

16、 C .Reverse Address Resolution Protocol (RARP) enables devices that know their MAC addresses to find their IP addresses and other information. Dumb terminals know their physical address but need RARP functionality in order to find the IP address and the location of where their operating system is stored to be downloaded if necessary. IPsec and L2TP are used in tunneling within VPNs.

17、 A .Address Resolution Protocol (ARP) helps the data link layer protocols to find the MAC address for the known IP address. Because this layer cannot understand IP addresses, it broadcasts requests to the designated IP address asking for its hardware address.

RARP works in the opposite direction, resolving MAC addresses to IP addresses. BOOTP is an enhancement to RARP running on diskless workstations and polling is simply a monitoring function.

18、C .Local area networks (LAN) are small networks, such as the network in a building, a floor or even a single room. Ethernet, a media sharing technology, is used specifically in LANs.

19、 B .Internet Control Message Protocol (ICMP) lies within the TCP/IP protocol suite and can be used in many ways including pinging. The PING function sends out ICMP ECHO REQUEST packets to the destination and waits for ECHO REPLY messages.

20、 C .File Transfer Protocol (FTP) runs on ports 20 and 21. When using these ports, FTP enables systems to transfer files between one another. Telnet operates on port 23; HTTP works on port 80; and SNMP runs on port 161 and 162.

21、 A .Telnet is a widely used protocol for remotely accessing devices and achieving command line control, however it does not offer network monitoring or polling functionality. SNMP, on the other hand, handles this type of service as it polls the entire network and presents results on a periodic basis.

22、 B .Asymmetric DSL is a common service for typical Internet users because it offers fast downstream speeds with lower upstream speeds. This is usually acceptable because most Internet users download information more often than uploading information. Data speeds vary per user as it is dependent upon the distance from the service provider's central office.

23、 A .Twisted pair cabling has been around for many years and comes in two forms: shielded twisted pair (STP) in which the cable is protected by an outside foil layer, and unshielded twisted pair (UTP) that offers no added protection. The twisting of the wires plays an integral role in

determining the strength of the signal that is being transmitted. The tighter the wire is twisted means the stronger the signals and longer the distances traveled.

24、 B .User Datagram Protocol (UDP) is connectionless and does not guarantee that its message will be delivered to the recipient, thus the name "best effort." In contrast to Transmission Control Protocol (TCP), UDP performs no handshaking nor does it set up a virtual connection. One benefit, however, is extremely low overhead. UDP is used when reliability is not an issue.

25、 C .A bridge uses physical or MAC addresses when making decisions on where to send traffic. Bridges can perform simple forwarding functionality or more complex filtering, but each function is based on the MAC address which lies within the data link layer of the OSI model.

26、 C .Some of today's bridges can forward frames based on MAC addresses and also have the functionality of routing, thus work at the network layer.

27、 C .UDP is commonly referred to as a "best effort" protocol, but this label describes any connectionless protocol, not just UDP.

28、 D .TCP is a connection-oriented protocol, meaning it provides a more reliable connection, controls data flow, error detection and correction, and sets up a virtual connection. UDP (and any connectionless protocol) does not provide any of these services.

29、 C .Stateful firewalls use state tables to keep track of each step of communication between systems. This provides a higher level of protection than packet filtering because it makes access decisions based on the already-completed steps in the dialogue.

30、 D .10Base2 is called Thin Net because it uses thin, flexible coaxial cable that is easy to work with. Its network segment length is 185 meters and can provide up to 10 Mbps bandwidth.

31、 B .L2TP can tunnel through networks that incorporate many types of protocols, such as X.25, ATM, and frame relay. PPTP and IPsec can work only over IP-based networks. L2TP does not provide any encryption and must be combined with IPsec if this type of protection is needed. L2TP was developed by combining the best of the L2F and PPTP protocols.

32、 A .A mesh topology does not provide the network structure of the other three mentioned topologies (bus, star, ring). In partial mesh topologies, all computers are connected in some way (i.e., the Internet), and in a full mesh each computer is connected to each and every other computer. A full mesh topology provides full redundancy but requires a lot of cabling.

33、 B .A screened subnet filters external traffic and passes it on to the firewall (the second screening device) and then onto the internal network. A screened subnet creates a DMZ by using two routers or firewalls. A screened host architecture is a screening router that is in front of a firewall but does not create a DMZ.

34、 D .Because application-level proxy firewalls work at such an intricate level, they typically reduce the overall network performance. Application-based proxy firewalls look at the data payload to make access decisions and can detect malicious code and commands, while the other firewall types cannot.

35、 C .Demilitarized zones (DMZ) provide a buffer and help protect the internal network from the untrusted, external network. A DMZ can be created by setting up two routers or firewalls. Only the necessary systems should be placed in the DMZ, since they will be the first ones accessed by people from the Internet or an untrusted network.

36、 C .Proxy firewalls provide better security as they act as middlemen, separating the trusted and untrusted networks. They actually break the connection and do not allow external users to have direct access to internal resources.

37、 D .Point-to-Point Protocol (PPP) replaced SLIP because it offers more capabilities such as error correction, better support of authentication, encapsulation of protocols other than IP, and it compresses header information. Both protocols are encapsulation protocols used to carry data over serial lines.

38、 B .Source routing uses the packet header information to determine destinations. If a packet has this routing information within its header, it can override the routes that routers are configured with. Routers should be configured to identify source routing packets and drop them instead of allowing them passage.

39、 C .Repeaters are simple devices that help extend the network by amplifying a signal so that it can pass on to the next segment. Otherwise, the signal weakens (attenuation) and may not be decipherable by the receiving system.

40、 A .Star topologies use a centralized device to connect all devices; the centralized device is a single point of failure.

41、 B .The Address Resolution Protocol (ARP) knows the IP address of a device and broadcasts messages to find the matching MAC address. ARP stores the IP and MAC mappings in an ARP table.

42、 C .Fiber Distributed Data Interface (FDDI) is a high-speed token-passing technology that offers transmission speeds of 100Mbps. It is used as a metropolitan area network (MAN) technology, meaning it connects different networks together. (FDDI can be used as a LAN technology, but the CISSP exam refers to it mainly as a MAN technology.)

43、 B .Each computer in a Token Ring network is connected to a Multi-station Access Unit (MAU), which acts as a central hub. The token will go around to each computer connected to this centralized device in a collapsed ring. In this example, the topology is a physical star while the technology works in a logical ring.

44、 B .10Base2, or Thin Net, should have a network segment length of up to 185 meters. If it is longer than that, the signal can degrade.

45、 C .Ethernet uses carrier sense multiple access with collision detection (CSMA/CD) which monitors transmission activity on the wire. A computer that wants to transmit data will listen to see if the "line is clear" before putting data onto the wire. This is done to help avoid collisions.

46、 D .Because connections must be established and terminated with each session, predictable and fixed delays are included with circuit-switched networks. Packet-switching connections will have variable delays because the packets can take different paths and be queued at different intermediate devices.

47、 B .A major security concern of cable modems is the fact that neighbors use the same coaxial network and can monitor each other's traffic. Cable provides are currently addressing this issue and it will not longer be an issue very soon.

48、 C .Basic Rate Interface (BRI) ISDN service provides two bearer, or B channels, and one D, or control channel. Data is transferred over B channels and the call setup, maintenance, and tear down takes place over the D channel. PRI ISDN service provides 23 B channels and one D channel.

49、A .Asynchronous Transfer Mode (ATM) is a cell-switching technology that provides extremely fast and efficient connection paths. It does not use packets, but uses fixed length cells.

50、 B .Attenuation occurs when electrical signals lose strength as they travel across wires. This happens because the electrons encounter resistance as they travel.

51、 C .Tightly twisted cabling ensures strong signal strengths and less noise interference. The categories of UTP have a direct correlation to the amount of twists implemented for the wiring.

52、 B .A Private Branch Exchange (PBX) is a device used within companies to provide multiple services to users throughout a building or facility. Several security concerns pertain to PBX: default configurations and passwords should be changed, maintenance modems should be enabled only when used, phone bills should be continually reviewed, and unused codes should be disabled.

53、 A .A multicast goes from one source to several destinations. The destinations that receive the data have chosen to participate and accept data from this source. A unicast is a one-to-one transmission and a broadcast is a one-to-all transmission.

54、 D .A router is a layer 3 device that looks at data held within the network header to make decisions on how to get the packet to its destination. Bridges work at the data link layer and repeaters work at the physical layer. Software gateways work at the application layer.

55、 A .Metropolitan area networks (MANs) typically use SONET or FDDI rings to connect businesses to the wide area network (WAN), other MANs, the Internet, and the telecommunication networks. They are referred to as backbones because of the high speed the data can travel over them compared to LAN-type transmissions.

56、 B .Software gateways are more complex devices than the other mentioned devices because they look within the frame to gain more than just address and routing information. Translation may need to be performed when entities on two unlike environments need to communicate, as in a Novell and Microsoft network using proprietary protocols. (Although gateways can work at different OSI layers, the CISSP exam usually puts them at the application layer.)

57、 C .Network address translation (NAT) allows companies to use a limited number of registered Internet addresses, which saves on funds and provides an amount of security. External entities can see only the address of the router (or the public address the NAT device is using) and not the true addresses of the internal hosts. The company can use private address schemes instead of having to pay for public addresses.

58、 B .Synchronous Optical Network (SONET) is a standard for fiber-optic cabling and uses self-healing network rings. SONET describes the interfaces that can be used over fiber lines and the signaling that must be employed. SONET works at the physical layer of the OSI model.

59、 B .A T3 can provide 45 Mbps of bandwidth and is the same as 28 T1 lines. T1 lines provide up to 1.544 Mbps and a fractional T1 is a fraction of that bandwidth. BRI is an ISDN service that provides up to 144 Kbps.

60、 A .Digital Subscriber Line (DSL) uses copper wires from the central office to the end user and is always connected, meaning the user does not need to reestablish a connection. This is true of the technology, but the service provider providing this service might allow a connection for only a certain time period. "Always on" technologies are targeted by attackers because the system is always connected and available.

61、 D .One of the biggest advantages of dedicated lines is that the connection is private, meaning that it is not a shared medium. This characteristic provides more security. Dedicated lines are usually much more expensive than public-switched technologies as in frame relay, X.25, and SMDS.

62、 A .Committed information rate (CIR) is a premium service offered by service providers in frame relay networks that guarantees a company a specified amount of bandwidth. Frame relay is burst-like in nature, meaning that a company may have access to a larger amount of bandwidth until the network gets busy. If a company needs to ensure it will have a certain amount of bandwidth always available, it will have to pay this extra rate.

63、 D .Wireless traffic can be easily eavesdropped on. Traffic analysis is watching the behavior of

traffic with the hopes of uncovering information not intended for the eavesdropper. Access point (AP) and station location can be uncovered by sniffing traffic. Integrity and authentication should not be affected if a user moves from one AP to another, and encryption is available in wireless technologies, referred to as Wired Equivalent Privacy (WEP).

64、 A .A man-in-the-middle attack is when an attacker inserts herself into an ongoing communication between two systems. The user spoofs her identity to fool the other entities, which is an example of masquerading. The attacker can then hijack the session, meaning take over the session. This can be done by "kicking" one of the users off by performing a denial-of-service attack. Digital signatures can prevent man-in-the-middle attacks because authentication takes place.

65、 C .Point-to-point Tunneling Protocol (PPTP) is a Microsoft virtual private network (VPN) protocol. It provides encapsulation, which means it repackages the original frame and encrypts it. This allows for secure communication via an untrusted network as in the Internet. L2TP is a protocol that would provide just encapsulation instead of encapsulation and encryption.

66、 B .Products that are based on the SOCKS firewall technology are circuit-level firewalls. This means that they look only at packet header information (address and port numbers) to make access decisions. They do not look into the packet's payload to review protocol commands or provide a proxy per service. These two are characteristics of an application-based proxy product.

67、 C .A socket is the combination of a node address and a port number. When a connection is made between two systems, the packets need to contain the address and port address of the sending and receiving system. This is so that the packet can be properly routed to the receiving system and so that the receiving system knows who to reply to.

68、 A .A circuit-based proxy firewall looks at header information to make decisions on whether a packet is deemed acceptable for access. This is a different approach than application-based firewalls, which look at the information within the payload of the packet. A stateful firewall maintains a state table to keep track of each communication dialogue taking place between systems and makes access decisions based on the information within this table.

69、 C .A centralized access technology must have a database of user information and authentication information so when users request access, their credentials can be properly checked. RADIUS and TACACS+ are examples of centralized access control technologies.

70、 B .Routers can provide packet filtering through the use of access control lists (ACLs). These ACLs are compared to incoming and outgoing traffic, and only the packets that are outlined as acceptable are allowed through. Packet filters cannot provide content filtering because they do not look that deep into the packet, and they do not provide application or circuit-based proxy protection. They are transparent to users because when a user requests access to a resource on the other side of the router, he does not have to log into that device or do anything special. The protection takes place without him knowing about it.

71、 A .Address Resolution Protocol (ARP) finds Media Access Control (MAC) addresses for IP addresses. It broadcasts a request and only the system with the IP address within the broadcast domain responds. ARP takes the MAC address from this response and places it in its ARP table. An attacker can manipulate this ARP table so that traffic with the correct IP address goes to an incorrect MAC address. The traffic goes to the attacker's MAC address instead of the intended receiver.

72、 C .Network sniffers are tools that read network traffic as it passes over a network interface card (NIC). When attackers use these, it is considered a passive attack because the attacker is not actually doing anything or modifying packets. Sniffers are not detectable or auditable, thus an administrator would not necessarily know that one is installed and working within her network.

73、 C .Connection-oriented protocols operating at the transport layer are responsible for end-to-end connectivity between systems. Session layer protocols are responsible for the session establishment, maintenance, and breakdown between applications.

74、 D .Asynchronous communication devices, such as modems, are not synchronized in that the devices involved can send data at will, sending a sequence of bits framed with start and stop bits that are reassembled into data at the receiving end. Synchronous communication devices, on the other hand, determine a synchronization scheme before data transmission.

75、 D .Internetwork Packet Exchange (IPX) is a protocol that exists at the network layer in the OSI model. A good way to remember this is to associate IPX with IP, since they both start with IP. IPX/SPX is the suite of protocols used originally in Novell Netware networks.

76、 A .Ethernet uses CSMA/CD (carrier sense multiple access with collision detection) and retransmits data after a collision takes place. FDDI and Token Ring use tokens to ensure that collisions do not take place. ATM can be used as a LAN backbone technology, although it is usually a WAN technology. ATM is not as susceptible to collisions as Ethernet.

77、 C .In a token passing technology, collisions on the network media are eliminated by allowing only the computer with the token to communicate. Collision avoidance is the method implemented in CSMA/CA, in which a transmitting device first sends a warning packet before placing data on the line. Collision detection is implemented in CSMA/CD. Polling is a method in which a primary device coordinates transmission with secondary devices.

78、 A .Cable malfunctions, cable breaks, and the length of the cable directly correlate to the possibility of weakening a signal, which is attenuation.

79、 B .Routers can block all broadcast traffic from passing. The other devices listed will allow broadcast data to pass through them to another network segment.

80、 B .A state table is used in stateful firewalls to track packets in order to provide a high level of

security. Stateful firewalls allow the device to keep state of a dialogue, which requires more intelligence and processing than that of the activities of a packet filter firewall.

81、 B .Packet switching is a component of a routing device. All of the other choices represent standard firewall features.

82、 A .An application-based proxy firewall reviews data and command structures in the data payload, thus it requires more processing that degrades performance. This ability to work on all layers of the OSI model, and even to be able to filter based on the data in a packet, gives it a security advantage over basic packet filtering.

83、 C .The B channels are used for sending data and the D channel is used to send control information.

84、 A .The more recently developed tunneling protocol, L2TP, allows for tunneling over frame relay and ATM as well as TCP/IP. PPTP can work only over IP networks. PPTP can encapsulate data other than IP, but it can move data only over networks that use the IP protocol.

85、 C .CSMA is a method used by data link technologies, whereby the various computers and devices have to share the same medium, as in Ethernet. Both flavors (CA and CD) are used to help reduce collisions from taking place. CSMA/CA will send out a message indicating to all other systems that it is going to put data on the line, and CSMA/CD will listen to the wire to try and figure out when would be the best time to put data on the line.

86、 B .The TCP/IP model is another model, like the OSI, that has been developed to modularize and try to explain conceptually where the different functions lie within a network stack. The TCP/IP model has only four layers: application, host-to-host, Internet, and network access. Sometimes the host-to-host layer is referred to as a transport layer.

87、 C .The "gap in the WAP" has to do with a wireless device transmitting encrypted data over the Internet. The wireless device may not use the TCP/IP stack, and it thus must use Wireless Transport Layer Security (WTLS) for encryption. Because the Internet does not understand this protocol, the data must be translated into SSL or TLS. This translation must take place within a window of time in which this confidential information is decrypted by a third party. Companies and individuals may not want third parties to have access to their data in this fashion.

88、A .The 802.11b standard works in the 2.4 GHz range and provides only up to 1 – 2 Mbps. The 802.11a works in the 5 GHz range and provides much higher data transfer rates. 802.11b is backward compatible with 802.11 implementations, but 802.11a is not.

89、 C .SKA means that the AP will authenticate the wireless device only if it proves that it has the necessary WEP key. That same key is used for encrypting data before it is sent over the airwaves.

90、 D .The SSID value is required for the wireless device to authenticate properly to the AP. This is not an actual security mechanism that should be depended upon because the AP usually broadcasts this value for anyone with a sniffer to capture.

91、 B .The 802.11i working group was developed to come up with solutions for dealing with all of the security flaws within the WEP protocol (used by all WLAN technologies today). This standard specifies the security mechanisms that should be used for wireless networks and addresses many of the security issues that were inherent to the implementation of WEP.

92、 C .The application layer in the TCP/IP architecture model would be equivalent to a combination of the application, presentation, and session layers in the OSI model.

93、 B .The communication between two pieces of the same software product that reside on different computers needs to be controlled, which is why session layer protocols even exist. Session layer protocols take on the functionality of middleware, which allow software on two different computers to communicate.

94、 A .The host-to-host transport layer in the TCP/IP architecture model would be equivalent to transport layer in the OSI model. This is where the SPX protocol resides.

95、 B .The Internet layer in the TCP/IP architecture model would be equivalent to the network layer in the OSI model, which is where all routing protocols work.

96、 D .The data link layer is divided into two functional sub-layers: the Logical Link Control (LLC) and the Media Access Control (MAC). The LLC, defined in the IEEE 802.2 specification, will communicate with the protocol immediately above it—the network layer—in either connection or connectionless mode. The MAC will have the appropriately loaded protocols to interface with the protocol requirements of the physical layer. The IEEE MAC specification for Ethernet is 802.3, Token Ring is 802.5, wireless is 802.11, etc. When you see IEEE standards as in 802.11, 802.16, 802.3, and so on, this is referring to the protocol working at the MAC sub-layer of the data link layer of a protocol stack.

97、 C .The network access layer in the TCP/IP architecture model would be equivalent to a combination of the data link and the physical layers in the OSI model, which is where PPP works.

98、 A .The data link layer has two sub-layers, the Logical Link Control (LLC) and Media Access Control (MAC) layers. The LLC provides a standard interface for whatever network protocol is being used. This provides an abstraction layer so that the network protocol does not need to be programmed to communicate with all of the possible MAC level protocols (Ethernet, Token Ring, WLAN, FDDI, etc..)

99、 D .Port numbers up to 1023 (0-1023) are called well-known ports, and almost every computer in the world has the exact same protocol mapped to the exact same port number. That is why they are called well-known—everyone follows this same standardized approach.

100、 A .Classless interdomain routing (CIDR) was created because it was clear that available IP addresses were running out as more individuals and corporations participated on the Internet. A class B address range is usually too large for most companies and a class C address range is too small. So CIDR provides the flexibility to increase or decrease the class sizes as necessary.

101、 B .To ensure that packets do not traverse a network forever, IP provides a Time to Live (TTL) value that is decremented every time the packet passes through a router.

102、 C .IP version 6, also called IP next generation (Ipng), has an address space of 128-bits, auto-configuration (which makes administration easier), and IPsec integrated, but it does not require NAT. NAT was developed when IPv4 addresses were running out. The IP address size could make NAT obsolete for the purpose of saving public addresses.

103、 A .It is more difficult to extract analog signals from background noise because the amplitudes and frequency waves slowly lose form. This is because an analog signal could have an infinite number of values or states, where a digital signal exists in discrete states. A digital signal is a square wave, which does not have all the possible values of amplitudes and frequencies of an analog signal.

104、 D .If a computer detects a problem with the network, it sends a beacon frame. This frame generates a failure domain, which is between the computer that issued the beacon and its neighbor downstream. The computers and devices within this failure domain will attempt to reconfigure certain settings to try and work around the detected fault.

105、 B .FDDI-2 provides fixed bandwidth that can be allocated for specific applications. This makes it work more like a broadband connection, allowing voice, video, and data to travel over the same lines.

106、 B .Network cabling that is placed in these types of areas, called plenum space, must meet a specific fire rating to ensure that it will not produce and release harmful chemicals in case of a fire. A building's ventilation usually takes place through this plenum space and if toxic chemicals get into that area, they could be easily spread throughout the building in minutes. Non-plenum cables usually have a polyvinyl chloride (PVC) jacket covering, whereas plenum-rated cables have jacket covers made of fluoropolymers.

107、 D .Internet Group Management Protocol (IGMP) is a protocol used to report multicast group memberships to routers. When a user chooses to accept multicast traffic, this means that she becomes a member of a particular multicast group. IGMP is the mechanism that allows her computer to inform the local routers that she is part of this group and to send traffic with a specific multicast address to her system.

108、 B .Some applications and network protocol algorithms work better if they can communicate at determined intervals, instead of "whenever the data arrives." In token passing

technologies, traffic arrives in this type of deterministic fashion because not all systems can communicate at one time, but only when a system has control of the token. The other answers describe Ethernet environments.

109、 D .Loki is actually a client/server program that is used by hackers to set up backdoors on systems. A computer is attacked and the server portion of the Loki software is installed. This server portion "listens" on a port, which is the backdoor that an attacker can use to access the system. To gain access and open a remote shell to this computer, an attacker sends commands inside of ICMP packets. This is usually successful because most routers are configured to allow ICMP traffic to come and go out of the network. ICMP has been seen as a basically benign protocol, since it was developed not to hold any data or a payload. The other attacks do not use the ICMP protocol.

110、 D .Today's layer 3, layer 4, and other layer switches have more enhanced functionality than layer 2 switches. These higher level switches offer routing functionality, packet inspection, traffic prioritization, and Quality of Service (QoS) functionality. They are referred to as multilayered switches because they combine data link layer, network layer, and other layer functionalities.

111、 B .Trunks are used to connect multiple switches for traffic of the same class. The best example of a trunk is the communication channel between two voice switches at a local phone company’s central office. The other answers refer to links or lines that connect endpoints to a larger network.

112、 D .Digital Subscriber Line (DSL) has a continuous connection, which offers convenience to a user, but can also offer security concerns, as it is “always on” for potential hackers to infiltrate. Basic Rate Interface (BRI) and Primary Rate Interface (PRI) are different ISDN offerings. Cable modems also use an “always-on” technology.

113、 B .Internet Protocol Security (IPsec) can be applied in two distinct ways: transport mode or tunnel mode. Transport mode refers to protecting just the data payload. In tunnel mode, the headers and data payload are protected. The other protocols do not provide protection and also work at the data link layer.

114、 B .Synchronous Data Link Control (SDLC) enables secondary devices to communicate with the primary stations or mainframes in an IBM architecture. SDLC is an IBM proprietary protocol. High-Level Data Link Control (HDLC) provides basically the same functionality and more, and is an open protocol.

115、 C .A campus area network (CAN) is a backbone network that joins local area networks together. In this example, each building’s network is a local area network (LAN). The LANs communicate with one another through the SONET network or CAN.

116、 A .Address Resolution Protocol (ARP) helps the data link layer protocols find the MAC address for the known IP address. Because this layer cannot understand IP addresses, it

broadcasts requests to the designated IP address, asking for its hardware address. RARP works in the opposite direction, resolving MAC addresses to IP addresses. BOOTP is an enhancement to RARP, running on diskless workstations, and polling is simply a monitoring function.

117、 C .Local area networks (LANs) are small networks, such as the network in a building, a floor, or even a single room. Ethernet, a media-sharing technology, is used in LANs.

118、 B .Internet Control Message Protocol (ICMP) lies within the TCP/IP protocol suite and can be used in many ways, including pinging. The ping function sends out ICMP ECHO REQUEST packets to the destination and waits for ECHO REPLY messages.

119、 B .Asymmetric DSL is a common service for typical Internet users because it offers fast downstream speeds with lower upstream speeds. This is usually acceptable because most Internet users download information more often than they upload it. Data speeds vary per user, as the speed is dependent upon the distance from the service provider’s central office.

120、 A .Twisted-pair cabling has been around for many years and comes in two forms: shielded twisted pair (STP) in which the cable is protected by an outside foil layer, and unshielded twisted pair (UTP) that offers no added protection. The twisting of the wires plays an integral role in determining the strength of the signal that is being transmitted. The tighter the wire is twisted, the stronger the signals and longer the distances traveled.

121、 C .Ethernet uses carrier sense multiple access with collision detection (CSMA/CD), which monitors transmission activity on the wire. A computer that wants to transmit data will listen to see if the “line is clear” before putting data onto the wire. This is done to help avoid collisions.

122、 A .A man-in-the-middle attack is when an attacker inserts herself into an ongoing communication between two systems. The user spoofs her identity to fool the other entities, which is an example of masquerading. The attacker can then hijack the session, meaning she takes it over. This can be done by “kicking” one of the users off by performing a denial-of-service attack. Digital signatures can help prevent man-in-the-middle attacks because authentication takes place.

123、 C .The application layer in the TCP/IP architecture model would be equivalent to a combination of the application, presentation, and session layers in the OSI model.

124、 B .The Internet layer in the TCP/IP architecture model would be equivalent to the network layer in the OSI model, which is where all routing protocols work.

125、 D .The data link layer is divided into two functional sublayers: the Logical Link Control (LLC) and the Media Access Control (MAC). The LLC, defined in the IEEE 802.2 specification, will communicate with the protocol immediately above it—the network layer—in either connection or connectionless mode. The MAC will have the appropriately loaded protocols to interface with the protocol requirements of the physical layer. The IEEE MAC specification for Ethernet is 802.3,

Token Ring is 802.5, wireless is 802.11, etc. When you see IEEE standards as in 802.11, 802.16, 802.3, and so on, this is referring to the protocol working at the MAC sublayer of the data link layer of a protocol stack.

126、 C .The network access layer in the TCP/IP architecture model would be equivalent to a combination of the data link and the physical layers in the OSI model, which is where PPP works.

127、 D .Port numbers up to 1023 (0–1023) are called well-known ports, and almost every computer in the world has the exact same protocol mapped to the exact same port number. That is why they are called well known—everyone follows this same standardized approach.

128、 A .Classless interdomain routing (CIDR) was created because it was clear that available IP addresses were running out as more individuals and corporations participated on the Internet. A class B address range is usually too large for most companies, and a class C address range is too small. So CIDR provides the flexibility to increase or decrease the class sizes as necessary.

129、 B .To ensure that packets do not traverse a network forever, IP provides a time to live (TTL) value that is decremented every time the packet passes through a router.

130、 C .IP version 6, also called IP next generation (IPng), has an address space of 128 bits, auto-configuration (which makes administration easier), and IPsec integrated, but it does not require NAT. NAT was developed when IPv4 addresses were running out. The IP address size could make NAT obsolete for the purpose of saving public addresses.

131、 A .It is more difficult to extract analog signals from background noise because the amplitudes and frequency waves slowly lose form. This is because an analog signal could have an infinite number of values or states, whereas a digital signal exists in discrete states. A digital signal is a square wave, which does not have all the possible values of amplitudes and frequencies of an analog signal.

132、 B .FDDI-2 provides fixed bandwidth that can be allocated for specific applications. This makes it work more like a broadband connection, allowing voice, video, and data to travel over the same lines.

133、 B .Network cabling that is placed in areas above a dropped ceiling or below a raised floor, called plenum space, must meet a specific fire rating to ensure that it will not produce and release harmful chemicals in case of a fire. A building’s ventilation usually takes place through this plenum space, and if toxic chemicals get into that area, they could be easily spread throughout the building in minutes. Nonplenum cables usually have a polyvinyl chloride (PVC) jacket covering, whereas plenum-rated cables have jacket covers made of fluoropolymers.

134、 D .Internet Group Management Protocol (IGMP) is a protocol used to report multicast group memberships to routers. When a user chooses to accept multicast traffic, this means that she becomes a member of a particular multicast group. IGMP is the mechanism that allows her

computer to inform the local routers that she is part of this group and to send traffic with a specific multicast address to her system.

135、 B .Some applications and network protocol algorithms work better if they can communicate at determined intervals, instead of “whenever the data arrive.” In token-passing technologies, traffic arrives in this type of deterministic fashion because not all systems can communicate at one time, but only when a system has control of the token. The other answers describe contention-based environments, as in Ethernet.

136、 D .Loki is actually a client/server program that is used by hackers to set up back doors on systems. A computer is attacked, and the server portion of the Loki software is installed. This server portion “listens” on a port, which is the back door that an attacker can use to access the system. To gain access and open a remote shell to this computer, an attacker sends commands inside of ICMP packets. This is usually successful because most routers are configured to allow ICMP traffic to come and go out of the network. ICMP has been seen as a basically benign protocol, since it was developed not to hold any data or a payload. The other attacks do not use the ICMP protocol.

137、D .Today’s layer 3, layer 4, and other layer switches have more enhanced functionality than layer 2 switches. These higher-level switches offer routing functionality, packet inspection, traffic prioritization, and Quality of Service (QoS) functionality. They are referred to as multilayered switches because they combine data link layer, network layer, and other layer functionalities.

138、 C .A Class B address range is usually too large for most companies, and a class C address range is too small, so CIDR provides the flexibility to increase or decrease the class sizes as necessary. CIDR is the method to specify more flexible IP address classes.

139、 A .To ensure that packets do not continually traverse a network forever, IP provides a time to live (TTL) value that is decremented every time the packet passes through a router.

140、 A .The scalability of multicast routing is improved by adding a “scope” field to multicast addresses.

141、 B .IPv4 limits packets to 65,535 octets of payload, and IPv6 extends this size to 4,294,967,295 octets. These larger packets are referred to as jumbograms and improve performance over high-MTU links. An IPv6 jumbogram is an IPv6 packet carrying a payload larger than 65,535octets.

142、 A .The IEEE 802.1AR standard specifies unique per-device identifiers (DevID) and the management and cryptographic binding of a device (router, switch, access point) to its identifiers. A verifiable unique device identity allows establishment of the trustworthiness of devices; thus, it facilitates secure device provisioning. A secure device identifier (DevID) is cryptographically bound to a device and supports authentication of the device’s identity. Locally significant identities can be securely associated with an initial manufacturer-provisioned DevID and used in

provisioning and authentication protocols to allow a network administrator to establish the trustworthiness of a device and select appropriate policies for transmission and reception of data and control protocols to and from the device.

143、 B .Classless interdomain routing is variable-length subnet masking, which allows a network to be divided into different-sized subnets. The goal is to increase the efficiency of the use of IP addresses, since classful addressing schemes commonly end up in unused addresses.

144、 B .6to4 is a transition mechanism for migrating from IPv4 to IPv6. It allows two systems using IPv6 to communicate if their traffic has to transverse an IPv4 network.

145、 D .A baseband technology uses the entire communication channel for its transmission, whereas a broadband technology divides the communication channel into individual and independent channels so different types of data can be transmitted simultaneously. Baseband permits only one signal to be transmitted at a time, whereas broadband carries several signals over different channels. Any transmission technology that “chops up” one communication channel into multiple channels is considered broadband. The communication channel is usually some frequency spectrum, and the broadband technology provides delineation between these frequencies and techniques on how to modulate the data onto the individual frequency channels.

146、 C .An effective method to shield networks from unauthenticated devices is through the use of DHCP snooping on network switches. DHCP snooping ensures that DHCP servers can assign IP addresses to only selected systems, identified by their MAC addresses. Also, advance network switches now have the capability to direct clients toward legitimate DHCP servers to get IP addresses and restrict rogue systems from becoming DHCP servers on the network.

147、 A .The two main components within SNMP are managers and agents. The manager is the server portion, which polls different devices to check status information. The server component also receives trap messages from agents, and provides a centralized place to hold all network-wide information. The agent is a piece of software that runs on a network device, which is commonly integrated into the operating system. The agent has a list of objects that it is to keep track of, which is held in a database-like structure called the Management Information Base (MIB). An MIB is a logical grouping of managed objects which contain data used for specific management tasks and status checks.

148、 B .A community string is basically a password a manager uses to request data from the agent, and there are two main community strings with different levels of access: read-only and read-write. As the names imply, the read-only community string allows a manager to read data held within a device’s MIB, and the read-write string allows a manager to read the data and modify them.

149、 B .A non-recursive query means that the request just goes to that specified DNS server, and either the answer is returned to the resolver or an error is returned. A recursive query means that the request can be passed on from one DNS server to another one until the DNS server with

the correct information is identified.

150、 B .DNS zone transfer is the process of replicating the databases containing the DNS data across a set of DNS servers.

151、 C .DNSSEC is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attack types.

152、 C .Sender Policy Framework (SPF) is an e-mail validation system designed to prevent e-mail spam by detecting e-mail spoofing, by verifying the sender’s IP address. SPF allows administrators to specify which hosts are allowed to send e-mail from a given domain by creating a specific SPF record in DNS. Mail exchanges use the DNS to check that mail from a given domain is being sent by a host sanctioned by that domain’s administrators.

153、 A .Multiprotocol Label Switching (MPLS) is a common component in high-performance networks that is used to direct traffic from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. Network addresses represent node endpoints, and labels represent paths between nodes.

154、 B .An attacker can have a system act as though it is a switch. The system understands the tagging values being used in the network and the trunking protocols, and can insert itself between other VLAN devices and gain access to the traffic going back and forth. Attackers can also insert tagging values to manipulate the control of traffic at the data link layer.

155、 A .Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet LAN and allows redundant links to be available in case connection links go down.

156、 B .Packet-filtering devices can block many types of attacks at the network protocol level, but they are not effective at protecting against attacks that exploit application-specific vulnerabilities. That is because filtering only examines a packet’s header (i.e., delivery information) and not the data moving between the applications. Thus, a packet-filtering firewall cannot protect against packet content that could, for example, probe for and exploit a buffer overflow in a given piece of software.

157、 A .Virtual firewalls can be bridge-mode products, which monitor individual traffic links between virtual machines, or they can be integrated within the hypervisor. The hypervisor is the software component that carries out virtual machine management and oversees guest system software execution. If the firewall is embedded within the hypervisor, then it can “see” and monitor all the activities taking place within the host system.

158、 B .Converged infrastructure means the combining of server, storage, and network capabilities into a single framework. This helps to decrease the costs and complexity of running

data centers and has accelerated the evolution of cloud computing. Converged infrastructures provide the ability to pool resources, automate resource provisioning, and increase and decrease processing capacity quickly to meet the needs of dynamic computing workloads.

159、 B .Access devices exist at customer’s premises, which connect the customer’s equipment to the service provider’s network. The service provider’s distribution network aggregates the traffic and sends it to the provider’s core network. From there, the traffic is moved to the next aggregation network that is closest to the destination. This is similar to how smaller highways are connected to larger interstates with on and off ramps that allow people to quickly travel from one location to a different one.

160、 A .High-speed fiber-optic connections are measured in optical carrier (OC) transmission rates. The transmission rates are defined by rate of the bit stream of the digital signal and are designated by an integer value of the multiple of the basic unit of rate. They are generically referred to as OCx, where the “x” represents a multiplier of the basic OC-1 transmission rate, which is 51.84 Mbps.

161、 A .Time-division multiplexing (TDM) is a type of multiplexing in which two or more bit streams or signals are transferred, apparently simultaneously, as subchannels in one communication channel, but are physically taking turns on the single channel.

162、 B .Controlling network traffic to allow for the optimization or the guarantee of certain performance levels is referred to as traffic shaping. Using technologies that have QoS capabilities allow for traffic shaping, which can improve latency, increase bandwidth for specific traffic types, bandwidth throttling, and rate limiting.

163、 A .PPP carries out several functions, including the encapsulation of multiprotocol packets. It has a Link Control Protocol (LCP) that establishes, configures, and maintains the connection. Network Control Protocols (NCPs) are used for network layer protocol configuration, and it provides user authentication capabilities through PAP, CHAP, and EAP protocols. The LCP is used to carry out the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link when necessary. LCP is the generic maintenance component used for each and every connection. So LCP makes sure the foundational functions of an actual connection work properly, and NCP makes sure that PPP can integrate and work with many different protocols. PPP has to “plug in” and work with different network layer protocols, and various network layer protocol configurations have to change as a packet moves from one network to another one. So PPP uses NCPs to be able to understand and work with different network layer protocols (IP, IPX, NetBEUI, AppleTalk).

164、 B .When Voice over IP (VoIP) is used, it employs the Session Initiation Protocol (SIP), which sets up and breaks down the call sessions, just as SS7 does for non-IP phone calls. SIP is an application layer protocol that can work over TCP or UDP. SIP provides the foundation to allow the more complex phone-line features that SS7 provides, such as causing a phone to ring, dialing

a phone number, generating busy signals, and so on.

165、 A .The U.S. National Security Agency uses a protocol encryptor that is based upon IPsec. A HAIPE (High Assurance Internet Protocol Encryptor) is a Type 1 encryption device that is based on IPsec with additional restrictions, enhancements, and capabilities. A HAIPE is typically a secure gateway that allows two enclaves to exchange data over an untrusted or lower-classification network. Since this technology works at the network layer, secure end-to-end connectivity can take place in heterogeneous environments. This technology has largely replaced link layer encryption technology implementations.

166、 B .L2TP is used when a PPP connection needs to be extended through a non-IP-based network.

167、 C .Orthogonal frequency-division multiplexing (OFDM) is a digital multicarrier modulation scheme that compacts multiple modulated carriers tightly together, reducing the required bandwidth. The modulated signals are orthogonal (perpendicular) and do not interfere with each other. OFDM uses a composite of narrow channel bands to enhance its performance in high-frequency bands. OFDM is officially a multiplexing technology and not a spread spectrum technology, but is used in a similar manner.

168、 A .Bluesnarfing is the unauthorized access from a wireless device through a Bluetooth connection. This allows access to a calendar, contact list, e-mails, and text messages, and on some phones users can copy pictures and private videos. The countermeasure is to put the Bluetooth-enabled device into nondiscoverable mode so others cannot identify this device in the first place.

169、A .Network convergence is the combining of server, storage, and network capabilities into a single framework, and uses protocols such as FCoE, Fibre Channel over Ethernet (FCoE), Multiprotocol Label Switching (MPLS), Voice over IP (VoIP), and Internet Small Computer System Interface (iSCSI).

170、 C D .Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are spread spectrum technologies. Orthogonal frequency-division multiplexing (OFDM) is a multiplexing technology, and Wi-Fi Protect Access 2 (WPA2) is a wireless security technology.

171、 D .Wired Equivalent Privacy (WEP) does not use Advanced Encryption Standard (AES). AES is used by Wi-Fi Protected Access 2 (WPA2).

172、 B .IEEE 802.11i, otherwise known as Wi-Fi Protected Access (WPA), is the security standard that became known as WPA2. IEEE 802.1X is a port security and authentication technology. IEEE 802.11b was one of the first wireless transmission standards, and uses WEP, not WPA2. IEEE 802.11g is a wireless transmission standard, which can use WPA or WPA2.

173、 C .802.11e provides Quality of Service support for multimedia traffic in wireless networks.

802.11i is a wireless security standard, and both802.11a and 802.11ac are wireless transmission standards.

174、 A .IP Security (IPsec) was developed to protect IP traffic. It can provide both authentication and encryption. It works within a local area network, as well as across the Internet, often providing security for virtual private networks (VPNs). HTTP Secure (HTTPS) only protects web traffic. Transport Layer Security (TLS) can protect all traffic, including IP traffic, but is typically used in HTTPS. Secure Shell (SSH) provides for secure remote access between hosts.

175、 B .Tunnel mode is used to create a secure tunnel through an untrusted network, such as the Internet.

176、 D .S-HTTPS is different from standard HTTP in that it protects each individual message between two computers. HTTP provides no security for web traffic. Both HTTPS and IPsec protect not only each individual message, but all communications between two computers.

177、 A .A cellular network distributes radio signals over delineated areas, called cells. This allows smartphones, since they are mobile devices, to travel between cells, maintaining constant connectivity.

178、 C .Direct sequence spread spectrum (DSSS) is a technology primarily used in IEEE 802.11 wireless networks. The other choices are multiple access technologies that have been used in cellular networks.

179、 C .During the third generation (3G) of cellular networks, there were many enhancements, including replacing circuit switching technologies with packet switching, as well as expanded services, higher capacities, and faster communications speeds. This is the generation that made all devices popular worldwide.

180、 B .Content distribution networks (CDNs) use multiple servers distributed across regions, to provide content that is optimized for users on a geographical basis. Examples of such services include Netflix and Hulu.

181、 A .The simple hub offers no advantages other than a physical electrical connection for multiple hosts. Since all these hosts are on the same collision and broadcast domain, no switching or routing takes place, which means collisions are not eliminated.

182、 D .A VLAN, or virtual LAN, is created in a layer 3 switch, and is essentially a software-defined network, because it is created using utilities in the switch's operating system.

183、 A .Ransomware is a relatively new form of attack, in which an attacker encrypts the user's data, through the use of malware installed on the host, and refuses to release the user's data, or even threatens to destroy it, unless the user pays some amount of money to the attacker. It is mitigated by maintaining up-to-date malware signatures, educating users, and storing critical

user data away from the host.

第五章题目

1. Brute force attacks are used most often against which types of access control? (Choose the two best answers.)
   A. Biometrics
   B. Passwords
   C. Cognitive passwords
   D. Cryptographic keys
2. Passwords are one of many types of authentication mechanisms. Which of the following is not true of a password?
   A. Is the least secure of access controls
   B. Is moderately used
   C. Can be automatically created by a password generator
   D. Relies heavily on the discipline of the user and the administrator
3. A single sign-on technology that offers symmetric and asymmetric keys for encryption and uses Privileged Attribute Certificates (PACs) for authentication is called _____.
   A. Thin clients
   B. SESAME
   C. Kerberos
   D. Cryptographic keys
   E. Directory Services
4. Which of the following biometric methods obtains the patterns and colors around a person's pupil?
   A. Iris scan
   B. Palm scan
   C. Retina pattern
   D. Fingerprint
5. Security labels are used in what type of model?
   A. Role-based access control model
   B. Mandatory acess control model
   C. Discretionary access control model
   D. Military access control model
6. Companies have different ways of coming up with passwords for use in authentication. Which of the following best describes a password advisor?
   A. A potential attack using a dictionary program
   B. An automated system that creates long-stringed passwords which are difficult to remember
   C. A list of questions for the user to answer
   D. A program that instructs users on creating passwords that are easy to remember and difficult to crack
7. Which of the following centralized access control protocols would a security professional choose if her network consisted of multiple protocols and had users connecting via wireless and

wired transmissions?

A. RADIUS

B. TACACS+

C. Diameter

D. Kerberos

8. Passwords are one of the most sought after items by attackers because of the level of access they can provide. Which of the following is least effective when trying to protect against password attacks?

A. Employing a password generator system

B. Not allowing passwords to be shown in cleartext

C. Using dictionary attack tools to identify weaknesses

D. Implementing encryption and hashing algorithms

9. There are security issues when a company allows users to have too many rights and permissions. Allowing a user the absolute minimum rights necessary when accessing a network is referred to as what?

A. Separation of duties

B. Least privilege

C. Full disclosure

D. Discretionary access control (DAC)

10. Which of the following access control types is considered a "soft" measure for protecting an organization as a whole?

A. Preventive-Administrative

B. Preventive-Physical

C. Predictive

D. Corrective

11. Which of the following best describes Extended TACACS (XTACACS)?

A. An Internet standard

B. Combines authentication and authorization

C. Separates authentication, authorization, and accounting processes

D. Has three-factor user authentication

12. Katie is an IT administrator who needs to set up an access control system that both designates users' permission to control some files but keeps database and network resource permissions in the hands of IT. What type of access control administration would she employ?

A. Hybrid

B. Decentralized

C. Centralized

D. Security labels

13. Guard dogs and closed-circuit TV (CCTV) would be examples of what type of access control?

A. Recovery

B. Corrective

C. Preventive-Technical

D. Preventive-Physical

14. There are several different types of single sign-on technologies. Which is the simplest technology?

A. Kerberos

B. Scripting

C. SESAME

D. KDC

15. A dynamic password is another name for what authentication mechanism?

A. Cognitive password

B. Smart card

C. Passphrase

D. One-time password

16. ATM machines limit users to only certain areas of the touch screen. This is an example of which of the following?

A. Constrained user interface

B. Passphrase

C. Dumb terminal

D. Preventive administrative control

17. Placing users into groups with predefined access criteria is known as what type of access model?

A. Mandatory access control

B. Discretionary access control

C. Role-based access control

D. Sensitivity label control

18. Different authentication components work in different ways and validate a user's identity through specific means. What are the three characteristics of authentication mechanisms?

A. Something a user knows, something a user has, and something a user is trying to get

B. Something a user knows, something a user has, and something a user is

C. Something a network needs, something a network is asking for, and something a user is assigned

D. Something a device knows, something a device is asking for, and something the network needs

19. Using a hidden program to capture the credentials a user has entered is an example of what?

A. Brute force attack

B. Keystroke monitoring

C. Masquerading

D. Dumpster diving

20. What is the single point of failure in a Kerberos architecture?

A. KDC

B. Client workstation

C. E-mail server

D. Application server

21. When a computer's operating system has been configured to allow only four failed login attempts, it is an example of _____.

A. An implementation of least privilege

B. A clipping level

C. A level of security clearance employed in MAC models

D. A threshold of data throughput that results in lost data when crossed

22. Which of the following is an example of a "database view" restricted interface?

A. Touch screen menu on an ATM machine

B. A limited list of executable commands on a user's system

C. A customer transaction report that hides fields pertaining to negotiated contract rates

D. A computer screen at a video store used to search for movie titles

23. A database that makes access decisions based upon the actual sensitivity of the data it holds is enforcing what type of access control technique?

A. Content-dependent

B. Context-dependent

C. Restricted interface

D. Role-based

24. A company's network that restricts users from accessing designated web sites has implemented what type of access control?

A. Role-based

B. Restricted interface

C. Rule-based

D. Database view

25. Which of the following authentication techniques is not based on something that you are?

A. One-time password

B. Palm scan

C. Keystroke dynamics

D. Retina pattern

26. Which of the following can help control physical access to areas of the organization with differing levels of sensitivity and access requirements?

A. Perimeter zones

B. Cordones

C. Control zones

D. DMZs

27. All of the following can be used to accomplish single sign-on (SSO) capabilities, except:

A. NTLM username and password combination

B. Kerberos

C. SESAME

D. LDAP

28. Which of the following allows for the exchange of authentication and authorization data between security domains?

A. XML

B. SAML

C. SSL

D. TLS

29. From where does information used for user provisioning come?

A. The employee

B. Supervisor

C. Internet

D. HR database

30. Which of the following is an example of a third-party identity management technology?

A. Kerberos

B. OpenID

C. Sesame

D. NTLM

31. During which process of user account creation would a user provide answers to personal questions to enable a self-service password reset?

A. Expiration

B. Modification

C. Registration

D. Application

32. Use of only one of the three common factors of authentication is known as _____ authentication.

A. multifactor

B. single-factor

C. two-factor

D. N-factor

33. All of the following are commonly used authentication factors, except:

A. Location

B. Knowledge

C. Posession

D. Biometric

34. The term "Verification 1:1" refers to which of the following?

A. The measurement of a single identity against multiple identities.

B. The measurement of an identity against a single claimed identity

C. The measurement of a single group identity against a single claimed identity

D. The measurement of a single group identity against a group claimed identity

35. What is the minimum number of factors required to be considered "strong authentication"?

A. One

B. Two

C. Three

D. Four

36. In order to hold a particular person responsible for their actions on the system, which of the following aspects of secure identities is required?

A. Nondescriptive

B. Issuance

C. Accountability

D. Uniqueness

37. What is the most important factor in successfully implementing a company-wide security program?

A. Realistic budget estimates

B. Hiring a reputable consulting firm

C. Security awareness

D. Having the support of senior management

38. How can one-time password generating tokens be considered two-factor authentication mechanisms?

A. The user may have to authenticate to the token device with a PIN before it will generate a one-time password. This is something a user knows (PIN) and something the user has (token device).

B. The user may have to authenticate to the system using his username and the one-time password, which is two-factor.

C. The user may have to authenticate to two systems using his username and the one-time password, which is two-factor.

D. The user may have to have the token and authenticate to the workstation during an authentication process, which is two-factor.

39. Companies should be aware of several issues before implementing a single sign-on technology. Which of the following does not describe a risk involved with this type of product implementation?

A. A single point of failure can be created, which would threaten the environment’s availability and productivity.

B. The technology, by default, is vulnerable to dictionary and brute force attacks, which allows easy entry into the environment.

C. If an attacker obtains a vaild set of credentials, she now has the "keys to the kingdom"—access to all of the company’s assets.

D. There is a high probability of incompatibility issues between current platforms and applications within the environment.

40. Often networking devices, databases, and programs will have their own access controls embedded in the software. Which of the following is the term used to define these types of controls?

A. Security perimeter

B. Trusted Kernel Base

C. Logical access controls

D. External access code

41. Your company has increased its physical security requirements and has asked you to implement a new biometric mechanism for controlling data center entrances. After presenting your analysis to the upper management team, they decide that they want the same level of security obtained with fingerprinting systems. However, they can't afford this system and have instructed you to find an alternative that provides virtually the same level of protection. To do so, you have to identify which one of the following controls?

A. Detective

B. Physical

C. Compensation

D. Corrective

42. All of the following terms are tools used to increase password security, except which one?

A. Password crackers

B. Password generators

C. Password policy

D. Password sharing

43. A company has recently changed the way it handles access control administration. Each business unit has been given full control of managing their own databases, systems, and user activities. The department head for each unit is now dictating user access control policies and making changes independently of other business units. Which of the following answers most accurately describes the access control administration being used enterprise wide?

A. A decentralized administration

B. A centralized administration

C. A RADIUS-controlled environment

D. A TACACS-controlled environment

44. Clement is the lead security professional within his company. One day he receives an e-mail from the CEO asking for information. The CEO wants to know all of the physical security controls currently in place. Clement has documented all of the security controls that have been implemented and begins to review his list. Which of the following controls should he not include in his reply?

A. IDS devices at the main entrance

B. Full-length walls in data centers

C. Demilitarized zone for all core systems

D. Proper lighting

45. Tyler has just been promoted from team lead to department manager and is moving into his new office. He was told he would receive a laptop computer now that he is a salaried employee and will be expected to work during off-hours occasionally. When he logs in to the new laptop, he discovers that he has inherited his boss's old computer and quickly finds confidential files containing salary information and performance ratings for all employees in the department, even those not reporting to him. What security violation has just occurred?

A. Piggybacking

B. Social engineering

C. Emanation

D. Object reuse

46. Brad is in charge of building a new data center with specific security requirements. He ensures all cables are shielded, builds solid walls that reach from the true floor to the true ceiling, and installs a white noise generator. What attack has Brad most likely been instructed to protect against?

A. Emanation attacks

B. Social engineering

C. Object reuse

D. Wiretapping

47. Aaron works from 7:00 A.M. to 5:00 P.M. during the normal business week and rarely works overtime. Lately, however, he has been coming into the office after 10 P.M and leaving again at midnight. Unknown to Aaron is that his boss, Kathleen, uses an auditing tool that monitors and analyzes activities and is aware of his abnormal behavior. What is this tool called?

A. Attack signature-detection tool

B. Variance-detection tool

C. Keystroke-monitoring tool

D. Scrubbing tool

48. Mike's company needs to implement a new security mechanism in order to monitor the following activities:

1) selected individuals' login attempts to a customer database;

2) commands executed by these individuals;

3) the files opened and closed in each session.

What tool could Mike utilize to obtain this information?

A. Host-based IDS

B. Network-based IDS

C. ACLs

D. Discretionary

49. Nathalie has access to the following: the customer provisioning database, shared network drive F:, the company's intranet, and the customer records database. These systems are referred to collectively as her what?

A. Trusted computing base

B. Clipping level

C. Domain

D. Virtual machine

50. Rob works in an IT department and is responsible for building user profiles and accounts for new employees. When he receives a work order to create a profile for Heather, a new operations technician, he simply assigns her to the Operations group, thus giving her all the necessary access rights and permissions to carry out her tasks. What type of access control model did Rob use?

A. Role-based

B. Rule-based

C. Mandatory

D. Discretionary

51. Kerberos is a single sign-on technology based on symmetric key cryptography. It is used as a way of authenticating users one time, which allows them to access many systems and network resources over a specified period of time. Which one of the following characteristics does not apply to Kerberos?

A. The KDC can be a single point of failure.

B. It uses session keys.

C. The KDC contains an authentication service and ticket-granting service.

D. It uses PACs between principals.

52. Biometric mechanisms are popular countermeasures among companies requiring high levels of security. But like all security controls, they are not perfect. If a security professional saw an abundance of Type I errors on a monthly biometrics report, what would this mean?

A. Unauthorized individuals were incorrectly granted access.

B. Access was granted to all individuals.

C. Authorized individuals were incorrectly rejected.

D. The system recorded errors but no security breaches were recorded.

53. Lisa was recently a victim of a computer attack. When she typed in her access credentials, an error message was displayed on the screen. She thought that she typed the password correctly,

but wasn't entirely sure, so she retyped it. The same thing happened again until finally after her third logon attempt, she was granted permission. Later, it was discovered her first logon attempt was actually captured by an attacker who logged the information and used it to authenticate as Lisa at a later time. What kind of attack does this describe?

A. Brute force attack

B. Dictionary

C. Honeypot

D. Spoofing

54. Physical, technical, and administrative controls can provide a variety of services in security, such as preventive, detective, corrective, deterrence, recovery, or compensation. What type of protection does rotation of duties provide?

A. Corrective

B. Detective

C. Compensation

D. Recovery

55. Intrusion detection systems (IDSs) are complex tools with many components. Each component serves a specific purpose. Which component actually initiates an alarm or activity when the system detects a violation?

A. Response box

B. Analysis reports

C. Central monitoring software

D. Database component

56. Single sign-on technologies, such as Kerberos and SESAME, are utilized in companies that use multiple systems, platforms, and programs. There are many advantages to both the administrator and the user. Which of the following characteristics would not be true of single sign-on technologies?

A. Can be useful when a user account needs to be closed out

B. Limits the potential for attackers to compromise multiple systems

C. Reduces the likelihood that users will write down multiple passwords

D. Improves employee productivity because of instant access to resources after authenticating one time

57. Passive attacks involve an attacker watching or listening to a network, a device, or an individual. There are several types, one of which is emanation attacks. In an emanation attack, a hacker uses tools to intercept electrical signals released from computers. Which one of the following countermeasures does not address emanation attacks?

A. TEMPEST

B. Mandatory access control

C. White noise

D. Zones

58. Most companies that have remote connectivity options for their employees use a RADIUS solution. RADIUS technology authenticates users over connections like network connections, PPP, and SLIP. Which one of the following sequences is in correct order for a RADIUS authentication process?

A. User dials into RADIUS server, RADIUS server prompts user for credentials, user inputs

credentials, RADIUS accepts or rejects user.

B. User dials into an access server, access server forwards the connection to RADIUS server, RADIUS server prompts user for credentials, user inputs credentials, access server accepts or rejects user.

C. User dials into a RADIUS server, RADIUS server initates a challenge, user enters credentials, RADIUS accepts or rejects user.

D. User dials into an access server, access server prompts user for credentials, user enters credentials, access server forwards credentials to RADIUS server, RADIUS server accepts or rejects request.

59. War dialing can take advantage of vulnerabilities in a network. It is often carried out by a software program that continually dials phone numbers and extensions within a company searching for modems. What countermeasure would not be effective at reducing the success of this kind of attack?

A. Perform wardialing on the company as part of a penetration test.

B. Have modems pick up after the fourth or fifth ring.

C. Aggressively pursue the attacker by publishing phone numbers that they will try to access.

D. Keep phone numbers private.

60. Which of the following is the best approach for validating a user's continued need for privileged access to system resources?

A. Periodic review of data classifications and system controls

B. Periodic review and recertification of privileged user needs

C. Periodic review of audit logs and access attempts by all users

D. Revoke processes used to grant these types of access

61. What do tickets allow within a Kerberos environment?

A. Grants user discretionary control to different resources

B. Enforces a mandatory access control approach

C. Permits a subject to access an object

D. Assures a user's accountability

62. Which of the following is not a single sign-on access approach?

A. Scripts

B. Thin clients

C. Kerberos

D. Discretionary

63. Which of the following is used to validate a user’s identity with a confidential number?

A. Key

B. Challenge

C. PIN

D. Initialization vector

64. Which of the following is the least important to include on a log that captures security violations?

A. User ID

B. Type of violation

C. Date and time of violation

D. Access control in place

65. Which of the following is not included in the classic ways of authenticating a user?

A. Something you know

B. Something you have

C. Something you control

D. Something you are

66. Which of the following can be used to detect new attacks not previously identified?

A. Signature-based IDS

B. Knowledge-based IDS

C. Behavior-based IDS

D. Expert system

67. Which of the following is not used to control "leakage" of electrical signals?

A. TEMPEST

B. Mandatory control

C. Control zone

D. White noise

68. Which of the following does not describe a synchronous token device?

A. Challenge-based

B. One-time password generator

C. Time-based

D. Authentication mechanism

69. Fact or opinion-based passwords are referred to as what?

A. One-time passwords

B. Cognitive passwords

C. Virtual password

D. Token device

70. Which of the following are the three types of models used in access control?

A. DAC, MAC, and RBAC

B. RBAC, LBAP, and TBAC

C. MAC, LBAP, and TBAP

D. DAC, MAC, and DDAC

71. Changes to payroll information require several steps of approval by different levels of management and personnel. Which access control technique would best describe this scenario?

A. DAC

B. Password security

C. Separation of duties

D. RADIUS

72. In Kerberos, what entity controls the keys?

A. Authentication service (AS)

B. Ticket granting service (TGS)

C. Ticket

D. Key Distribution Center (KDC)

73. TACACS+ provides what type of access control administration?

A. Centralized

B. Mandatory

C. Discretionary

D. Decentralized

74. An intrusion detection system that monitors activities within a particular system is called?

A. Host-based

B. Statistical

C. Network-based

D. Knowledged-based

75. What is another name for a dynamic password?

A. One-time password

B. Passphrase

C. Virtual password

D. Cognitive password

76. Which of the following is not an example of a preventive physical access control?

A. Fence

B. Security guard

C. Locks

D. Passwords

77. If a company is going to use keystroke monitoring to monitor their employees they need to do all but which one of the following?

A. A banner should be displayed during logon describing the possibility of monitoring.

B. It should be included in security awareness training.

C. Employees should be informed that monitoring is taking place.

D. It should be addressed in a security policy

78. Access controls that give subjects and objects a range of upper and lower bound capabilities are called _____.

A. Security labels

B. Lattice-based

C. Mandatory

D. Task-based

79. Which of the following is an example of a preventive-physical access control?

A. Implementing preemployment background checks

B. Conducting security awareness training

C. Configuring access control lists on routers

D. Locking laptop docking stations

80. The process of identifying an individual by the unique blood vessel pattern on the back of the eyeball is called what?

A. Retina scan

B. Iris scan

C. Facial scan

D. Blood scan

81. What type of control is auditing?

A. Preventive

B. Administrative

C. Technical

D. Physical

82. What important variable is used when evaluating the effectiveness of biometric systems?

A. False acceptance rate (FAR)

B. Acceptance by society

C. False rejection rate (FRR)

D. Crossover error rate (CER)

83. Which biometric mechanism identifies an individual by electrical signals emitted by their physical movement?

A. Facial scan

B. Hand geometry

C. Signature dynamics

D. Finger scan

84. Which of the following is not a weakness of Kerberos?

A. Secret keys are vulnerable when they are temporarily stored on users' workstations.

B. Network traffic is not protected if encryption is not enabled.

C. More and more products are beginning to support it.

D. The KDC is a single point of failure.

85. Capability tables are bound to_____.

A. Objects

B. Users

C. Subjects

D. Models

86. Which of the following administrative controls is not considered detective?

A. Incidence response

B. Inspections

C. Separation of duties

D. Job rotation

87. Determining what a user can access based on the data, not the subject's identity, is called what?

A. Content-based access control

B. Role-based access control

C. Rule-based access control

D. Capability table access control

88. Privileged Attribute Certificates (PACs) are used in what single sign-on technology?

A. Kerberos

B. Scripting

C. Thin clients

D. SESAME

89. All of the following are technical controls except?

A. Auditing

B. Testing

C. Network architecture

D. Encryption

90. What is the study and control of spurious electrical signals that are emitted by electrical

equipment called?

A. IDS

B. Zones

C. White noise

D. TEMPEST

91. A server with open ports placed within a network to entice an attacker is called what?

A. Entrapment

B. Honeypot

C. DMZ

D. KDC

92. An intrusion detection system works on the premise of which one of the following?

A. A pattern of malicious activity can be distinguished from normal usage.

B. A pattern of malicious activity can be distinguished from attacks.

C. A pattern of malicious activity cannot be identified.

D. A pattern of malicious activity can be contained.

93. Using a PIN and a token device accomplishes which one of the following?

A. Four-factor authentication

B. Three-factor authentication

C. One-factor authentication

D. Two-factor authentication

94. What are the two types of one-time password generator token devices?

A. Event- and time-driven

B. Synchronous and asynchronous

C. Central and decentralized

D. Discretionary and mandatory

95. Which of the following cannot be detected by a network-based intrusion detection system?

A. Brute force attack from thin clients and dumb terminals

B. Internal attack

C. DoS attack

D. Attack coming in through a SSL connection

96. How are smart cards and memory cards functionally different?

A. Memory cards process information while smart cards can store information but not process it.

B. Memory cards store, but do not process, information while smart cards can process information.

C. Memory cards and smart cards store and process information but do so in different ways.

D. Memory cards use integrated circuits and a processor.

97. Single sign-on systems have a main strength and a main weakness. Choose the answer that best identifies the strength and weakness.

A. Users do not need to remember multiple passwords, but access to many systems can be obtained by cracking only one password, making it less secure.

B. They allow the user to make use of very simple passwords; it puts undue burden on IT to administer the system.

C. They force the user to make use of stronger passwords; it makes it easier for users but

encourages laxness in regard to security policies.

D. They remove the burden of remembering multiple passwords from users; users need to type the same password when confronted with authentication requests for different resources.

98. How can logging play a role in stopping security breaches in a system?

A. Logging is the activity of collecting system information that will be used for monitoring and auditing to enable early detection of security problems.

B. Logging is the cataloguing of performance issues to fight intruders.

C. Logging plays a very minimal role in system security; it is used more as a housekeeping measure than as a factor in an effective security program.

D. Logging is the process of identifying user errors and not security breaches.

99. Which of the following accurately describes the architecture of a Kerberos authentication system?

A. An architecture with a central server that issues tickets to allow one principal (e.g., a user) to authenticate itself to another (e.g., a server).

B. A peer-to-peer system where peers authenticate themselves directly with other peer machines.

C. A centralized system that generates tickets to allow principles to exchange public keys.

D. A single sign-on architecture used for remote dial-in users to authenticate to a domain controller.

100. Your office is implementing an access control policy based on decentralized administration which is controlled directly by the owners and creators of files. What is the major advantage and disadvantage of such an approach?

A. It puts access control into the hands of those most accountable for the information, but requires security labels for enforcement.

B. It puts access control into the hands of those most accountable for the information, but leads to inconsistencies in procedures and criteria.

C. It puts access control into the hands of IT administrators, but leads to procedures and criteria that are too rigid and inflexible.

D. It puts access control into the hands of IT administrators, but forces them to overly rely upon the file owners to implement the access controls IT puts in place.

101. Which of the following best describes access control?

A. A method of ensuring that a subject (user, program, or process) is the entity it claims to be

B. Requiring the subject to provide a second piece to the credential set, as in a password, passphrase, cryptographic key, or token

C. Security features that control how users and systems communicate and interact with other systems and resources

D. Controls how an active object accesses a passive subject

102. The steps of an access control model should follow which logical flow?

A. Identification, authorization, authentication

B. Authorization, identification, authentication

C. Identification, authentication, authorization

D. Identification, accountability, authorization

103. Which of the following gives an accurate picture of biometrics?

A. Relatively inexpensive, well received by society, and highly accurate

B. Very expensive, moderately received by society, and moderately accurate

C. Very expensive, very well received by society, and highly accurate

D. Very expensive, not well received by society, and highly accurate

104. Your biometric system has been known to accept imposters. What type of error is this?

A. CER

B. Bioacceptance error

C. Type II error

D. Type I error

105. You are trying to implement a strong authentication system. Which one of the following would be the appropriate system to implement?

A. A smart card reader

B. Username and password

C. A token card that requires a PIN

D. A biometric device

106. What type of operating parameter can an administrator set that would lock out a user after a certain amount of failed logon attempts?

A. Clipping level

B. Password checker

C. Cognitive checker

D. Password management

107. What is the appropriate default level for an access control mechanism?

A. Everyone full control

B. Everyone read access

C. No access

D. Administrator full control, everyone else write access

108. What would be a common access control technique used in firewalls and routers for processing packets?

A. Role-based access control

B. Rule-based access control

C. Restricted interfaces

D. Access control matrix

109. Which centralized access control authentication protocol is an open protocol?

A. RADIUS

B. TACACS

C. TACACS +

D. Extended TACACS (XTACACS)

110. Which answer best describes the benefits of using cognitive passwords?

A. The password can only be used once and then it is destroyed.

B. Users do not need to remember one specific password.

C. It protects from eavesdropping of passwords.

D. It is turned into a virtual password by the system.

111. What are the types of components or services used for technical (logical) controls?

A. System access, encryption and protocols, auditing

B. System access, testing, network segregation, auditing

C. Policies and procedures, personnel controls, testing

D. Perimeter security, data backup, cabling

112. Categories within a security label are used to enforce which one of the following?

A. Need to know

B. Clearance

C. Classification

D. Clipping levels

113. What is the electronic phenomenon that allows data to escape in a bundle of network cables?

A. Tempest

B. Cross-talk

C. Attenuation

D. Covert channels

114. Why are biometric systems considered more accurate than many of the other types of authentication technologies in use today?

A. They are less accurate.

B. They are harder to circumvent than other mechanisms.

C. Biometric systems achieve high CER values.

D. They have less Type I errors than Type II errors.

115. Choose the following answer that has the correct definitions for false rejection rate (FRR) and false acceptance rate (FAR).

A. FAR is a Type I error and FRR is a Type II error.

B. FAR is the value of authorized individuals who were improperly rejected and FRR is a Type I error.

C. FRR is a Type I error and FAR is the number of imposters who were rejected.

D. FRR is the amount of authorized users who were improperly rejected and the FAR is a Type II error.

116. Which of the following is the best definition for equal error rate (EER)?

A. Type I error equals Type II error

B. When a dictionary attack creates as many errors as an exhaustive attack

C. The amount of errors created in a behavioral IDS

D. When DAC and MAC systems allow the same amount of unauthorized access attempts

117. There are different types of biometric systems available today. Some make authentication decisions based on behavior and some make authentication decisions based on physical attributes. Which of the following is the best description of their differences?

A. A system that uses physical attributes provides more accuracy than one that uses behaviors.

B. A system that uses behavior attributes provides more accuracy than one that uses physical attributes.

C. A fingerprint system is an example of a physical attribute and an iris system is an example of a behavior system.

D. A voice print system is an example of a behavior and signature dynamics is an example of a physical attribute.

118. When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A. How long it takes to setup individual user accounts.

B. The amount of time it takes to convert biometric data into a template on a smart card.

C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information.

D. The amount of time and resources that are necessary to maintain a biometric system.

119. Syskey is a technology provided and used in Microsoft Windows environments. What is Syskey and what is its importance?

A. It is a utility that can be used to encrypt the database that holds all of the system's, or network's, passwords.

B. It is a utility that uses a 128-bit key to encrypt individual passwords.

C. It is the utility that is used to encrypt passwords before they are sent over the network.

D. It is the utility that uses MD4 to hash all passwords.

120. What is a salt and what is it used for in a Linux or Unix system?

A. A salt is a value that is used to encrypt passwords before they are stored in the registry.

B. A salt is a value that adds randomness to the process of encrypting passwords.

C. A salt is also called a shadow file and is not readable by all users.

D. A salt is the utility that is used to encrypt and hash passwords.

121. Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on physical attributes.

B. An authentication system that creates one-time passwords that are encrypted with secret keys.

C. A biometric system that bases authentication decisions on behavioral attributes.

D. An authentication system that uses passphrases that are converted into virtual passwords.s

122. Joan's two network engineers are in a passionate debate over the value of a soft token versus a hard token device. Which of the following best describes a soft token?

A. Software that creates one-time passwords

B. Software that creates passwords for users, also called a password generator

C. A time-based one-time password generating device

D. A dynamic password versus a static password

123. A passphrase is turned into a virtual password, but what exactly is a virtual password?

A. The length and format required for a specific system or application

B. When a passphrase is turned into an encryption key

C. A hashed version of the passphrase

D. An encrypted version of the passphrase

124. Which of the following is a true statement pertaining to the different types of smart cards and their characteristics?

A. A contact smart card has its own power supply and communicates to a reader through an interface.

B. A contactless smart card has an antenna and communicates to the reader through radio waves.

C. A contact smart card contains a combi chip which furnishes it with a power supply.

D. A contactless smart card and a contact smart card are the same, except the contact smart card has its own power supply and the contactless card does not.

125. Paul has been handed two different smart cards and is told that one is a combo card and one is a hybrid card. What is the difference between the two?

A. Both can work as a contact or a contactless card. A combi has two chips and a hybrid card has one chip.

B. Both can work as a contact or a contactless card. A hybrid has two chips and a combi card has one chip.

C. Both can work as a contact or a contactless card, but the hybrid has an antenna.

D. Both can work as a contact or a contactless card, but the combi has an antenna.

126. Match one of the following to this definition: "The use of needles to remove the outer protective material on the card's circuits, by using ultrasonic vibration. Once this is completed then data can be accessed and manipulated by directly tapping into the card's ROM chips."

A. Microprobing

B. Differential power analysis

C. Electromagnetic analysis

D. Software attacks

127. Standards are critical for interoperability between different vendors' products. Which of the following is the ISO/IEC standard created for smart cards?

A. ISO/IEC 15442

B. ISO/IEC 15443

C. ISO/IEC 14442

D. ISO/IEC 14443

128. What is authorization creep and what is the best defense against it?

A. Employees continually being given more rights and permissions. The best countermeasure is to continue to review employees' need to know.

B. Employees continually being given less rights and permissions. The best countermeasure is to continue to review employees' need to know.

C. Employees continually being given more rights and permissions. The best countermeasure is to continue to review employees' job performance.

D. Employees continually being given less rights and permissions. The best countermeasure is to continue to review employees' collusion possibilities.

129. Which of the following is not true of Kerberos?

A. It is not based on symmetric cryptography.

B. It is a proprietary protocol.

C. It is an authentication protocol.

D. Its security relies in the integrity of the KDC.

130. Which of the following is a true characteristic of Kerberos?

A. The user sends over his username and password to obtain a ticket.

B. The TGT is generated to allow a principal to be able to communicate with the TGS.

C. The TGS creates a ticket that contains two secret keys encrypted with session keys.

D. The AS creates the ticket that allows the two communicating principals to obtain a session key.

131. How is Kerberos a single sign-on technology?

A. The user enters his credentials one time and obtains a TGT. The user uses the TGT each time he needs to communicate with a network resource.

B. The user enters his credentials one time and obtains a TGS. The user uses the TGS each time he needs to communicate with a network resource.

C. The AS keeps the user's authentication information in memory to ensure that an authenticated user does not need to continue to enter credentials.

D. The TGS keeps the user's authentication information in memory to ensure that an authenticated user does not need to continue to enter credentials.

132. Most Kerberos implementations use an authenticator. What is an authenticator and what is its purpose?

A. Principal identification and a timestamp encrypted with a shared secret key. It is used to authenticate the requesting principal and is a countermeasure against replay attacks.

B. Principal identification and a timestamp encrypted with a shared session key. It is used to authenticate the requesting principal and is a countermeasure against dictionary attacks.

C. TGS identification and a timestamp encrypted with a shared session key. It is used to authenticate the requesting principal and is a countermeasure against replay attacks.

D. Principal identification and a timestamp encrypted with a shared session key. It is used to authenticate the requesting principal and is a countermeasure against replay attacks.

133. Which of the following best describes the Lightweight Directory Access Protocol?

A. It allows subjects to access resources within a hierarchical database.

B. It allows objects to access resources within a hierarchical database.

C. It allows subjects to access resources within a flat directory.

D. It allows objects to access resources within a flat directory.

134. A directory service allows objects to be managed in databases by assigning which of the following?

A. LDAP names

B. Object identifiers

C. Distinguished names

D. Hierarchical domain names

135. Clement has been asked to work on the meta-directory portion of his company’s new identity management system. What is a meta-directory?

A. A virtual container for data from multiple sources

B. A central directory for all passwords and passphrases for proper password management

C. A component of an identity store that contains data from a single source

D. A tool that allows an administrator to manage physical identity data

136. How does a virtual directory play a role within an identity management system?

A. It has the same role and can be used instead of a password management tool.

B. It has the same role and can be used instead of a directory service.

C. It has the same role and can be used instead of a meta-directory.

D. It has the same role and can be used instead of a web access tool.

137. There are two ways that cookies on a computer can be dealt with. Which of the following does not describe these ways the best?

A. Permanent or session-based

B. Stored on hard drive or in memory

C. Sensitive data wiped and nonsensitive data stored

D. Transport-based and session-based

138. Many identity management systems have various types of password management approaches. Which of the following is not a common approach?

A. Password synchronization

B. Self-service password reset

C. Assisted password reset

D. Administrative password reset

139. Which of the following statements correctly describes biometric methods compared to most other commonly used authentication technologies?

A. They are the least expensive and provide the most protection.

B. They are the most expensive and provide the least protection.

C. They are the least expensive and provide the least protection.

D. They are the most expensive and provide the most protection.

140. What is derived from a passphrase?

A. Personal password

B. Virtual password

C. User ID

D. Valid password

141. Which of the following statements correctly describes passwords when compared to other commonly used authentication methods?

A. They are the least expensive and most secure.

B. They are the most expensive and least secure.

C. They are the least expensive and least secure.

D. They are the most expensive and most secure.

142. What is the reason for enforcing the separation of duties?

A. No one person can complete all the steps of a critical activity.

B. It induces an atmosphere for collusion.

C. It increases dependence on individuals.

D. It makes critical tasks easier to accomplish.

143. Which of the following is not a logical access control?

A. Encryption

B. Network architecture

C. ID badge

D. Access control matrix

144. An access control model should be applied in a _____ manner.

A. detective

B. recovery

C. corrective

D. preventive

145. How is a challenge/response protocol utilized with token device implementations?

A. This protocol is not used; cryptography is used.

B. An authentication service generates a challenge, and the smart token generates a response based on the challenge.

C. The token challenges the user for a username and password.

D. The token challenges the user’ s password against a database of stored credentials.

146. Which access control method is user directed?

A. Nondiscretionary

B. Mandatory

C. Identity based

D. Discretionary

147. Which one of the following provides the best authentication?

A. What a person knows

B. What a person is

C. What a person has

D. What a person has and knows

148. Which item is not part of a Kerberos authentication implementation?

A. Message authentication code

B. Ticket-granting service

C. Authentication service

D. Users, programs, and services

149. Which model implements access control matrices to control how subjects interact with objects?

A. Mandatory

B. Centralized

C. Decentralized

D. Discretionary

150. What does authentication mean?

A. Registering a user

B. Identifying a user

C. Validating a user

D. Authorizing a user

151. If a company has a high turnover rate, which access control structure is best?

A. Role based

B. Decentralized

C. Rule based

D. Discretionary

152. A password is mainly used for what function?

A. Identity

B. Registration

C. Authentication

D. Authorization

153. The process of mutual authentication involves _____.

A. A user authenticating to a system and the system authenticating to the user

B. A user authenticating to two systems at the same time

C. A user authenticating to a server and then to a process

D. A user authenticating, receiving a ticket, and then authenticating to a service

154. In discretionary access control security, who has delegation authority to grant access to data?

A. User

B. Security office

C. Security policy

D. Owner

155. Which of the following could be considered a single point of failure within a single sign-on implementation?

A. Authentication server

B. User’s workstation

C. Logon credentials

D. RADIUS

156. What role does biometrics play in access control?

A. Authorization

B. Authenticity

C. Authentication

D. Accountability

157. What determines if an organization is going to operate under a discretionary, mandatory, or nondiscretionary access control model?

A. Administrator

B. Security policy

C. Culture

D. Security levels

158. What type of attack attempts all possible solutions?

A. Dictionary

B. Brute force

C. Man in the middle

D. Spoofing

159. Spoofing can be described as which of the following?

A. Eavesdropping on a communication link

B. Working through a list of words

C. Session hijacking

D. Pretending to be someone or something else

160. Which of the following is not an advantage of a centralized access control administration?

A. Flexibility

B. Standardization

C. Higher level of security

D. No need for different interpretations of a necessary security level

161. Which of the following best describes what role-based access control offers companies in reducing administrative burdens?

A. It allows entities closer to the resources to make decisions about who can and cannot access resources.

B. It provides a centralized approach for access control, which frees up department managers.

C. User membership in roles can be easily revoked and new ones established as job assignments dictate.

D. It enforces an enterprise-wide security policy, standards, and guidelines.

162. Passwords are one of many types of authentication mechanisms. Which of the following is

not true of a password?

A. It is the least secure of access controls.

B. It is moderately used.

C. It can be automatically created by a password generator.

D. It relies heavily on the discipline of the user and the administrator.

163. A single sign-on technology that offers symmetric and asymmetric keys for encryption and uses Privileged Attribute Certificates (PACs) for authentication is called _____.

A. thin clients

B. SESAME

C. Kerberos

D. cryptographic keys

164. Which of the following biometric methods obtains the patterns and colors around a person's pupil?

A. Iris scan

B. Palm scan

C. Retina pattern

D. Fingerprint

165. Security labels are used in what type of model?

A. Role-based access control model

B. Mandatory access control model

C. Discretionary access control model

D. Military access control model

166. Passwords are one of the most sought-after items by attackers because of the level of access they can provide. Which of the following is the least effective when trying to protect against password attacks?

A. Employing a password generator system

B. Not allowing passwords to be shown in cleartext

C. Using dictionary attack tools to identify weaknesses

D. Implementing encryption and hashing algorithms

167. Which of the following access control types is considered a "soft" measure for protecting an organization as a whole?

A. Preventive-administrative

B. Preventive-physical

C. Predictive

D. Corrective

168. Which of the following best describes Extended TACACS (XTACACS)?

A. An Internet standard

B. Combines authentication and authorization

C. Separates authentication, authorization, and accounting processes

D. Has three-factor user authentication

169. A dynamic password is another name for what authentication mechanism?

A. Cognitive password

B. Smart card

C. Passphrase

D. One-time password

170. Which of the following best describes the difference/relation between a web portal and web portlets?

A. A web portal is an interactive application that provides web service functionality. Web portlets combine these portals into one interface.

B. A web portal is a centralized method of accessing various portlets in a unified manner.

C. A web portal is based upon HTML, and web portlets are based upon XML.

D. A web portal is used for federated identification, and web portlets carry out back-end authentication services.

171. Over the years the industry has developed and used various markup languages to be able to format various material for a wide range of users. There came a time when one overarching language was needed to provide a way to create different markup languages but still be interoperable. Which of the following is that overarching language?

A. Service Provisioning Markup Language

B. Extensible Markup Language

C. Security Assertion Markup Language

D. Security Markup Language

172. Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP). Which of the following is an incorrect definition or characteristic of this protocol?

A. Based upon XML

B. Provides a structured model for messaging

C. Only compatible with the application protocol HTTP

D. Exchanges data between web services

173. Which of the following best describes how SAML, SOAP, and HTTP commonly work together in an environment that provides web services?

A. Security attributes are put into SAML format. Web service request and authentication data are encrypted in a SOAP message. Message is transmitted in an HTTP connection.

B. Security attributes are put into SAML format. Web service request and authentication data are encapsulated in a SOAP message. Message is transmitted in an HTTP connection over TLS.

C. Authentication data are put into SAML format. Web service request and authentication data are encapsulated in a SOAP message. Message is transmitted in an HTTP connection.

D. Authentication data are put into SAML format. HTTP request and authentication data are encapsulated in a SOAP message. Message is transmitted in an HTTP connection.

174. Frank is the security manager of a financial institution. He has found out that the institution’s online banking application has allowed reply attacks to take place and attackers had fraudulently withdrawn some customers’ funds. Which of the following is not the most appropriate countermeasure that the institution could implement to thwart this type of threat?

A. Timestamping

B. Nonce

C. Session tokens

D. Cryptography

175. Ron needs to restrict employee access to the central database by only allowing access Monday through Friday and from 7 A.M. until 6 P.M. Which of the following best describes this

type of access control?

A. Temporal

B. Logical

C. Administrative

D. Physical

176. There are many activities and configurations that should be put into place to enforce proper access control. Which of the following is not one of these items that should be followed to enforce access control?

i. Deny access to systems to undefined users or anonymous accounts.

ii. Limit and monitor the usage of administrator and other powerful accounts.

iii. Suspend or delay access capability after a specific number of unsuccessful logon attempts.

iv. Remove obsolete user accounts as soon as the user leaves the company.

v. Suspend inactive accounts after 30 to 60 days.

vi. Disable unneeded system features, services, and ports.

vii. Replace default password settings on some accounts.

A. ii, iii

B. iv, v

C. vi, vii

D. iv, vii

177. Which of the following best describes why a behavior-based intrusion detection system (IDS) provides stronger protection against zero-day attacks compared to signature-based IDS?

A. This is a state-based attack type.

B. This type of solution maps the pattern of the attack type to the malicious packets.

C. There are no signatures for these types of attacks.

D. This type of attack only takes place through behaviors.

178. Jan has been told that the IDS product that is installed within her company's network assigns packets an anomaly score. Which of the following is most likely the type of IDS installed?

A. Signature based

B. Behavior based

C. Pattern based

D. Prevention based

179. _____ is a type of social engineering with the goal of obtaining personal information, credentials, credit card numbers, or financial data.

A. Pharming

B. Spear-phishing

C. Phishing

D. Spamming

180. Which of the following are specialized attacks that take more time for the hacker to craft because unique information has to be gathered about the target?

A. Rainbow tables

B. Pharming

C. Spear-phishing

D. Social engineering

181. John is the network administrator for a medical supply company. While reviewing some DNS

records on the DNS server he sees that some website addresses are actually pointing to incorrect IP addresses. Which of the following is the type of activity that has most likely taken place?

A. Pharming

B. Phishing

C. Masquerading

D. ARP poisoning

182. Sarah and her security team have carried out many vulnerability tests over the years to locate the weaknesses and vulnerabilities within the systems on the network. The CISO has asked her to oversee the development of a threat model for the network. Which of the following best describes what this model is and what it would be used for?

A. A threat model can help to assess the probability, the potential harm, and the priority of attacks, and thus help to minimize or eradicate the threats.

B. A threat model combines the output of the various vulnerability tests and the penetration tests carried out to understand the security posture of the network as a whole.

C. A threat model is a risk-based model that is used to calculate the probabilities of the various risks identified during the vulnerability tests.

D. A threat model is used in software development practices to uncover programming errors.

183. _____ is a set of precomputed hash values that represent password combinations.

A. Collision table

B. Password file

C. Cognitive table file

D. Rainbow table

184. The _____ allows for the automation of user management (account creation, amendments, revocation) and access entitlement configuration related to electronically published services across multiple provisioning systems.

A. Service Provisioning Markup Language

B. eXtensible Access Control Markup Language

C. Security Assertion Markup Language

D. Security Access Control Markup Language

第五章答案

1、 B D .Passwords and cryptographic keys are susceptible to brute force attacks. A brute force attacker tries every possible sequence of characters or bits to achieve their goal. Biometric and cognitive passwords can also be vulnerable to brute force attacks, but they are not as commonly attacked in this manner.

2、 B .While passwords are insecure and often implemented incorrectly, they remain the most popular authentication control used today. Because they impose little burden on the user and are simple and inexpensive to implement, companies continue to employ passwords within their systems and networks.

Passwords are not used moderately, but very frequently.

3、 B .Secure European System for Applications in a Multivendor Environment (SESAME) is actually a technology built upon the Kerberos foundation. However, SESAME provides different capabilities and uses public key cryptography. SESAME differs from Kerberos in that it uses PACs for authentication instead of the Kerberos ticket exchange methodology.

4、 A .An iris scan system records the colors and patterns around a pupil of a person's eye. This is different than a retina scan, which records the blood vessel patterns at the back of the eye.

5、 B .Mandatory access control (MAC) models use security labels to hold classification information assigned to objects. If a user wants to access an object, she must have an equal or greater level of clearance. Although military organizations commonly use security labels, the answer "military access control model" does not really exist.

6、 D .A password advisor is a very effective way of improving the creation of new passwords. This program allows the user to select their own password, which means they will be more likely to remember it. However, the advisor creates options for the user that are more out-of-the-ordinary than typical user-chosen codes.

7、 C .Diameter is a more diverse centralized access control administration technique than RADIUS and TACACS+ because it supports a wide range of protocols that often accompany wireless technologies. RADIUS supports PPP, SLIP, and network connections. TACACS+ is a RADIUS-like methodology that is Cisco-proprietary. Kerberos is a single sign-on technology, not a centralized access control administration protocol.

8、 A .While password generators protect against dictionary attacks, they often force users to write down their password, which creates a new vulnerability. Having an office full of sticky notes with scribbled passwords is an attractive atmosphere for a potential hacker.

9、 B .Least privilege is a security principle that grants users access only to those resources that are mandatory to fulfilling their responsibilities. A common breach of least privilege is when an employee transfers to another department but maintains his previous access permissions even though it is not necessary. This is referred to as authorization creep.

10、 A .Organizations use a variety of techniques to protect themselves, such as employee background checks, drug screens, security training, policies, procedures, standards, and hiring and firing policies. These types of actions fall under the preventive-administrative category, which is often referred to as "soft" access controls.

11、 C .Terminal Access Controller Access Control System has three versions: TACACS, XTACACS, and TACACS+. Each version offers different functionality, but it is XTACACS that separates authentication, authorization, and accounting processes.

12、 A .Hybrid administration is a common access control method. It combines the centralized and decentralized approaches. Individual users may be able to dictate who can access their shared and local files, but the IT administration would control access to file servers, network printers, and network devices.

13、 D .Guard dogs and CCTV are mechanisms used to protect the physical surroundings of a building or campus. Other examples of preventive physical controls are fences, alarm systems, and access badges.

14、 B .Scripting is a very simplistic method of achieving single sign-on capabilities. A command string is written for each user containing his credentials. When he attempts to access a device, the script is initiated, providing the necessary sign-on information to allow access. Scripts are also the least secure; username and password are stored in plain text files on the system.

Kerberos and SESAME are more complicated architecture systems that must be installed on users' machines in order to communicate with a central server. KDC is the core component within Kerberos.

15、 D .One-time or dynamic passwords provide an increased level of security as they are valid for only one logon transmission. They can be generated by a token device and help prevent replay attacks.

16、A .Constrained user interfaces are effective security measures because they protect sensitive areas of systems and their data. By limiting ATM users to certain functions (withdrawals, deposits, inquiries), the chances of user error or mischief is significantly decreased. The fewer capabilities an interface provides translates into fewer opportunities for an attacker.

17、 C .In role-based access control (RBAC) models, users are assigned certain roles. These roles have access restrictions and permissions already established, so once the user is assigned to the role, she inherits the properties of that role. Large companies with high staff turnover will often use a role-based model because it is easier to maintain than the other model types.
Rights assigned to an individual are explicitly assigned. Rights assigned to a role or group that are inherited by the user are implicitly assigned.

18、 B .Authentication is the next security phase after identification. It involves proving that the subject is who he says he is. Something a user knows can be a password. Something a user has can be an access badge. Something a user is, is a biometric physical attribute. Strong authentication, also referred to as two-factor, uses two out of these three.

19、 B .Keystroke monitoring can be used both by a security professional and a hacker. Hackers typically use this technique by planting a program on the victim's computer that records important inputted information, such as user IDs and passwords. However, keystroke monitoring can also be used ethically if strict security and privacy regulations are followed. For example, if an

employee is suspected of fraudulent behavior, management can request that his keystrokes be captured so that they can be analyzed. Notifying employees of this practice is very important, however. Typically, companies will inform employees that their computers, including all data and correspondence, is subject to continual surveillance.

20、 A .The Key Distribution Center (KDC) is the core component within Kerberos. It houses all of the principles' keys and performs authentication functionality. If the KDC goes down, users and network services could not authenticate to each other.

21、 B .One security mechanism that can be used with passwords is a clipping level. When an attacker tries guessing a user's password, she is given only a certain number of attempts before being "locked out." This protects the system from brute force attacks. The security professional sets the clipping level and determines when the account will be "unlocked."

A clipping level is another name for a threshold and is not used solely for describing passwords or login attempts. The word can be used anywhere the word 'threshold' is used.

22、 C .Database views help to conceal certain categories of information within databases depending upon who is accessing it. In a customer transaction database, customer service representatives may be able to see all information needed to perform their jobs, but they would not need to know the contract details agreed upon with the sales manager.

An ATM touch screen and a video store movie library are examples of physically constrained interfaces.

A list of executable commands on a user's system is an example of menus and shells.

23、 A .Content-dependent access control considers the sensitivity of the data to determine who can access it. A good example is payroll information in a personnel database. Fields that include salary information will be restricted from most users.

Context-dependent access is based on previous access requests.

Context-dependent access control uses many factors in granting access: user credentials, resource credentials, and the sequence of transactions prior to the access attempt.

24、 C .Rule-based access control restricts or permits access based upon a set of rules. This control cannot be modified by users.

In this example, the IT administrator may restrict all users from certain web sites based upon company policy.

It is ruled-based in that it affects all users across the board. Access decisions are not based on user identity.

25、 A .One-time passwords are used to authenticate users only once. They have the characteristic of "something that you have" because a user does not know or remember the one-time password. Instead, the user has something that generates that password.

The other choices are all examples of biometrics, which are based on what a user is.

26、 C .The company facility should be split up into control zones depending upon the sensitivity of the activity that takes place in each area.

27、 A .NTLM username and password combinations do not typically allow for single sign-on capabilities.

28、 B .The Security Assertion Markup Language (SAML) allows for the exchange of authentication and authorization da between security domains.

29、 D .Most identity management solutions pull user information from the HR database, because the data is already collected and held in one place and are constantly updated as employees' or contractors' statuses change. This is referred to as the authoritative source for the user provisioning information.

30、 B .OpenID is an open standard for user authentication by third parties. It is a lot like SAML, except that the users' credentials are maintained not by their company but by a third party such as Google, Microsoft, or Yahoo!.

31、 C .During the registration process of user account creation, users provide answers to personal questions to enable a self-service password reset in the event they forget their passwords.

32、 B .Single-factor authentication uses only one of the common authentication factors, such as the knowledge factor, for example, used in username and password combinations.

33、 A .Common factors used in authentication are something you know (knowledge factor), something you have (possession factor, and something you are (biometric factor).

34、 B .Verification 1:1 is the measurement of an identity against a single claimed identity.

35、 B .Strong authentication is also considered "multifactor" authentication, and uses at least two of the common authentication factors.

36、 D .Accountability is assured by the uniqueness of an identity, and its binding to a single individual. Accountability itself is not a characteristic of an identity.

37、 D .Without the support of senior management, a security program has little chance of

survival. More than any other, a company's leadership group will determine the program's success. Their authority within the company is a key factor. Budget approval, resource commitments, and company-wide participation also require buy-in from senior management.

38、 A .Two-factor authentication means that two of the three authentication methods are used: something you have, something you know, or something you are.

If a user needs to authenticate to the token, it means he will need to enter a PIN on the token device before he can use it. The PIN is something he knows and the token device is something he has. The user does not know the one-time password. He has something that generates it.

39、 B .The server that allows for single sign-on can be a single point of failure. Since the users only need to remember one set of credentials, the attacker only needs to uncover one set. And the technology needs to convert the credentials into a format that the various operating systems and applications understand.

This type of technology is no more vulnerable to dictionary and brute force attacks than other types of technologies.

40、 C .Logical access controls are built-in technical controls within a device or application. They are put into place mainly to protect the system and data.

41、 C .A compensation control is an alternative to the first choice. A company may need the protection that control A provides, but they cannot afford it or the cost-benefit analysis indicates that the potential loss does not warrant spending this much money on the control. In either case, the company finds a different control (control B), usually a cheaper one.

42、 D .Password generators create complex passwords for individuals.

Security professionals use password crackers to see how long it would take an attacker to uncover the passwords. The results may indicate that stronger passwords should be used.

43、 A .Decentralized administration spreads the access control authority, meaning no single group controls access for the whole company. Furthermore, no individual governing entity enforces and manages access controls.

RADIUS and TACACS are both technologies used in a centralized administration.

A peer-to-peer setup can also be an example of a decentralized administration configuration.

Although each business unit is using a centralized approach individually, the question asked specifically about what was being used enterprise wide.

44、 C .The CEO was looking for physical controls in place. A demilitarized zone (DMZ) is actually a

technical control designed to protect unauthorized access to data and systems. It is made up of systems and their configurations. It protects against logical intrusions.

The other answers are physical controls. Remember an intrusion detection system (IDS) can be a type of motion detector used in physical security and not necessarily the IDS used to monitor packet traffic.

45、 D .Object reuse is extremely dangerous but also extremely common in companies today. Because of employee turnover, as well as the continual evolution of computing supplies, it is common for computers to be handed down to other employees. A good countermeasure in this scenario is to have a standing policy stating that all files and media must be cleared before transferring computers to their new owners.

46、 A .Emanation attacks are the act of intercepting electrical signals that radiate from computing equipment. There are several countermeasures including shielded cabling, white noise, control zones, and TEMPEST equipment.

47、 B .Variance-detection tools focus on computer and resource usage. They identify trends and report any variances. A variance-detection tool is one of many automated auditing tools that can help to alert security professionals and managers of potential wrongdoing.

They can work as a behavior-based system by looking at things that are out of the "norm."

48、 A .Host-based intrusion detection systems (IDSs) can be installed on individual workstations and servers to watch for inappropriate or anomalous activity and insider attacks. Host-based IDSs are usually used to make sure users do not accidentally delete system files, reconfigure important settings, or put the system at risk in any other way.

A network-based IDS monitors network traffic, not individual files being opened and closed.

49、 C .A domain just means the resources that are available to subjects for carrying out their tasks. The subjects can be users, applications, or processes.

50、 A .The role-based access control model uses groups as containers for users. Each group is assigned specific permissions and rights. When a new user is added to the group, the user inherits all of its properties.

51、 D .The Key Distribution Center (KDC) contains all of the principals' secret keys and has an authentication service and ticket-granting service. Kerberos uses session and secret keys. It also uses tickets, not Privileged Attribute Certificates (PACs), which are used by SESAME.

52、 C .While Type I errors are bothersome to a person being rejected, they are errors that a company may choose to tolerate if they need to make sure no Type II errors take place. Type II errors are dangerous because they involve the access of an unauthorized person.

53、 D .Login spoofing screens can be very difficult for a user to detect. An attacker inserts a logon screen, which looks exactly like the normal screen. Most users just assume that they entered their credentials incorrectly and continue entering their information until they succeed.

54、 B .Rotation of duties is a control that can be used to detect fraudulent activities. If Bob was rotated into Sally's position, Bob may uncover some suspicious activities that Sally had been carrying out.

55、 A .Response boxes, as their name states, respond to an event. They receive a command within the intrusion detection system (IDS) and then perform an action. The IDS may send a page, e-mail a message, log the activity, attempt to reset the connection, or modify firewall configurations.

56、 B .Single sign-on technologies can actually make it easier on an attacker. Instead of having to work to steal multiple passwords, the attacker can focus on just one. With one user's credentials he will have access to all of the systems—a very dangerous situation for a company. This is referred to as the "keys to the kingdom."

Single sign-on technologies can be useful when closing out a computer account because the act of removing credentials from a network involves only a single step instead of many.

57、 B .Mandatory access control does not prevent the act of intercepting electrical signals.

TEMPEST provides a faraday cage around a device. White noise is a jamming signal. A zone is reinforced ceilings and walls within a facility.

58、 D .RADIUS solutions involve three components: a user, an access server, and a RADIUS server. The access server typically has a modem pool that a user dials into when trying to connect to a network. The access server is often referred to as a RADIUS client. It prompts the user for credentials and then sends them to the RADIUS server for authentication.

59、 C .A long list of phone numbers are inserted into a war dialing program in hopes of finding a modem that can be exploited to gain unauthorized access. A program is used to go through many phone numbers and weed out the numbers that are used for voice calls and fax machine services. The company can use these tools on itself to identify vulnerabilities. Many war dialers are configured to hang up after the third ring.

Modem and internal phone numbers should not be made public.

60、 B .A periodic review of the rights and permissions granted to all users (especially those with privileged access) and what they need in order to complete their tasks is the best approach for validating the reasons for access. A user may no longer need full control to specific resources and files, but a company would not uncover this without reviewing the actual needs of this user.

61、 C .Tickets are given from the ticket granting service (TGS) to subjects so that they can authenticate to resources and objects and access them.

62、 D .Companies can use scripts to hold user credentials, thin clients to access servers or mainframes, or Kerberos to provide a single sign-on environment. Discretionary does not have anything to do with single sign-on approaches.

63、 C .A PIN is a confidential number used in the authorization phase of access control. It is usually accompanied by a username or account number and the PIN is used to validate the identity of the user.

64、 D .The other three items should be included for each security violation detected. Systems can have several access controls in place, making it troublesome to log. In addition, the access control in place does not need to be in this type of documentation.

65、 C .Authentication is based on something that you know (password, PIN), something that you are (biometrics), and something that you have (memory or smart card or token device).

66、 C .One of the benefits of a behavior-based intrusion detection system (IDS) is that it can detect new attacks because it is not comparing strings within packets against a static database. A signature-based IDS cannot detect new attacks that have not been previously identified.

67、 B .Mandatory controls do not prevent leakage of electrical signals. The other three items can be used to control the amount of electrical radiation emitted from devices in the hopes of not disclosing information in an unauthorized manner.

68、 A .A synchronous token device is driven by time or events to authenticate users. An asynchronous token device uses a challenge-based mechanism during its authentication process.

69、 B .Cognitive passwords allow users to answer questions about themselves that are easy to remember but hard for an attacker to uncover. Some examples are a person's alma mater, mother's maiden name, favorite color, or pet's name.

70、 A .Access control can be implemented using three different models: discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). These models are integrated within the operating system and applications. DAC allows the data owner discretion on what subjects can access resources, MAC uses security labels, and RBAC uses roles and groups as containers for users.

71、 C .Separation of duties is put into place to ensure that one entity cannot perform a critical task alone. For fraud to actually take place, people would need to participate in collusion, which means more than one person work together to commit fraud.

72、 D .The Key Distribution Center (KDC) is the most important part of Kerberos because it holds all the cryptographic keys for the principals within a realm. The KDC can also be a single point of failure in this type of environment.

73、 A .TACACS+ is a client/server protocol used in dial-up access centralized environments. Centralized access control administration has one entity that makes all access decisions. In most implementations a firewall or router would have TACACS+ implemented and be the central authentication mechanism.

74、 A .Host-based intrusion detection systems are installed on individual systems to protect them from failures, accidental deletions, unauthorized reconfigurations, and attacks.

75、 A .One-time or dynamic passwords are good for only one session and are used in environments that require more security than a static password. If these passwords are intercepted by an attacker, they are only good for a small window of time, thus there is a smaller chance of successful replay attacks.

76、 D .Passwords are preventive controls, but are considered technical controls.

77、 C .As long as employees are properly notified, the company can implement keyboard monitoring with or without their consent.

78、 B .Lattice-based access controls provide upper and lower bounds of access for a subject pertaining to a specific object. When a subject makes an access attempt, the system will first check if it is allowed, and then determine the range of access the subject actually has. A subject may be able to "read" but not "write" to that object, thus "write" is outside of its lattice bounds.

79、 D .Locking laptop docking stations represent a physical access control and are considered preventive in nature. Background checks and awareness training are preventive-administrative and access controls on routers are technical in nature.

80、 A .Retina scans offer an effective way of identifying individuals by projecting a beam into the eye to distinguish between different blood-vessel patterns.

81、 C .Auditing is an important technical control that can be used to track the activities of systems, networks, or users. This is not referring to an auditor evaluating a company and its procedures, but rather to logs that are generated by operating systems and applications.

82、 D .The crossover error rate (CER) is the point at which Type I errors and Type II errors are equal and represents the best way of measuring a biometrics' effectiveness. A system with a lower CER value provides more accuracy than a system with a higher CER value.

83、 C .When a person signs his name, a unique physical motion can be captured electronically which provides a method of authentication. Signature dynamics capture the pressure someone

uses, the slant of holding the pen, the speed of writing, and the resulting static signature.

84、 C .Kerberos is an authentication protocol that allows principals to authenticate to each other. The Key Distribution Center (KDC) is the single point of failure, keys are temporarily stored on users' workstations, which can be compromised, and if encryption is not enabled then network traffic is not protected from eavesdropping. Kerberos is also vulnerable to dictionary attacks.

85、 C .A capability table is a list of the objects a subject has access to along with the operations the subject can carry out on those objects. A capability table is bound to a subject and an access control list is bound to an object. Together, they make up an access control matrix, the capability table being a row and access control list being a column.

86、 C .Separation of duties is put in place to ensure that one person cannot single-handedly perform a critical task. This is a preventive measure, intended to prevent fraud. Job rotation puts different people in different positions in order to detect possible fraudulent activities. Incident response looks into specific events, and inspections are conducted to search for suspicious activity and ensure normal procedures are taking place.

87、 A .Content-based access controls look at the sensitivity of the data to determine if a subject can access it or not. This mainly occurs in databases.

88、 D .The Secure European System for Applications in Multivendor Environments (SESAME) was developed to address weaknesses in Kerberos and uses a ticket authorization method called Privileged Attribute Certificate (PAC).

89、 B .Testing is an example of an administrative control. Although it seems that testing could be a technical control, it is management's responsibility to ensure that proper testing takes place. Auditing is a technical control as it pertains to software collecting data about the events that take place within a system.

90、 D .TEMPEST was developed in the 1950s by the US government to address electromagnetic radiation being emitted from electrical equipment. Data can be captured via electrical signals and reconstructed, which threatens the confidentiality of sensitive data.

91、 B .A honeypot is a sacrificial lamb placed in an area most likely to be attacked. It is made attractive by having several services running and ports open. The hope is that the attacker will only interact with that system and not the more critical production servers. Using a honeypot is an ethical way of enticing attackers and is a common security technique used within companies.

92、 A .Behavior-based intrusion detection systems (IDSs) build a profile that captures a network's "normal" characteristics and behavior. All proceeding activities are compared to this profile and anything falling outside of what is considered normal is considered an attack. This is how these types of IDS products uncover malicious activity.

93、 D .There are three main characteristics of authentication: what you know, what you have, and what you are. If a system requires one of these items, it is a one-factor system, if it requires the use of two for authentication purposes, then it is considered a two-factor system. Two-factor authentication is also known as strong authentication.

94、 B .A token device can create a one-time password for user authentication. There are two basic types: synchronous and asynchronous. Synchronous systems require that the token device and authentication system be synchronized by event or time. Asynchronous token devices require that the authentication system perform a challenge-response authentication procedure.

95、 D .A network-based intrusion detection system (IDS) will not be able to detect an attack that is encrypted. SSL is a protocol that encrypts a full communication channel, thus if an attack was coming through this channel the IDS could not identify it. An IDS should be able to detect the other mentioned attacks.

96、 B .Memory cards store, but do not process, information while smart cards can process information. Smart cards have microprocessors and integrated circuits.

97、 A .Single sign-on technologies are easier for users because they only need to enter one credential set. They also make administration easier for IT staff. It causes security concerns because now an attacker only needs to uncover one credential set to have access to all resources.

98、 A .Events are logged in the hope of uncovering anomalies that may indicate a security breach. They are also logged for performance tracking. Logs should be reviewed either manually or through automated means periodically.

99、 A .Kerberos uses a centralized server (KDC) that authenticates principals and generates tickets to allow the principals to authenticate to each other.

100、 B .This question is describing a DAC implementation, which allows the data owners to make the decision on who can access the resources they own. In that sense, control is located at a lower level than in a MAC environment. The question also refers to decentralized access control, which means there is no single entity controlling access rules. This can lead to inconsistencies as everyone makes up their own rules.

101、 C .Access control is all about controlling how active subjects access and use passive objects. The subjects can be users, programs, or processes.

102、 C .A subject's identity must first be submitted, then it needs to be verified, which is authentication. Then the system must decide what this subject can and cannot do, which is authorization.

103、 D .Compared to the other available authentication mechanisms, biometrics are the most expensive and least accepted by society. Biometrics are also much harder to fool or spoof than

the other mechanisms—this is what is meant by highly accurate.

104、 C .A Type II error means that the system has authenticated a person who should not be allowed into the environment. A Type I error means that the system did not successfully authenticate someone who is authorized to access the environment.

105、 C .The definition of strong authentication is two-factor, meaning two out of the three possibilities (something you know, have, or are). The only answer that is two-factor is a token card that requires a PIN.

106、 A .A clipping level is another name for a threshold. It is an old mainframe term. An administrator can set a threshold to allow a certain amount of failed logins before the user is locked out.

107、 C .Any security mechanism should default to no access. This means that no subject will be granted access unless the administrator or security professional specifically grants that subject access.

108、B .Rule-based access control means that all subjects will be restricted by a particular rule or rule set. A router and firewall make access decisions based on the characteristics of the packets themselves and less on the identity of the sender of the packets.

109、 A .RADIUS is the only open protocol listed. An open protocol means that different vendors can obtain a copy of the source code and change it to work with their product or environment. The other protocols are Cisco-proprietary protocols, thus the source code is not available.

110、 B .When cognitive passwords are used, the user is asked several questions about their life experience: mother’s maiden name, favorite color, pet’s name, etc. The user will most likely not have a hard time remembering this information compared to a password.

111、 A .All items in the correct answer are considered technical controls. Testing, policies and procedures, and personnel issues are administrative controls. The other items listed are physical controls.

112、 A .The categories indicate which subsets of data the user has been granted a need to know. The label has another section that dictates the necessary clearance level.

113、 B .When wires are twisted around each other or are in close proximity, cross-talk can occur. Cross-talk means that signals from one wire "spill over" and disrupt signals on another wire. UTP has different categories and ratings. Many of the different ratings pertain to how tightly the wires are twisted around each other. The tighter the twisting, the less vulnerable the wires are to cross-talk.

114、 B .Biometric systems make access decisions based on physical attributes of human beings.

These attributes are much harder to impersonate compared to a password, passphrase, cryptographic key, or token devices. CER and Type I and II errors pertain only to biometric systems and not to any other authentication technologies.

115、 D .FAR is a Type II error and is when an imposter is authenticated. FRR is a Type I error and is when a user who should be authenticated is rejected. These errors are used to measure the accuracy of biometric systems.

116、 A .Equal error rate (EER) is another name for crossover error rate (CER). EER is when the number of Type I errors is equal to the number of Type II errors. It is a metric that is used to indicate the accuracy of a biometric system.

117、 A .A biometric system can make authentication decisions based on an individual's behavior (signature dynamics, voice prints), but these can change over time and possibly be forged. Biometric systems that base authentication decisions on physical attributes (iris, retina, fingerprint) offer more accuracy because these attributes do not change as often and are more difficult to impersonate.

118、 C .When reviewing biometric devices for purchase, one component to take into consideration is how long it takes to actually authenticate users. From the time a user inserts data until she receives an accept or reject response should take between 5 – 10 seconds.

119、 A .In most situations, if an attacker sniffs your password from the network wire, she still has some work to do before she actually knows your password value. This is because most systems hash the password with a hashing algorithm, commonly MD4 or MD5, to ensure that passwords are not sent in clear text. The operating system encrypts the password into a hashed value, not the Syskey utility. In a Windows environment the passwords are stored in a Security Accounts Management (SAM) database in their hashed version. For extra protection, administrators can use a Syskey utility that encrypts the database storing the passwords with a locally stored system key.

120、 B .Unix systems, and Linux systems, do not use registries and SAM databases, but contain their user passwords in a file cleverly called /etc/passwd. A password is used to encrypt a block of bits with a one-way function and the resulting value is stored in this file. Salts are random values that are added to the encryption process to add more randomness. The more randomness to the encryption process, the harder it is for attackers to decrypt and uncover your password.

121、 B .There are two main types of synchronized token one-time password generators: counter-based and time-based. If the token device and authentication service use counter-synchronization, the user will need to initiate the logon sequence on the computer and push a button on the token device. This causes the token device and the authentication service to advance to the next authentication value. This value and a base secret is hashed and displayed to the user. This is the user's one-time password.

122、 A .One-time passwords can also be generated in software, instead of requiring a piece of hardware as in a token device. These are referred to as soft tokens and require that the authentication service and application contain the same base secrets, which are used to generate the one-time passwords.

123、 A .A virtual password is the length and format that is required by the application. For example, an application may require your virtual password to be 64 bits to be used as a key with the AES algorithm. Not all applications would require that passphrases be turned into key sizes, this is just one example.

124、 B .Two general categories of smart cards are the contact and the contactless types. When a contact smart card is fully inserted into a card reader, electrical fingers wipe against the card in the exact position that the chip contacts are located. This supplies power and data I/O to the chip for authentication purposes. The contactless smart card has an antenna wire that surrounds the perimeter of the card. When this card comes within an electromagnetic field, the antenna within the card generates enough energy to power the internal chip. Neither card type has its own power supply.

125、 B .A variation of a contact and a contactless smart card is referred to as a hybrid or combo smart card. The hybrid cards have a dual chip in them with the capability of utilizing both the contact formats and the contactless antenna model. They both have an antenna in order to work in contactless mode.

126、 A .Microprobing uses needles to remove the outer protective material on the card's circuits by using ultrasonic vibration. Once this is completed then data can be accessed and manipulated by directly tapping into the card's ROM chips. This is considered an invasive attack that can be used against smart cards.

127、 D .ISO/IEC 14443 outlines the following items for smart card standardization:

- ISO/IEC 14443-1 — Physical characteristics
- ISO/IEC 14443-2 — Radio frequency power and signal interface
- ISO/IEC 14443-3 — Initialization and anti-collision
- ISO/IEC 14443-4 — Transmission protocol

128、 A .Authorization creep is when individuals are given more and more access rights over time. It can be a large risk for a company when too many users have too much privileged access to company assets. Users' access needs and rights should be periodically reviewed to ensure that they only have access to the resources they need to complete their tasks.

129、 B .Kerberos is an open authentication protocol (not a proprietary one) that is based on symmetric cryptography. It is used because the individual principals do not trust each other enough to communicate directly. The KDC holds all of the secret keys, it vouches for the identity of the other principals, and it has to be completely protected from corruption.

130、 B .The user only sends over his username to the authentication service (AS). The AS creates a ticket granting ticket (TGT) which is encrypted with the user's secret key. The TGT is used to communicate to the ticket granting service (TGS). The TGS creates a ticket that contains two instances of the same session key that is encrypted with the individual principals' secret keys. It is this second ticket that allows the two principals to obtain their session keys.

131、 A .The user enters his credentials and obtains a TGT. The TGT has a timestamp that makes it valid for 8 – 10 hours, depending upon how the network administrator configured it. Each time the user needs to access a network resource his Kerberos client sends the TGT to the TGS which creates a second ticket. The second ticket is used by the user to authenticate to the network resource.

132、 D .If a Kerberos implementation is configured to use an authenticator, the user will send the network resource her identification information and a timestamp encrypted with the session key they share. The resource will decrypt this information and compare it with the identification data the KDC sent regarding the requesting user. If the data is the same, the resource allows the user to communicate with it. The timestamp is used to help fight against replay attacks. The resource will compare the sent timestamp with its own internal time. This will help determine if the ticket had been sniffed and copied by an attacker and submitted at a later time in the hope of impersonating the legitimate user to gain unauthorized access.

133、 A .Lightweight Directory Access Protocol (LDAP) allows subjects and applications to interact with a directory. Applications can request information about a particular user by making an LDAP request to the directory, and users can request information about a specific resource by using a similar request.

134、 C .Each directory service has a way of identifying and naming the objects it will manage. In databases based on the X.500 standard that are accessed by LDAP, the directory service assigns distinguished names (DNs) to each object.

135、 B .A meta-directory gathers the necessary information from multiple sources and stores it in one central directory. This provides a unified view of all users’ digital identity information throughout the enterprise. The meta-directory synchronizes itself with all of the identity stores periodically to ensure that the most up-to-date information is being used by all applications and identity management components within the enterprise.

136、 C .A virtual directory plays the same role and can be used instead of a meta-directory. The difference between the two is that the meta-directory physically has the identity data in its directory, whereas a virtual directory does not and points to where the actual data reside.

137、 D .A cookie can be in the format of a text file stored on the user’s hard drive (permanent), or it can be held in memory only (session). If the cookie contains any type of sensitive information, it should only be held in memory and should be erased once the session has

completed.

138、 D .The goal is to minimize the time administrators spend on password management. The following are the most common ways identity management deals with password management:

- Password synchronization reduces the complexity of keeping up with different passwords for different systems.
- Self-service password reset reduces help-desk call volumes by allowing users to reset their own passwords.
- Assisted password reset reduces the resolution process for password issues for the help desk. This may include authentication with other types of authentication mechanisms (biometrics, tokens).

139、 D .Compared to the other available authentication mechanisms, biometric methods provide the highest level of protection and are the most expensive.

140、 B .Most systems do not use the actual passphrase or password the user enters. Instead, they put this value through some type of encryption or hashing function to come up with another format of that value, referred to as a virtual password.

141、C .Passwords provide the least amount of protection, but are the cheapest because they do not require extra readers (as with smart cards and memory cards), do not require devices (as do biometrics), and do not require a lot of overhead in processing (as in cryptography). Passwords are the most common type of authentication method used today.

142、 A .Separation of duties is put into place to ensure that one entity cannot carry out a task that could be damaging or risky to the company. It requires two or more people to come together to do their individual tasks to accomplish the overall task. If a person wanted to commit fraud and separation of duties was in place, he would need to participate in collusion.

143、 C .A logical control is the same thing as a technical control. All of the answers were logical in nature except an ID badge. Badges are used for physical security and are considered physical controls.

144、 D .The best approach to security is to try to prevent bad things from happening by putting the necessary controls and mechanisms in place. Detective controls should also be put in place, but a security model should not work from a purely detective approach.

145、 B .An asynchronous token device is based on challenge/response mechanisms. The authentication service sends the user a challenge value, which the user enters into the token. The token encrypts or hashes this value, and the user uses this as her one-time password.

146、D .The DAC model allows users or data owners to grant access to other users to access their resources. DAC is implemented by ACLs, which the data owner can configure.

147、 D .This is considered a strong authentication approach because it has two factors—it uses two out of the possible three authentication techniques (something a person knows, is, or has).

148、 A .Message authentication code (MAC) is a cryptographic function and is not a key component of Kerberos. Kerberos is made up of a KDC, a realm of principals (users, services, applications, and devices), an authentication service, tickets, and a ticket-granting service.

149、 D .DAC is implemented and enforced through the use of access control lists (ACLs), which are held in a matrix. MAC is implemented and enforced through the use of security labels.

150、 C .Authentication means to validate the identity of a user. In most systems, the user must submit some type of public information (username, account number) and a second credential to prove this identity. The second piece of the credential set is private and should not be shared.

151、 A .It is easier on the administrator if she only has to create one role, assign all of the necessary rights and permissions to that role, and plug a user into that role when needed. Otherwise, she would need to assign and extract permissions and rights as each individual came and left the company.

152、 C .Passwords are the most common authentication mechanism used today. They are used to validate a user’s identity.

153、 A .Mutual authentication means that it is happening in both directions. Instead of just the user having to authenticate to the server, the server also has to authenticate to the user.

154、 D .Only the data owner can decide who can access the resources she owns. She may be a user and she may not. A user is not necessarily the owner of the resource. Only the actual owner of the resource can dictate what subjects can actually access the resource.

155、 A .In a single sign-on technology, all users are authenticating to one source. If that source goes down, authentication requests cannot be processed.

156、 C .Biometrics is a technology that validates an individual’s identity by reading a physical attribute.

157、 B .The security policy sets the tone for the whole security program. It dictates the level of risk the management and company are willing to accept. This, in turn, dictates the type of controls and mechanisms that are to be put into place to ensure that this level of risk is not exceeded.

158、 B .A brute force attack tries a combination of values in an attempt to discover the correct sequence that represents the captured password or whatever the goal of the task is. It is an exhaustive attack, meaning the attacker will try over and over again until she is successful.

159、 D .Spoofing is the process of pretending to be another person or process, with the goal of obtaining unauthorized access. Spoofing is usually done by using a bogus IP address, but it could be done by using someone else’s authentication credentials.

160、 A .A centralized approach does not provide as much flexibility as decentralized access control administration does because one entity is making all the decisions instead of several entities that are closer to the resources. A centralized approach is more structured in nature, which means that there is less flexibility.

161、C .An administrator does not need to revoke and reassign permissions to individual users as they change jobs. Instead, the administrator assigns permissions and rights to a role, and users are plugged into those roles.

162、 B .While passwords are insecure and often implemented incorrectly, they remain the most popular authentication control used today. Because they impose little burden on the user and are simple and inexpensive to implement, companies continue to employ passwords within their systems and networks. Passwords are not used moderately, but very frequently.

163、 B .Secure European System for Applications in a Multivendor Environment (SESAME) is actually a technology built upon the Kerberos foundation. However, SESAME provides different capabilities and uses public key cryptography. SESAME differs from Kerberos in that it uses PACs for authentication instead of the Kerberos ticket exchange methodology.

164、 A .An iris scan system records the colors and patterns around a pupil of a person’s eye. This is different from a retina scan, which records the blood vessel patterns at the back of the eye.

165、 B .Mandatory access control (MAC) models use security labels to hold classification information assigned to objects. If a user wants to access an object, she must have an equal or greater level of clearance. Although military organizations commonly use security labels, the answer “military access control model” does not really exist.

166、 A .While password generators protect against dictionary attacks, they often force users to write down their password, which creates a new vulnerability. Having an office full of sticky notes with scribbled passwords is an attractive atmosphere for a potential hacker.

167、 A .Organizations use a variety of techniques to protect themselves, such as employee background checks, drug screens, security training, policies, procedures, standards, and hiring and firing policies. These types of actions fall under the preventive-administrative category, which is often referred to as “soft” access controls.

168、 C .Terminal Access Controller Access Control System has three versions: TACACS, XTACACS, and TACACS+. Each version offers different functionality, but it is XTACACS that separates authentication, authorization, and accounting processes.

169、 D .One-time, or dynamic, passwords provide an increased level of security, as they are valid for only one logon transmission. They can be generated by a token device and help prevent replay attacks.

170、 B .Web portals are parts of a website that act as points of access to information in a unified manner. A web portal is made up of portlets, which are pluggable user-interface software components that present information from other systems. In addition, a portlet is an interactive application that provides a specific type of web service functionality (e-mail, news feed, weather updates, forums).

171、 B .Extensible Markup Language (XML) is a universal and foundational standard that provides a structure for other independent markup languages to be built from and still allow for interoperability.

172、 C .Simple Object Access Protocol (SOAP) is a specification that outlines how information pertaining to web services is exchanged in a structured manner. It provides the basic messaging framework, which allows users to request a service and, in exchange, the service is made available to that user. SOAP can work with other application layer protocols than just HTTP.

173、 C .As an example, when you log in to your company’s portal and double-click a link for (e.g., Salesforce), your company’s portal will take this request and your authentication data and package it up in an SAML format and encapsulate that data into a SOAP message. This message would be transmitted over an HTTP connection to the Salesforce vendor site, and once you are authenticated you can interact with the vendor software. SAML packages up authentication data, SOAP packages up web service request and SAML data, and the request is transmitted over an HTTP connection.

174、 D .Timestamping provides a window of time indicating how long a message is valid. A nonce is a random value that is used to periodically authenticate the receiving system. Session tokens are used in stateless communication transmissions and contain a unique session ID. Each of these can be used to reduce the threat of replay attacks.

175、 A .Temporal isolation is a type of access control that can be implemented to restrict access during specific time periods. The goal is to reduce the window of opportunity for an attacker to carry out malicious activities without being detected.

176、 D .Explanation: The following items are the ones that should be implemented and enforced:

- Deny access to systems to undefined users or anonymous accounts.
- Limit and monitor the usage of administrator and other powerful accounts.
- Suspend or delay access capability after a specific number of unsuccessful logon attempts.
- Remove obsolete user accounts as soon as the user leaves the company.
- Suspend inactive accounts after 30 to 60 days.

- Disable unneeded system features, services, and ports.
- Replace default password settings on all accounts.

177、 C .Behavior-based IDS does not need predefined signatures to detect attacks. A zero-day attack means that there is no known solution or signature for a specific attack, thus it cannot be detected by signature-based IDS.

178、 B .In behavior-based IDS products each packet is given an anomaly score, which indicates its degree of irregularity. If the score is higher than the established threshold of “normal” behavior, then the preconfigured action will take place.

179、 C .Phishing is a type of social engineering with the goal of obtaining personal information, credentials, credit cards number, or financial data. The attackers lure, or fish, for sensitive data through various methods.

180、 C .When a phishing attack is crafted to trick a specific target and not a large generic group of people, this is referred to as a spear-phishing attack. These specialized attacks take more time for the hacker to craft because unique information has to be gathered about the target, but they are more successful because they are more convincing.

181、 A .Pharming is an attack type that can redirect a victim to a seemingly legitimate, yet fake, website. In this type of attack, the attacker carries out DNS poisoning, in which a DNS server resolves a hostname into an incorrect IP address.

182、 A .Threat modeling is a structured approach to identifying potential threats that could exploit vulnerabilities. A threat modeling approach looks at who would most likely want to attack an organization and how could they successfully do this. A threat model can help to assess the probability, the potential harm, and the priority of attacks, and thus help to minimize or eradicate the threats. Threat modeling is a process of identifying the threats that could negatively affect an asset and the attack vectors they would use to achieve their goals.

183、 D .A rainbow table is a set of precomputed hash values that represent password combinations. These are used in password attack processes and usually produce results more quickly than dictionary or brute force attacks.

184、 A .The Service Provisioning Markup Language allows for the automation of user management (account creation, amendments, revocation) and access entitlement configuration related to electronically published services across multiple provisioning systems.

第六章题目

1. To what does the term "footprinting" refer?
   A. A distributed denial-of-service attack

B. Social engineering method of tracing a target’ s steps with intent to impersonate

C. Information-gathering technique

D. Trojan horse – based method of compromising a password

2. Which of the following is not a requirement of penetration testing?

A. Outlined goals

B. Limited time-line agreed upon

C. Management approval

D. Intrusion detection controls

3. What is the reason for performing a penetration test?

A. To ensure that all systems meet a specific security rating

B. To quantify the true liability a company faces

C. To ensure all users are being properly authenticated

D. To identify vulnerabilities within systems and an environment, and exploit them

4. Which of the following terms describes a systematic assessment of the security controls on information systems?

A. Penetration test

B. Vulnerability test

C. Audit

D. Gray box test

5. What is the first step in an audit?

A. Determine goals

B. Identify scope

C. Determine what entity will perform the audit

D. Conduct the audit

6. In which scenario is an audit more likely to be conducted by an external team?

A. A data breach

B. Regulatory compliance audit

C. Vulnerability assessment

D. A log review

7. All of the following are benefits of using an internal audit team, except:

A. Familiarity with the organization and its workings

B. Readily available team, who can audit at anytime

C. Complete independence

D. Ability to be agile in assessment processes and procedures

8. All of the following are advantages of using external or third-party auditors, except:

A. Cost

B. Ability to be independent of agendas or politics

C. Expanded knowledge due to having seen and tested many different types of information

D. Supports compliacnce with certain external governance requirements, such as laws or regulations

9. Which of the following is a necessary step in using an external audit team?

A. Training the audit team

B. Familiarizing the audit team with your organization

C. Supplying equipment to the audit team

D. Signing of a nondisclosure agreement

10. Which of the following was an early standard for an audit that is carried out by a third party to assess the internal controls of a service organization?

A. National Institute of Standards and Technology (NIST) Special Publication 800-30, Guide for Conducting Risk Assessments

B. Statement on Auditing Standards No. 70: Service Organizations (SAS 70)

C. Defense Information Assurance Certification and Accreditation Program (DIACAP)

D. The NIST Risk Management Framework (RMF)

11. Which of the following is a set of auditing standards for service organizations, defined in the American Statement on Standards for Attestation Engagements (SSAE) 16 and the International Computing Centre’ s (ACC) International Standard on Assurance Engagements (ISAE) No. 3402?

A. Service Organization Controls (SOC)

B. Statement on Auditing Standards No. 70: Service Organizations (SAS 70)

C. The NIST Risk Management Framework (RMF)

D. ISACA's Risk IT Framework

12. Which of the following types of reports from the American Statement on Standards for Attestation Engagements (SSAE) 16 and the International Computing Centre’s (ACC) International Standard on Assurance Engagements (ISAE) No. 3402 is a detailed type of report that provides data pertaining to controls for trust services, and contains highly sensitive data for an organization?

A. SOC 1

B. SOC 2

C. SOC 3

D. SOC 4

13. Which of the following is considered the definition of a technical control?

A. A security control implemented through the use of an IT asset

B. A security control implemented through the use of policies and procedures

C. A security control implemented through the use of physical mechanisms

D. A security control implemented through the use of operational procedures and processes

14. All of the following are ways of auditing security controls, except:

A. Penetration testing

B. Vulnerability testing

C. War dialing

D. Integration testing

15. What is the purpose of vulnerability testing?

A. To exploit systems and attempt to knock them offline in order to test the skills of network defenders

B. To evaluate the security posture of the system and determine its vulnerabilities

C. To perform a risk assessment on a system to determine threats, vulnerabilities, likelihood, and impact

D. To review security policies and procedures

16. Which of the following statements is true concerning a vulnerability assessment?

A. Once a vulnerability assessment is performed, the organization never needs to perform one again.

B. A vulnerability assessment attempts to exploit any type of discovered vulnerabilities in order to discover the true security posture of the system.

C. Vulnerability assessments are merely a snapshot in time, and provide the security posture of the system as it is at the time of the assessment.

D. Vulnerability assessments only involve technical testing.

17. Vulnerability testing tests all of the following areas, except:

A. Personnel

B. Physical mechanisms

C. Technical controls

D. Likelihood and impact

18. In which types of testing do testers have limited knowledge of the target infrastructure?

A. Black box testing

B. White box testing

C. Gray box testing

D. Gray hat testing

19. What is the critical difference between vulnerability testing and penetration testing?

A. Vulnerability testing attempts to exploit discovered vulnerabilities. Penetration testing only discovers vulnerabilities, but does not attempt to exploit them.

B. Penetration testing attempts to exploit discovered vulnerabilities. Vulnerability testing discovers vulnerabilities, but does not attempt to exploit them.

C. Vulnerability testing is performed by black hat hackers, but Penetration testing is performed by white hat hackers.

D. Penetration testing is performed by black hat hackers, but Vulnerability testing is performed by white hat hackers.

20. Vulnerability scanners are used to provide all of the following information, except:

A. Identification of the normal usage of the host

B. Identification of active hosts and vulnerable services

C. Identification of operating systems and applications

D. Identification of misconfigured settings

21. All of the following are elements of information that are provided from penetration testing reports, except:

A. Identification of vulnerabilities and their severity

B. Information on how to remediate vulnerabilities

C. Method of exploiting the vulnerabilities

D. Assigned responsibility to personnel required to remediate vulnerabilities

22. What is a potential negative side effect of penetration testing?

A. Discovering which vulnerabilities can be exploited by an attacker

B. Confirming or invalidating vulnerability assessment results

C. Inadvertently damaging or disabling network hosts or resources

D. Adding to the security budget burden of the organization

23. What is a common name for the authorization document that allows you to perform penetration testing on an organization's infrastructure?

A. "Free pass"

B. "No harm letter"

C. "Get out of jail free card"

D. "Hold harmless license"

24. Which of the following is not a part of the overall five-step process for performing a penetration test?

A. Enumeration

B. Exploiting systems beyond the organization's infrastructure

C. Vulnerability mapping

D. Reporting to management

25. During which of the following steps of the penetration testing process do you perform port scans and identify resources?

A. Discovery

B. Vulnerability mapping

C. Exploitation

D. Enumeration

26. Which of the following types of testing corresponds to having full knowledge of the target?

A. White box testing

B. Gray box testing

C. Black box testing

D. Red team testing

27. During which type of penetration test does not only the penetration tester have little to no knowledge about the network, but additionally the defending security staff have no knowledge about the test?

A. Blind test

B. Double-blind test

C. Targeted

D. Gray box

28. Which of the following statements best describes a targeted attack?

A. Carrying out a focused test on a specific system or application

B. Carrying out a wide range of tests against a particular target organization

C. Carrying out focused tests on several target organizations

D. Carrying out a wide range of tests on several target organizations

29. Which of the following statements best describes war dialing?

A. Using Voice over Internet Protocol (VoIP) phones and networks to carry out phishing attacks

B. Carrying out a denial-of-service attack against an organization's phone switch

C. Dialing large blocks of phone numbers in search of connected modems within an organization

D. Spoofing an organization's telephone numbers

30. Which commonly exploited vulnerability occurs below the level of the user interface, inside the core of the operating system?

A. Buffer overflow

B. Kernel flaw

C. File descriptor

D. Symbolic link

31. Vulnerabilities that result from poor programming practices, and allow more input than the

program has allocated memory space to store it are called _____.

A. Buffer overflows

B. Kernel flaws

C. File descriptors

D. Symbolic links

32. Which of the following statements best describes an attack using symbolic links?

A. A flaw in the operating system's kernel allows an attacker to gain root access to the system.

B. A flaw in the program's memory allocation allows it to be overflowed with additional data, permitting an attacker to execute arbitrary code.

C. An attacker follows a link to a file, and alters either the link or the file to cause users to access an incorrect file, such as a password file.

D. An attacker takes advantage of an unsafe use of a file descriptor, causing unexpected input into the program or unexpected output, typically with the privileges of the executing program.

33. Which of the following attacks takes advantage of the numbers an operating system uses to represent open files in a process?

A. Kernel flaw attack

B. File descriptor attack

C. Buffer overflow attack

D. Symbolic link attack

34. Which of the following terms is used to describe the state a program is in when its design leaves it temporarily vulnerable before mitigating that vulnerability?

A. Race condition

B. Stateless

C. Stateful

D. Overflow condition

35. What is an effective countermeasure to detect altered files in a system?

A. Antimalware

B. Increased file and directory permissions

C. Secure programming practices

D. File integrity checkers

36. How often should virus detection software be run on a system, at minimum?

A. Weekly

B. Monthly

C. Quarterly

D. Semi-annually

37. What is a critical element in ensuring that logs are consistent across all devices in the network?

A. Syslog server

B. Defined auditable events

C. Standardized time across the network

D. An auditors group

38. Which of the following is the most authoritative level of time sources?

A. Stratum 0

B. Stratum 1

C. Stratum 2

D. Stratum 3

39. What transport layer protocol and port does the Network Time Protocol (NTP) use?

A. TCP port 123

B. UDP port 123

C. TCP port 119

D. UDP port 119

40. All of the following are best practices for maintaining log files, except:

A. Define auditable events

B. Send all log files to a central server

C. Automate log review to the greatest extent possible

D. Allow all personnel to be able to review system event logs

41. Which of the following statements best describes a security information and event manager (SIEM)?

A. Centralized syslog server

B. Intrusion detection system

C. Intrusion protection system

D. Centralized log collection and analysis system

42. Which the following statements best describes a synthetic transaction?

A. A user-generated transaction

B. A script-generated transaction

C. A signature-based transaction

D. An anomaly-based transaction

43. What is the benefit of using synthetic transactions?

A. They allow administrators to systematically test the behavior and performance of critical services.

B. They ease the work burden of users.

C. They are more accurate than user-initiated transactions.

D. They can be preprogrammed with particular security services, such as encryption and authentication.

44. Which of the following statements best describes real user monitoring (RUM)?

A. Passive method of monitoring user interactions within a web application or system

B. Uses active scripting to simulate user interactions with the system

C. Uses real users to run preprogrammed scripts to interact with a system or application

D. Creates scripts based upon the interactions of real users in order to test systems and applications

45. Which of the following terms best describes misuse case testing?

A. Structured scenarios that are commonly used to describe required functionality in an information system

B. Unstructured scenarios that are commonly used to describe required functionality in an information system

C. A scenario that includes threat actors and the actions they want to perform on the system

D. A scenario that depicts the expected reaction of a system to an incorrect input

46. Use cases and misuse cases are depicted using what type of language?

A. XML

B. HTML

C. UML

D. SML

47. Which of the following terms describes a systematic examination of the instructions that comprise a piece of software, performed by an independent entity?

A. Application test

B. Code review

C. Unit test

D. Integration test

48. All of the following are items to look for during a code review, except:

A. Inclusion of test code

B. Structure and format

C. Uncalled or unneeded functions

D. Compile errors

49. Which of the following security controls relates to user-supplied data and is checked during a code review?

A. Buffer overflow conditions

B. Race conditions

C. Input validation

D. Code injection

50. Which of the following terms refers to an exchange point for data between systems and users?

A. User interface

B. Entry point

C. User space

D. User-level processes

51. What is the overall term for creating, modifying, deleting, or otherwise using accounts?

A. User management

B. Password management

C. Account management

D. System management

52. All of the following should be included in the process of creating user accounts, except:

A. Having the user review and sign the organization's acceptable use policy

B. Having human resources confirm that the user is a valid employee

C. Supervisor verification of the employee's need to have a specific account on certain systems

D. Granting user permissions to a particular resource, such as a shared folder or printer

53. Which the following is the best reason to audit account modification actions?

A. To ensure that account operators follow proper procedures

B. To prevent privilege accumulation

C. To ensure that accounts are created or deleted correctly

D. To ensure tha taccount operators are not abusing privileges

54. All of the following reasons for auditing and testing backup data are valid, except:

A. To test for proper user permissions

B. To ensure that data integrity is maintained on backup media

C. To ensure that the backups can be restored in the event they are needed

D. To ensure that backup procedures are properly performed

55. Which of the following statements best describes the characteristics of business continuity and disaster recovery?

A. Disaster recovery details ensuring that the business can function after a catastrophe.

B. Business continuity and disaster recovery are synonymous terms.

C. Disaster recovery focuses on restoring systems and facilities, and protecting people immediately after a catastrophe, and business continuity focuses on resuming business operations after a catastrophe.

D. Business continuity focuses on recovering from a catastrophe immediately after the event.

56. How often should disaster recovery plans and business continuity plans be tested?

A. At least monthly

B. At least quarterly

C. At least annually, or as changes occur

D. At least every two years

57. All of the following are types of disaster recovery and business continuity tests, except:

A. Structured walk-through test

B. Checklist test

C. Parallel test

D. Compliance test

58. Which the following types of tests involves testing both the primary and alternate processing sites simultaneously?

A. Checklist test

B. Full-interruption test

C. Structured walk-through test

D. Parallel test

59. Which type of business continuity and disaster recovery test involves specific scenarios that test the reactions of each operational and support area, but does not involve actually relocating to the alternate processing facility?

A. Simulation test

B. Checklist test

C. Parallel test

D. Full-interruption test

60. Which of the following is the most important aspect of emergency response and disaster recovery?

A. Quickly backing up data

B. Protecting facilities

C. Shutting down equipment

D. Protection of human life

61. Which of the following terms refers to the process of teaching a skill or set of skills that will allow people to perform specific functions better?

A. Security training

B. Security awareness

C. Security education

D. Security indoctrination

62. Which of the following terms refers to the process of exposing people to security issues so that they may be able to recognize them and better respond to them?

A. Security training

B. Security education

C. Security awareness

D. Security indoctrination

63. Which form of social engineering was actually legal in the United States until 2007, as long as it was not used to obtain financial records?

A. Phishing

B. Pretexting

C. Shoulder surfing

D. Dumpster diving

64. Which of the following types of attack can be triggered simply by visiting a malicious website?

A. Cross-site scripting attack

B. Command injection attack

C. XML injection attack

D. Drive-by download

65. Which of the following metrics is a measure of how well things are going currently within the organization and its infrastructure?

A. Key risk indicator

B. Key performance indicator

C. Qualitative risk measurement

D. Quantitative risk measurement

66. Which of the following is a metric that identifies potential negative events or abnormal variances?

A. Key risk indicator

B. Key performance indicator

C. Quality of service indicator

D. Threat modeling

67. Which type of report is written in the context of a system under study (SUS)?

A. Executive summary

B. Test report

C. Technical report

D. Management review

68. Which of the following statements best describes a management review?

A. A formal meeting of senior organizational leaders to determine whether the management systems are effective at accomplishing their goals

B. A management review of an audit report, including the technical report and executive summaries

C. An external audit focused on the administrative and management processes within an organization

D. An internal audit of administrative controls within the organization, such as policies,

procedures, and standards

69. Which of the following is a social engineering attack typically instigated through email?

A. Phishing

B. Pretexting

C. Vishing

D. Tailgating

70. One source of data leakage from an organization that is typically perpetrated by users posting sensitive information online is _____.

A. Texting

B. Social media

C. Private chat

D. E-mail

第六章答案

1、 C .Footprinting is a method used by an attacker to learn information about a victim before actually carrying out scanning and probing activity.

2、 D .A penetration test is performed to understand the true protection current security controls are providing and is conducted by identifying current vulnerabilities, and then exploiting them. It is important to secure management's support before beginning such a test because it can be very intrusive. Also, goals and a timeline need to be agreed upon. Different tests may have different goals, and funding usually will dictate the time-line of the test.

3、 D .A penetration test identifies vulnerabilities within the systems in the environment by uncovering the true protection current security controls are providing. The test should use a vulnerability scanner and several tools and scripts to emulate an actual attack.

4、 C .An audit is a systematic assessment of the security controls on information systems. It can take place at many levels, including a documentation review, log reviews, vulnerability testing, and penetration testing, and could include any or all of these methods. Audits are used to verify compliance with security policies.

5、 A .Determining goals is the first step of an audit. You must know what you want to achieve by performing one.

6、 B .In the case of regulatory compliance, an external team may perform an audit, to verify that the organization complies with the standards set forth by law or regulation. This would be an independent validation, since an internal team may be biased in some way.

7、 C .An internal audit team cannot be completely independent from internal organizational structures and politics, so their work may be influenced by upper management, or

cross-functional interference.

8、 A .Cost is a disadvantage because hiring an external audit team will likely be more expensive than using internal auditors who are already part of the organization.

9、 D .A signed nondisclosure agreement is a necessary requirement before allowing a third party to audit an organization's systems. This ensures that the third-party audit team will keep sensitive information confidential, and not release it inappropriately to competitors, business partners, or the general public.

10、 B .Statement on Auditing Standards No. 70: Service Organizations (SAS 70) was an early standard for an audit that is carried out by a third party to assess the internal controls of a service organization. It was originally intended to assess financial controls, but has since been expanded by organizations to ensure that their service providers are providing the necessary protection of digital information.

11、 A .Service Organization Controls (SOC) are auditing standards for service organizations, defined in the American Statement on Standards for Attestation Engagements (SSAE) 16 and the International Computing Centre’s (ACC) International Standard on Assurance Engagements (ISAE) No. 3402.

12、 B .Service Organization Controls (SO) 2 pertains to trust services (Security, Availability, Confidentiality, Process Integrity, and Privacy) as does SOC 3, but SOC 2 more detailed and considered an internal document due to its sensitivity. SOC 3 is of a more generic nature, and can typically be released publicly.

13、 A .In general terms, a technical control is a security control implemented through the use of an IT asset. This could mean by using encryption, security devices, secure protocols, authentication processes, secure code, and so forth.

14、 D .Integration testing is part of the system development life cycle, where individual components are integrated as a system and tested together to determine their effect on each other's operations.

15、 B .The purpose of vulnerability testing is to evaluate the security posture of the system and determine its vulnerabilities.

16、 C .Management must understand that vulnerability assessments are merely a snapshot in time, and provide the security posture of the system as it is at the time of the assessment. As the system operating environment changes, (e.g., is upgraded), new software is installed, and new vulnerabilities are discovered, the security posture of the system can change over time. Therefore, vulnerability assessments should be performed periodically.

17、 D .Likelihood and impact are determined as a result of determining threats and

vulnerabilities to an asset, and are critical in determining overall risk for a system. A vulnerability test is only part of risk determination.

18、 C .A gray box test is the midpoint between a black box test and a white box test. The tester has some limited knowledge of the target infrastructure, usually provided by someone in management within the organization. It's usually just information enough for the tester to get started, but not enough to give them any serious, in-depth information about the organization, its infrastructure, or its vulnerabilities.

19、 B .Vulnerability testing discovers vulnerabilities but does not attempt to exploit them. It only reports the potential for exploitation. Penetration testing actually attempts to exploit discovered vulnerabilities, revealing a more realistic assessment of the security posture of the system.

20、 A .Vulnerability scanners can provide a lot of information about a host on the network, including its operating system, its applications, how it is configured, it's services, and any misconfigured settings. Vulnerability scanners can also report patching levels on the system. However, they cannot provide information on how the system is normally used.

21、 D .Penetration testing reports typically identify vulnerabilities and their severity, the method that was used to exploit the vulnerabilities, and information on how to remediate those same vulnerabilities. A penetration testing report does not attempt to assign blame for vulnerabilities, nor can it assign responsibilities to those personnel responsible for mitigating them. Only the organizational management can do that, after the fact.

22、 C .During a penetration test, there is always a risk of inadvertently damaging or disabling network hosts or resources due to the nature of exploiting vulnerabilities.

23、C .The popular phrase "Get out of jail free" refers to the authorization document provided by someone in the organization who has the authority to allow you to test organizational infrastructures. This document prevents penetration testers from being arrested or prosecuted for their testing activities, which may otherwise be illegal without the authorization.

24、 B .Exploiting systems beyond the organization's infrastructure is usually something that is out of scope of the test, and not part of the written agreement you have with the organization. It's also typically illegal. Normally, you are allowed to exploit systems within a defined perimeter, but not beyond that perimeter. Even if the organization is connected to a partner's network, you typically won't have authorization to test that network.

25、 D .During the enumeration step, you perform port scans and identify resources that are part of the target network. This is different from the discovery step, because during discovery you gather general information about the target, which is not very detailed.

26、 A .White box testing means that the tester has intimate knowledge about the target system, as opposed to black box testing, which means the tester has no knowledge about the

target system. Gray box testing simply means that the tester has partial knowledge about the target system. Red team testing is a type of penetration testing in which the target has no knowledge at all that testing is taking place.

27、 B .A double-blind test means that not only does the assessor have very little to no knowledge about the network infrastructure, but the security staff and defenders of the target network are not notified of the test. This allows the test to evaluate the network's security level and the incident response actions.

28、 A .A targeted attack means that you are carrying out focused tests on specific areas of interest, such as a new application or a new system. During this type of test, use specific techniques and tools that are particular to the target, and start at a very basic level and work your way up to more complex attacks.

29、 C .War dialing allows attackers to dial large blocks of an organization's phone numbers in hopes of finding connected modems.

30、 B .Kernel flaws are vulnerabilities in the operating system kernel, below the user interface level. A flaw in the kernel that can be reached by an attacker and exploited gives an attacker the most powerful level of control over the system.

31、 A .A buffer overflow is a vulnerability that allows more input than the program has allocated memory space to store it. This overwrites data or memory at the end of the buffer, sometimes allowing the attacker to inject arbitrary code and cause the processor to execute it.

32、 C .In a symbolic link attack, the attacker follows a link to a file and alters either the link or the file to cause users to access an incorrect file, such as a password file

33、 B .In a file descriptor attack, a program may make unsafe use of a file descriptor (one of the numbers an operating system uses to represent open files in a process) allowing an attacker to cause unexpected input or output.

34、 A .Race conditions exist when the design of a program puts it in a vulnerable condition before ensuring that those vulnerable conditions are mitigated

35、 D .File integrity checkers can detect alterations to files and alert administrators. Files can be modified to include malware, or to install rootkits on a system.

36、 A .Virus detection software, or antimalware, should be run weekly at a minimum, but ideally it should be run daily.

37、 C .To ensure that logs are consistent across the enterprise, a standardized time source should be implemented. This will enable you to ensure that logs can be correlated with each other to establish the timeline of an event.

38、 A .A stratum 0 time source is the most authoritative level. Time sources at this level are typically atomic clocks, global positioning system clocks, or radio clocks.

39、 B .Since the Network Time Protocol is a connectionless protocol, it uses the User Datagram Protocol (UDP), on port 123.

40、 D .System and event logs can contain sensitive information, and should be accessed only by authorized personnel, such as auditors or administrators.

41、 D .A security information and event manager (SIEM) is a system that allows for the centralization, correlation, analysis, and retention of event data from a wide variety of sources, in order to generate automated alerts and perform trend analysis.

42、 B .A synthetic transaction is one that is not generated by a person, but by script.

43、 A .Because synthetic transactions are scripted, they allow administrators to rapidly and systematically test the behavior and performance of critical services and systems.

44、 A .Real user monitoring (RUM) is a passive way to monitor the interactions of real users with a web application or system. It uses agents to capture metrics such as delay, jitter, and errors from the user’s perspective. RUM differs from synthetic transactions in that it uses real people instead of scripted commands. While RUM more accurately captures the actual user experience, it tends to produce noisy data and thus may require more back-end analysis.

45、 C .A misuse case is a scenario that includes threat actors and the actions they want to perform on the system. It describes how a threat actor may misuse the system, versus how users may correctly interact with the system.

46、 C .Unified Modeling Language (UML) is a simple language used to create diagrams depicting use cases and misuse cases.

47、 B .A code review is a systematic examination of the instructions, or code, that comprise a piece of software, performed by an independent entity. Code reviews can be manual or automated.

48、 D .Compile errors are typically experienced after the code is reviewed and during the compile process. They may point to issues with the compiler, such as missing external libraries.

49、 C .lack of input validation is a security vulnerability that leads to many other vulnerabilities, including injection attacks. If a piece of software performs input validation, it can significantly reduce many other forms of attack.

50、 A .The user interface is the exchange point for data between the system and its users. It can

be graphical, command line, or even an application programming interface.

51、 C .Account management is the term used for the overall management of accounts, whether they are user, system, or application accounts. This also involves managing user credentials, such as passwords, tokens, and certificates. It typically does not involve managing the authorizations users have to access resources.

52、 D .Normally, granting user permissions are not part of the account creation process, although the accounts initially may be placed in groups that grant them certain permissions automatically.

53、 B .Often, when accounts are modified, their privileges may increase as a result of being assigned to a new group or being given greater access. Auditing, modification can help prevent privilege accumulation.

54、 A .Auditing and testing backup data normally do not indicate if users have proper permissions to resources, even data that is being backed up.

55、 C .Disaster recovery focuses on restoring systems and facilities, and protecting people immediately after a catastrophe, and business continuity focuses on resuming business operations after a catastrophe. While the terms are closely related, they are not synonymous. Disaster recovery is a subset of business continuity, and focuses primarily on the immediate time frame after a disaster, where the protection of lives and property is of paramount importance. Business continuity is a longer-term event that can only take place after disaster recovery.

56、 C .Business continuity plans and disaster recovery plans should be tested at least annually, or when major changes occur to the plans or the environment in which the business operates.

57、 D .Compliance testing is normally not performed on disaster recovery and business continuity plans. Testing is performed to ensure that the plans can be properly enacted and are validated as sound and thorough.

58、 D .A parallel test involves testing both the primary and alternate sites at one time and ensuring that systems can adequately perform at the alternate facility while also maintaining the primary facility in operation.

59、 A .In a simulation test, all functional areas come together to practice executing the disaster recovery plan based upon specific scenarios. Specific areas are simulated, and the test is conducted up until the point where it actually involves relocating processing to the alternate facility, which is not done.

60、 D .Protection of human life is always the most important aspect of emergency response and disaster recovery. Human lives cannot be replaced, but equipment, data, and facilities can be.

61、 A .Security training involves teaching skills that allow people to perform specific functions better.

62、C .Security awareness refers to the process of exposing people to security issues so that they may be able to recognize them and better respond to them.

63、 B .Pretexting is a form of social engineering in which the adversary invents a believable scenario in an effort to persuade the target to violate security policy, or give up information. It was actually legal in the United States until 2007, as long as it was not used to obtain financial records. However, due to unethical acts by Hewlett-Packard, pretexting was made illegal by the Telephone Records and Privacy Protection Act of 2006.

64、 D .The drive-by download is an automatic attack vector triggered simply by visiting a malicious website. It involves execution of malware on the client computer without additional user interaction beyond simply visiting the website.

65、 B .A key performance indicator (KPI) is a metric that informs management of how well the organization is performing in certain areas, such as security, resiliency, reliability, and so forth.

66、 A .A key risk indicator (KRI) is a metric that indicates when a potential risk has exceeded the threshold of the organization’s range of acceptable risk. It can indicate abnormal variances in performance or tolerances, as well as negative events.

67、 C .A technical report is the application of the standard methodology to the specific context of the system under study. It is not simply the output of an automated scanning tool or generic checklist.

68、 A .A management review is a formal meeting of senior organizational leaders to determine whether the management systems are effective at accomplishing their goals.

69、 A .Phishing is a social engineering attack typically carried out through e-mail. The attacker sends a crafted e-mail to the user, in an attempt to get the user to click a specific link embedded in the e-mail. When the user clicks the link, it takes them to a special website set up by the attacker to attempt to steal personal information from the user, such as credit card numbers, Social Security numbers, usernames, passwords, and so forth.

70、 B .While data can be leaked using any of the methods listed in the answer choices, posting information online is typically done through social media, whereas the other methods may be between an employee and only a single party. Social media is of particular concern because the information is available to large numbers of people and organizations at once.

第七章题目

1. An edict stating that all evidence be labeled with information about who secured it and who validated it is called _____.

A. CERT

B. Chain of custody

C. Direct evidence

D. Incident response policy

2. Computer-generated or electronic information is most often categorized as what type of evidence?

A. Best

B. Hearsay

C. Corroborative

D. Opinion

3. What is the first step in forensic analysis at a cybercrime scene?

A. Execute the primary programs on the computer to obtain more information.

B. Capture log files on the computer.

C. Notify customers of potential outages.

D. Capture a complete image of the system.

4. Which of the following is a critical first step in disaster recovery and contingency planning?

A. Complete a business impact analysis.

B. Determine offsite backup facility alternatives.

C. Organize and create relevant documentation.

D. Plan testing and drills.

5. There are different types of offsite facilities, either subscription-based or company owned. Which type of subscription-based backup facility is used most often?

A. Cold

B. Warm

C. Hot

D. Redundant

6. In disaster recovery, each level of employee should have clearly defined responsibilities. Which of the following is a responsibility of senior executives?

A. Develop testing plans.

B. Establish project goals and develop plans.

C. Identify critical business systems.

D. Oversee budgets.

7. Which of the following is not a reason to develop a business continuity plan?

A. To train employees on how to keep the company in business after a disaster

B. To restrict business productivity

C. To include procedures on how to move to and from an offsite facility

D. To limit business interruption

8. A company that has to guarantee zero downtime and 100 percent functionality would choose which type of backup facility?

A. Redundant

B. Rolling site

C. Cold

D. Warm

9. There are several reasons for a company to develop and implement a disaster recovery plan. What is the most important goal of disaster recovery?

A. Protect the integrity of the business.

B. Protect critical operating systems.

C. Protect human life.

D. Protect customer relationships.

10. What is the maximum tolerable downtime (MTD) for urgent systems and functions?

A. Minutes to hours

B. 24 hours

C. 4 – 6 hours

D. 72 hours

11. Which of the following threats cripples a business, destroys the original facility, and requires short- and long-term recovery planning?

A. Non-disaster

B. Disaster

C. Man-made disaster

D. Catastrophe

12. Disaster recovery and contingency plans become outdated for all of the following reasons except which one?

A. A company's infrastructure changes.

B. Too many drills cause the plan to become inaccurate.

C. Personnel turnover

D. Company and departmental reorganizations

13. What percent of businesses would go out of business if they had to close for only one week due to a disaster or disruption?

A. 10

B. 100

C. 65

D. 25

14. Which of the following facility backup options involves one company allowing another to use its facility in the event of a disaster?

A. Rolling hot site

B. Good neighbor agreement

C. Reciprocal agreement

D. Redundant site

15. Which step is not part of the business impact analysis (BIA)?

A. Determine MTD values.

B. Interview key personnel.

C. Identify critical business functions.

D. Report findings to the company.

16. An IT administrator is charged with the task of ensuring that data files are backed up at a remote location in case there is ever a disaster that destroys the main facility. Which of the following would be the best option?

A. Disk shadowing

B. Manual file copying and manual transport to the remote facility

C. Electronic vaulting

D. Disk duplexing

17. In the moments following a disaster, who should be called first?

A. CEO

B. The person designated in the continuity plan

C. Board of directors

D. Family of the injured

18. Different threats need to be properly classified so that a company knows how to react to different situations. A key operating system that fails and goes offline for three hours would be classified as a _____.

A. Disaster

B. Non-disaster

C. Catastrophe

D. Mishap

19. Members of the business continuity committee would do all of the following tasks except _____.

A. Gather data from other departments.

B. Ensure budgets are ontrack.

C. Complete a BIA.

D. Report findings to senior management.

20. What type of test should be completed before an actual simulation test occurs?

A. Parallel test

B. Structured walk-through test

C. Full-interruption test

D. Emergency procedures test

21. Which of the following best describes the difference between hierarchical storage management and storage area network technologies?

A. HSM uses optical or tape jukeboxes and SAN is a network of connected storage systems.

B. SAN uses optical or tape jukeboxes and HSM is a network of connected storage systems.

C. HSM and SAN are one and the same. The difference is in the implementation.

D. HSM uses optical or tape jukeboxes and SAN is a standard of how to develop and implement this technology.

22. Which entity would handle BCP tasks such as making insurance claims, assessing damage value, and estimating recovery expenses?

A. Departmental leads

B. Senior executives

C. HR

D. Financial representative to the BCP committee

23. Which of the following mechanisms could be used in business continuity?

A. Closed-circuit TV monitoring system

B. Data backup automation to a remote site

C. Calling tree

D. All of the other choices

24. Preparing for a damaging event before it takes place in order to minimize loss and ensure that the business continues to operate is the definition of _____.

A. Business impact analysis

B. Recovery planning

C. Business continuity planning

D. Emergency response

25. What is the first step in planning disaster response procedures?

A. Identify a team.

B. Create documentation.

C. Identify threats.

D. Gather data.

26. Following a disaster, which of the following steps should be taken by employees?

A. Make plans to reenter the facility if it looks safe.

B. Call customers to notify them of the situation.

C. Allow the BCP chair to give directions.

D. Attempt to remotely log in to systems to see if they are operational.

27. Which backup facility alternative would be the best choice for a company that needed a long-term recovery solution with minimal downtime?

A. Rolling hot site

B. Cold site

C. Redundant site

D. All of the other choices

28. Disasters can be manmade, technical, or a natural disaster. Which of the following is a manmade disaster?

A. Power failure

B. Sabatoge

C. Flooding

D. Fire caused by shorts in wiring

29. Which of the following has the ultimate responsibility for authorizing expenditures and acting on the suggestions of the BCP committee and the results of a business impact analysis?

A. Individual department managers

B. Senior management

C. Functional manager of that site

D. Security officer

30. The use of a librarian to manage the company resources such as laptops, CD-ROMs, files, and others is what type of control?

A. Physical control

B. Access control

C. Media control

D. Employee control

31. Which of the following is not a correct way in which an operating system responds to a failure?

A. System reboot

B. Emergency system restart

C. System cold start

D. Not starting

32. There are several ways of completely erasing data from different types of media. Which is not a method of media sanitization?

A. Deleting a file from a hard drive

B. Degaussing

C. Overwriting

D. Physical destruction

33. Which of the following security practices is often compared to the "prudent person" concept?

A. Least privilege

B. Man-in-the-middle

C. Due care

D. Proximate causation

34. Which is not true regarding "authorization creep?"

A. Typically occurs when employees transfer to new departments or change positions

B. Violates "least privilege"

C. Enforces the need to know concept

D. Tendency of users to request additional privileges but seldom ask for it to be taken away

35. A senior member of the IT programming staff who has been extremely loyal and valuable is suspected of fraud by a vice president. But the executive has no proof and does not want to make unfound allegations. What operations control would be best to identify if the programmer is committing fraud?

A. Job rotation

B. Mandatory vacation

C. Least privilege

D. Need to know

36. Reviewing audit logs is an example of what type of a security control?

A. Deterrent

B. Detective-Physical

C. Detective-Technical

D. Preventive-Technical

37. Which of the following controls are used to amend a situation after an attack has occurred or a vulnerability has been identified?

A. Deterrent

B. Corrective

C. Preventive

D. Recovery

38. A reservationist at a travel agency is allowed to commit two mistakes per month without consequence. An automated system tracks these errors and alerts appropriate personnel when this limit is exceeded. What is the limit referred to as?

A. Clipping level

B. Maximum fault tolerance

C. Proximate causation

D. Due care

39. Operations departments should back up data in all of the following situations except which of the following?

A. Once per year

B. Immediately following a reorganization

C. After a system upgrade

D. For authorized on-demand requests

40. An operations control that identifies potential fraudulent activity by requiring different personnel to switch job functions on a regular basis is called _____.

A. Mandatory vacation

B. Need to know

C. Separation of duties

D. Job rotation

41. Generating magnetic fields to erase the content on a type of media is called _____.

A. Sniffing

B. Degaussing

C. Wiretapping

D. Magnetizing

42. Which of the following is not considered a countermeasure to port scanning and operating system fingerprinting?

A. Allow access at the perimeter network to all internal ports.

B. Remove as many banners as possible within operating systems and applications.

C. Use TCP Wrappers on vulnerable services that have to be available.

D. Disable unnecessary ports and services.

43. Enabling Tier1 network technicians read-only access to border routers is an example of _____.

A. Biba model concept

B. Separation of duties

C. Least privilege

D. Due care

44. A tool used to detect penetration of a computer system and to identify misuse is called what?

A. Audit trail

B. Documentation

C. Security policy

D. Security model

45. Computer product evaluation criteria that look at clipping level configurations, unit testing, and configuration management are categorized as what?

A. Operational assurance

B. Life cycle assurance

C. Contingency criteria

D. Accreditation

46. Which of the following change management sequences is in the correct order?

A. Request, approve, document, test, implement, report

B. Test, request, approve, implement, document, report

C. Request, approve, test, implement, report, document

D. Request, approve, test, document, report, implement

47. A system that automatically restarts due to an uncontrolled or unusual failure is performing what?

A. System reboot

B. Cold reboot

C. Cold restart

D. Emergency system restart

48. Which of the following works as a transfer agent?

A. SET

B. IP

C. SMTP

D. ASCII

49. Similar activities are carried out by hackers and security professionals performing an assessment. Identifying openings in a victim's network is called _____.

A. Port scanning

B. TCP Wrapping

C. Fingerprinting

D. Man-in-the-middle

50. What is superzapping?

A. A slang term for NAT

B. A function of SMTP

C. A utility used to bypass access controls of an operating system

D. A tool used to monitor network traffic

51. Juggernaut and Hunt are tools used for what kind of attack?

A. Password cracking

B. Session hijacking

C. Dictionary attack

D. Piggybacking

52. A reality check of a system's security controls is referred to as what?

A. Sniffing

B. Detection controls

C. Penetration testing

D. Accreditation

53. Human resources procedures requiring all new employees to pass background checks and drug screens are what types of controls?

A. Preventive-Administrative

B. Deterrent

C. Preventive-Technical

D. Corrective

54. A device used to ensure facsimile security so that transmissions are not sent in cleartext is called a _____.

A. Firewall

B. Fax encryptor

C. Security policy

D. TCB

55. Which is not an example or characteristic of Qualitative Risk Analysis?

A. Delphi technique

B. Storyboarding

C. Single loss expectancy calculations

D. Opinion

56. Which of the following do companies commonly omit from their security programs?

A. Responsibility assignments

B. Penalties for noncompliance

C. Risk analysis

D. Awareness

57. Which of the following best describes S-RPC?

A. A remote procedure call algorithm that uses asymmetric and symmetric algorithms

B. A remote procedure call protocol that uses asymmetric and symmetric algorithms

C. A remote procedure call protocol that uses asymmetric algorithms only

D. A remote procedure call protocol used for data integrity

58. Which of the following cannot be used to prevent security breaches within an organization?

A. Administrative controls

B. Encryption

C. User authentication

D. Business continuity planning

59. Which of the following best describes the main focus of operational security?

A. It outlines and defines the access users have to company resources.

B. It performs assessments to determine who should have access to software and to what degree.

C. It maintains controls for access to hardware and media to ensure production stays operational and secure.

D. It identifies, implements, and maintains policies to ensure that production stays operational.

60. How should storage media that is no longer needed but contains/contained sensitive information be handled?

A. Sold to customers with a licensing agreement

B. Formatted and then discarded

C. Overwritten securely or physically destroyed

D. Data should be deleted and media thrown away

61. Which of the following best describes why configuration management is put into place within most environments?

A. To properly control, test, and implement changes to software, firmware, hardware, and documentation to protect against improper and potentially dangerous modifications.

B. To properly control, test, and implement changes to software, hardware, and

documentation to protect against improper and potentially dangerous modifications.

C. To properly control, test, and implement changes to software, firmware, hardware, and documentation to protect against proper modifications.

D. To properly control, test, and implement changes to software, firmware, hardware, and documentation to protect against proper and potentially beneficial modifications.

62. When a team conducts a BIA to understand the functions and resources an organization requires for productivity, the team must calculate the maximum tolerable downtime. To determine this, which of the following needs to be properly identified for each resource?

A. Vulnerabilities

B. Criticality

C. Threats

D. Risks

63. Which of the following includes ensuring that baseline versions of all software products are saved and protected as an assurance that if something bad happened, the system could be properly rebuilt?

A. Change control process

B. Custodian responsibilities within the operations department

C. Resource protection

D. Trusted recovery and degaussing

64. Once the continuity plan is developed, which of the following is not a good practice?

A. The plan should be safely kept at the primary site instead of an offsite facility where it will not be updated properly.

B. The plan should be tested and drills should be carried out to determine if items have been missed within the plan.

C. A process should be set up to ensure that the plan is continually updated.

D. Different scenarios should be used in different drills to fully test the plan in different types of situations.

65. Walt is preparing his presentation to the senior leadership team in his company. He has been appointed leader of contingency planning. He has outlined his presentation by the primary phases of the project that will be carried out. Which of the phases below is in correct order?

A. Initiate project, create strategy, create plan, perform BIA, test, implement, maintain

B. Initiate project, create strategy, perform BIA, create plan, implement, maintain, test

C. Initiate project, perform BIA, create strategy, create plan, implement, test, maintain

D. Initiate project, create strategy, create plan, perform BIA, test, implement, maintain

66. Just as new software code needs to be tested before it's ready for production, disaster recovery procedures need to be tested over and over again before a disaster actually occurs. Which of the following would not be continually tested as part of the BCP?

A. Backup magnetic media holding critical files

B. A cold site facility backup

C. A hot site facility backup

D. Emergency response procedures

67. When deciding how essential files should be moved to an offsite facility, the manager indicates that once a full set of files is moved to the offsite facility he only wants the changes transferred, not the entire files. So, it is decided that logs with the changes will be sent to an

offsite facility through an automatic system. What is this process called?

A. Disk shadowing

B. Disk duplexing

C. Remote journaling

D. Electronic vaulting

68. A company backed up its data for years and paid a courier service to pick up the tapes and bring them to an offsite facility to be maintained and protected. After finding out that some of the tapes were damaged in transit, they decided to move to an automated system instead of a manual one. Which of the following describes this new process?

A. Tape duplexing

B. Tape remote journaling

C. Tape vaulting

D. Tape mirroring

69. One day Ethan receives an interoffice mail delivery directed to all department heads. Inside the envelope is a booklet with subsections for each functional department within the company. Each recipient is instructed to review his/her section for accuracy. The sections identify key systems, backup procedures, and emergency and contingency procedures. Ethan has to sign the form, offer feedback, and return it in one week. What is the name of this process?

A. Business impact analysis

B. Checklist test

C. Simulation test

D. Structured walk-through test

70. Larry is the CIO of a data storage company. He was just recently promoted into his new position and is learning about some of the established procedures, contracts, and policies put in place by his predecessor. One contract is with a company in a city 50 miles away. The contract states that Larry's company can use this company's facilities for a period of seven days in the event of a disaster. What is the contract referred to as?

A. Redundant site

B. Merging of assets agreement

C. Reciprocal agreement

D. Dual-company contingency agreement

71. An IT director in charge of business contingencies has noticed that over time the plans become outdated. Among other things, procedures are not being followed, the project is not visible to senior management, and events are not communicated company-wide. The director has many options to improve the situation. Which of the solutions below would not be a viable option?

A. Incorporate BCP tasks into employee performance plans.

B. Implement an employee retention bonus program to decrease employee turnover.

C. Begin routine testing and drills.

D. Audit the plans regularly.

72. A contingency planner for a DSL service provider, Doug, is finishing up the BCP for all departments. One department that has outstanding action items is the ATM switch group. Doug is working with the Joe, the group's manager. Which of the following action items is Doug responsible for?

A. Working through known bugs in the switches that could affect the backup systems

B. Reviewing how long it will take for the ATM switch group's equipment to activate and carry the necessary load at the offsite facility if it has to be relocated there

C. Testing the existing backup hardware by performing unit tests and integration tests

D. Reviewing how long it will take for the ATM switch group's equipment to deactivate and carry the necessary load at the offsite facility if it has to be relocated there

73. Often systems will have backup mechanisms built into their operating procedures. This can be helpful when planning how to properly store files and ensure that data will be protected at offsite facilities. Which of the following describes database disk shadowing?

A. A system that writes to two different disks for redundancy

B. A system that has two controllers. If one fails, the other immediately takes over.

C. A system that periodically saves files to external media devices

D. A system that captures redundant copies of log files for redundancy

74. Mr. Frazier is a senior vice president of a nonprofit organization. He is championing a BCP effort that is well underway. However, over the last few weeks, he begins to wonder if he is too involved in the process and needs to take a step back. Some of his primary activities are shown below. Which one should he step away from?

A. Review budget and forecast estimates.

B. Drive each phase to ensure projects are on track.

C. Implement and assess the effectiveness of threat countermeasures identified during BIA.

D. Approve phased plans when complete.

75. Software backup is an ongoing task and one that is critical for BCP. Differential, incremental, and full backups are all different types of backup procedures for a security professional to consider. There are automated tools that perform these functions as well. What is the name of the system that provides continuous online backup functionality?

A. Disk shadower

B. HSM

C. Disk duplexer

D. DBS

76. Terry is told by his boss that he needs to implement a networked switched infrastructure that allows several systems to be connected to any storage device. What does Terry need to roll out?

A. Electronic vaulting

B. Hierarchical storage management

C. Storage area network

D. Remote journaling

77. The BCP planning committee needs to realize that during different types of disasters the telephone system may be unavailable and that there need to be alternate ways of communicating. Which of the following are the best alternative communication means in these types of situations?

A. Using ham radios and pagers

B. Using fax systems and cell phones

C. Using cell phones and ham radios

D. Using fax systems and pagers

78. A medical dispatching company is in the process of determining facility backup options. Their

number one objective is to ensure zero downtime. In addition, the senior executives are extremely focused on contingency planning and insist that testing take place throughout the year. Which of the following alternatives would serve the company best?

A. Warm site

B. Redundant site

C. Hot site

D. Reciprocal agreement

79. During the business impact analysis, the business continuity team estimates that if the web server farm is down for four hours it will cost the company $120,000. They also calculated that if a specific database was down for 72 hours it would cost the company approximately $300. Which of the following best describes the categories these two assets should be put into?

A. The web farm should be in the "important" category and the database should be in the "critical" category.

B. The web farm should be in the "nonessential" category and the database should be in the "important" category.

C. The web farm should be in the "critical" category and the database should be in the "important" category.

D. The web farm should be in the "normal" category and the database should be in the "important" category.

80. On a Tuesday morning, Jami is summoned to the office of the security director where she finds six of her peers from other departments. The security director gives them instructions about an event that will be taking place in two weeks. Each of the individuals will be responsible for removing specific systems from the facility, bringing them to the offsite facility, and implementing them. Each individual will need to test the installed systems and ensure the configurations are correct for production activities. What event is Jami about to take part in?

A. Parallel test

B. Full-interruption test

C. Simulation test

D. Structured walk-through test

81. Rita has been assigned the following tasks by the security management team: 1) Serve as disaster response coordinator for her floor; 2) Ensure all of her department coworkers have access to and understand the emergency response procedures; 3) Serve as the spokesperson to customers after a disaster in order to give them all updates on possible outages, service disruptions, etc. Rita's assignments can be categorized best as what type of control?

A. Informative

B. Administrative

C. Physical

D. Technical

82. Team members and management can decide which type of test to carry out. In fact, some companies will use several different types of test. There are many reason to include testing as part of these plans. Which of the following is the best reason for doing so?

A. To keep senior management in the loop

B. To create more opportunities for employees to get involved

C. To ensure the accuracy of the plans

D. To improve awareness

83. Which of the following best describes a hot site, compared to the other types of offsite facilities?

A. Can be up and running in a week.

B. Data and people are the only missing resources.

C. Systems and data are the only missing resources.

D. Peripheral devices and systems are the only missing resources.

84. Which of the following best describes a resource that is commonly forgotten about when developing a business continuity plan?

A. Software and its proper configurations necessary to recreate the production environment

B. Human resources and their true availability after a disaster. If the disaster was large, they may not need to be at home taking care of their families and are not available to work.

C. Human resources and their true availability after a disaster. If the disaster was large, they may need to be at home taking care of their families and are not available to work.

D. Proprietary software and devices

85. A company built its offsite facility 10 miles away from its primary location. Which of the following would be a better approach?

A. The offsite facility should be at least 125 miles from the primary facility.

B. The offsite facility should be at least 35 miles from the primary facility.

C. The offsite facility should be at least 55 miles from the primary facility.

D. The offsite facility should be at least 25 miles from the primary facility.

86. Which of the following best describes the differences between full, incremental, and differential backups?

A. A differential backup takes longer to restore than an incremental and removes the archive attribute. A full backup removes the archive attribute and must be restored before an incremental or differential backup.

B. An incremental backup takes longer to restore than a differential and removes the archive attribute. A full backup removes the archive attribute and must be restored before an incremental or differential backup.

C. An incremental backup takes longer to restore than a differential and removes the archive attribute. A differential removes the archive attribute and must be restored before an incremental or full backup.

D. An incremental backup takes longer to restore than a differential and neither removes the archive attribute. A full backup removes the archive attribute and must be restored before an incremental or differential backup.

87. Dave is an operations technician who troubleshoots customer network problems. He has access to all of the company's core switching and routing equipment and is able to remotely manage many of his customers' endpoint equipment. One week out of every month, however, Dave works in his cubicle going over trouble tickets from other technicians, while Michael replaces him on the operations floor. What operations control is being implemented here?

A. Job rotation

B. Mandatory vacations

C. Need to know

D. Least privilege

88. On his last day of work, Cory deletes all of his personal files from his hard drive by selecting each file and pressing the delete key. The next day one of his former coworkers moves into his office and turns on his newly acquired computer. Inside the recycle bin are 15 personal files that Cory intended to delete. What are these files called?

A. Metadata

B. Audit trails

C. Data remanence

D. Sanitized data

89. An attacker has infiltrated a company's network and is using a network mapping tool to learn about different devices. The tool sends out multiple ping commands and port scans and waits for responses from all of the devices. The tool then analyzes the responses to identify the operating system type, services running, and ports that are open. What is the process called?

A. Fingerprinting

B. Port scanning

C. TCP Wrapping

D. Ping evaluations

90. Trusted recovery is an important concept when understanding how computers protect themselves. Systems use several methods when they come upon situations they cannot deal with. Which of the following best describes a cold start?

A. The computer restarts when normal recovery procedures cannot execute due to TCB or media failures.

B. The computer restarts as a result of being shut down in a controlled manner.

C. The computer is restarted by user intervention due to the computer being unable to execute normal recovery procedures.

D. The computer restarts again and again due to a harmful boot sector virus.

91. There are different controls and technologies that can be implemented by the operations department. One technology that many organizations use is called RAID, a data storage system that can provide redundancy and efficiency. It functions by writing data across several aggregate drives. What is this called?

A. Parity

B. Striping

C. Degaussing

D. Data mining

92. Administrators do not want anyone to be able to arbitrarily connect to ports on critical systems and use the corresponding services. To ensure that these requests are safe and authenticated, what type of tool can be used?

A. Superzapper

B. TCP Wrapper

C. Sniffer

D. Protocol analyzer

93. Which of the following best describes the difference between slamming and cramming?

A. Cramming is when no charges have been added to a customer's bill. Slamming is when a customer's service provider has been changed without her consent.

B. Slamming is when extra charges have been added to a customer's bill. The customer did not

request or receive these services. Cramming is when a customer's service provider has been changed without her consent.

C. Cramming is when extra charges have been added to a customer's bill. The customer did not request or receive these services. Slamming is when a customer's service provider has been changed without her consent.

D. Cramming is when extra charges have been added to a customer's bill. The customer did not request or receive these services. Slamming is when a customer's bill is sent to the wrong customer on purpose.

94. Max has just finished developing a new software feature that the network provisioners have been requesting for some time. Anxious to get this to the group, Max installs the patch on a production system. The next day he is summoned to his boss's office who is very angry. His boss says, "You didn't submit a request, get approval, document anything, or do proper testing." What procedure is Max's boss referring to?

A. Sanitization

B. Due care

C. Change control

D. Operational assurance

95. In a 24-hour time frame, Aaron does the following: 1) Scavenges through a dumpster outside of the accounting wing of his company; 2) Reviews sensitive data on a private network by entering unauthorized access credentials; and 3) Compiles a list of system passwords from engineering by watching over the shoulder of a new engineer. These activities are collectively referred to as _____.

A. Physical attacks

B. Browsing

C. Cracking

D. Hijacking

96. Which of the following acts test the effectiveness of security mechanisms placed within a network by performing strikes against different access points?

A. Penetration testing

B. Network mapping

C. Session hijacking

D. Port scanning

97. Tim is an entry-level customer service representative working with a client on a service escalation. After working through several issues, the customer asks Tim if he can verify the annual service charge and opt-out provisions of his contract. Tim unhappily responds that he only has access to technical and operations data and cannot access contract information. He says he must transfer the customer to customer service. What type of control is described in this example?

A. Clipping level

B. Least privilege

C. Operations security

D. ACL

98. There should be one role or committee that is responsible for enforcing and maintaining the change control process within a company. Which of the following functions is not the

responsibility of this group?

A. To properly modify the change control process depending upon the logic of the change that was requested

B. To provide formal approval or rejection of the change to the requester

C. To enforce strict, consistent company-wide procedures

D. To provide clear instructions to all employees on how to initiate a change request

99. Robert is one of 100 order-entry clerks handling customer requests. He enters thousands of orders each day and must abide by strict policies and procedures when doing so. On Tuesday, Robert has a particularly bad day and acknowledges to himself that he probably made several mistakes. On Wednesday afternoon, he is called into his boss's office where he learns that he made ten critical errors. An automated system most likely used which of the following to detect these errors?

A. Administrative controls

B. Clipping levels

C. IDS

D. Fingerprinting

100. Which of the following terms best describes when an operating system and its kernel are being loaded into memory?

A. Loading of the initial program

B. Initial program load

C. Superzapping of the system

D. Checkpointing of a system

101. In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name

B. A blacklist of companies that have their mail server relays configured to be wide open

C. Mail relaying, which is a technique of bouncing e-mail from internal to external mail servers continuously

D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally

102. Pertaining to operational security, which of the following best describes "deviation from standards?"

A. Performing at the same level of the standard set baseline of security and functionality

B. Performing at a different level than the standard set baseline of security and functionality

C. Performing at a higher level than the standard set of procedures put in place

D. Performing at a level that is different than other systems in the same environment

103. The three main types of operational controls are technical, administrative, and physical. There are several mechanisms for each of these types that provide different services. What service does passwords, ACLs, and ID badges all provide?

A. Deterrent

B. Correction

C. Prevention

D. Compensation

104. Which of the following backup facilities is the most expensive?

A. Cold

B. Hot

C. Warm

D. Rolling hot site

105. Which of the following is the main reason business continuity plans become outdated?

A. They are viewed as regulatory.

B. They are viewed as mandatory.

C. They are viewed as necessities.

D. They are viewed as a project.

106. A disaster recovery procedure that involves all affected departments acting out a specific scenario but does not go to an offsite facility, is referred to as a _____.

A. Simulation test

B. Structured walk-through test

C. Checklist test

D. Parallel test

107. Following a disaster, what should be done first when the original facility is operational again?

A. Inform the media and stockholders.

B. Move the most critical systems to the original facility.

C. Move the most critical functions to the original facility.

D. Move the least critical functions to the original facility.

108. What is the switched fabric in a storage area network?

A. The paths between the nodes and the servers. It provides fault tolerance, but no redundancy.

B. The paths between the nodes and the back-end storage devices. It provides fault tolerance and redundancy.

C. The paths between the nodes and the back-end storage devices. It provides integrity and confidentiality.

D. The paths between the nodes and the servers. It provides integrity and confidentiality.

109. Which of the following disaster recovery tests is the most intrusive to business operations?

A. Parallel

B. Simulation

C. Full-interruption

D. Checklist

110. Talking to external organizations after a disaster is important for all of the following reasons except which one?

A. To inform customers and shareholders of the company's status

B. To redirect unfavorable attention to other entities

C. To ensure that the media is reporting the facts accurately

D. To help stop rumors from developing

111. A business impact analysis includes any of the following except for _____.

A. Calculating risk

B. Identifying threats

C. Selecting team members

D. Identifying critical functions of the company

112. Which of the following is not a senior management task in disaster recovery?

A. Approve final plans.

B. Oversee budget.

C. Drive all phases of plan.

D. Implement the plans.

113. Organizations should not view business continuity as _____.

A. A committed expense

B. A discretionary expense

C. An enforcement of legal statutes

D. A profitable agreement

114. Which of the following is not an offsite transaction redundancy implementation for database security?

A. Onsite mirroring

B. Electronic vaulting

C. Remote journaling

D. Database shadowing

115. Prior to a live full-interruption disaster test, which of the following is most important?

A. Restore all files in preparation for the test.

B. Document expected findings.

C. Arrange physical security for the test site.

D. Conduct a successful structured walk-through.

116. Of all business process interruptions, the most devastating are ones resulting from _____.

A. Loss of hardware/software

B. Loss of data

C. Loss of communication links

D. Loss of applications

117. What are critical support areas defined as?

A. Business units or functions that must be present to sustain continuity of business, maintain life safety, and avoid public embarrassment

B. Business units or functions that may be replaced by others in a disaster situation

C. Human resource technologies

D. Business units or functions that require support against manmade disasters

118. Which of the following is not a direct benefit of successful business continuity planning?

A. Maintaining business continuity

B. Protecting critical data

C. Increasing IS performance

D. Minimizing impact of a disaster

119. Which of the following is not a reason to develop and implement a disaster recovery plan?

A. Provides procedures for emergency responses

B. Extends backup operations to include more than just backing up data

C. Provides steps for a post-disaster recovery

D. Outlines business functions and systems

120. Which of the following is not a control that can be used to secure faxing of sensitive data?

A. Using a fax encryptor

B. Sending to e-mail boxes instead of printing

C. Printing a "sensitivity banner" on each page

D. Disabling printing

121. What is the purpose of configuration management?

A. Controlling access to protected assets

B. Controlling changes that happen to hardware and software

C. Controlling who accesses the facility

D. Controlling who sniffs network traffic

122. Which of the following is not considered an administrative control?

A. Rotation of duties

B. Implementation of WEP keys

C. Separation of duties

D. Enforcing mandatory vacations

123. Which of the following does not fall under the responsibilities of the operations department?

A. Deviation of standards

B. Unexplained software or hardware occurrences

C. Unscheduled initial load programs

D. Developing policies

124. Which of the following is not a method of properly protecting from the threats connected to object reuse?

A. Zeroization

B. Destroying

C. Deleting

D. Degaussing

125. Pretending to be another person in order to gain privileges is an example of what kind of attack?

A. Scavenging

B. Spoofing

C. Keystroke monitoring

D. Man-in-the-middle

126. NetBus is used to carry out which of the following activities?

A. Allows for single sign-on functionality, similar to RADIUS

B. Carrying out logic bombs and virus filtration

C. Remote control of a system

D. Conducts teardrop attacks

127. A utility used in IBM mainframe centers for administrative maintenance procedures which can bypass access controls is called _____.

A. Superzapper

B. Scanner

C. Browser

D. Sniffer

128. Looking through another person's computer files is an example of what type of attack?

A. DoS

B. Hijacking

C. Dictionary

D. Browsing

129. What is SATAN used for?

A. To identify vulnerabilities within a network

B. To open network security holes

C. To reamplify a signal

D. To track network connections

130. Sending packets with the same source and destination addresses would be considered what type of attack?

A. Denial-of-service attack

B. Asynchronous attack

C. Distributed attack

D. Timing attack

131. What is configuration management used for in many different environments?

A. Controlling changes in testing procedures

B. Controlling testing environments and documentation of testing

C. Ensuring changes in design and its verification of process, testing, and implementation

D. Controlling changes in design and its verification of process, testing, and implementation

132. The basic features and architecture of a system are the focus of _____.

A. Life cycle assurance

B. Operational assurance

C. Hidden channel assurance

D. Level A1

133. Which of the following ensures that security is not compromised when a system crashes or a component failure occurs?

A. Trusted recovery

B. Hot swappable

C. Redundancy

D. Secure boot

134. Overwriting and/or degaussing is used to clear and purge all of the following except _____.

A. Random access memory

B. Data buses

C. Secondary storage

D. Magnetic hard disks

135. Operations security seeks to protect a company primarily against _____.

A. Object reuse

B. Asset threats

C. Compromising emanations

D. Facility disaster

136. Which of the following refers to the data left on the media after the media has been erased?

A. Semi-hidden

B. Dregs

C. Sticky bits

D. Remanence

137. Which of the following does not need to be on the label for company backup tapes?

A. Date of creation

B. Authors of documents

C. Classification

D. Retention period

138. What role should accountability play in the access to media and auditing portion of a company's operations security strategy policies?

A. None. Accountability is managed by corporate security policies, not at the operator level.

B. Accountability is the other side of the coin of auditing. If a user is properly authorized, any violations or errors he makes can be traced back to him if auditing is in place.

C. Accountability means that the creator of the company’s access policy bears final accountability for any improper accesses.

D. Accountability means that the entire IT department, as creator of the company’s access policy, bears final accountability for any improper accesses.

139. Which of the following is a correct description of S-RPC?

A. Uses RSA for secret key determination and is used to encrypt remote procedure calls between systems

B. Uses Diffie-Hellman for secret key determination and is used to encrypt remote procedure calls between systems

C. Uses Diffie-Hellman for asymmetric key determination and is used to encrypt local procedure calls between systems

D. Uses Diffie-Hellman for secret key determination and is used to encrypt local procedure calls between systems

140. Which of the following steps in the incident response process is considered the most important?

A. Response

B. Detection

C. Mitigation

D. Recovery

141. All of the following are steps in the incident response process, except:

A. Detection

B. Mitigation

C. Prevention

D. Remediation

142. Which of the following publications provides guidance on supply chain management?

A. ISO 27001

B. ISO/IEC 14443

C. ISO 28000

D. ISO 17799

143. All of the following are types of analysis a forensic investigator can perform on an embedded device, except:

A. Dedicated appliance attack points

B. Workstation attack analysis

C. Embedded operating systems, virtualized software, and hypervisor analysis

D. Firmware and dedicated memory inspections

144. Which of the following terms refers to the set of all activities required to provide one or more new information services to a user or group of users?

A. Provisioning

B. Installing

C. Acquiring

D. Supply chain management

145. Which of the following terms refers to the process of establishing and maintaining consistent baselines on all organizational systems?

A. Control management

B. Configuration management

C. Change management

D. Asset management

146. Which of the following might be provisioned for a single new user of a cloud service?

A. Physical server

B. Virtual server

C. Hardware RAID array

D. Software RAID

147. Because a SAN provides redundancy, fault tolerance, reliability, and backups, it allow users and administrators to interact with it as _____.

A. Separate devices

B. Mapped drives

C. One virtual entity

D. Virtual drives

148. In which of the following overall management processes would service level agreements (SLAs) be included?

A. Third-party security policies

B. Internal contractor management processes

C. Vendor management governing processes

D. Internal interdepartmental agrements

149. All of the following typically can be provisioned using cloud services, except:

A. Software-as-a-Service

B. Platform-as-a-Service

C. Authentication-as-a-Service

D. Infrastructure-as-a-Service

150. Which of the following terms refers to allowing only certain applications to run, or allowing only certain DNS domains to be accessible to the network?

A. Blacklisting

B. Proxying

C. Whitelisting

D. Greylisting

151. What is developed and shared with others at the end of the remediation phase of the incident management process?

A. Incident report

B. Lessons learned

C. Vulnerability report

D. Law enforcement report

152. All of the following are characteristics of high availability, except:

A. Recovery time objective

B. Redundancy

C. Fault tolerance

D. Failover

153. A _____ is a device that is developed in order to deceive attackers into believing it is a real production system, entice and allow these adversaries to compromise it, and then monitor their activities on the compromised system to observe and learn their behaviors.

A. DMZ

B. Bastion host

C. Honeypot

D. Screened subnet

154. How will individuals know what is expected of them during a disaster or its recovery operations?

A. Briefing

B. Policy document

C. Written procedures

D. In-depth training

155. A critical first step in disaster recovery and contingency planning is which of the following?

A. Complete a business impact analysis.

B. Determine offsite backup facility alternatives.

C. Organize and create relevant documentation.

D. Plan testing and drills.

156. There are different types of offsite facilities, either subscription based or company owned. Which type of subscription-based backup facility is used most often?

A. Cold

B. Warm

C. Hot

D. Redundant

157. In disaster recovery, each level of employee should have clearly defined responsibilities. Which of the following is a responsibility of senior executives?

A. Develop testing plans

B. Establish project goals and develop plans

C. Identify critical business systems

D. Oversee budgets

158. Which of the following is not a reason to develop a business continuity plan?

A. To train employees on how to keep the company in business after a disaster

B. To restrict business productivity

C. To include procedures on how to move to and from an offsite facility

D. To limit business interruption

159. A company that has to guarantee near 100 percent functionality would choose which type of backup facility?

A. Redundant

B. Rolling hot site

C. Cold

D. Warm

160. There are several reasons for a company to develop and implement a disaster recovery plan. What is the most important goal of disaster recovery?

A. Protect the integrity of the business

B. Protect critical operating systems

C. Protect human life

D. Protect customer relationships

161. Which of the following threats cripples a business, destroys the original facility, and requires short- and long-term recovery planning?

A. Nondisaster

B. Disaster

C. Manmade disaster

D. Catastrophe

162. Disaster recovery and contingency plans become outdated for all of the following reasons except _____.

A. A company’s infrastructure changes

B. Too many drills cause the plan to become inaccurate

C. Personnel turnover

D. Company and departmental reorganizationsTesting helps keep disaster recovery and contingency plans alive.

163. Which step is not part of the business impact analysis (BIA)?

A. Determine MTD values

B. Interview key personnel

C. Identify critical business functions

D. Report findings to the staff

164. An IT administrator is charged with the task of ensuring that data files are backed up at a remote location in case there is ever a disaster that destroys the main facility. Which of the following would be the best option?

A. Disk shadowing

B. Manual file copying and manual transport to the remote facility

C. Electronic vaulting

D. Disk duplexing

165. In the moments following a disaster, who should be called first?

A. CEO

B. The person designated in the continuity plan

C. Board of directors

D. Family of the injured

166. Different threats need to be properly classified so that a company knows how to properly react to the different situations. A workstation that fails and goes offline for three hours would be most commonly classified as a _____.

A. Disaster

B. Nondisaster

C. Catastrophe

D. Mishap

167. Members of the business continuity committee would do all of the following tasks except _____.

A. Gather data from other departments

B. Ensure budgets are on track

C. Complete a BIA

D. Report findings to senior management

168. What type of test should be completed before an actual simulation test occurs?

A. Parallel test

B. Structured walk-through test

C. Full-interruption test

D. Emergency procedures test

169. Which entity would handle business continuity planning (BCP) tasks, such as making insurance claims, assessing damage value, and estimating recovery expenses?

A. Department leads

B. Senior executives

C. HR

D. Financial representative to the BCP committee

170. Which of the following mechanisms could be used in business continuity?

A. Closed-circuit TV (CCTV) monitoring system

B. Data backup automation to a remote site

C. Calling tree

D. All of the other choices

171. What is the first step in planning disaster response procedures?

A. Identify a team.

B. Create documentation.

C. Identify threats.

D. Gather data.

172. Which backup facility alternative would be the best choice for a company that needed a long-term recovery solution with minimal downtime?

A. Rolling hot site

B. Cold site

C. Redundant site

D. All of the other choices

173. Which of the following has the ultimate responsibility for authorizing expenditures and acting on the suggestions of the BCP committee and the results of a business impact analysis?

A. Individual department managers

B. Senior management

C. Functional manager of that site

D. Security officer

174. Once the continuity plan is developed, which of the following is not a good practice?

A. The plan should be safely kept at the primary site instead of an offsite facility where it will not be updated properly.

B. The plan should be tested and drills should be carried out to determine if items have been missed within the plan.

C. A process should be set up to ensure that the plan is continually updated.

D. Different scenarios should be used in different drills to fully test the plan in different types of situations.

175. Walt is preparing his presentation to the senior leadership team in his company. He has been appointed leader of contingency planning. He has outlined his presentation by the primary phases of the project that will be carried out. Which of the following phases is in the correct order?

A. Initiate project, create strategy, create plan, perform BIA, test, implement, maintain

B. Initiate project, create strategy, perform BIA, create plan, implement, maintain, test

C. Initiate project, perform BIA, create strategy, create plan, implement, test, maintain

D. Initiate project, create strategy, create plan, perform BIA, test, implement, maintain

176. Just as new software code needs to be tested before it’s ready for production, disaster recovery procedures need to be tested over and over again before a disaster actually occurs. Which of the following would not be continually tested as part of the BCP?

A. Backup magnetic media holding critical files

B. A cold site facility backup

C. A hot site facility backup

D. Emergency response procedures

177. When deciding how essential files should be moved to an offsite facility, the manager indicates that once a full set of files is moved to the offsite facility he only wants the changes transferred, not the entire files. So, it is decided that logs with the changes will be sent to an offsite facility through an automatic system. What is this process called?

A. Disk shadowing

B. Disk duplexing

C. Remote journaling

D. Electronic vaulting

178. A company backed up its data for years and paid a courier service to pick up the tapes and bring them to an offsite facility to be maintained and protected. After finding out that some of the tapes were damaged in transit, they decided to move to an automated system instead of a manual one. Which of the following describes this new process?

A. Tape duplexing

B. Tape remote journaling

C. Remote journaling

D. Electronic vaulting

179. One day Ethan receives an interoffice mail delivery directed to all department heads. Inside the envelope is a booklet with subsections for each functional department within the company. Each recipient is instructed to review his or her section for accuracy. The sections identify key systems, backup procedures, and emergency and contingency procedures. Ethan has to sign the form, offer feedback, and return it in one week. What is the name of this process?

A. Business impact analysis

B. Checklist test

C. Simulation test

D. Structured walk-through test

180. Larry is the CIO of a data storage company. He was just recently promoted into his new position and is learning about some of the established procedures, contracts, and policies put in place by his predecessor. One contract is with a company in a city 50 miles away. The contract states that Larry's company can use this company's facilities for a period of seven days in the event of a disaster. What is the contract referred to as?

A. Redundant site

B. Merging of assets agreement

C. Reciprocal agreement

D. Dual-company contingency agreement

181. An IT director in charge of business contingencies has noticed that over time the plans become outdated. Among other things, procedures are not being followed, the project is not visible to senior management, and events are not communicated company-wide. The director has many options to improve the situation. Which of the following solutions would not be a viable option?

A. Incorporate BCP tasks into employee performance plans.

B. Implement an employee retention bonus program to decrease employee turnover.

C. Begin routine testing and drills.

D. Audit the plans regularly.

182. Software backup is an ongoing task and one that is critical for BCP. Differential, incremental, and full backups are all different types of backup procedures for a security professional to consider. There are automated tools that perform these functions as well. What is the name of the system that provides continuous online backup functionality?

A. Disk shadower

B. Hierarchical storage management (HSM)

C. Disk duplexer

D. DBS

183. The BCP planning committee needs to realize that during different types of disasters the telephone system may be unavailable and that there need to be alternate ways of communicating. Which of the following are the best alternative communication means in these types of situations?

A. Using ham radios and pagers

B. Using fax systems and cell phones

C. Using cell phones and ham radios

D. Using fax systems and pagers

184. A medical dispatching company is in the process of determining facility backup options. Their number one objective is to ensure zero downtime. In addition, the senior executives are extremely focused on contingency planning and insist that testing take place throughout the year. Which of the following alternatives would serve the company best?

A. Warm site

B. Redundant site

C. Hot site

D. Reciprocal agreement

185. During the business impact analysis, the business continuity team estimates that if the Web server farm is down for four hours it will cost the company $120,000. They also calculated that if a specific database was down for 72 hours it would cost the company approximately $300. Which of the following best describes the categories these two assets should be put into?

A. The Web farm should be in the “important” category and the database should be in the “critical” category.

B. The Web farm should be in the “nonessential” category and the database should be in the “important” category.

C. The Web farm should be in the “critical” category and the database should be in the “important” category.

D. The Web farm should be in the “normal” category and the database should be in the “important” category.

186. Rita has been assigned the following tasks by the security management team: 1) Serve as disaster response coordinator for her floor; 2) Ensure all of her department coworkers have access to and understand the emergency response procedures; 3) Serve as the spokesperson to customers after a disaster in order to give them all updates on possible outages, service disruptions, etc. Rita’s assignments can be categorized best as what type of control?

A. Informative

B. Administrative

C. Physical

D. Technical

187. Team members and management can decide which type of test to carry out on business continuity plans. In fact, some companies will use several different types of tests. There are many reasons to include testing as part of these plans. Which of the following is the best reason for doing so?

A. To keep senior management in the loop

B. To create more opportunities for employees to get involved

C. To ensure the accuracy of the plans

D. To improve awareness

188. Which of the following best describes a hot site, compared to the other types of offsite facilities?

A. Can be up and running in a week.

B. Data and people are the only missing resources.

C. Systems and data are the only missing resources.

D. Peripheral devices and systems are the only missing resources.

189. Which of the following best describes a resource that is commonly forgotten about when

developing a business continuity plan?

A. Software and its proper configurations necessary to re-create the production environment

B. Human resources and their true availability after a disaster. If the disaster was large, they may not need to be at home taking care of their families and are not available to work.

C. Human resources and their true availability after a disaster. If the disaster was large, they may need to be at home taking care of their families and are not available to work.

D. Proprietary software and devices

190. Which of the following best describes the differences between full, incremental, and differential backups?

A. A differential backup takes longer to restore than an incremental and removes the archive attribute. A full backup removes the archive attribute and must be restored before an incremental or differential backup.

B. An incremental backup takes longer to restore than a differential and removes the archive attribute. A full backup removes the archive attribute and must be restored before an incremental or differential backup.

C. An incremental backup takes longer to restore than a differential and removes the archive attribute. A differential removes the archive attribute and must be restored before an incremental or full backup.

D. An incremental backup takes longer to restore than a differential, and neither removes the archive attribute. A full backup removes the archive attribute and must be restored before an incremental or differential backup.

191. Which of the following is the main reason business continuity plans become outdated?

A. They are viewed as regulatory.

B. They are viewed as mandatory.

C. They are viewed as necessities.

D. They are viewed as a project.

192. The _____ is the earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity.

A. Recovery time objective

B. Recovery time point

C. Maximum tolerable downtime

D. Phase I

193. Recovery time objective (RTO) usually deals with getting the infrastructure and systems back up and running. What metric is commonly used to deal with restoring data, testing processes, and then making everything “live” for production purposes?

A. Maximum tolerable downtime

B. Work recovery time

C. Recovery point objective

D. Mean time to recover

194. What component of BCP/DRP focuses on restoring an organization’s (usually a headquarters element) essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations?

A. Continuity of operations

B. Recovery point objective

C. Recovery time objective

D. Maximum tolerable downtime

195. What are some of the major pitfalls affecting law enforcement, the court system, and the legal community when it comes to cybercrimes?

A. Technology is changing exponentially, therefore making it difficult for the law to keep up.

B. Misunderstanding of technological terms and concepts.

C. Their lack of skill in the computing world and the complexity of issues involved.

D. All of the other choices.

196. The seriousness and volume of cybercrimes will continue to grow because:

A. Society is constantly increasing its dependence upon and improving its use of technology.

B. Criminals are able to get away with larger crimes.

C. The legal system has no precedence for prosecuting a cybercriminal.

D. Companies aren't taking steps to ensure their networks are secure.

197. Bill, a cybercriminal who lives in Germany, has been able to get away with stealing millions of dollars from American companies. These companies are limited in how they can prosecute because Bill is living in another country. What is this an example of?

A. Globalization

B. Jurisdiction limitations

C. Lack of funding for law enforcement

D. Extortion

198. Which of the following statements is true?

A. If hackers do not profit from their hacking efforts, it is not a crime.

B. Systems should be protected, so if they are not locked down, it is the victim's fault and not the hacker's fault.

C. Writing viruses is not protected by the First Amendment.

D. Information should be available to everyone; thus, acquiring it is not illegal.

199. The act of committing small crimes in hopes that the larger overall crime goes unnoticed is known as:

A. Data diddling

B. Cooking the books

C. Dumpster diving

D. Salami attack

200. The "Safe Harbor" privacy framework was created to:

A. Ensure that personal information should be collected only for a stated purpose by lawful and fair means and with the knowledge or consent of the subject

B. Provide a streamlined means for U.S. organizations to comply with European privacy laws

C. Require the federal government to release to citizens the procedures for how records are collected, maintained, used, and distributed

D. None of the others

201. Which of the following acts requires financial institutions to notify customers on how their private information will be protected and distributed to third parties?

A. Gramm-Leach-Bliley Financial Modernization Act

B. The Electronic Communications Privacy Act

C. Fair Credit Reporting Act

D. Federal Wiretap Act

202. The European Union's Directive on Data Protection forbids the transfer of individually identifiable information to a country outside the EU, unless:

A. The receiving country grants individuals adequate privacy protection.

B. The receiving country pays a fee to the EU.

C. There are no exceptions; no information is ever transferred.

D. The receiving country is a member of the Fair Trade Organization.

203. What is the Federal Wiretap Act?

A. A criminal law that forbids unauthorized people from accessing or damaging electronic messages in storage

B. A criminal law that punishes unauthorized interception of electronic communications in transit

C. Also known as the "antihacking law"

D. The most commonly used law in prosecuting computer crimes

204. Under the Economic Espionage Act of 1996, the U.S. Department of Justice is granted the authority to prosecute for the theft of:

A. Individual financial information

B. Personal identification information

C. Trade secrets

D. All of the other choices

205. The Anticybersquatting Consumer Protection Act (ACPA) was enacted to protect which type of intellectual property?

A. Trade secrets

B. Copyrights

C. Trademarks

D. Patents

206. Why are computer crimes so difficult to investigate and prosecute?

A. Jurisdiction issues.

B. Evidence is intangible and hard to collect.

C. Lack of reporting of crimes by organizations.

D. All of the other choices.

207. What is the difference between best evidence and direct evidence?

A. Best evidence is the most reliable, such as a signed document, whereas direct evidence can prove a fact all by itself, without supporting information.

B. Best evidence is often not viewed as reliable and strong in proving innocence and guilt, whereas direct evidence can be information from a witness, such as oral testimony.

C. Best evidence is often original documents—no copies—whereas direct evidence is irrefutable and cannot be contradicted.

D. Best evidence and direct evidence mean the same thing.

208. What is the importance of an audit trail?

A. It reveals the who, what, where, and how for all logged activity.

B. It ensures the segregation of duties and, therefore, improves the security of the overall system.

C. It can assist in providing regular business records, which ultimately have more weight as evidence in prosecuting computer crimes.

D. Both A and C are correct.

209. What is the proper order of steps in the investigation process?

A. Containment, Collection, Analysis, Preservation, Discovery, Presentation, Decision

B. Identification, Analysis, Collection, Discovery, Examination, Presentation, Decision

C. Identification, Preservation, Collection, Examination, Analysis, Presentation, Decision

D. Collection, Containment, Examination, Identification, Analysis, Presentation, Decision

210. Which of the following is not a technique for seizing and preserving electronic evidence?

A. Restrict all physical and remote access to the computer.

B. Photograph any images on the screen showing the state of the system.

C. Conduct all forensic analysis operations of the evidence on imaged copies of the original disk.

D. Attempt to log into the computer to find any evidence.

211. What is the difference between an event and an incident?

A. An event is an occurrence of an activity that can be detected, verified, analyzed, and documented; an incident is an occurrence of an activity that cannot be detected, verified, analyzed, or documented.

B. An event is a large occurrence that does not go unnoticed; an incident is a small occurrence that may or may not be noticed.

C. An event is an occurrence of an activity that can be detected, verified, analyzed, and documented; an incident is one or more events that adversely affect the organization—an incident can be an event.

D. An event is a small occurrence that may or may not be noticed; an incident is a large occurrence that does not go unnoticed.

212. What does downstream liability mean?

A. When a company implements the required legal minimum to ensure their systems will not have a negative impact on others

B. Dissemination of helpful information for the protection of all organizations

C. The evolution of cyberlaws in relation to the changes in policies and procedures of organizations

D. When a vulnerable company’s system ends up being compromised and used to conduct a denial-of-service attack on another company

213. A software program would be protected from illegal distribution under what law?

A. Trademark

B. Copyright

C. Trade secret

D. SPA

214. What is one of the items that the G8 has agreed to work together on?

A. To fight against cybercrime

B. To legislate on economic espionage

C. To protect employee privacy rights

D. To prosecute software pirates

215. An edict stating that all evidence be labeled with information about who secured it and who

validated it is called _____.

A. CERT

B. Chain of custody

C. Direct evidence

D. Incident response policy

216. The golden arches of McDonald’s are protected under what intellectual property law?

A. Trademark

B. Trade secret

C. Logo protection law

D. Copyright

217. Computer-generated or electronic information is most often categorized as what type of evidence?

A. Best

B. Hearsay

C. Corroborative

D. Opinion

218. Which type of law punishes the individuals with financial restitution instead of with jail penalties?

A. Tort

B. Administrative

C. Criminal

D. Regulatory

219. Which of the following is an attack that uses tools to intercept electronic communication signals usually passively instead of actively?

A. Masquerading

B. Social engineering

C. Wiretapping

D. Salami

220. If a waiter tells his friends how the restaurant’s famous secret sauce is made, what law has he violated?

A. No law was violated

B. Trademark

C. Trade secret

D. Copyright

221. What is the first step in forensic analysis at a cybercrime scene?

A. Execute the primary programs on the computer to obtain more information

B. Capture log files on the computer

C. Notify customers of potential outages

D. Capture a complete image of the system

222. A witness testimony would be classified as what type of evidence?

A. Real

B. Secondary

C. Best

D. Conclusive

223. Which of the following would protect a senior executive in a liability lawsuit brought on by an employee?

A. He is able to demonstrate that due diligence and due care were established and followed.

B. He was on vacation during the incident.

C. The incident was not covered in the company’s security policy.

D. The employee was not in good standing.

224. Who usually blows the whistle on illegal software usage within companies?

A. IT administrators

B. CISSPs

C. Disgruntled employees

D. Managers

225. Which person would not be part of the Internet Architecture Board?

A. Software programmer

B. IT executive

C. Technology researcher

D. Appointed FCC representative

226. The investigation process of a computer crime is very similar to investigating many other types of crimes. What is the “who” and “why” of a crime?

A. Motives

B. Opportunities

C. Means

D. Capabilities

227. Which of the following was the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation?

A. Council of Global Convention on Cybercrime

B. Council of Europe Convention on Cybercrime

C. Organisation for Economic Co-operation and Development

D. Organisation for Cybercrime Co-operation and Development

228. Lee is a new security manager who is in charge of ensuring that his company complies with the European Union Principles on Privacy when his company is interacting with their European partners. The set of principles that deal with transmitting data considered private are encompassed within which of the following?

A. Data Protection Directive

B. Organisation for Economic Co-operation and Development

C. Federal Private Bill

D. Privacy Protection Law

229. A construct that outlines how U.S.-based companies can comply with the EU privacy principles has been developed; this framework outlines how any entity that is going to move privacy data to and from Europe must go about protecting them. Which of the following best describes this construct?

A. Organisation for Economic Co-operation and Development

B. Global Privacy Protection Initiative

C. Data Protection Regulatory Standards

D. Safe Harbor

230. Which world legal system was developed in England and is based on previous interpretations of laws where judges and juries of peers are commonly used?

A. Code law system

B. Common law system

C. Criminal law system

D. Religious system

231. The common law system is broken down into which of the following categories?

A. Common, civil, criminal

B. Legislation, bills, regulatory

C. Civil, criminal, regulatory

D. Legislation, bills, civil

232. Which of the following is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services that circumvent access control measures that are put into place to protect copyright material?

A. Copyright law

B. Digital Millennium Copyright Act

C. Federal Privacy Act

D. SOPA

233. Privacy is becoming more threatened as the world relies more and more on technology. There are several approaches to addressing privacy, including the generic approach and regulation by industry. Which of the following best describes these two approaches?

A. The generic approach is vertical enactment. Regulation by industry is horizontal enactment.

B. The generic approach is horizontal enactment. Regulation by industry is vertical enactment.

C. The generic approach is government enforced. Regulation by industry is self-enforced.

D. The generic approach is self-enforced. Regulation by industry is government enforced.

234. Which of the following is a Canadian law that deals with the protection of personal information?

A. Personal Information Protection and Electronic Documents Act

B. Personal Information Protection and Electronic Act

C. Canadian Personal Information Protection and Electronic Act

D. Canadian Personal Information Protection and Electronic Documents Act

235. Jeff has been told that an audit needs to be carried out to ensure their partner has the proper internal controls in place. Which of the following should Jeff ensure is carried out?

A. SAS 70

B. COBIT

C. COSO

D. SABSA

236. Jan has been told that she needs to develop key performance indicators for the organization’s governance, risk, and compliance program. Which of the following best describes how these items relate to each other?

A. Key performance indicators are used to determine the organization’s compliance level.

B. Key performance indicators are used to determine how well governance, risk, and compliance service-level agreements are taking place within the organization.

C. Key performance indicators are used to determine the offset of the governance, risk, and compliance tasks within the organization.

D. Key performance indicators are used to determine how well governance, risk, and compliance are taking place within the organization.

237. Viruses in public networks are referred to as what?

A. Production-ready

B. In the zoo

C. In the wild

D. A Trojan horse

238. Which of the following is an object-oriented programming language that runs on many platforms?

A. Java

B. HTTP

C. OLE

D. ActiveX

239. In the project initiation phase of software development, all of the following tasks should be performed except _____.

A. Conduct a kick-off meeting

B. Perform a risk analysis

C. Analyze threats

D. Define security controls

240. Malware that is embedded within a program and executes harmful actions behind the scenes while the victim believes the program is operating normally is called what?

A. Trojan horse

B. Stealth virus

C. Smurf attack

D. Multipartite virus

241. The artificial neural network (ANN) is based on which of the following?

A. The combined security policies of all connected computers

B. The human brain

C. The least common denominator

D. Rule-based administration

242. In relational databases, several different terms are used to describe the different components of the database. What is a tuple?

A. A column in a database

B. A row in a database

C. A collection of tables

D. A view or partition of data

243. The act of compiling data from several databases so that the information may be better analyzed is called _____.

A. Data mining

B. Partitioning

C. Interference

D. Data warehousing

244. A virus is planted within a drafting program on a user's machine. When the user clicks Save, the program instead deletes all the files on the hard drive. This is an example of what?

A. Logic bomb

B. DDoS

C. Smurf attack

D. Timing attack

245. A collection of data from different sources that is targeted at one group or for a specific objective is called a _____.

A. Data mart

B. Data warehouse

C. Metadata

D. Data center

246. Several different terms within object-oriented programming describe types of objects and their activities. What does polyinstantiation mean?

A. A mechanism used to take a copy of an object and repopulate it with different data or modify its characteristics in some way

B. An act of two objects responding differently to the same command

C. The process of hiding data

D. The translation of two different languages on one platform

247. Different activities need to take place during software development. What does debug mean?

A. To magnetically erase data from a medium

B. To trace and fix software failures

C. To change security levels

D. To change assembly language into machine language

248. Unit testing is performed in what phase of the software development life cycle?

A. Acceptance testing/implementation

B. Operations/maintenance

C. System design specifications

D. Software development

249. Generation One of program languages includes which of the following?

A. Machine language

B. Assembly language

C. Object-oriented language

D. Artificial intelligence

250. Computer programs that are based on human logic by using "if/then" statements and inference engines are called _____.

A. ANN

B. Artificial expert systems

C. Expert systems

D. ActiveX

251. What is CORBA?

A. A design framework for applications written in Java

B. A standard to allow communications between programs written in different languages and

platforms

C. A Microsoft model aimed at allowing objects to communicate with objects on different computers

D. An object-oriented programming language developed by Sun Microsystems

252. A change control committee is formed to evaluate all proposed changes in order to ensure what?

A. Comprehensiveness and timeliness

B. Business impact and security

C. Project milestones and timeliness

D. Correctness and desirability

253. A processor can work in different modes. If it is working in "supervisor" mode, what does that mean?

A. It cannot accept software or hardware interrupts.

B. It is working at a lower privilege than user mode.

C. It has access to privileged and nonprivileged instructions.

D. It is computing nonprivileged instructions.

254. Your company has several applications that rely on each other for information and processes. Several of the systems use different programming languages, so each has adhered to a CORBA framework. When one system sends a request to an object on another system, what component does the request actually go to?

A. EJB

B. ORB

C. COM

D. Active X

255. Ron and Kathy work in two different departments and perform two different job functions. However, both utilize the same database for their jobs. When Ron opens his database, he sees four pages of input fields, while Kathy only sees two pages. What type of security protection has been implemented in their database?

A. Views

B. Data warehousing

C. Perturbation

D. Checkpointing

256. Which of the following best describes the differences between object-oriented databases and relational databases?

A. Relational databases are more dynamic than object-oriented databases, and the objects contain the procedures within them.

B. Object-oriented databases are more dynamic than relational databases, and the objects contain the procedures within them.

C. Object-oriented databases are more dynamic than relational databases, and the relational tables contain the procedures that interact with the objects.

D. Relational databases are more dynamic than object-oriented databases, and the objects extract the procedures from the applications.

257. Before George rolls out the new antivirus software product to all 30,000 systems, he needs to test its configurations and reactions to identified viruses. What type of test will George carry

out?

A. RAD

B. Release a live virus on the subnet

C. EICAR

D. Flooding attack on the product

258. Jim is a construction manager who has asked his drafters and foreman to provide him with their individual project summaries. His first summary report is a Microsoft Word document that has a Microsoft Excel spreadsheet within it that outlines all the requirements, timelines, and expenses. When Jim double-clicks the spreadsheet, it launches his Excel program. Which technology made this possible?

A. OLE

B. Back door

C. Covert channels

D. EJB

259. A computer being used in an attack, such as a distributed denial-of-service, without the owner’s knowledge is called what?

A. Zombie

B. Logic bomb

C. Trojan horse

D. Worm

260. What protection should be put into place in case a software development company goes out of business?

A. Message digests

B. Logical and physical controls

C. Software escrow

D. Separation of duties

261. Which of the following is a back door to an application or system created by the developer?

A. Loop hole

B. Trapdoor

C. Easter egg

D. Trojan horse

262. In application development, good separation-of-duties practice states that the developer should not do what?

A. Change production code

B. Request management approval of a code change before developing the change

C. Perform unit tests

D. Pass the code to quality assurance and then to the librarian prior to its entry into production

263. Katie is developing a proprietary system that works with several complicated systems, networks, and protocols. Her company dictates that all software developers follow a software programming model that uses discrete phases and reviews before the next phase of development is carried out. What type of model is this?

A. CASE

B. Cleanroom

C. Waterfall

D. JAD

264. John is leading the new software development project for a reservations system for a car rental agency. He has been given strict instructions by his CIO that the exact requirements set by the customer must be met. His CIO has strongly recommended that a “cleanroom” approach be used for this project. What is a cleanroom?

A. An approach built on formal development and testing procedures

B. An approach that runs at maximum efficiency by incorporating job rotation among team members

C. A classic approach that ensures each phase of development flows from one to the next

D. An approach that guarantees quick analysis by providing a “proof of concept”

265. A system has its own developmental life cycle, which is collectively referred to as a system development life cycle (SDLC). It is made up of the following phases: _____, _____, _____, _____and _____.

A. Initiation, development, implementation, operation, disposal

B. Initiation, maintenance, implementation, operation, disposal

C. Initiation, development, acquisition, operation, disposal

D. Initiation, development, implementation, operation, maintenance

266. Henry is the team leader of a group of software designers. They are at a stage in their software development project where they need to reduce the amount of code running, reduce entry points available to untrusted users, reduce privilege levels as much as possible, and eliminate unnecessary services. Which of the following best describes the first step they need to carry out to accomplish these tasks?

A. Attack surface analysis

B. Software development life cycle

C. Risk assessment

D. Unit testing

267. It is very difficult for programmers to understand all the attack types that could negatively affect the product they are building. They need to follow a systematic approach that will allow them to understand how different compromises could be successful. Which of the following best describes this exercise?

A. Attack surface analysis

B. Threat modeling

C. Penetration testing

D. Double-blind penetration testing

268. Polly is a new manager for a team of programmers at a retail company. She has found that many of the teams carry out tasks in a very manual manner. In a meeting she has explained to her team that they need program editors, debuggers, code analyzers, version-control mechanisms, and other similar tools. What are these types of tools collectively referred to as?

A. Threat modeling tools

B. Protocol analyzers

C. Computer-aided software engineering

D. Fuzzers

269. Paul is the manager of a team of software developers. He has instructed them to run automated tools on their software code before it is compiled so that they can identify errors.

Which of the following type of testing is Paul instructing his team to follow?

A. Unit testing

B. Static analysis

C. Dynamic analysis

D. Integrated production testing

270. A software development company released a product that committed several errors once deployed in their customers' environments that was not expected. All of the software code went through a long list of tests before being released. The team manager found out that after a small change was made to the code, it was not tested before it was released. Which of the following test was most likely not conducted?

A. Unit

B. Compiled

C. Integration

D. Regression

271. Robby is new to the software programming team. He has been asked to carry out tests on newly developed code after it has been compiled and while it is running. Which of the following best describes this type of test?

A. Dynamic analysis

B. Static analysis

C. Compiled fuzzing

D. Cross-site injection

272. During the process of testing a newly developed software product, an analyst sends random data to the software so that failures can be identified. Which of the following best describes this technique?

A. Cross-site injection

B. Fuzzing

C. Validation triggering

D. Parameter injection

273. Which of the following is a standard within the ISO/IEC 27000 series that addresses application security management processes and application security validation?

A. ISO/IEC 27022

B. ISO/IEC 27005

C. ISO/IEC 27001

D. ISO/IEC 27034

274. Which of the following software development models uses a linear-sequential life-cycle approach, where each phase must be completed in its entirety before the next phase can begin? At the end of each phase a review takes place to make sure the project is on the correct path and if the project should continue.

A. Waterfall

B. Rapid prototyping

C. Incremental

D. Spiral

275. In this software development model a version of the software is created in the first iteration and then it passes through each phase of the next iteration process. The software continues

through the iteration of phases until a satisfactory product is produced. Which of the following best describes this model?

A. Waterfall

B. Rapid prototyping

C. Incremental

D. Spiral

276. The software development model _____ uses an iterative approach to software development and places emphasis on risk analysis. The model is made up of four main phases: planning, risk analysis, development and test, and evaluation.

A. V-model

B. Evolution prototyping

C. Iterative

D. Spiral

277. Jack needed to use a software development model that could allow for improvements to be interleaved with the process of developing the software. Which of the following would be the best model for Jack to follow?

A. Rapid application development

B. Prototyping

C. V-model

D. SDLC

278. Trent is the manager of a software development team at a new company. The team has been desperately trying to get their first product completed and released to the market, but the various software development models they have followed have not allowed changes to be integrated smoothly into the process. New requirements for the product would be identified and then the team had to start from the beginning of the software development project. Which of the following models would be useful in this situation?

A. Agile model

B. Waterfall model

C. Cleanroom model

D. Incremental

279. Sally has found out that software programmers in her company will make changes to software components and upload them to the main software repository without following version control or documenting their changes. This has caused a lot of confusion and has caused several teams to use the older versions. Which of the following would be the best solution for this situation?

A. Software change control management

B. Software escrow

C. Software configuration management

D. Software configuration management escrow

280. _____ allows for direct control of very basic activities within a computer system, as in pushing data on a memory stack and popping data off a stack. Attackers commonly use this language to tightly control how malicious instructions are carried out on victim systems.

A. Machine language

B. Assembly language

C. Complied language

D. C++

281. Which of the following is a web-based distributed computing technology that provides standardized access to services that are provided in distinct units?

A. Service-oriented architecture

B. Grid computing

C. Cloud computing services

D. Mashups

282. _____ provides a machine-readable description of the specific operations provided by a specific web service. _____ provides a method for web services to be registered by service providers and located by service consumers.

A. Web Services Description Language; Universal Description, Discovery, and Integration

B. Universal Description, Discovery, and Integration; Web Services Description Language

C. Web Services Description Language; Simple Object Access Protocol

D. Simple Object Access Protocol; Universal Description, Discovery, and Integration

283. John has been told by his manager that the company's website should combine Google Maps, LinkedIn, and YouTube functionality into its current portal. Which of the following provides this type of functionality?

A. SOAP

B. Cloud computing

C. Mashup

D. Grid

284. Which of the following is a software delivery model that allows applications and data to be centrally hosted and accessed by web browsers?

A. Software as a Service

B. Portal

C. Web 2.0

D. Grid computing

285. Sally has found out that an attacker has figured out how to bypass configured authentication settings and gain access to back-end database records. Which of the following best describes this type of attack?

A. Man-in-the-middle

B. Client-side injection

C. Network transversal

D. SQL injection

286. Patty has found out that her company's website allows attackers to inject malicious code, which can execute on visitors' web browsers and carry out malicious activities. Which of the following best describes this type of attack?

A. Cross-site scripting

B. Server-side execution

C. Invalid parameter validation

D. Buffer overflow

287. The use of a librarian to manage company resources such as laptops, CD-ROMs, files, etc., is what type of control?

A. Physical control

B. Access control

C. Media control

D. Employee control

288. Which one of the following is not a correct way for an operating system to respond to a failure?

A. System reboot

B. Emergency system restart

C. System cold start

D. Not starting

289. There are several ways of truly erasing data from different types of media. Which is not a method of media sanitation?

A. Deleting a file from a hard drive

B. Degaussing

C. Overwriting

D. Physical destruction

290. Which is not true regarding “authorization creep”?

A. It typically occurs when employees transfer to new departments or change positions.

B. It is a violation of least privilege.

C. It enforces the need-to-know concept.

D. It is the tendency of users to request additional privileges but seldom ask for them to be taken away.

291. A senior member of the IT programming staff who has been loyal and is extremely valuable is suspected of fraud by a vice president. But the executive has no proof and does not want to make unfounded allegations. What operations control would be best to determine if the programmer is committing fraud?

A. Separation of duties

B. Mandatory vacation

C. Least privilege

D. Need-to-know

292. Reviewing audit logs is an example of what type of security control?

A. Deterrent

B. Detective—Physical

C. Detective—Technical

D. Preventive—Technical

293. Operations departments should back up data in all of the following situations except which?

A. Once per year

B. Immediately following a reorganization

C. After a system upgrade

D. For authorized on-demand requests

294. An operations control that identifies potentially fraudulent activity by requiring different personnel to switch job functions on a regular basis is called _____.

A. Mandatory vacation

B. Need-to-know

C. Separation of duties

D. Job rotation

295. Generating magnetic fields to erase the content on a type of media is called what?

A. Sniffing

B. Degaussing

C. Wiretapping

D. Magnetizing

296. Which of the following is not considered a countermeasure to port scanning and operating system fingerprinting?

A. Allow access at the perimeter network to all internal ports

B. Remove as many banners as possible within operating systems and applications

C. Use TCP wrappers on vulnerable services that have to be available

D. Disable unnecessary ports and services

297. Enabling Tier I network technicians with read-only access to border routers is an example of _____.

A. Biba model concept

B. Separation of duties

C. Least privilege

D. Due care

298. A tool used to detect penetration of a computer system and to identify misuse is called _____.

A. Audit trail

B. Documentation

C. Security policy

D. Security model

299. Computer product evaluation criteria that look at clipping-level configurations, unit testing, and configuration management are categorized as what?

A. Operational assurance

B. Life-cycle assurance

C. Contingency criteria

D. Accreditation

300. Which of the following change management steps are in the correct order?

A. Request, approve, document, test, implement, report

B. Test, request, approve, implement, document, report

C. Request, approve, test, implement, report, document

D. Request, approve, test, document, report, implement

301. A system that automatically restarts due to an uncontrolled or unusual failure is performing what?

A. System reboot

B. Cold reboot

C. Cold restart

D. Emergency system restart

302. Which of the following works as a transfer agent?

A. SET

B. IP

C. SMTP

D. ASCII

303. Similar activities are carried out by hackers and security professionals performing an assessment. Identifying openings in a victim’s network is called _____.

A. Port scanning

B. TCP wrapping

C. Fingerprinting

D. Man-in-the-middle

304. Which of the following controls is used to amend a situation after an attack has occurred or a vulnerability has been identified?

A. Deterrent

B. Corrective

C. Preventive

D. Recovery

305. Which of the following best describes S-RPC?

A. A remote procedure call algorithm that uses asymmetric and symmetric algorithms

B. A remote procedure call protocol that uses asymmetric and symmetric algorithms

C. A remote procedure call protocol that uses asymmetric algorithms only

D. A remote procedure call protocol used for data integrity

306. Which of the following best describes the main focus of operational security?

A. It outlines and defines the access users have to company resources.

B. It performs assessments to determine who should have access to software and to what degree.

C. It maintains controls for access to hardware and media to ensure production stays operational and secure.

D. It identifies, implements, and maintains policies to ensure that production stays operational.

307. Dave is an operations technician who troubleshoots customer network problems. He has access to all of the company’s core switching and routing equipment and is able to remotely manage many of his customers’ endpoint equipment. One week out of every month, however, Dave works in his cubicle going over trouble tickets from other technicians, while Michael replaces him on the operations floor. What operations control is being implemented here?

A. Job rotation

B. Mandatory vacations

C. Need to know

D. Least privilege

308. Administrators do not want anyone to be able to arbitrarily connect to ports on critical systems and use the corresponding services. To ensure that these requests are safe and authenticated, what type of tool can be used?

A. Superzapper

B. TCP wrapper

C. Sniffer

D. Protocol analyzer

309. Human resources procedures requiring all new employees to pass background checks and

drug screens are what types of controls?

A. Preventive—administrative

B. Deterrent—technical

C. Preventive—technical

D. Corrective—administrative

310. A device used to ensure facsimile security so that transmissions are not sent in cleartext is called a _____.

A. Firewall

B. Fax encryptor

C. Security policy

D. TCB

311. How should storage media that is no longer needed but contains/contained sensitive information be handled?

A. Sold to customers with a licensing agreement

B. Formatted and then discarded

C. Overwritten securely or physically destroyed

D. Data should be deleted and media thrown away

312. Which of the following best describes why configuration management is put into place within most environments?

A. To properly control, test, and implement changes to software, firmware, hardware, and documentation to protect against improper and potentially dangerous modifications

B. To properly control, test, and implement changes to software, hardware, and documentation to protect against improper and potentially dangerous modifications

C. To properly control, test, and implement changes to software, firmware, hardware, and documentation to protect against proper modifications

D. To properly control, test, and implement changes to software, firmware, hardware, and documentation to protect against proper and potentially beneficial modifications

313. Which of the following includes ensuring that baseline versions of all software products are saved and protected as an assurance that if something bad happens, the system could be properly rebuilt?

A. Change control process

B. Custodian responsibilities within the operations department

C. Resource protection

D. Trusted recovery and degaussing

314. On his last day of work, Cory deletes all of his personal files from his hard drive by selecting each file and pressing the DELETE key. The next day, one of his former coworkers moves into his office and turns on his newly acquired computer. Inside the Recycle Bin are 15 personal files that Cory intended to delete. What are these files called?

A. Metadata

B. Audit trails

C. Data remanence

D. Sanitized data

315. Trusted recovery is an important concept when understanding how computers protect themselves. Systems use several methods when they come upon situations they cannot deal with.

Which of the following best describes a cold start?

A. The computer restarts when normal recovery procedures cannot execute due to TCB or media failures.

B. The computer restarts as a result of being shut down in a controlled manner.

C. The computer is restarted by user intervention due to the computer being unable to execute normal recovery procedures.

D. The computer restarts again and again due to a harmful boot sector virus.

316. Different controls and technologies can be implemented by the operations department. One technology that many organizations use is called RAID, a data storage system that can provide redundancy and efficiency. It functions by writing data across several aggregate drives. What is this called?

A. Parity

B. Striping

C. Degaussing

D. Data mining

317. Max has just finished developing a new software feature that the network provisioners have been requesting for some time. Anxious to get this to the group, Max installs the patch on a production system. The next day, he is summoned to his boss's office, who is very angry. His boss says, "You didn't submit a request, get approval, document anything, or do proper testing." What procedure is Max's boss referring to?

A. Sanitization

B. Due care

C. Change control

D. Operational assurance

318. Which of the following acts test the effectiveness of security mechanisms placed within a network by performing strikes against different access points?

A. Penetration testing

B. Network mapping

C. Session hijacking

D. Port scanning

319. Tim is an entry-level customer service representative working with a client on a service escalation. After working through several issues, the customer asks Tim if he can verify the annual service charge and opt-out provisions of his contract. Tim unhappily responds that he only has access to technical and operations data and cannot access contract information. He says he must transfer the customer to customer service. What type of control is described in this example?

A. Clipping level

B. Least privilege

C. Security operations

D. ACL

320. One role or committee should be responsible for enforcing and maintaining the change control process within a company. Which of the following functions is not the responsibility of this group?

A. To properly modify the change control process, depending upon the logic of the change that

was requested

B. To provide formal approval or rejection of the change to the requester

C. To enforce strict, consistent, company-wide procedures

D. To provide clear instructions to all employees on how to initiate a change request

321. Robert is one of 100 order-entry clerks handling customer requests. He enters thousands of orders each day and must abide by strict policies and procedures when doing so. On Tuesday, Robert has a particularly bad day and acknowledges to himself that he probably made several mistakes. On Wednesday afternoon, he is called into his boss’ s office where he learns that he made ten critical errors. An automated system most likely used which of the following to detect these errors?

A. Administrative controls

B. Clipping levels

C. IDS

D. Fingerprinting

322. The three main types of operational controls are technical, administrative, and physical. There are several mechanisms for each of these types that provide different services. What service does passwords, ACLs, and ID badges all provide?

A. Deterrent

B. Correction

C. Prevention

D. Compensation

323. Operations security seeks to protect a company primarily against _____.

A. Object reuse

B. Asset threats

C. Compromising emanations

D. Facility disaster

第七章答案

1、 B .A thorough and accurate chain of custody record is critical in an investigation process. The process includes labeling physical evidence and compiling a complete history of how evidence was collected, analyzed, transported, and preserved.

2、 B .Because computer files and systems can be modified after the fact without others being aware, they are considered hearsay evidence. Hearsay evidence is not considered reliable or trustworthy because it is not firsthand evidence.

3、 D .The first step in a forensic investigation is to make a copy of the hard drive. This method ensures that the original system is not altered in any way during the investigation process. Following this procedure ensures an accurate chain of custody.

4、 A .The first step in disaster recovery and contingency planning is implementing a business

impact analysis (BIA). The step involves identifying all possible threats and measuring the effect each can have on the company. This also includes identifying critical company functions and resources and calculating outage times.

5、 B .Warm sites offer an even mix of advantages and disadvantages. These backup locations have power and network turned up, but have only a portion of the hardware and software installed. An advantage of a warm site is that it is less expensive than a hot site. A disadvantage is that testing capabilities are not available as they are with hot sites.

A redundant site is not subscription-based, but owned by the company.

6、 D .Senior executives have several key responsibilities in disaster recovery. These include: support and approval of plans, sponsoring all aspects of plans, verifying testing phases are being carried out, and overseeing budgets.

Having the dedicated and consistent support of senior management is critical in the success of disaster recovery and contingency planning.

7、 B .The CISSP exam has recently combined disaster recovery and business continuity under one topic, which is called business continuity.

Previously the test defined disaster recovery as the planning and analysis of what to do if a disaster occurs and business continuity as steps to keep the business running afterward.

The business continuity plan covers all of the answers, but should not restrict business productivity.

Establishing emergency response procedures is part of disaster recovery planning.

8、 A .Although a hot site would be a good option, a redundant site is the best choice in this scenario. Redundant sites are configured exactly like the original site. The site has power, network wiring established, and all hardware and software is configured.

A redundant site is the most expensive option out of all the answers, including hot sites. It is a mirrored environment of the production environment.

9、 C .Even though the thought of losing systems, hardware, software, and ultimately profits seems devastating to a company, these things pale in comparison to the thought of losing human life. The protection of people at a facility will always be the most important goal in disaster recovery planning.

10、 B .Maximum tolerable downtime (MTD) is a measurement to indicate how long the company can be without a specific resource.

General MTD estimates are:

Critical = minutes to hours
Urgent = 24 hours
Important = 72 hours
Normal = 7 days
Nonessential = 30 days

11、 D .Catastrophes have the most significant physical impact on businesses. They can come in the form of earthquakes, tornados, fires, or floods.

The distinguishing difference between catastrophes and disasters is that catastrophes destroy a facility altogether. To resume operations, short- and long-term solutions must be developed. Disasters typically involve the facility only being partially destroyed and the business being impacted temporarily.

12、B .There are many reasons plans can become outdated, however, performing drills is not one of them. Testing helps to keep disaster recovery and contingency plans alive even if it identifies inaccuracies in the plan.

Personnel turnover, reorganizations, and infrastructure changes are classic examples of why these plans can become outdated.

13、 C .According to many studies, 65 percent of businesses would fail if they were forced to shut down operations for a one-week time period. This fact alone enforces the need for disaster recovery and contingency planning. The loss of revenue combined with a loss of reputation in the community can be devastating to companies when a disaster hits.

14、 C .Reciprocal agreements can be effective in certain situations, but generally have too many problems to be the primary backup plan for a company. Even though they offer a cheap alternative to a company, they are not enforceable.

Reciprocal agreements can be a safe second option in case your warm or hot site is not functioning properly or available.

15、 D .Much of the work that goes into BIA involves gathering and analyzing data to see how it will affect the company. Interviewing employees is an important part of the data gathering process. Also, it is critical to have management's support when developing a disaster recovery and contingency plan.

Once the plans are developed, then the entire company should be made aware of them.

16、 C .Electronic vaulting is an automated way of sending files that have been modified to a remote location. Although manually backing up each file and physically taking it to the remote

location would work, it is far more time consuming and more likely to have errors than electronic vaulting.

Disk shadowing and disk duplexing are methods of backing up systems and files onsite, but would not help in this example.

17、 B .The business continuity plan should have clear instructions on who is in charge during a disaster. This person could be an executive, a public relations representative, or a task force representative. It is up to this person to decide how to communicate and inform the appropriate parties.

18、 B .A disaster is defined as an event that affects a business for one day or longer. This example, although damaging, is not significant enough to be called a disaster.

Catastrophes are events that require long term solutions and affect a business for weeks, months, or years.

19、 B .The committee members have many responsibilities, however budget management should remain with executive management. This is another way of keeping the leadership group involved in the process. Watching dollars spent is usually incentive enough to keep an executive in the game.

20、 B .Structured walk-through tests bring together all appropriate representatives to go over the plan in detail. This is a chance to identify items that have been missed. It takes place after a checklist test, where each department verifies its tasks.

Parallel tests, simulation tests, and full-interruption tests typically come after the structured walk-through test to ensure all the details are correct.

21、 A .Hierarchical storage management (HSM) combines hard disk technology with the cheaper and slower optical or tape jukeboxes. Storage area network (SAN) is made up of several storage systems that are connected together to form a single backup network.

22、 D .Although senior executives will most likely keep an eye on all phases of BCP, the financial committee member should carry out these types of tasks following a disaster. Departmental leads and human resources may play small roles in this process, but it will be up to the financial representative to delegate tasks and manage the process.

23、 D .All of these choices would be helpful in the event of a disaster. CCTV could help identify the intruder and pinpoint the areas that were harmed inside the facility. Data backup is crucial at keeping the business running. Also, a calling tree is used to know who to contact and at what locations.

24、 C .Business continuity planning encompasses the other three answers. It involves both how

to react during a disaster to protect people and systems and how to keep the business functioning following the incident.

25、 A .It is important to form a team that is a true representation of the entire company before doing anything else. Once the group is created, then roles can be assigned, data can be gathered, threats can be identified, and documentation can be written.

26、 C .Immediately following a disaster, the BCP committee chair should dictate the next course of action for all employees. Clear instructions should be given to everyone.

The BCP chair will delegate tasks and will make decisions like notifying customers, families, and the media if necessary.

27、 C .A redundant site is the best choice in this scenario because the site is already configured with duplicate systems, software, workstations, etc. There would be minimal downtime because this environment is hot in nature, meaning it can be up and running very quickly.

Although a rolling hot site could be quickly turned up, its mobile nature doesn't work well in long-term solutions. Cold sites have significant downtime, and reciprocal agreements cannot guarantee availability.

28、 B .Disaster can come in many forms: human, natural , or technological. A manmade disaster could come in the form of planting a virus, revealing trade secrets, or committing arson. Sabotage is a classic example of a manmade disaster.

29、 B .Senior management is ultimately responsible for all activities within an organization. They are responsible for acting upon the outcome of the business impact analysis and allotting funds to be spent to ensure that the company stays in business after a disruption or disaster.

30、 C .Media controls help protect company resources and keep them from unauthorized individuals. Librarians are keepers of resources such as data files, programs, laptops, and backups.

31、 D .Computers have defense mechanisms in order to protect the operating system from potential danger. When the system senses a problem, it can react in one of three ways:

- System reboot
- Emergency system restart
- System cold start

32、 A .Permanently erasing the contents from a medium is called sanitization. There are several ways to accomplish this:

1. Degaussing — Erasing data magnetically.

2. Overwriting — Replacing old content with new content. This is also called zeroization when the new content contains null values.
3. Physical destruction — If the medium cannot be properly sanitized, it must be destroyed.

33、 C .A prudent person is responsible, careful, cautious, and practical. Companies are required to execute due care in order to protect the security of the business and the employees.

34、 C .Authorization creep is the process of an individual retaining privileges that are not necessary to performing his job function. This is commonly caused by promotions or transfers.

Authorization creep violates both the least privilege and need to know concepts.

35、 B .Enforcing the mandatory vacation control is the best option for the vice president. This will allow another person to perform the job function and identify potential fraud while the original programmer is on vacation. The good thing about mandatory vacations is that it can be spun in a positive light by the executive. Telling an employee to take a vacation can usually be interpreted in a positive way. Instituting a job rotation on the other hand may clue in the programmer to the executive's suspicion.

36、 C .Detective controls help identify breakdowns in access controls. For example, a security professional who reviews a long distance telephone billing sheet in an operations center can uncover potential fraud by operations employees.

37、 B .Corrective controls are used to fix a problem. For example, when it is determined that an unauthorized user gained access to a network segment, a corrective control would address the access control vulnerability that allowed the user access.

38、 A .Clipping levels are thresholds set by management of acceptable numbers of mistakes or errors made by employees. The reason clipping levels are set is to notify security or management when innocent mistakes become routine enough to suspect fraudulent behavior.

39、 A .Backing up data is critical within operations organizations. The most important step to take is to create a backup plan. This will detail when and what to backup, as well as where to store the files.

Even though each entity will require different phases of backups, it is not realistic to provide proper data security when only backing up data once per year.

40、 D .Job rotation is the correct answer. It involves training more than one person for a specific job. This accomplishes more than simply identifying potential fraud. It also creates redundancy in the event that one employee leaves the company.

Separation of duties is closely related to job rotation but is slightly different. The separation of duties ensures that one person is not solely working on critical projects or critical functions. This

would be a major security vulnerability.

41、 B .Degaussing is an effective way of destroying content on a floppy disk or hard drive. The process creates strong magnetic fields that return the flux of the electrons back to their original state.

Degaussing will also eliminate all of the information that outlines the tracks and sectors of the media, so it may need to be returned to the vendor for this data to be reapplied.

42、 A .Several countermeasures should be put in place to reduce this threat.

- Disable unnecessary ports and services.
- Block access at the perimeter network using firewalls, routers, and proxy servers.
- Use an IDS to identify this type of activity.
- Use TCP Wrappers on vulnerable services that have to be available.
- Remove as many banners as possible within operating systems and applications.
- Upgrade or update to more secure operating systems, applications, and protocols.

43、 C .Least privilege ensures that individuals have permissions to only what is required for their job and no more. In this question, Tier 1 technicians would only need read access to network devices. Having the ability to make changes to a border router would violate the least-privilege policy.

44、 A .Audit trails are effective tools and are considered detective-technical controls. They can be used to display all commands that have been entered into a system, authentication attempts into a network, or systems and files that have been accessed or modified.

45、 B .One phase of product evaluation that is intimate to operations groups is life cycle assurance. It deals with the system's architecture and associated maintenance procedures.

Operational assurance, on the other hand, deals with the system's architecture and associated features and functionality. It looks at only certain portions of the life cycle of a product, while life cycle looks at all phases.

46、 A .Although each company will implement its own change management policy, the general procedures will remain the same. The correct order follows:

1. Request a change
2. Approve a change
3. Document a change
4. Test a change
5. Implement a change
6. Report a change to management

47、 D .A computer that senses abnormal procedures or uncontrolled activities may enact an emergency system restart. This is done to protect the operating system from bad programming code, viruses, or any other failure that could disrupt the system.

48、 C .SMTP acts as a transferring agent from a user's computer to an e-mail server and from server to server.

SMTP uses TCP as its transport protocol.

49、 A .Port scanning is used by attackers to identify open ports in a victim's network. Obtaining this kind of information can be useful in determining what kind of services are running and how to attack their vulnerabilities.

50、 C .Superzapping tools enable a user to override access controls when trying to connect to a system.

The activities that are carried out by the superzapper are not auditable.

51、 B .Session hijacking involves a third party inserting herself between two connected computers without being noticed. Juggernaut and Hunt are two programs used to accomplish this. The tools allow the attacker to then take over the session.

52、 C .Penetration testing is an important procedure that attempts to beat the set security controls of a system. This is a good reality check to see if the system is safe from attacks.

Penetration testing should be done on a regular basis.

53、 A .Preventive controls are used to discourage unethical activity or potential damages from occurring. There are three types of preventive controls:

Administrative — HR policies, separation of duties, employee management, security policies

Technical — Password, biometrics, firewalls

Physical — Fences, security guards, surveillance systems

54、 B .Fax encryptors are used when high levels of security are required for fax transmissions. Just like data encryption, fax files are encrypted into ciphertext so that if intercepted, they will be unreadable.

55、 C .Qualitative Risk Analysis does not focus on real number calculations, but instead assigns rankings to threats and countermeasures and focuses on judgment, intuition, and experience.

Single loss expectancy (SLE) is a method used in Quantitative Risk Analysis.

56、 B .A common mistake that many companies make is failing to include penalties in the security program that will be enforced if\when individuals do not comply with outlined directives. As with any rule or law, it is unlikely that the instruction will be followed without known consequences.

Security awareness is included in most security policies, however follow through with the awareness objective is not as common.

57、 B .Secure Remote Procedure Call (S-RPC) uses the Diffie-Hellman asymmetric algorithm to determine the shared secret key for encryption with the DES algorithm. If S-RPC is used in an environment, a sniffer can capture this data, but not necessarily decrypt it.

58、 D .The goal of business continuity planning is not to prevent security breaches, but to keep a company in business after a disruption or disaster.

Administrative controls can be preventive, as in employee management (hiring and firing practices) and developing policies and standards.

Encryption is a preventive control used to protect the confidentiality of data. User authentication is a preventive control used to prevent unauthorized users from accessing systems and making modifications.

59、 C .Operations' goal is to keep production in proper working order and, in most environments, they have a focus of protecting the company's hardware and media from unauthorized access. They are usually the maintainers or custodians of the environment and not the group that is responsible for developing and implementing policies. They should not have the power to make decisions on what users can access, including software. These access decisions are passed down to them and operations just ensures that the controls enforcing these decisions are in proper working order.

60、 C .If some type of storage media is going to be retired and it contains sensitive information, that data needs to be properly erased before the media is discarded. Formatting media just clears out the file allocation table and does not securely delete the files. Deleting data on media just deletes the pointers to the files, not the files themselves. So the media needs to be properly erased through some type of zerorization process, degaussing, or physically destroyed.

61、 A .Configuration management is the process of identifying, controlling, accounting for and auditing changes made to the baseline TCB, which includes changes to hardware, software and firmware. It is a system that will control changes to test and maintenance documentation through the operational life cycle of a system. Its major objective is system and environment stability.

62、 B .All of these items need to go into the BIA, but when calculating the amount of downtime a company can endure, the team must determine how critical the different resources are to the

company. The more critical resources need to come online first and should have the smaller amount of downtime compared to other resources.

63、 B .The operations department has the responsibility of making sure changes to production systems are done in an approved and controlled manner. They are also responsible for ensuring that the systems and environment are in stable working condition. This includes making sure that systems can be rebuilt if necessary.

64、 A .Copies of the plans should be kept in more locations than just the primary site. This is important because if the primary site is destroyed or negatively affected, the continuity plan is still available to the teams.

65、 C .After the project kicks off, the first step for the team is performing a business impact analysis (BIA). The results from the BIA are given to management and they determine what should happen next.

If management gives the green light and provides the necessary resources, then the team can create their strategy before they actually develop the plan. The plan captures what has been laid out in the strategy phase. Then the plan is implemented, tested, and maintained.

66、 B .One of the biggest weaknesses in the use of cold site facilities is that they are not configured with any equipment, so testing is impossible. This type of backup option only provides the company with a bare-boned facility in which to transfer over equipment if a disaster were to hit.

It usually takes weeks for a cold site to be up and running, thus it is extremely hard to test.

67、 C .Remote journaling is an automatic function that sends transaction logs of the backed up files to an offsite location. This does not take as many resources as electronic vaulting, which moves the entire file after it is modified.

68、 C .In tape vaulting, the data is sent over a serial line to a backup tape system at the offsite facility. The company that is maintaining the offsite facility will maintain the systems and change out tapes when necessary. Data can be quickly backed up and retrieved when necessary. This technology reduces the manual steps in the traditional tape back up procedures.

69、 B .Checklist tests are good ways to get a wide range of feedback on procedures and ensure accuracy without disrupting business operations. In a checklist test, all departments are given a copy of the continuity plan. Each department must review and confirm that the information is correct.

70、 C .Reciprocal agreements are made between companies with the understanding that available facilities can be used by a company in the event of a disaster. These agreements come with a handful of problems, however. One problem is that they are not legally binding. Also, there

are confidentiality issues. Most companies would not want to migrate their business operations into the house of another company, possibly revealing proprietary information.

71、 B .While employee turnover can contribute to plans becoming outdated, this is not an issue the IT director is responsible for. Starting an employee retention program to improve turnover rates would be an HR/management issue. It would be a good idea to recommend a program like this, but developing it independently would be inappropriate.

The other answers are procedures that should be implemented that directly affect the efficiency and effectiveness of the plan.

72、 B .Doug is not responsible for all the technical details of testing, bug fixing, and code writing that goes along with specific software and devices. The BCP committee is not so technically focused. Instead, it takes a broader view of how to keep the company going and relies on the different departments to test and understand their equipment. The committee does need to know how quickly the equipment can come online at the offsite facility.

73、 A .Disk-shadowing systems are built for redundancy. The system has two disks, both of which are written to simultaneously. One disk is referred to as the primary, while the other is the secondary or backup.

Disk duplexing has two controllers, not disk shadowing.

74、 C .Implementing and assessing countermeasures should be the responsibility of the appointed security professional. Results would be presented to Mr. Frazier and he can offer feedback.

The other choices are all necessary tasks of a senior management member.

75、 B .A hierarchical storage management (HSM) system is an automated data storage system. It provides continuous online backup functionality.

76、 C .Storage area network (SAN) is made up of several storage systems that are connected together to form a single backup network. A SAN is a networked infrastructure that allows several systems to be connected to any storage device. This is usually provided by using switches to create a switching fabric.

The switching fabric allows for several devices to communicate with back-end storage devices and provides redundancy and fault tolerance by not depending upon one specific line or connection. Private channels or storage controllers are implemented so hosts can access the different storage devices transparently.

77、 C .After a disaster, telephone service may not be available. For communication purposes there should be alternatives in place, such as cell phones or ham radios.

Cell phones work on a different telephone system and network and may not have been affected during the disaster.

78、 B .Redundant sites provide the most advantages to a company that needs to ensure no, or a small amount of, downtime. These also offer the quickest recovery time in the event of a disaster. A redundant site could realistically be up and running within minutes of an event. Redundant and hot sites both provide good testing capabilities and ensure availability.

79、 C .The BIA identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events. The outage time that can be endured by a company is referred to as the maximum tolerable downtime (MTD).

Here are some MTD estimates that may be used within an organization:

- Nonessential = 30 days
- Normal = 7 days
- Important = 72 hours
- Urgent = 24 hours
- Critical = Minutes to hours

Each critical business function and asset should be placed in one of the previous categories, depending upon how long the company can survive without it.

80、 A .Parallel tests are similar to simulation tests, except that parallel tests include moving some of the systems to the offsite facility. Simulation tests stop just short of the move. Parallel tests are effective because they ensure that specific systems work at the new location, but the test itself does not interfere with business operations at the main facility.

81、 B .Rita is an example of an employee who will play an active role in helping the company deal with disasters. It is management's responsibility that these types of roles are defined and filled with competent people.

82、 C .All of these answers would be legitimate reasons for conducting testing on the business continuity plans. However, the number one objective is to make sure that the plans work. A company can have everyone involved, superior company awareness, a management closely following each step, but if the plan is wrong and not useful, then it is all for naught.

83、 B .The only missing resources from a hot site are the data and people. The data will be retrieved from a backup site and restored.

84、 C .If a large disaster took place that affected not only the company's facility but surrounding areas and housing areas, do you think your employees will be more worried about your company

or their families? Some companies assume that employees will be ready and available to help them get back into production, when in fact they may need to be at home because they have family responsibilities.

85、 D .The backup site should be at least 25 miles away from the primary site to give the company maximum protection in cases of regional disasters.

86、 B .An incremental backup is a procedure that backs up only those files that have been modified since the pervious backup of any sort. It does remove the archive attribute.

A differential backup is a procedure that backs up all files that have been modified since the last full backup. It does not remove the archive attribute.

A full backup is a procedure that backs up all files, modified or not, and removes the archive attribute.

Incremental backups finish more quickly than differential backups, but they take longer to restore because each incremental backup has to be restored since the last full backup.

87、 A .The correct answer is job rotation. Michael routinely replaces Dave on the operations floor. This is a security control because if Dave were to always handle his customer accounts alone, he may have a greater potential to commit fraud.

88、 C .Data remanence is remaining data. In this example, Cory was not well-educated on data sanitization techniques. Simply deleting a file from a hard drive does not remove the data from the medium. The new user can perform a routine "restore" command to view the files.

89、 A .Network mapping tools perform fingerprinting functions within networks. The responses received from ping commands and port scans can help provide useful information to the requester, such as clarifying what type of device it is connected to. The attacker can also learn what operating system software and applications are running.

90、 C .There are three primary types of recovery procedures for computers:

1. System reboot — Restarts in a controlled manner.
2. Emergency reboot — Restarts when normal procedures cannot be initiated.
3. System cold start — Operating system brings the system down to maintenance mode and operator intervention is required to complete the recovery.

91、 B .Redundant array of inexpensive disks (RAID) uses a function called striping. Striping is the process of writing data across several aggregate drives. The trick in this technique is that data retrieval is dramatically improved because many device heads are utilized.

92、 B .These wrappers monitor incoming network traffic and controls what can and cannot

access the services mapped to specific ports.

When a request comes to a computer at a specific port, the target operating system will check to see if this port is enabled. If it is enabled and the operating system sees that the corresponding service is wrapped, it knows to look at an access control list, which spells out who can access this service.

93、 C .Slamming is when a user's telephone service provider has been changed without that user's consent. Cramming is adding on bogus charges for services the user did not request or receive.

94、 C .Change control procedures are critical to maintaining proper levels of security within an operations environment. In this example, Max's software enhancement may or may not have caused problems with the operating system or connecting devices. However, ensuring that every change, regardless of size or scope, goes through formal levels of approval will help to ensure that no negative effects will occur.

95、 B .A browsing attack is a broad term for attempts by an individual to gain information he is not authorized to access. It means that someone is looking for sensitive data without knowing what format it is in. The sensitive data could be in a word document, spreadsheet, database, or in printed material.

96、 A .Penetration testing is a way of knowing how strongly the network will hold up against attacks. The test should cover many of the possible attack types administered by hackers.

97、 B .Tim has been given least-privilege access to company data. This means that he can only read what is absolutely necessary to fulfill his job requirements. While it would be nice to have access to billing records, Tim doesn't need them in order to do his normal activities.

98、 A .Change control administrators are responsible for keeping the procedure updated and alive in the eyes of the company. Their role within the procedure is to give formal approval or rejection to the requester.

The actual process should stay the same for every type of change request. The process and logic of the change are separate. The type of change should not influence the procedures of the change control process.

99、 B .Clipping levels are thresholds. In this example, it would be very difficult for Robert's boss to manually monitor all of his employees and the hundreds of thousands of transactions they process each day. But, with automation, a system notifies him if certain error thresholds are exceeded.

100、 B .Initial program load (IPL) is a mainframe term for loading the operating system's kernel into the computer's main memory. On a personal computer, booting or rebooting into the

operating system is the equivalent of IPLing. This activity takes place to prepare the computer for user operation.

The operations team would need to investigate computers that reboot for no reason, which could indicate that the operating system is experiencing major problems.

101、 B .If a company does not properly configure their mail-relaying agents, their server can be used to distribute advertisements for other companies, spam messages, and pornographic material.

It is important that mail servers have proper antispam features enabled, which are actually antirelaying features. A company's mail server should only accept mail destined for its domain and not forward messages onto other domains.

102、 B .Standards pertain to computing service levels and how they are measured. Each device can have certain standards applied to it including the hours of time to be online, the amount of requests that can be processed within a defined period of time, bandwidth usage, and performance counters. These standards provide a baseline that is used to determine if there is a problem with the device or not.

If a system cannot process the load of work it usually handles, then it is working at a different level than the standard set baseline for its functionality.

103、 C .Passwords, ACLs, and ID badges are all preventive mechanisms designed to stop unauthorized access. Passwords and ACLs are considered preventive-technical controls, while ID badges are preventive-physical controls.

104、 B .Hot sites are fully equipped with redundant systems and network configurations which are extremely expensive to maintain. Companies need to perform a business impact analysis to understand how long the business can be out of production before it becomes detrimental. If the company can only be down for a day or two, it may be necessary to pay for a hot site to be available.

105、 D .Often companies view developing continuity plans as a project, meaning the project starts and then stops. It is not seen as an ongoing activity. This mentality can cause the plan to become quickly outdated because it is not being maintained.

106、 A .Simulation tests measure the responsiveness of each department during an emergency situation. A scenario is constructed—as in a flood, earthquake, or terrorist attack— and people carry out the tasks expected of them.

107、 D .To ensure that critical business functions and systems continue to operate during a move back to the original facility, the first step should be reinstating the least critical functions.

108、B .Storage area network (SANs) are made up of several storage systems connected together to form a single backup network. A SAN is a networked infrastructure that allows several systems to be connected to any storage device. This is usually provided by using switches to create a switching fabric. The switching fabric allows for several devices to communicate with back-end storage devices and provides redundancy and fault tolerance by not depending upon one specific line or connection.

109、 C .Full-interruption tests require the original site to be completely shut down and all processes moved to an alternate site. This can be very disruptive to a company, but is really the only way to be sure the disaster recovery plan will work when it is needed.

110、 B .Informing the public and affected groups is a critical part of disaster recovery so that the company's reputation and overall business status are not damaged. The information that will be reported should be prepared beforehand, along with the individual responsible for communicating the message to the public and press.

111、 C .Selecting team members is an important part of disaster recovery, but is not a necessary step in a business impact analysis (BIA). BIA is performed to identify the critical areas of a company, the resources needed to keep those areas functioning, and the amount of outage time that can be endured, as well as to identify and calculate the risk of those threats.

112、 D .Senior management should support all functions of disaster recovery and business continuity. They should oversee the progress of developing, implementing, and testing the plans. They should also ensure that the proper resources and budget are available, but they are not usually the ones who implement the plans.

113、 B .Businesses need to treat disaster recovery planning as a committed expense, much like how insurance is a requirement. In many sectors, disaster recovery is a legal requirement. Companies should not view this as optional. It is a must for company survival.

114、 A .The question asks about offsite redundancy, thus onsite mirroring would not be an option. The other answers are different types of technologies that can be used to save data to an offsite facility.

115、 D .A structured walk-through test involves bringing representatives from different departments together to discuss the details of all possible disaster recovery scenarios. This type of test should take place before the more intrusive tests, especially a full-interruption test. It is better to uncover as many problems as necessary in a meeting environment than finding them in situations that can negatively affect production.

116、 B .Data loss needs to be addressed as a top priority. Today, data and information are considered gold to many companies, the loss of which could be devastating.

117、 A .Business units or functions that must be present to sustain continuity of business,

maintain life safety, and avoid public embarrassment need to be identified by the analysis team. These are the critical areas that must be highly protected and must come online first to continue production in a healthy manner.

118、 C .Increasing information system performance is not a benefit or goal of developing disaster recovery or continuity plans.

119、 D .The disaster recovery plan should address the other three answers. It does not outline business functions and systems, which are handled in the business impact analysis.

120、 C .Actually printing a sensitivity banner on each page could invite more people to look at the document instead of discouraging it.

121、 B .Configuration management is put into place to ensure that changes to hardware and software do not take place unintentionally and that the changes are approved and tested.

122、 B .Enforcing WEP keys is a technical control and not an administrative control. The other answers are common examples of administrative controls.

123、 D .The operations department is responsible for the first three items, but is not responsible for developing security policies. Development of policies is a management responsibility.

124、 C .Deleting a file does not make the data disappear; it only deletes the pointers to the data that still exists on the media. Object reuse is when more than one subject uses the same media. The media can be a hard drive, floppy disk, or memory segment. All sensitive information should be deleted before the next subject can use the media, which may be accomplished by zeroization (overwriting with a series of 0s) or degaussing (using a device that has a large magnet). If these do not work, the media must be physically destroyed.

125、 B .Spoofing can occur by a person pretending to be another person or pretending to have another IP address, also referred to as IP spoofing.

126、 C .An attacker can compromise a computer and install a backdoor program or hide the code within a virus or Trojan horse that will install a backdoor when a predefined event takes place. Many times these backdoors are installed so that the attacker can later control the computer remotely to perform the tasks she is interested in.

127、 A .Superzapping programs are often used by administrators to perform quick reconfigurations of the system. They are very powerful and dangerous if they get into the wrong hands because their actions are not auditable. This means that if an attacker uses a superzapper, her activities will not be shown in any log.

128、 D .A browsing attack is looking for sensitive information without knowing what format it is in.

129、 A .Security Administrator Tool for Analyzing Networks (SATAN) is a scanning tool that can uncover weaknesses within a network.

130、 A .A denial-of-service (DoS) attack carries out some type of activity that renders the victim system unable to perform its tasks. A land attack is when an attacker modifies a packet to contain the same source and destination address. A system vulnerable to this type of attack does not know what to do with these types of packets and may freeze. Making a system freeze renders it unable to perform its tasks, thus this is a DoS attack.

131、 D .Configuration management is a process to control the changes that take place while a system or application is being developed. This control happens throughout the lifetime of the system or application, so any changes to it in production also fall under configuration management. Configuration management does not ensure that changes take place, but controls the changes to make sure they are carried out properly.

132、 B .Examples of operational assurances examined in the evaluation process are access control mechanisms, the separation of privileged and user program code, auditing and monitoring capabilities, covert channel analysis, and trusted recovery when the product experiences unexpected circumstances. Life cycle assurance pertains to the product's architecture and how it was developed and maintained. Each stage of the product's life cycle has standards and expectations it must fulfill before it can be deemed a highly trusted product. Examples of life cycle assurance standards are design specifications, clipping level configurations, unit and integration testing, configuration management, and trusted distribution.

133、 A .Trusted recovery refers to the right procedures following a system failure and can be classified as either a system reboot, emergency system restart, or a cold start. Trusted recovery is carried out so that even if a system fails, it is not put into an insecure state.

134、 B .The process of degaussing is achieved by passing the magnetic media through a powerful magnetic field to rearrange the electrons, removing any semblance of the previously recorded signal. Degaussing, overwriting, and destruction constitute the sanitization of different media types. This addresses storage facilities (storage and memory), not data buses. A data bus is used in the computer to move data from one component to another. Data is not stored in a data bus.

135、 B .The main goal of operations security is to protect the company’s resources (assets). It is also concerned with hardware and software performing in predictable and acceptable ways.

136、 D .The remanence data is the magnetic induction that remains in a material after removal of the magnetizing field. This can be used to recover lost data, potentially even after deletion.

137、 B .Backup tape media should contain the date of creation, the name of the creator, how long it is good for (retention period), classification, and volume name and version. The label

should contain the name of the person who backed up the data, but not necessarily who wrote the data.

138、 B .Mechanisms must be employed that can map a user to his actions. This would allow the tracing of violations and errors to the responsible individual.

139、 B .Secure Remote Procedure Call (S-RPC) uses Diffie-Hellman public key cryptography to determine the shared secret key for encryption with the DES algorithm. If S-RPC is used in an environment, a sniffer can capture this data, but not necessarily decrypt it.

140、 B .Detection is the most important step in the incident response process. The first and most important step in responding to an incident is realizing that you have a problem in the first place.

141、 C .Prevention isn't part of incident response; it should be done to help prevent incidents.

142、 C .The International Organization for Standardization published ISO 28000:2007 as a means for organizations to use a consistent approach to securing their supply chains.

143、 B .Workstations are not normally embedded devices.

144、 A .Provisioning is the set of all activities required to provide one or more new information services to a user or group of users.

145、 B .Configuration management is the process of establishing and maintaining consistent baselines on all organizational systems. It could be considered a sub-area of change management.

146、 B .A virtual server might be provisioned for a single new user of a cloud service, for their exclusive use. A physical server might be provisioned for an entire organization, but typically not for a single user.

147、 C .Because a storage area network (SAN) provides redundancy, fault tolerance, reliability, and backups, it allow users and administrators to interact with it as one virtual entity.

148、 C .Service level agreements (SLAs) are normally included in vendor management governing processes.

149、 C .Authentication-as-a-Service is not typically a service provisioned for cloud services, but is usually kept internal to the organization, and used to access cloud services to which the organization subscribes.

150、 C .Whitelisting refers to allowing only certain applications to run, or allowing only certain DNS domains to be accessible to the network.

151、 B .Lessons learned are developed and shared with others, as appropriate, to correct incident response deficiencies and improve incident management processes.

152、 A .Redundancy, fault tolerance, and failover capabilities increase the levels of high availability for an infrastructure. The organization's recovery time objective (RTO) may rely on high-availability technologies, but it is not a characteristic of them.

153、 C .A honeypot is a device that is developed in order to deceive attackers into believing it is a real production system, entice and allow these adversaries to compromise it, and then monitor their activities on the compromised system to observe and learn their behaviors.

154、 D .In-depth training teaches individuals what to do during an emergency or disaster, or its subsequent recovery. The other options listed would not be sufficient to guarantee that individuals would know what to do and be able to perform their duties during contingencies.

155、 A .The first step in disaster recovery and contingency planning is performing a business impact analysis (BIA). This step involves identifying all possible threats and measuring the effect each can have on the company. This also includes identifying critical company functions and resources and estimating maximum allowable outage times.

156、 B .Warm sites offer an even mix of advantages and disadvantages. These backup locations have power and network turned up, but only a portion of the hardware and software installed. A positive attribute of a warm site is that they are less expensive than a hot site. A downside is that testing capabilities are not available, as they are with hot sites. A redundant site is not subscription based, but owned by the company.

157、 D .Senior executives have several key responsibilities within disaster recovery, which include supporting and approving plans, sponsoring all aspects of plans, verifying that testing phases are being carried out, and overseeing budgets. Having the dedicated and consistent support of senior management is critical in the success of disaster recovery and contingency planning.

158、 B .The CISSP exam has recently combined disaster recovery and business continuity under one topic, which is called business continuity. Previously, the test considered disaster recovery as the planning and analysis of what to do if a disaster occurs, and business continuity as steps to keep the business running after a disaster occurs. The business continuity plan covers all of the answers, but should not restrict business productivity. Establishing emergency response procedures is part of disaster recovery planning.

159、 A .Although a hot site would be a good option, a redundant site is the best choice in this scenario. Redundant sites are configured exactly like the original site. The site has power, network wiring is established, and all hardware and software are configured. A redundant site is the most expensive option out of all the answers, including hot sites. It is a mirrored environment

of the production environment.

160、 C .Even though the thought of losing systems, hardware, software, and ultimately profits seems devastating to a company, these things pale in comparison to the thought of losing human life. The protection of people at a facility will always be the most important goal in disaster recovery planning.

161、 D .Catastrophes have the most significant physical impact on businesses. They can come in the form of earthquakes, tornados, fires, and floods. The distinguishing difference between catastrophes and disasters is that catastrophes destroy a facility altogether. To resume operations, short- and long-term solutions must be developed. Disasters typically involve the facility only being partially destroyed and the business being affected temporarily.

162、 B .There are many reasons why plans can become outdated; however, performing drills is not one of them. Testing helps to keep disaster recovery and contingency plans alive, even if it identifies inaccuracies in the plan. Personnel turnover, reorganizations, and infrastructure changes are classic examples of why these plans can become outdated.

163、 D .Much of the work that goes into the BIA involves gathering and analyzing data to see how they will affect the company. Interviewing employees is an important part of the data-gathering process. It is critical to have management’s support when developing a disaster recovery and contingency plan. Once the plans are developed, the entire company should be made aware of them.

164、 C .Electronic vaulting is an automated way of sending files that have been modified to a remote location. Although manually backing up each file and physically taking it to the remote location would work, it is far more time consuming and more likely to introduce errors than electronic vaulting. Disk shadowing and disk duplexing are methods of backing up systems and files onsite, but would not help in this example.

165、 B .The business continuity plan should have clear instructions on who is in charge during a disaster. This person could be an executive, a public relations representative, or a task force representative. It is up to this person to decide how to communicate and inform the appropriate parties.

166、 B .A disaster is defined as an event that affects a business for one day or longer. This example, although damaging, is not significant enough to be called a disaster. Catastrophes are events that require long-term solutions and affect a business for weeks, months, or years.

167、 B .The committee members have many responsibilities; however, budget management should stay in the hands of executive management. This is another way of keeping the leadership group involved in the process. Watching dollars being spent is usually incentive enough to keep an executive in the game.

168、 B .Structured walk-through tests bring together all appropriate representatives to go over the plan in detail. This is a chance to identify items that have been missed. It takes place after a checklist test, where each department verifies its tasks. Parallel tests, simulation tests, and full-interruption tests typically come after the structured walk-through test to ensure that all the details are correct.

169、 D .Although senior executives will most likely keep an eye on all phases of BCP, the financial committee member should carry out these types of tasks following a disaster. Departmental leads and human resources (HR) may play small roles in this process, but it will be up to the financial representative to delegate tasks and manage the process.

170、 D .All of these choices would be helpful in the event of a disaster. CCTV could help identify the intruder and pinpoint the areas that were damaged inside the facility. Data backup is crucial for keeping the business running. And a calling tree is used to know who to contact and at what locations.

171、 A .It is important to form a team that is a true representation of the entire company before doing anything else. Once the group is created, then roles can be assigned, data can be gathered, threats can be identified, and documentation can be written.

172、 C .A redundant site is the best choice in this scenario because the site is already configured with duplicate systems, software, workstations, etc. There would be minimal downtime because this environment is hot in nature, meaning it can be up and running very quickly. Although a rolling hot site could be quickly turned up, its mobile nature doesn’t work well in long-term solutions. Cold sites have significant downtime, and reciprocal agreements cannot guarantee availability.

173、 B .Senior management is ultimately responsible for all activities within an organization. They are responsible for acting upon the outcome of the business impact analysis and allotting funds to be spent to ensure that the company stays in business after a disruption or disaster.

174、 A .Copies of the plans should be kept in more locations than just the primary site. This is important because if the primary site is destroyed or negatively affected, the continuity plan is still available to the teams.

175、 C .After the project kicks off, the first step for the team is performing a business impact analysis (BIA). The results from the BIA are given to management, and they determine what should happen next. If management gives the green light and provides the necessary resources, then the team can create their strategy before they actually develop the plan. The plan captures what has been laid out in the strategy phase. Then the plan is implemented, tested, and maintained.

176、 B .One of the biggest weaknesses in the use of cold site facilities is that they are not configured with any equipment, so testing is impossible. This type of backup option only provides

the company with a bare-bones facility in which to transfer over equipment if a disaster were to hit. It usually takes weeks for a cold site to be up and running; thus, it is extremely hard to test.

177、 C .Remote journaling is an automatic function that sends transaction logs of the backed up files to an offsite location. This does not take as many resources as electronic vaulting, which moves the entire file after it is modified.

178、 C .In tape vaulting, the data are sent over a serial line to a backup tape system at the offsite facility. The company that is maintaining the offsite facility will maintain the systems and change out tapes when necessary. Data can be quickly backed up and retrieved when necessary. This technology reduces the manual steps in the traditional tape back-up procedures.

179、 B .Checklist tests are good ways to get a wide range of feedback on procedures and ensure accuracy without disrupting business operations. In a checklist test, all departments are given a copy of the continuity plan. Each department must review and confirm that the information is correct.

180、 C .Reciprocal agreements are made between companies with the understanding that available facilities can be used by a company in the event of a disaster. These agreements come with a handful of problems, however. One problem is that they are not legally binding. Also, there are confidentiality issues. Most companies would not want to migrate their business operations into the house of another company, possibly revealing proprietary information.

181、 B .While employee turnover can contribute to plans becoming outdated, this is not an issue the IT director is responsible for. Starting an employee retention program to improve turnover rates would be an HR/management issue. It would be a good idea to recommend a program like this, but developing it independently would be inappropriate. The other answers are procedures that should be implemented that directly affect the efficiency and effectiveness of the plan.

182、 B .A hierarchical storage management (HSM) system is an automated data storage system. It provides continuous online backup functionality on low-speed/low-cost storage media.

183、 C .After a disaster, telephone service may not be available. For communication purposes there should be alternatives in place, such as cell phones or ham radios. Cell phones work on a different telephone system and network and may not have been affected during the disaster.

184、 B .Redundant sites provide the most advantages to a company that needs to ensure no, or a small amount of, downtime. These also offer the quickest recovery time in the event of a disaster. A redundant site could realistically be up and running within minutes of an event. Redundant and hot sites both provide good testing capabilities and ensure availability.

185、 C .The BIA identifies the company’s critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events. The outage time that can be endured by a company is referred to as the maximum tolerable

downtime (MTD). Here are some MTD estimates that may be used within an organization:

- Nonessential = 30 days
- Normal = 7 days
- Important = 72 hours
- Urgent = 24 hours
- Critical = Minutes to hours

Each critical business function and asset should be placed in one of the previous categories, depending upon how long the company can survive without it.

186、 B .Rita is an example of an employee who will play an active role in helping the company deal with disasters. It is management’s responsibility that these types of roles are defined and filled with competent people.

187、 C .All of these answers would be legitimate reasons for conducting testing on the business continuity plans. However, the number one objective is to make sure that the plans work. A company can have everyone involved, superior company awareness, and a management closely following each step, but if the plan is wrong and not useful, then it is all for naught.

188、 B .The only missing resources from a hot site are the data and people. The data will be retrieved from a backup site and restored.

189、 C .If a large disaster took place that affected not only the company’s facility but surrounding areas and housing areas, do you think your employees will be more worried about your company or their families? Some companies assume that employees will be ready and available to help them get back into production, when in fact they may need to be at home because they have family responsibilities.

190、 B .An incremental backup is a procedure that backs up only those files that have been modified since the previous backup of any sort. It does remove the archive attribute. A differential backup is a procedure that backs up all files that have been modified since the last full backup. It does not remove the archive attribute. A full backup is a procedure that backs up all files, modified or not, and removes the archive attribute. Incremental backups finish more quickly than differential backups, but they take longer to restore because each incremental backup has to be restored since the last full backup.

191、 D .Often companies view developing continuity plans as a project, meaning the project starts and then stops. It is not seen as an ongoing activity. This mentality can cause the plan to become quickly outdated because it is not being maintained.

192、 A .The recovery time objective (RTO) is the earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity.

193、 B .The work recovery time (WRT) is the remainder of the overall MTP value. RTO usually

deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything “live” for production purposes.

194、 A .Continuity of operations (COOP) is a U.S. government initiative, required by presidential directive, to ensure that agencies are able to continue operations after a disaster or disruption. BCP and COOP have the same basic goals, but BCP is commonly private-sector oriented and COOP is commonly public-sector oriented. COOP focuses on restoring an organization’s (usually a headquarters element) essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations.

195、 D .Law enforcement, the court system, and the legal community are definitely experiencing growth pains as they are being pulled into the technology of the 21st century.

196、 A .Fraud, theft, and embezzlement have always been part of life, but the computer age has brought on new opportunities for thieves and crooks. A new degree of complexity has been added to accounting, record keeping, communication, and funds transfer. This degree of complexity brings along its own set of vulnerabilities, which many crooks are all too eager to take advantage of.

197、 B .One country may not consider some issues against the law at all, whereas another country may determine that the same issue demands five years in prison. One of the complexities in these issues is jurisdiction. If a cracker from another country steals a bunch of credit card numbers from an American financial institution and he is caught, a court in America would want to prosecute him. His homeland may not see this issue as illegal at all. Although the attackers are not restricted or hampered by country borders, the laws are in many cases.

198、 C .There are many common fallacies when it comes to cybercrimes. Although the First Amendment protects a person’s free speech and expression, it does not include writing computer viruses.

199、 D .The most common example of a salami attack involves subtracting a small amount of funds from several accounts with the hope that such an insignificant amount would be overlooked.

200、 B .The U.S. approach to privacy protection relies on industry-specific legislation, regulation, and self-regulation, whereas the European Union relies on comprehensive privacy regulation. In order to bridge these different privacy approaches, the U.S. Department of Commerce and the European Commission developed a “Safe Harbor” framework.

201、 A .The Gramm-Leach-Bliley Financial Modernization Act requires financial institutions to develop privacy notices that must be given to each of its customers. The privacy notice gives the customer the option of prohibiting the bank from sharing his or her information with any nonaffiliated third-party organization. The act also requires each financial institution to have a comprehensive information security program in place.

202、 A .The European Union has restrictions on “transborder data flows” that would allow private data to flow to countries whose laws would not protect that data. The “Safe Harbor” privacy framework was developed between the United States and the EU to provide a streamlined means for U.S. organizations to comply with the European privacy laws.

203、 B .The Federal Wiretap Act, also known as the Electronic Communications Act of 1996, is a criminal law that punishes unauthorized interception of electronic communications in transit.

204、 C .The Economic Espionage Act of 1996 dictates that taking, downloading, or possessing trade secrets can merit up to $10 million in fines and up to 15 years in prison.

205、 C .The ACPA was enacted for trademark owners to have legal recourse to protect the illegal registration of their domain names. It is only relevant under the following categories: domain name registrant has the intent to profit from registering the trademark domain name; the registrant registers or uses a domain name that at the time of registration is identical or confusingly similar to an existing distinctive mark, or is identical or confusingly similar to a famous mark; or is a trademark, word, or name protected by certain sections of the U.S. Code.

206、 D .Computer crimes are so difficult to investigate and prosecute for many reasons: jurisdiction issues, law enforcement agencies are behind in manpower and skill, current laws may not directly apply to new computer crimes, lack of reporting of crimes by organizations, evidence is often intangible and hard to collect, it is difficult to explain complex technical concepts to judges and juries, and finally, lawyers that specialize in this type of law can be difficult to identify.

207、 A .Best evidence is often the most reliable primary evidence; it can include original documents and is never oral evidence. Direct evidence can prove a fact by itself, does not need corroborative information, and can be information from witnesses, such as oral testimony.

208、 D .An audit trail is important because it is a detailed record of events that took place on a system. It reveals the who, what, where, and how for all logged activity.

209、 C .The investigation process consists of the following steps in that order: Identification, Preservation, Collection, Examination, Analysis, Presentation, and Decision.

210、 D .When seizing and preserving electronic evidence, it is important to restrict all physical and remote access to the computer, photograph any images on the screen showing the state of the system, do not touch the keyboard, and conduct all forensic analysis operations of the evidence on imaged copies of the original disk in order to prevent inadvertent alteration of the original evidence.

211、 C .An incident is made up of one or more events that adversely affect the organization. An event may or may not become an incident. Some examples of incidents include breach of security, loss of functionality necessary to conduct business, and damage to the organization’s reputation.

212、 A .If a company does not afford the necessary level of protection and this affects another company they are working with, the affected company can hold the other one liable. Downstream liability is a way for companies to ensure they are implementing the required legal minimum to ensure their systems will not have a negative impact on others.

213、 B .Copyright law protects the expression of an idea such as a book, a song, a painting, or even software code. When properly copyrighted, these items cannot be copied or distributed without permission from the owner. While the Software Protection Association (SPA) works hard to protect software vendors from piracy, it is an organization, not a law. Trade secrets protect resources that are proprietary and absolutely necessary for survival. Trademarks are symbols, words, or pictures that uniquely identify something.

214、 A .Because of the growing occurrences of cybercrime, leading industrial countries and Russia joined together in 2000 to bring cybercrime to the attention of the G8 summit. This group works to develop laws related to cybercrime so that consistent prosecution will take place globally.

215、 B .A thorough and accurate chain-of-custody record is critical in an investigation process. The process includes labeling physical evidence and compiling a complete history of how evidence was collected, analyzed, transported, and preserved.

216、 A .Trademarks can exist in a variety of forms—a word, a shape, a graphic, or a phrase. The determining factor is whether or not it alone represents the larger organization in the eyes of the outside world. McDonald’s, for example, is known worldwide for its golden arches. This symbol is an identifier of the restaurant, and thus falls under trademark law.

217、 B .Because computer files and systems can be modified after the fact without others being aware of it, they are considered hearsay evidence. Hearsay evidence is not considered reliable or trustworthy because it is not firsthand evidence.

218、 A .A tort or civil law deals only with financial restitution or community service as punishments. Typically, civil lawsuits do not require the degree of burden of proof that criminal cases require. Administrative law deals with government-imposed regulations on large organizations and companies in order to protect the safety and best interest of their employees and customers.

219、 C .Wiretapping is the act of intercepting electronic signals. Under the U.S. Federal Wiretap Law, it is illegal without a court order. The most common example of wiretapping is with law enforcement agencies. In order for these organizations to legally tap into a suspect’s line, there must be a court-approved order allowing it.

220、 C .A trade secret can be many things, but the cardinal rule is that it must provide the company with a competitive advantage. A restaurant’s secret sauce would qualify as a trade

secret, which means it could prosecute the waiter for violating the law.

221、 D .The first step in a forensic investigation is to make a copy of the hard drive. This method ensures that the original system is not altered in any way during the investigation process. Following this procedure ensures an accurate chain of custody.

222、 B .Secondary evidence is not a reliable form of evidence. Typically, oral evidence like testimonies is placed in this category. Also, copies of documents are considered secondary in nature. The other choices are all types of evidence that can stand alone.

223、 A .The Federal Sentencing Guidelines were developed to establish more detail in what is expected of executives within companies. The regulation promotes consistent due diligence and due care by the management team. If the executive can prove that proper due diligence and due care were practiced, then it is conceivable that he would not be liable in the suit.

224、 C .Even though it is the duty of every CISSP to report software piracy, disgruntled employees report the activity most often.

225、 D .The Internet Architecture Board (IAB) is an independent board made up of researchers, engineers, executives, and other technical personnel with experience and interest in the Internet industry. The IAB does not have a government affiliation, so an FCC representative would not be appointed to the group.

226、 A .A good way to investigate cybercrime is with the acronym MOM: motives, opportunities, and means. Motives are the who and why of a crime. Opportunities are the where and when, and means involve the capabilities of criminals.

227、 B .The Council of Europe (CoE) Convention on Cybercrime is one example of an attempt to create a standard international response to cybercrime. It is the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation. The convention’s objectives include the creation of a framework for establishing jurisdiction and extradition of the accused. For example, extradition can only take place when the event is a crime in both jurisdictions.

228、 A .The European Union (EU) in many cases takes individual privacy much more seriously than most other countries in the world, so they have strict laws pertaining to data that are considered private, which are based on the European Union Principles on Privacy. This set of principles addresses using and transmitting information considered private in nature. The principles and how they are to be followed are encompassed within the EU’s Data Protection Directive. All states in Europe must abide by these principles to be in compliance, and any company wanting to do business with an EU company that will include exchanging privacy type of data must comply with this directive.

229、 D .A construct that outlines how U.S.-based companies can comply with the EU privacy

principles has been developed, which is called the Safe Harbor Privacy Principles. If a non-European organization wants to do business with a European entity, it will need to adhere to the Safe Harbor requirements if certain types of data will be passed back and forth during business processes. Europe has always had tighter control over protecting privacy information than the United States and other parts of the world. So in the past when U.S. and European companies needed to exchange data, confusion erupted and business was interrupted because the lawyers had to get involved to figure out how to work within the structures of the differing laws. To clear up this mess, a "Safe Harbor" framework was created, which outlines how any entity that is going to move privacy data to and from Europe must go about protecting them. U.S. companies that deal with European entities can become certified against this rule base so data transfer can happen more quickly and easily.

230、 B .It was developed in England and based on previous interpretations of laws. Today, the common law system uses judges and juries of peers. If the jury trial is waived, the judge decides the facts. Typical systems consist of a higher court, several intermediate appellate courts, and many local trial courts. Precedent flows down through this system. Tradition also allows for "magistrate's courts," which address administrative decisions.

231、 C .The common law system is broken down into the following:

- Criminal
- Based on common law, statutory law, or a combination of both.
- Addresses behavior that is considered harmful to society.
- Punishment usually involves a loss of freedom, such as incarceration, or monetary fines.
- Civil/tort
- Offshoot of criminal law.
- Under civil law, the defendant owes a legal duty to the victim. In other words, the defendant is obligated to conform to a particular standard of conduct, usually set by what a "reasonable man of ordinary prudence" would do to prevent foreseeable injury to the victim.
- Administrative (regulatory)
- Laws and legal principles created by administrative agencies to address a number of areas, including international trade, manufacturing, environment, and immigration.

232、 B .The Digital Millennium Copyright Act (DMCA) makes it illegal to create products that circumvent copyright protection mechanisms. DMCA is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services that circumvent access control measures that are put into place to protect copyright material. So if you figure out a way to "unlock" the proprietary way that Barnes & Noble protects its e-books, you can be charged under this act. Even if you don't share the actual copyright-protected books with someone, you still broke this specific law and can be found guilty.

233、 B .The generic approach is horizontal enactment—rules that stretch across all industry boundaries. It affects all industries, including government. Regulation by industry is vertical enactment. It defines requirements for specific verticals, such as the financial sector and health care. In both cases, the overall objective is twofold. First, the initiatives seek to protect citizens'

personally identifiable information (PII). Second, the initiatives seek to balance the needs of government and businesses to collect and use PII with consideration of security issues.

234、 A .Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian law that deals with the protection of personal information. One of its main goals is to oversee how the private sector collects, uses, and discloses personal information in regular business activities. The law was enacted to help and promote consumer trust and facilitate electronic commerce. It was also put into place to reassure other countries that Canadian businesses would protect privacy data so that cross-border transactions and business activities could take place in a more assured manner.

235、 A .A Statement on Auditing Standards No. 70: Service Organizations (SAS 70) is an audit that is carried out by a third party to assess the internal controls of a service organization. When companies come together to work in an integrated manner, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability, and responsibility, which should be clearly defined in the contracts each party signs. Auditing and testing should be performed to ensure that each party is indeed holding up its side of the bargain.

236、 D .It is common for organizations to develop governance, risk, and compliance (GRC) programs, which allow for the integration and alignment of the activities that take place in each one of these silos of a security program. If the same key performance indicators (KPIs) are used in the governance, risk, and compliance auditing activities, then the resulting reports can effectively illustrate the overlap and integration of these different concepts. For example, if an organization is not compliant with various HIPAA requirements, this is a type of risk that management must be aware of so that the right activities and controls can be put into place. Also, how does executive management carry out security governance if it does not understand the risks the company is facing and the outstanding compliance issues? It is important for all of these things to be understood by the decision makers in a holistic manner so that they can make the best decisions pertaining to protecting the organization as a whole. The agreed-upon KPI values are commonly provided to executive management in dashboards or scorecard formats, which allow them to quickly understand the health of the organization from a GRC point of view.

237、 C .A slang term for viruses being sent to a public network is “in the wild.” Just as wild animals are more dangerous than animals confined to a zoo, viruses on public networks are more dangerous than viruses “in the zoo,” or in controlled environments.

238、 A .Java is a programming language that works on multiple platforms and environments. The system can use mini-programs, called applets, and a code translator, called the Java Virtual Machine (JVM).

239、 D .Reviewing customer requirements is a task completed in the second phase of software development, the functional design analysis and planning phase. Project initiation is the formal introduction of the project to all participating parties. The entire scope of the effort is overviewed, and an initial risk analysis is performed. The customer’s requirements are more

granular issues than what is required in the first phase.

240、 A .Trojan horses are common attack methods used to spread malware. Once planted on a user’s machine, they act in complete disguise. As a program is initiated, the Trojan horse begins to work, but the power in the malware is that it goes unsuspected by the user.

241、 B .Artificial neural networks (ANNs) are built on the functionality of the human brain. The objective of the model is to allow systems to recognize patterns and learn from different situations. ANN uses small units that mimic human neurons. These are used to communicate with transmitters, which is how the learning process is carried out.

242、 B .A tuple is a database term for a row. It is defined as a row in a relational database model representing a relationship among a set of values.

243、 D .Data warehousing is a valuable tool that brings together several databases and compiles the different data into one data warehouse. The data can then be analyzed in different ways, which is called data mining.

244、 A .Logic bombs are types of malware that rely on some action by the user or meeting some predefined condition during the execution of the program. In this instance, the action is the user trying to save the file. The logic bomb overrides the command and executes a new set of instructions, which in this case is to delete all files on the hard drive.

245、 A .Data marts are closely tied to data warehouses, but there is a distinct difference. Data marts are collections of data from different databases or systems that fulfill a specific need. Data warehouses are collections of data from different databases or systems that could cover a wide variety of objectives. However, it is common for data marts to be subsets of data warehouses.

246、 A .Polyinstantiation is the concept of type (class, database row) being instantiated into multiple independent instances (objects, copies). In the case of database polyinstantiation, two different instances have the same name (primary key).

247、 B .Debugging is a common term used in the software industry. It is a part of the development life cycle and involves tracing and repairing faults in software. The faults that are being fixed are often called bugs.

248、 D .Unit testing is part of the software development phase. This phase involves the developers actually writing and testing the code. Part of writing code is doing unit testing as different milestones are reached throughout the process.

249、 A .Computer programming has gone through many generations of growth. Generation One is the earliest stage and offers the lowest levels of functionality. Here is the list of programming language generations:
One—Machine language

Two—Assembly language
Three—High-level language
Four—Very high-level language
Five—Artificial intelligence and natural network language

250、 C .Expert systems are built on the foundation of human logic. The programs use a knowledge base that is filled with information from subject matter experts. The decision-making process involves “if/then” statements and an inference engine.

251、 B .Common Object Request Broker Architecture (CORBA) is a standard that enables objects to communicate with one another, regardless of their programming language or platform type. CORBA was created by the Object Management Group (OMG).

252、 D .The committee is formed to ensure that all changes are properly submitted, tested, and approved. The goal is for changes to be desirable and beneficial for the company as a whole, and that the change be developed and implemented in a correct manner.

253、 C .A processor can be executing applications in user mode, a lower privilege mode than supervisory mode (also called privileged mode). The processor will execute instructions in this mode to ensure that rogue code does not access sensitive and critical system resources. A processor can execute in supervisory mode. This usually takes place when a process of high system privilege sends a request to the processor. If the processor is in supervisory mode, it has access to user-level (nonprivileged) and supervisor (privileged) code.

254、 B .Platforms using the CORBA standards use object request brokers (ORBs) to allow two systems with different languages to communicate with one another. So when one application sends a request to another application, the message first goes to the ORB. The ORB is responsible for knowing the location of the other application and sending the request to it.

255、 A .Database views are a common method of hiding information from people who do not have a need to know specific types of data. In this example, both Ron and Kathy are accessing the same system, but they only have views of fields that relate to their job functions.

256、 B .An object-oriented database is more dynamic in nature when compared to a relational database because objects can be created when needed and the data and procedure go with the object when it is requested. In a relational database, an application uses its procedures to obtain data from the database; the database does not actually provide procedures as object-oriented databases do. The object-oriented database has classes to define the attributes and procedures of its objects.

257、 C .An EICAR test is done with antivirus software by introducing a benign virus to test detection and reaction activities of the software. EICAR is a test file designed to test the integrity and configurations of antivirus software.

258、 A .Object linking and embedding (OLE) provides a way for objects to be shared on a local personal computer, and uses COM as its foundation base. OLE enables objects to be embedded into documents—like graphics, pictures, and spreadsheets. The capability for one program to call another program is linking. The capability to place an object inside a foreign document is embedding.

259、 A .A distributed denial-of-service attack (DDoS) involves a master/zombie relationship where an attacker gains control of the zombie computer and uses it to execute attack commands. The zombie computer becomes such by allowing the attacker to install compromising software on it. The software will, in turn, be used when it is called on to attack a specific victim.

260、 C .Software escrow is a service provided by a third party. When a company pays another company to develop software for them, a copy of all source code is stored by this third party, which is referred to as software escrow. If the software development company goes out of business, the paying customer will still have access to their product, the source code. The third party is paid for this service, and there are a lot of legal issues involving the exact type of service they will provide.

261、 B .This type of trapdoor is usually invoked by a series of keystrokes or commands that will allow the programmer easy access to the program at a later date. Easter eggs are typically harmless code within programs that developers insert into the program for the sake of entertaining curious geeks. A trapdoor may also be called a maintenance hook.

262、 A .Production code should not be modified by developers in any way. This goes against proper change control, can break other components in production, and can disrupt the standardization of code in production across the board.

263、C .Waterfall is a classical method that uses discrete phases of development requiring formal reviews and documentation before moving to the next phase of the project.

264、 A .The cleanroom development model is used to create critical applications. Strict testing procedures are followed throughout this approach to ensure that no mistakes are made. This model is used to provide a very high-quality product.

265、A .A system has its own developmental life cycle, which is made up of the following phases: initiation, acquisition/development, implementation, operation/maintenance, disposal. Collectively, these are referred to as a system development life cycle (SDLC). Here are the basic components of each phase:

- Initiation—need for a new system is defined
- Acquisition/development—new system is either created or purchased
- Implementation—new system is installed into production environment
- Operation/maintenance—system is used and cared for
- Disposal—system is removed from production environment

266、 A .The aim of an attack surface analysis is to identify and reduce the amount of code accessible to untrusted users. The basic strategies of attack surface reduction are to reduce the amount of code running, reduce entry points available to untrusted users, reduce privilege levels as much as possible, and eliminate unnecessary services. Attack surface analysis is generally carried out through specialized tools to enumerate different parts of a product and aggregate their findings into a numeral value. Attack surface analyzers scrutinize files, registry keys, memory data, session information, processes, and services details.

267、 B .Threat modeling is a systematic approach used to understand how different threats could be realized and how a successful compromise could take place. A threat model is a description of a set of security aspects that can help define a threat and a set of possible attacks to consider. It may be useful to define different threat models for one software product. Each model defines a narrow set of possible attacks to focus on. A threat model can help to assess the probability, the potential harm, and the priority of attacks, and thus help to minimize or eradicate the threats.

268、 C .There are many computer-aided software engineering (CASE) tools that programmers can use to generate code, carry out debugging activities, and perform software testing. When these types of activities can take place through automated tools, development usually takes place more quickly with fewer errors. CASE refers to any type of software that allows for the automated development of software, which can come in the form of program editors, debuggers, code analyzers, version-control mechanisms, and more. These tools aid in keeping detailed records of requirements, design steps, programming activities, and testing. A CASE tool is aimed at supporting one or more software engineering tasks in the process of developing software. Many vendors can get their products to the market faster because they are “computer aided.”

269、 B .Static analysis is a debugging technique that is carried out by examining the code without executing the program and therefore is carried out before the program is compiled. The term static analysis is generally reserved for automated tools that assist programmers and developers, whereas manual inspection by humans is generally referred as code review. Static analysis allows developers to quickly scavenge their source code for known programming flaws and vulnerabilities. In addition, static analysis provides a scalable method of security code review and ensures that secure coding policies are being followed. There are numerous manifestations of static analysis tools, ranging from tools that simply consider the behavior of single statements to tools that analyze entire source codes at once.

270、 D .Regression testing should take place after a change to a system takes place, retesting to ensure functionality, performance, and protection.

271、 A .Dynamic analysis refers to the evaluation of a program in real time, i.e., when it is running. Dynamic analysis is carried out once a program has cleared the static analysis page and basic programming flaws have been rectified offline. Dynamic analysis enables developers to trace subtle logical errors in the software architecture. In dynamic testing the software must actually be compiled and run, and commonly involves giving input values and checking if the

output is as expected.

272、 B .Fuzzing is a technique used to discover flaws and vulnerabilities in software. Fuzzing is the act of sending random data to the target program in order to trigger failures. Attackers can manipulate these errors and flaws to inject their own code into the system and compromise its security and stability. Fuzzing tools are commonly successful at identifying buffer overflows, DoS vulnerabilities, injection weaknesses, validation flaws, and other activities that can cause software to freeze, crash, or throw unexpected errors.

273、 D .The ISO/IEC 27034 standard covers the following items: application security overview and concepts, organization normative framework, application security management process, application security validation, protocols application security control data structure, and security guidance for specific applications. It is part of the ISO/IEC 27000 series, which allows the security software development processes to be in alignment with ISO/IEC’s information security management system (ISMS) model.

274、 A .The Waterfall model uses a linear-sequential life-cycle approach. Each phase must be completed in its entirety before the next phase can begin. At the end of each phase a review takes place to make sure the project is on the correct path and if the project should continue. This is a very rigid approach that could be useful for smaller projects that have all of the requirements fully understood, but is a dangerous model for complex projects, which commonly contain many variables that affect the scope as the project continues.

275、 C .If a development team follows the Incremental model, this allows them to carry out multiple development cycles on a piece of software throughout its development stages. This would be similar to having “multi-waterfall” cycles take place on one piece of software as it matures through the development stages. A version of the software is created in the first iteration and then it passes through each phase (requirements, design, implementation, testing) of the next iteration process. The software continues through the iteration of phases until a satisfactory product is produced.

276、 D .The Spiral model uses an iterative approach to software development and places emphasis on risk analysis. The model is made up of four main phases: planning, risk analysis, development and test, and evaluation.

277、 A .The Rapid Application Development (RAD) model relies more on the use of rapid prototyping instead of extensive upfront planning. In this model the planning of how to improve the software is interleaved with the processes of developing the software, which allows for software to be developed quickly.

278、 A .The Agile model is an umbrella term for several development methodologies. It focuses not on rigid linear stepwise processes, but incremental and iterative development methods that promote cross-functional teamwork and continuous feedback mechanisms. This model is considered “lightweight” compared to the traditional methods that are “heavyweight,” which

just means this model is not confined to a tunneled vision and overly structured approach. It is nimble and flexible enough to adapt to each project’s needs. The industry found out that even an exhaustive library of defined processes cannot handle every situation that could arise during a development project. So instead of investing time and resources into big upfront design analysis, this model focuses on small increments of functional code that are created based upon business need. This model promotes adaptive planning, evolutionary development and delivery, and encourages rapid and flexible response to change. This model can handle changes that are described in the question effectively.

279、 C .When changes take place to a software product during its development life cycle a configuration management system can be put into place that allows for change control processes to take place through automation. A product that provides software configuration management (SCM) identifies the attributes of software at various points in time, and performs a methodical control of changes for the purpose of maintaining software integrity and traceability throughout the software development life cycle. It defines the need to track changes and provides the ability to verify that the final delivered software has all of the approved changes that are supposed to be included in the release. During a software development project the centralized code repositories are often kept in systems that can carry out SCM functionality, which manage and track revisions made by multiple people against a single master set. The SCM system should provide concurrency management, versioning, and synchronization.

280、 B .Assembly language allows for direct control of very basic activities within a computer system, as in pushing data on a memory stack and popping data off a stack. Attackers commonly use this language to tightly control how malicious instructions are carried out on victim systems. An assembly language is considered a low-level programming language and is the symbolic representation of machine-level instructions. It is “one step above” machine language. It uses symbols (called mnemonics) to represent complicated binary codes.

281、 A .A distributed computing technology provides commonly needed application functionality and procedures across various environments. A service-oriented architecture (SOA) provides standardized access to the most needed services to many different applications at one time. Application functionality is separated into distinct units (services) and offered up through well-defined interfaces and data-sharing standardization. This means that individual applications do not need to possess the same redundant code and functionality. The functionality can be offered by an individual entity, and then all other applications can just call upon and use the one instance. This is really the crux of all distributed computing technologies and approaches; SOA is just a more web-based approach.

282、 A .Services within an SOA are usually provided through web services. A web service allows for web-based communication to happen seamlessly using web-based standards, as in Simple Object Access Protocol (SOAP); HTTP; Web Services Description Language (WSDL); Universal Description, Discovery, and Integration (UDDI); and XML. WSDL provides a machine-readable description of the specific operations provided by the service. UDDI is an XML-based registry that lists available services. UDDI provides a method for services to be registered by service providers

and located by service consumers.

283、 C .A mashup is the combination of functionality, data, and presentation capabilities of two or more sources to provide some type of new service or functionality. Open APIs and data sources are commonly aggregated and combined to provide a more useful and powerful resource.

284、 A .Software as a Service (SAAS) is a software delivery model that allows applications and data to be centrally hosted and accessed by thin clients, commonly web browsers.

285、 D .SQL injection is where instead of valid input, the attacker puts actual database commands into the input fields, which are then parsed and run by the application. SQL (Structured Query Language) statements can be used by attackers to bypass authentication and reveal all records in a database.

286、 A .The term “cross-site scripting” (XSS) refers to an attack where a vulnerability is found on a website that allows an attacker to inject malicious code into a web application. XSS attacks enable an attacker to inject their malicious code (in client-side scripting languages, such as JavaScript) into vulnerable web pages. When an unsuspecting user visits the infected page, the malicious code executes on the victim’s browser and may lead to stolen cookies, hijacked sessions, malware execution, bypassed access control, or aid in exploiting browser vulnerabilities.

287、 C .Media controls help to protect company resources and keep them from unauthorized individuals. Librarians are keepers of resources such as data files, programs, laptops, and backups.

288、 D .Computers have defense mechanisms in order to protect the operating system from potential danger. When the system senses a problem, it can react in one of three ways: system reboot, emergency system restart, or system cold start.

289、 A .Permanently erasing the contents from a medium is called sanitation. There are several ways to accomplish this:

- Degaussing Erasing data magnetically.
- Overwriting Replacing old content with new content. This is also called zeroization when the new contents contain null values.
- Physical destruction If the medium cannot be properly sanitized, it must be destroyed.

290、 C .Authorization creep is the process of an individual keeping privileges that are not necessary to perform his job function. This is commonly caused by promotions or transfers. Authorization creep violates both the least privilege and need-to-know concepts.

291、 B .Enforcing the mandatory vacation control is the best option for the vice president. This will allow another person to perform the job function and identify potential fraud while the original programmer is on vacation. The good thing about mandatory vacations is that they can

be spun in a positive light by the executive. Telling an employee to take a vacation can usually be interpreted in a positive way. Instituting a job rotation, on the other hand, may clue in the programmer to the executive’s suspicion.

292、 C .Detective controls help identify breakdowns in access controls. For example, a security professional who reviews a long-distance telephone billing sheet in an operations center can uncover potential fraud by operations employees.

293、 A .Backing up data is critical within operations organizations. The most important step to take is to create a backup plan. This will detail when and what to back up, as well as where to store the files. Even though each entity will require different phases of backups, it is not realistic to provide proper data security when only backing up data once per year.

294、 D .Job rotation is the correct answer. It involves training more than one person for a specific job. This accomplishes more than simply identifying potential fraud. It also creates redundancy in the event that an employee leaves the company. Separation of duties is closely related to job rotation, but it is slightly different. The separation of duties ensures that one person is not solely working on critical projects or critical functions.

295、 B .Degaussing is an effective way of destroying content on a floppy disk or hard drive. The process creates strong magnetic fields that return the flux of the electrons back to their original state. This will also get rid of the information that outlines the tracks and sectors of the media, so it may need to be returned to the vendor for this data to be reapplied.

296、 A .Several countermeasures should be put in place to reduce this threat:

- Disable unnecessary ports and services.
- Block access at the perimeter network using firewalls, routers, and proxy servers.
- Use an IDS to identify this type of activity.
- Use TCP wrappers on vulnerable services that have to be available.
- Remove as many banners as possible within operating systems and applications.
- Upgrade or update to more secure operating systems, applications, and protocols.

297、 C .Least privilege ensures that individuals have permissions only to what is required to do their job and no more. In this question, Tier I technicians would only need read access to network devices. Having the ability to make changes to a border router would violate the least-privilege policy.

298、 A .Audit trails are effective tools and are considered detective-technical controls. They can be used to display all commands that have been entered into a system, authentication attempts into a network, or systems and files that have been accessed or modified.

299、 B .One phase of product evaluation that is intimate to operations groups is life-cycle assurance. It deals with the system’s architecture and associated maintenance procedures. Operational assurance, on the other hand, deals with the system’s architecture and associated

features and functionality. Operational assurance looks at only certain portions of the life cycle of a product, while life-cycle assurance looks at all phases.

300、 A .Although each company will implement its own change management policy, the general procedures will remain the same. The correct order is:
1. Request a change
2. Approve a change
3. Document a change
4. Test a change
5. Implement a change
6. Report a change to management

301、 D .A computer that senses abnormal procedures or uncontrolled activities may enact an emergency system restart. This is done to protect the operating system from bad programming code, viruses, or any other failure that could disrupt the system.

302、 C .SMTP (Simple Mail Transport Protocol) acts as a transferring agent from a user's computer to an e-mail server and from server to server. SMTP uses TCP as its transport protocol.

303、A .Port scanning is used by attackers to identify open ports in a victim's network. Obtaining this kind of information can be useful in determining what kind of services are running and how to attack their vulnerabilities.

304、B .Corrective controls are used to fix a problem. For example, when it is determined that an unauthorized user gained access to a network segment, a corrective control will address the access control vulnerability that allowed the user access.

305、 B .Secure Remote Procedure Call (S-RPC) uses the Diffie-Hellman asymmetric algorithm to determine the shared secret key for encryption with a symmetric algorithm. If S-RPC is used in an environment, a sniffer can capture this data but not necessarily decrypt them.

306、 C .Operations' goal is to keep production in proper working order and, in most environments, they have a focus on protecting the company's hardware and media from unauthorized access. They are usually the maintainers or custodians of the environment and not the group that is responsible for developing and implementing policies. They should not have the power to make decisions on what users can access, including software. These access decisions are passed down to them, and operations just ensures that the controls enforcing these decisions are in proper working order.

307、 A .The correct answer is job rotation. Michael routinely replaces Dave on the operations floor. This is a security control, because if Dave were to always handle his customer accounts alone, he may have a greater potential to commit fraud.

308、 B .These wrappers monitor incoming network traffic and control what can and cannot

access the services mapped to specific ports. When a request comes to a computer at a specific port, the target operating system will check to see if this port is enabled. If it is enabled and the operating system sees that the corresponding service is wrapped, it knows to look at an access control list, which spells out who can access this service.

309、 A .Preventive controls are used to discourage unethical activity or potential damages from occurring. There are three types of preventive controls:

- Administrative HR policies, separation of duties, employee management, security policies
- Technical Password, biometrics, firewalls
- Physical Fences, security guards, surveillance systems

310、 B .Fax encryptors are used when high levels of security are required for fax transmissions. Just like data encryption, fax files are encrypted into ciphertext so that if intercepted, they will be unreadable.

311、 C .If some type of storage media is going to be retired and it contains/contained sensitive information, that data need to be properly erased before the media is discarded. Formatting media just clears out the file allocation table and does not securely delete the files. Deleting data on media just deletes the pointers to the files, not the files themselves. So the media needs to be properly erased through some type of zerorization process, degaussing, or physically destroyed.

312、 A .Configuration management is the process of identifying, controlling, accounting for, and auditing changes made to the baseline TCB, which includes changes to hardware, software, and firmware. It is a system that will control changes to test and maintenance documentation through the operational life cycle of a system. Its major objective is system and environment stability.

313、 B .The operations department is responsible for making sure changes to production systems are done in an approved and controlled manner. They are also responsible for ensuring that the systems and environment are in stable working condition. This includes making sure that systems can be rebuilt if necessary.

314、 C .Data remanence is remaining data. In this example, Cory was not well educated on data sanitization techniques. Simply deleting a file from a hard drive does not remove the data from the medium. The new user can perform a routine “restore” command to view the files.

315、 C .There are three primary types of recovery procedures for computers:

- System reboot Restarts in a controlled manner
- Emergency reboot Restarts when normal procedures cannot be initiated
- System cold start Operating system brings the system down to maintenance mode, and operator intervention is required to complete the recovery

316、 B .Redundant array of inexpensive disks (RAID) uses a function called striping. Striping is the process of writing data across several aggregate drives. The trick in this technique is that data retrieval is dramatically improved because many device heads are utilized.

317、 C .Change control procedures are critical to maintaining proper levels of security within an operations environment. In this example, Max’s software enhancement may or may not have caused problems with the operating system or connecting devices. However, ensuring that every change, regardless of size or scope, goes through formal levels of approval will help to ensure that no negative effects occur.

318、 A .Penetration testing is a way of knowing how strongly the network will hold up against attacks. The test should cover many of the possible attack types administered by hackers.

319、 B .Tim has been given least-privilege access to company data. This means that he can only read what is absolutely necessary to fulfill his job requirements. While it would be nice to have access to billing records, Tim doesn’t need them in order to do his normal activities.

320、 A .Change control administrators are responsible for keeping the procedure updated and alive in the eyes of the company. Their role within the procedure is to give formal approval or rejection to the requester. The actual process should stay the same for every type of change request. The process and logic of the change are separate. The type of change should not influence the procedures of the change control process.

321、 B .Clipping levels are thresholds. In this example, it would be difficult for Robert’s boss to manually monitor all of his employees and the hundreds of thousands of transactions they process each day. But with automation, a system notifies him if certain error thresholds are exceeded.

322、 C .Passwords, ACLs, and ID badges are all preventive mechanisms designed to stop unauthorized access. Passwords and ACLs are considered preventive-technical controls, while ID badges are preventive-physical controls.

323、 B .The main goal of operations security is to protect the company’s resources (assets). It is also concerned with hardware and software performing in predictable and acceptable ways.

第八章题目

1. Malware that executes only after a certain condition is met is called a _____.
   A. Smurf attack
   B. Worms
   C. Logic bomb
   D. DoS attack
2. Worms are different from viruses because they are _____.
   A. In the wild
   B. Not considered malware

C. Rely on an event to occur

D. Self-contained

3. What are viruses in public networks referred to as?

A. Production-ready

B. In the zoo

C. In the wild

D. A Trojan horse

4. An object-oriented programming language that runs on many platforms is called _____.

A. Java

B. HTTP

C. OLE

D. ActiveX

5. In the project initiation phase of software development, all of the following tasks should be performed except _____.

A. Hold a kick-off meeting.

B. Perform a risk analysis.

C. Analyze threats.

D. Review customer requirements.

6. Malware that is embedded within a program and executes harmful actions behind the scenes while the victim believes the program is operating normally is called what?

A. Trojan horse

B. Stealth virus

C. Smurf attack

D. Multiparty virus

7. The artificial neural network (ANN) both attempts to mimic and is based on which of the following?

A. The combined security policies of all connected computers

B. The human brain

C. The least common denominator

D. Rule-based administration

8. The act of two different objects responding to the same command in different ways is called _____.

A. Abstraction

B. Object reuse

C. Polymorphism

D. Polyinstantiation

9. In relational databases there are several different terms used to describe the different components of the database. What is a tuple?

A. A column in a database

B. A row in a database

C. A collection of tables

D. A view or partition of data

10. There are several different types of viruses that work differently and reside within different

portions of a computer system. A virus that affects both a boot record and files in a directory is which of the following?

A. Logic bomb

B. Multipartite virus

C. Self-garbling virus

D. Stealth virus

11. The act of compiling data from several databases so that the information may be better analyzed is called _____.

A. Data mining

B. Partitioning

C. Inference

D. Data warehousing

12. A virus is planted within a drafting program on a user's machine. When the user clicks "save," the program instead deletes all the files on the hard drive. This is an example of what?

A. Logic bomb

B. DDoS

C. Smurf attack

D. Timing attack

13. Which of the following is used in web sites as a way to respond dynamically to inputted data?

A. Applets

B. ActiveX

C. CGI

D. Cookies

14. A collection of data from different sources that is targeted at one group or for a specific objective is called a _____.

A. Datamart

B. Data warehouse

C. Metadata

D. Data center

15. Which of the following tasks does not happen during the acceptance testing/implementation phase of the software development life cycle?

A. Product is used within the intended environment.

B. QA performs testing.

C. Product is given to customer for certification and accreditation.

D. Product is integrated into the desired network.

16. Uncovering restricted information by using permissible data is referred to as_____.

A. Aggregation

B. Data mining

C. Perturbation

D. Cell suppression

17. There are several different terms within object-oriented programming which describes the type of objects and their activities. What does polyinstantiation mean?

A. A mechanism used to take a copy of an object and repopulate it with different data or

modify its characteristics in some way

B. An act of two objects responding differently to the same command

C. The process of data hiding

D. The translation of two different languages on one plaform

18. Different activities need to happen during software development. What does debug mean?

A. To magnetically erase data from a medium

B. To trace and fix software failures

C. To change security levels

D. To change assembly language into machine language

19. Which of the following is not an example of "mobile code?"

A. Java applets

B. ActiveX

C. CGI

D. Active scripts in an e-mail attachment

20. Unit testing is performed in what phase of the software development life cycle?

A. Acceptance testing/implementation

B. Operations/maintenance

C. System design specifications

D. Software development

21. Generation One of program languages includes which of the following?

A. Machine language

B. Assembly language

C. Object-oriented language

D. Artificial intelligence

22. Which of the following is a collection of interrelated data stored in a meaningful way allowing multiple users and applications to access, view, and modify it?

A. ANN

B. Hierarchical

C. Database

D. Expert system

23. Computer programs that are based on human logic by using "if/then" statements and inference engines are called _____.

A. ANN

B. Artificial expert systems

C. Expert systems

D. ActiveX

24. What is CORBA?

A. A design framework for applications written in Java

B. A standard to allow communications between programs written in different languages and platforms

C. A Microsoft model aimed at allowing objects to communicate wth objects on different computers

D. An object-oriented programming language developed by Sun Microsystems

25. In which phase of software development are security requirements defined?

A. Project initiation

B. Functional design analysis and planning

C. System design specifications

D. Software development

26. A change control committee is formed to evaluate all proposed changes in order to ensure what?

A. Comprehensiveness and timeliness

B. Business impact and security

C. Project milestones and timeliness

D. Correctness and desirability

27. Polyinstantiation is a technique used in databases to thwart what type of threat?

A. Aggregation

B. Inference

C. Traffic analysis

D. Zero proof knowledge

28. Which of the following is a type of artificial intelligence that has the ability to learn through different scenarios and uses decision-making procedures during its computation of inputted data?

A. Neural networks

B. Expert systems

C. Knowledge bases

D. Inference engines

29. A processor can work in different modes. If it is working in "supervisor" mode, what does that mean?

A. It cannot accept software or hardware interrupts.

B. It is working at a lower privilege than user mode.

C. It has access to privileged and non-privileged instructions.

D. It is computing non-privileged instructions.

30. Security has historically not been a major focus of software development. In many cases, implementing proper protection tools are left to a security professional after the fact. Which of the factors below is not a reason that security has been excluded from typical software development?

A. Security was not taught in computer science classes in the past.

B. Software vendors are anxious to rush their products out the door.

C. Security is not a programmer's job; it is the job of a security professional.

D. The software industry has grown tolerant of flaws, bugs, and vulnerabilities.

31. Your company has several applications that rely on each other for information and processes. Several of the systems use different programming languages, so each has adhered to a CORBA framework. When one system sends a request to an object on another system, what component does the request actually go to?

A. EJB

B. ORB

C. COM

D. Active X

32. Applications and operating systems have several vulnerabilities that can be used for attacks. Knowing these weaknesses is the job of security professionals. One attack is when a process modulates its resource as a way of communicating to another process. What is this called?

A. Overt timing channel

B. Covert timing channel

C. Overt storage channel

D. Covert storage channel

33. Ron and Kathy work in two different departments and perform two different job functions. However, both utilize the same database for their jobs. When Ron opens his database, he sees four pages of input fields, while Kathy only sees two pages. What type of security protection has been implemented in their database?

A. Views

B. Data warehousing

C. Perturbation

D. Checkpointing

34. As part of a software development team, Darren and Denise are asked to identify the security objectives of the product and to perform an initial risk analysis. What phase of the software life cycle are they working on?

A. Project initiation

B. Functional design analysis and planning

C. System design specifications

D. Software development

35. A fraud analyst with a national insurance company uses database tools every day to help identify violations. These tools help identify relationships between a wide variety of information types. What kind of Knowledge Discovery in Database (KDD) is this considered?

A. Probability

B. Statistical

C. Classification

D. Behavioral

36. Bryce is working diligently on coding a software product. One day as he is nearing completion and ready for testing, the software development project manager brings over another programmer, Danielle, to his desk. The project manager asks Bryce to walk Danielle through the coding so that she will fully understand how it was designed and implemented. What software development principle has the project manager just enacted?

A. Split knowledge procedures

B. Joint analysis development

C. Job rotation

D. Data mining

37. Which of the following best describes the Capability Maturity Model (CMM)?

A. It improves software quality, reduces the life cycle of development, and provides better project management capabilities.

B. It improves software quality, increases the life cycle of development, and provides better project management capabilities.

C. It describes procedures, principles, and practices that underline software process maturity

with the goal of not improving software development processes.

D. It describes procedures, principles, and practices that underline software process immaturity with the goal of improving software development processes.

38. The Capability Maturity Model (CMM) has five maturity levels that can be assigned to software development companies after a certification process. Which of the following lists the correct five levels?

A. Initial, repeatable, qualified, managed, optimizing

B. Initial, repeatable, defined, managed, optimizing

C. Initial, repeatable, defined, managed, custom

D. Initial, non-repeatable, defined, managed, optimizing

39. A company hires a software development company to create a customized application. The software development company suggests that a software escrow should be set up. What does this mean?

A. The source code is split up and held at three different agencies to enforce separation of duties.

B. The source code is split up and held at two different agencies to enforce separation of duties.

C. A third party will keep a copy of the source code to protect the software developer.

D. A third party will keep a copy of the source code to protect the customer.

40. When multiple databases exchange transactions, each database is updated. This can happen many times and in many different ways. To protect the integrity of the data, databases should incorporate a concept known as an ACID test. What does this acronym stand for?

A. Availability, confidentiality, integrity, durability

B. Availability, consistency, integrity, durability

C. Atomicity, confidentiality, isolation, durability

D. Atomicity, consistency, isolation, durability

41. Katie is developing a proprietary system that works with several complicated systems, networks, and protocols. Her company dictates that all software developers follow a software programming model that uses discrete phases and reviews before the next phase of development is carried out. What type of model is this?

A. CASE

B. Cleanroom

C. Waterfall

D. JAD

42. Which of the following best describes the differences between object-oriented databases and relational databases?

A. Relational databases are more dynamic than object-orlented databases and the objects contain the procedures within them.

B. Object-oriented databases are more dynamic than relational databases and the objects contain the procedures within them.

C. Object-oriented databases are more dynamic than relational databases and the relational tables contain the procedures that interact with the objects.

D. Relational databases are more dynamic than object-oriented databases and the objects extract the procedures from the applications.

43. In software programming, a basic rule of thumb is that individual modules should be able to perform tasks on their own, with the least amount of help of other modules. They should be self-contained. In addition, when modules do intersect, they should not impact each other. Given this, which of the following is true?

A. Modules should be highly cohesive and have high coupling.

B. Modules should be highly cohesive and have low coupling.

C. Modules should have low cohesion and high coupling.

D. Modules should have low cohesion and low coupling.

44. Some steps need to be performed for each and every project, so it would be more efficient if they were automated. Which of the following is an automated tool used to accomplish activities such as debugging, coding, and version control?

A. Cleanroom

B. CASE

C. RAD

D. JAD

45. Distributed applications can be written in Java. Which of the following describes the Java structural design used for developing these types of applications?

A. Enterprise JavaBeans (EJB) dictates the protocols, components, and platforms that have to be implemented to allow different applications to communicate in a distributed environment.

B. Enterprise Knowledge System (EKS) dictates the interfaces that have to be implemented to allow different applications to communicate in a distributed environment.

C. EJB dictates the interfaces that have to be implemented to allow different applications to communicate in a distributed environment.

D. EJB dictates the applets that have to be implemented to allow different applications to communicate in a single, centralized system.

46. Before George rolls out the new antivirus software product to all 30,000 systems, he needs to test its configurations and reactions to identified viruses. What type of test will George carry out?

A. RAD

B. Release a live virus on the subnet

C. EICAR

D. Flooding attack on the product

47. Expert systems are built to provide human-type logic. One component of an expert system is its "if/then" logic. What is "if/then" logic called?

A. Rule-based programming

B. Role-based programming

C. Inference engine

D. Knowledge base

48. An attacker can use UDP packets against his victims. He sends out spoofed UDP packets to the victim's entire network requesting a response. All systems in the network immediately respond to the victim's computer. Because the victim's computer cannot handle the traffic overload, it freezes and stops functioning. What is this type of attack called?

A. SYN flood

B. Smurf

C. Worm

D. Fraggle

49. John is leading the new software development project for a reservations system of a car rental agency. He has been given strict instructions by his CIO that the exact requirements set by the customer must be met. He has strongly recommended that a "cleanroom" approach be used for this project. What is a cleanroom?

A. An approach built on formal development and testing procedures

B. An approach that runs at maximum efficiency by incorportating job rotation between team members

C. A classic approach that ensures that each phase of development flows from one to the next

D. An approach that guarantees quick analysis by providing a "proof of concept"

50. Jim is a construction manager who has asked his drafters and foreman to provide him with their individual project summaries. His first summary report is a Word document that has an Excel spreadsheet within it that outlines all the requirements, timelines, and expenses. When Jim double clicks on the spreadsheet, it launches his Excel program. Which technology below made this possible?

A. OLE

B. Backdoor

C. Covert channels

D. EJB

51. What is a polymorphic virus?

A. A virus that infects the boot sector and the hard drive

B. A virus that is written in a macro language

C. A virus that self-garbles

D. A virus that makes copies of itself and changes those copies

52. A computer being used in an attack such as distributed denial-of-service without the owner's knowledge is called what?

A. Zombie

B. Logic bomb

C. Trojan horse

D. Worm

53. Which of the following is true of data warehouses?

A. They are simply redundant databases.

B. They combine data from several databases in a useful way to provide better analysis.

C. They mirror data from multiple databases.

D. They are used in ANNs as a knowledge base.

54. What is the product of data mining?

A. Checkpoints

B. Savepoints

C. Metadata

D. Data dictionary

55. Which of the following is the electronic model based on the neural structure of the brain?

A. Expert system

B. ANN

C. Knowledge-based systems

D. Inference engine

56. What is it called when a database periodically saves data to protect it from being lost in the event of a failure?

A. Commit

B. Aggregation

C. Checkpoints

D. Integrity

57. In relational databases, what is the unique identifier of a row called?

A. Foreign key

B. Primary key

C. Cell

D. Attribute

58. Human reasoning capabilities are built into which one of the following?

A. Expert systems

B. Biometric systems

C. Data warehouses

D. Signature-based systems

59. Which database model is the most widely used today?

A. Logical

B. Distributed

C. Hierarchical

D. Relational

60. What type of security mechanism is used in ActiveX?

A. Bytecode

B. Sandbox

C. Virtual machine

D. Digital signature

61. Short Java programs that run within a user's browser are called _____.

A. Malware

B. Plugins

C. Applets

D. Sandboxes

62. Sending malformed fragmented packets to a computer in order to make it freeze or reboot is what type of attack?

A. Winnuke

B. Teardrop

C. Smurf

D. Fraggle

63. Which of the following describes a SYN attack?

A. Sending small packets to a system that is unable to process them

B. Using spoofed UDP packets to learn about the topology of the victim's network

C. Overwhelming a computer by sending multiple communication requests

D. Using PING commands to overwhelm a system

64. The formal authorization given by management to allow a system to operate in a specific

environment is called _____.

A. Accreditation

B. Certification

C. System requirements gathering

D. Risk analysis

65. System functionality is broken down into a more detailed level at what phase of software development?

A. Implementation

B. Functional design analysis and planning

C. Design specifications

D. Project initiation

66. Which of the following is a Microsoft component that works as a database driver manager?

A. COM

B. DCOM

C. OLE

D. ODBC

67. Which of the following database models uses a tree structure?

A. Hierarchical

B. Relational

C. Object-oriented

D. Discretionary

68. In what software development phase does informal and formal testing begin?

A. Installation

B. Testing/Validation

C. Functional design

D. Project initiation

69. Which of the following can provide rapid prototyping of programs, as well as debugging, code analyzing, and version controlling functions?

A. Sniffer tool

B. Terminal emulation tool

C. CASE tool

D. Analyst tool

70. Which is not true of OOP?

A. Groups objects into classes

B. Self-contained

C. Highly modular

D. More expensive than classic approach to programming

71. What uses GUIDs to keep track of different objects?

A. OOD

B. OOA

C. DCOM

D. DCE

72. Which of the following is used with HTTP connections to help identify and remember users?

A. Cookies

B. Applets

C. Scripts

D. CGI

73. When a database cancels changes that are being made and returns to the previous state, it is called _____.

A. Commit

B. Rollback

C. Submit

D. Checkpoint

74. Which of the following is the best definition of a pseudo-flaw?

A. Backdoor inserted into a system

B. Trojan horse

C. Buffer overflow

D. Code inserted to trap intruders

75. What protection should be put into place in case a software development company goes out of business?

A. Message digests

B. Logical and physical controls

C. Software escrow

D. Separation of duties

76. Which of the following is the most critical component for systems that will provide integrity?

A. Trojan horse vulnerabilities

B. Trusted paths

C. System design

D. Classification

77. Expert systems do not have which of the following components?

A. Rule-based programming

B. Statistical behavior – based engine

C. Inference engine

D. Knowledge base

78. What components are needed to perform a smurf attack?

A. Attacker, victim, amplifying network

B. Attacker, victim, packet fragmentation, amplifying network

C. Attacker, victim, packet fragmentation

D. Attacker, victim, out-of-band data

79. Which of the following is an example of why polyinstantiation would be used?

A. To allow one object to have two security classifications

B. To protect the integrity of a database by implementing content and context control

C. To protect the integrity of a database by implementing checkpoints and savepoints

D. To allow two objects to accept the same input and provide different results

80. What are aggregation and inference?

A. Gathering information to ensure that no private information can be reconstructed into its original format

B. Protecting the integrity of a database by implementing checkpoints

C. Protecting the integrity of a database by implementing content and context control

D. Gathering information and constructing private information from available resources

81. Which of the following is a backdoor to an application or system created by the developer?

A. Loop hole

B. Trapdoor

C. Easter egg

D. Trojan horse

82. In application development, good separation-of-duties practice states that the developer should not do what?

A. Change production code.

B. Request management approval of a code change before developing the change.

C. Perform unit tests.

D. Pass the code to quality assurance and then to the librarian prior to its entry into production.

83. Code is released "in the wild" and its intent is to start deleting the data off of hard drives on 04-04-04 at 1:00 P.M. This code is best described as a _____.

A. Worm

B. Snake

C. Stink bomb

D. Logic bomb

84. According to the separation- of-duties principle, which of the following is true?

A. Programmers should be the only ones testing their own code.

B. Someone other than the programmers should test their code.

C. Test code should go directly to production.

D. Programmers should interact with code in production.

85. Aggregation is _____.

A. The act of collecting information based on the flickering of a hard disk’s LED lights

B. The act of repeatedly guessing at a password or clearance code

C. The act of combining information from separate sources and then surmising the contents of a highly sensitive object

D. Sending data in groups through interprocess communication (IPC)

86. In programming, what language type represents data in binary to the processor?

A. Electrical signal language

B. Assembly language

C. High-level language

D. Machine language

87. What is the goal of data or information hiding in object-oriented programming?

A. To prevent one component from needing to know how another component functions

B. To ensure that users cannot read objects above their security level

C. To ensure that data is only accessible based on security labels

D. To preserve data integrity through hashing

88. Which of the following is not used for turning source code into machine or object code?

A. Assembler

B. Interpreter

C. Compiler

D. Analyzer

89. Which of the following produces code that is platform independent?

A. Java

B. ActiveX

C. VB

D. C

90. Which of the following is not a primary component of a smurf attack?

A. ICMP

B. IGMP

C. Amplifying network

D. IP spoofing

91. What is put into place to ensure that a primary key does not contain a null value?

A. Entity integrity

B. Message digests

C. Data mining tool

D. ODBC

92. Which of the following is not considered a timing attack?

A. Line disconnect

B. Between the lines

C. NAK attack

D. SYN attack

93. Which of the following best describes the reason for an EICAR test?

A. To identify DoS possibilities in the perimeter network

B. To test antivirus software detection and alerting configurations

C. To identify spoofed ICMP messages

D. To test for fragment attacks

94. Which of the following properly describes the Capability Maturity Model (CMM)?

A. An integrity model used to ensure lower-level subjects cannot access higher-level objects

B. A confidentiality model used to ensure that information does not flow in a way that will negate the security policy

C. A model used by software development companies to provide repeatable procedures that can be continually improved upon

D. An information flow model that is used to protect the integrity of sensitive objects' internal data

95. Which of the following is a software code base management solution that offers reliable versioning?

A. Code repository

B. Software escrow

C. Key escrow

D. Software baseline

96. What is the best way to protect code repositories?

A. Separation of duties

B. Air gapping

C. Encryption

D. Escrow

97. Which of the following types of tests ensure the code meets customer requirements?

A. Unit testing

B. Regression testing

C. Integration testing

D. Acceptance testing

98. Which the following is NOT a method used to assess the security impact of acquired software?

A. Formal risk assessment

B. Security functional requirements analysis

C. Security assurance requirements analysis

D. Penetration testing

99. During which phase of the software development life cycle should attack surface analysis and threat modeling be performed?

A. Design

B. Requirements gathering

C. Development

D. Testing/validation

100. What is the mechanism that allows one software object to communicate with another?

A. Cohesion

B. Coupling

C. Application programming interface

D. Polymorphism

第八章答案

1、 C .A logic bomb relies on an event to occur before it will initiate. A common example is a logic bomb being planted on a victim's computer. When the user executes a command or a program, the malware starts.

It can also be date- and time-driven. For example, on 27 March at 12:01 A.M., the malware executes.

2、 D .Worms are self-contained programs, meaning they can operate independently. Viruses, on the other hand, require some type of application for reproduction. Worms reproduce by themselves while residing on a victim's computer.

3、 C .A slang term for viruses being sent to a public network is "in the wild." Just as wild animals are more dangerous than animals confined to a zoo, viruses on public networks are more dangerous than viruses "in the zoo," or in controlled environments.

4、 A .Java is a programming language that works on multiple platforms and environments. The system can use mini-programs, called applets, and a code translator, called the Java Virtual Machine (JVM).

5、 D .Reviewing customer requirements is a task completed in the second phase of software development—the functional design analysis and planning phase.

Project initiation is the formal introduction of the project to all participating parties. The entire scope of the effort is overviewed and an initial risk analysis is performed.

Customer's requirements are more granular issues than what is required in the first phase.

6、 A .Trojan horses are common attack methods used to spread malware. Once planted on a user's machine, they act in complete disguise. As a program is initiated, the Trojan horse begins to work, but the power in the malware is that it goes unsuspected by the user.

7、 B .Artificial neural networks (ANN) are built on the functionality of the human brain. The objective of the model is to allow systems to recognize patterns and learn from different situations. ANN uses small units that mimic human neurons. These are used to communicate with transmitters, which is how the learning process is carried out.

8、 C .Polymorphism exists within object-oriented programming applications. Objects are derived from different classes which make them respond differently to commands. So, when two objects, each in a different class, are presented with the same command, their class properties tell them how to respond. When they respond differently to the same command it is called polymorphism.

The objects could come from the same class but inherit behaviors for different sub-classes.

9、 B .A tuple is a database term for a row. It is defined as a row in a relational database model representing a relationship among a set of values.

10、 B .A multipartite virus can be very damaging to a network and users. Because it goes after boot records and system files, it can be more destructive, affecting more areas of a system.

11、 D .Data warehousing is a valuable tool that brings together several databases and compiles the different data into one data warehouse. The data can then be analyzed in different ways, which is called data mining.

12、 A .Logic bombs are types of malware that rely on some action by the user. In this instance, the action is the user trying to save the file. The logic bomb overrides the command and institutes a new set of instructions, which in this case, is to delete all files on the hard drive.

13、 C .Common Gateway Interface (CGI) is used in web sites that require a user to input

information. CGI scripts or executables are used to translate, respond to request, build a new web page, and then send it to the user. The user is then presented with data based on her request.

14、 A .Datamarts are closely tied to data warehouses, but there is a distinct difference. Datamarts are a collection of data from different databases or systems that fulfill a specific need. Data warehouses are a collection of data from different databases or systems that could cover a wide variety of objectives. It is common for datamarts to be subsets of data warehouses.

15、 A .The product is not actually used in a production environment until the life cycle reaches the operations/maintenance phase.
The acceptance testing/implementation phase leads to this next level, but certain tasks must be completed before the product can be used. Testing, certifying, and integration tasks must all be completed first to ensure the product functions properly and coexists with other network devices and software successfully.

16、 A .Aggregation and inference go hand-in-hand. For example, a user who uses data from a public database in order to figure out classified information is exercising aggregation and can then infer the relationship between that data and the data he does not have access to. This is called an inference attack.

17、 A .Polyinstantiation is an access control used mainly in databases to allow multiple rows to be tied to one primary key. Data can then be accessed in different ways and by different levels of users.

18、 B .Debugging is a common term used in the software industry. It is a part of the development life cycle and involves tracing and repairing faults in either software. The faults that are being fixed are often called "bugs."

19、 C .Mobile code is small programs that can be transmitted as an e-mail attachment or by downloading from different web sites. Java applets, ActiveX, and active scripts are all considered mobile code.

CGI is unrelated to mobile code, but instead is a web server interface technology.

20、 D .Unit testing is part of the software development phase. This phase involves the actual code writing by the developers and the developers testing their own code. Part of code writing is doing unit testing as different milestones are reached throughout the process.

21、 A .Computer programming has gone through many generations of growth. Generation One is the earliest stage and offers the lowest levels of functionality. Here is the list of programming generations:

- One — Machine language

- Two — Assembly language
- Three — High-level language
- Four — Very high-level language
- Five — Artificial intelligence and natural language

22、 C .Databases allow companies to work with data from one, centralized location. They promote consistency, data integrity, and security. They allow data to be presented in a useful manner and allow relationships between different types of data to be set up.

23、 C .Expert systems are built on the foundation of human logic. The programs use a knowledge base that is filled with information from subject matter experts. The decision-making process involves "if/then" statements and an inference engine.

24、 B .Common Object Request Broker Architecture (CORBA) is a standard that enables objects to communicate with one another regardless of their programming language or platform type. CORBA was created by the Object Management Group (OMG).

25、 B .Security requirements should be defined during the functional design analysis and planning phase of software development. This phase should result in a formalized, functional baseline which includes security tasks, test plans, and checkpoints.

26、 D .The committee is formed to ensure that all changes are properly submitted, tested, and approved. The goal is that the changes are desirable and beneficial for the company as a whole, and that the change is developed and implemented in a correct manner.

27、 B .Polyinstantiation means that a copy of an object is made and the characteristics of the second object are modified in some way. Within databases this technique can be used to allow more than one row to contain the same primary key.

The different rows contain data that resides at different security levels, thus the different rows have different classifications. This way when a subject accesses the database, only the row that matches his security clearance will be available. If this technique was not used when a subject attempted to access a row above his clearance, he would be told that the data is unavailable or that the he did not have the security rights to view it. This would allow low-level users to infer the existence of highly classified information.

28、 A .Neural networks are created to mimic the way human brains think, learn, and deal with different situations and data. They are put through different scenarios and the data inputted into the systems are weighted depending upon importance.

Expert systems use knowledge bases with inference engines to identify patterns and relationships between different types of data, but they cannot learn through experience.

29、 C .A processor can be executing applications in user mode, a lower privilege mode than

supervisory mode (also called privileged mode). The processor will execute instructions in this mode to ensure that rogue code does not access sensitive and critical system resources.

A processor can execute in supervisory mode. This usually takes place when a process of high system privilege sends a request to the processor. If the processor is in supervisory mode it has access to user-level (non-privileged) and supervisor (privileged) code.

30、 C .Although progress is being made, security has not typically been a focus in software development. Most programmers who went to school several years ago weren't taught about all of the security mechanisms available, not to mention that many of the today's viruses and attack types may not have existed then. It has also become all too common for customers to accept software flaws.

31、 B .Platforms using the CORBA standards use object request brokers (ORBs) to allow two systems with different languages to communicate with one another. So, when one application sends a request to another application, the message first goes to the ORB. The ORB is responsible for knowing the location of the other application and sending the request to it.

32、 B .Covert channels are ways that attackers can allow processes to use items for communication. The items were not developed to be used for communication purposes in this way.

A covert channel is the act of using an unintended communication path to send and receive messages.

An overt channel is using a communication path that was intended for communication.

33、 A .Database views are a common method of hiding information from people who do not have a need to know of specific types of data. In this example, both Ron and Kathy are accessing the same system, but they only have views of fields that relate to their job functions.

34、 A .The first phase of a project life cycle is the project initiation phase. The following steps are commonly executed in this phase:

- Decide on the definition or scope of the project.
- Perform an initial risk analysis.
- Assess threats and countermeasures.
- Determine security objectives of the product that will be developed.

35、 B .Data mining is also known as Knowledge Discovery in Database (KDD), which are techniques of identifying valid and useful patterns. Different types of data can have various interrelationships and the methods used depends on the type of data and patterns that are sought after. The following are three approaches used in KDD systems to uncover these patterns:

• Classification — Data is grouped together according to shared similarities.
• Probabilistic — Data interdependencies are identified and probabilities are applied to their relationships.
• Statistical — Identifies relationships between data elements and uses rule discovery.

36、 A .Split knowledge procedures ensure that no one person possesses all the necessary steps for carrying out important tasks. It is a way of spreading the knowledge. A company is at risk if it relies too heavily on one employee for critical functions.

37、 A .Capability Maturity Model (CMM) describes procedures, principles, and practices that underline software process maturity. This model was developed to help software vendors improve their development processes by providing an evolutionary path from an ad hoc, "fly by the seat of your pants," approach to a more disciplined and repeatable approach that improves software quality, reduces the life cycle of development, provides better project management capabilities, allows for milestones to be created and met in a timely manner, and takes a more proactive approach versus the less effective reactive approach.

38、 B .There are five maturity levels:

1. Initial — Development process is ad hoc or even chaotic. The company does not use effective management procedures and plans. No assurance of consistency and quality is unpredictable.

2. Repeatable — A formal management structure, change control, and quality assurance is in place. The company can properly repeat processes throughout each project. The company does not have a formal process model defined.

3. Defined — Formal procedures are in place that outline and define the processes carried out in each project. The organization has a way to allow for quantitative process improvement.

4. Managed — The company has formal processes in place to collect and analyze qualitative data and metrics are defined and fed into the process improvement program.

5. Optimizing — The company has budgeted and integrated plans for continuous process improvement.

39、 D .Software escrow means that there is a third party involved. This third party will keep a copy of the source code, and possibly other materials, which will only be released to the customer if specific circumstances arrive, mainly if the vendor who developed the code goes out of business or for some reason is not meeting its obligations and responsibilities.

This is put into place to protect the company, because it has paid for this source code to be developed.

40、 D .The ACID test concept should be incorporated into the software of a database. ACID

means:

• Atomicity - Divides transactions into units of work and ensures that either all modifications take effect or none take effect. The changes are either committed or the database is rolled back.

• Consistency — A transaction must follow the integrity policy developed for that particular database and ensure that all data is consistent in the different databases.

• Isolation — Transactions execute in isolation until completed, without interacting with other transactions. The results of the modification are not available until the transaction is completed.

• Durability — Once the transaction is verified as accurate on all systems it is committed and the databases cannot be rolled back.

41、 C .Waterfall is a classical method that uses discrete phases of development requiring formal reviews and documentation before moving into the next phase of the project.

42、 B .An object-oriented database is more dynamic in nature when compared to a relational database because objects can be created when needed and the data and procedure go with the object when it is requested.

In a relational database an application uses its procedures to obtain data from the database; the database does not actually provide procedures as object-oriented databases do.

The object-oriented database has classes to define the attributes and procedures of its objects.

43、 B .A cohesive module does just one function, and it does it with little interaction from other modules. The more a module can do on its own, the better, because requiring a lot of interaction between modules makes it harder to modify one module later without affecting other modules.

The lower the coupling, the better the software design, because it promotes module independence.

High cohesion results in low coupling and low cohesion results in high coupling.

44、 B .Computer-aided software engineering (CASE) tools are broad and far reaching in functionality and uses. CASE tools is a general term for many types of automated tools used by programmers, developers, project managers, and analysts that help them make program applications more quickly and with fewer errors and run the project in a controlled and organized manner.

45、 C .Enterprise JavaBeans (EJB) is a structural design for the development and implementation of distributed applications written in Java. EJB provides interfaces and methods to allow different applications to communicate across a networked environment.

Java is a multiplatform language. The applications are not tied to specific protocols.

46、 C .An EICAR test is done with antivirus software by introducing a benign virus to test detection and reaction activities of the software.

47、 A .Rule-based programming is the basis for expert systems. A list of "if/then" statements is supplied to the system and it uses an inference engine to identify patterns and establish rules for the computer to follow.

48、 D .Fraggle is an attack similar to smurf, but instead of using ICMP, it uses User Datagram Protocol (UDP) as its transport protocol. The attacker broadcasts a spoofed UDP packet to the amplifying network, which in turn replies to the victim's system. The larger the amplifying network, the larger the amount of traffic that is pointed at the victim's system.

49、 A .The cleanroom development model is used to create critical applications. Strict testing procedures are followed throughout this approach to ensure no mistakes are made. This model is used to provide a very high quality product.

50、 A .Object linking and embedding (OLE) provides a way for objects to be shared on a local personal computer and use COM as its foundation base. OLE enables objects to be embedded into documents—like graphics, pictures, and spreadsheets.

The capability for one program to call another program is linking. The capability to place an object inside a foreign document is embedding.

51、 D .A polymorphic virus will reproduce like all viruses, but it will modify its children with the hopes that at least some of the children's (or copies') signatures will not be the same as the signature in the antivirus software product. The goal is self-preservation.

52、A .A distributed denial-of-service attack (DDoS) involves a master/zombie relationship where an attacker gains control of the zombie computer and uses it to execute attack commands. The zombie computer becomes such by allowing the attacker to install compromising software on it. The software will, in turn, be used when it is called on to attack a specific victim.

53、 B .Data warehouses combine and process data from multiple databases and data sources and present the information in useful ways for analytical and reporting needs. Data is normalized, meaning redundancies are stripped out, and then the data is usually mined to uncover relationships and patterns.

54、 C .Data mining helps to identify unusual or hidden patterns and relationships within databases. The results are represented to the user in a form called metadata. Metadata is data about data.

55、 B .Artificial neural network (ANN) is a computer network that mimics the functionality of the brain. It has units that mimic neurons and that attempt to simulate thought so that it can learn from different experiences. The more that the ANN can learn, the better results it can present to the users of the system.

56、 C .Checkpoints save data to ensure that the least amount of data will be lost in the event of a system or application failure.

57、 B .Databases use primary keys to track records and to relate them to other records. All the data that is within one row is referred to as a record and they are all linked to one value, which is the primary key. Each row has to have a unique primary key, and the primary key cannot have a null value.

58、 A .Expert systems use artificial intelligence and nonnumeric algorithms to solve complex problems that require human intelligence and intuition to solve. Expert systems can be used to provide intrusion detection capabilities by identifying patterns in network traffic and security logs.

59、 D .Relational databases are the most popular type of database and use two-dimensional tables to store data. Each row has a unique primary key, and relationships between records are made by linking these primary keys in some way.

60、 D .ActiveX controls are software components and are digitally signed to prove where they came from and who developed them. ActiveX is platform dependent, meaning it runs only on Windows-based systems, and language independent, meaning the controls can be written in any programming language. Java uses bytecode and sandboxes; ActiveX does not.

61、 C .Java applets are downloaded to a user's browser and converted from bytecode into machine-level code specific to that computer's CPU and platform. Applets have limited access to system resources because they are controlled within a virtual machine called a sandbox.

62、 B .Teardrop attacks take advantage of weaknesses in some computer systems that are not able to handle packets not fragmented properly. Most of today's systems are no longer vulnerable to this type of attack.

63、 C .SYN attacks use up system resources by sending multiple communication requests to a computer until it can no longer process future communication requests. This is one example of a denial-of-service attack.

64、 A .The accreditation process is the formal management approval of a system and the protection level it provides. Accreditation comes after the certification process.

65、 C .The system design specifications phase involves mapping components and procedures at a more granular level. The design phase provides a higher-level look and analysis of the project

and product.

66、 D .Open Database Connectivity (ODBC) is a standard that allows different types of applications to communicate with different types of databases. The applications send requests to the ODBC and it finds the necessary driver and sends the request to the database.

67、 A .Hierarchical databases use tree structures and are useful when mapping one-to-many relationships. The database has parent data elements, which can have none, one, or several child data elements underneath it.

68、 B .The Testing/Validation phase is when informal and formal testing begins. Programmers should not be the only ones testing their code. A totally different department, usually quality assurance, should perform extensive testing also.

69、 C .Computer-aided software engineering (CASE) tools are useful to software developers by providing automation and increased speed of development procedures. CASE tools usually aid individuals by performing the redundant tasks that programmers, project managers, or analysts have to perform for each project.

70、 D .Object-oriented programming (OOP) improves efficiency, reduces complexity, and saves time and money when compared with the classical way of programming. This approach allows developers to create objects that can be reused in different instances and different environments.

71、 C .Distributed Component Object Model (DCOM) is an architecture that allows objects within the different systems to communicate. It uses globally unique identifiers (GUIDs) to keep track of objects.

72、 A .HTTP is not a stateful protocol, meaning that it cannot remember individual users or connections. Cookies can be used to keep state on connections and are often used on web sites and for electronic transactions. Cookies may be persistent, meaning they stay on the user's hard drive, or may be dynamic and session-oriented, meaning they are destroyed when a session ends. If cookies store sensitive data, their contents should be encrypted.

73、 B .A rollback is a defense mechanism when the database experiences specific problems. If a glitch or disruption is experienced, the database returns to a state in time when it knew that things were stable. It does not save the information that the user was using or inputting into the system because it cannot be sure if it actually received all changes and that the changes did not get corrupted.

74、 D .A pseudo-flaw is code inserted into an application or operating system with the sole purpose of trapping intruders who break into these systems.

75、 C .Software escrow is a service provided by a third party. When a company pays another

company to develop software for them, a copy of all source code is stored by this third party, which is referred to as software escrow. If the software development company goes out of business, the paying customer will still have access to their product, the source code. The third party is paid for this service, and there are a lot of legal issues involving the exact type of service they will provide.

76、 C .Trusted paths, data classifications, and possible Trojan horse vulnerabilities are part of the actual design of a system. The design of a system determines the level of integrity, confidentiality, and overall protection that the system can actually provide.

77、 B .Expert systems use knowledge bases, which is a large amount of data extracted from experts within a specific field. They also have inference engines, which create metadata from the data held within the knowledge base. The systems also use rule-based programming, which is made up of "if/then" statements. A knowledge base engineer and subject matter expert work to fill the knowledge base with the necessary information that will be called upon by future users.

78、 A .A smurf attack is when an attacker spoofs an ICMP broadcast packet and sends them to a network. This ICMP broadcast is sent to all systems on the network segment where the victim is located, and all nodes respond to the source address within the packet, which is the victim. This results in a DoS attack and can bring down the victim's system. The amplifying network is all the systems on the victim's local network segment.

79、 A .Polyinstantiation is when one object is copied and the attributes of the second object are modified. Many times the copy of the object is also assigned a different security classification. This is done so that someone with a top secret clearance, for example, can read the data held within the original object. A person who has a secret clearance may then only have access to the second object, which has different information. This protects the confidentiality of information at higher levels of security.

80、 D .Aggregation is the act of gathering available information from different sources, and inference is putting that data together and figuring out information that is not explicitly available. For example, if a user has access to only four fields in a ten-field database, she might access the data elements in those four fields, and infer from that information what is held in one or more of the other six fields.

81、 B .This type of trapdoor is usually invoked by a series of keystrokes or commands that will allow the programmer easy access to the program at a later date. Easter eggs are typically harmless code within programs that developers insert into the program for the sake of entertaining curious geeks. A trapdoor may also be called a maintenance hook.

82、 A .Production code should not be modified by developers in any way. This goes against proper change control, can break other components in production, and can disrupt the standardization of code in production across the board.

83、 D .A logic bomb contains code that performs an action triggered by a specific event or condition.

84、 B .Testing should be done by a different person or department to ensure that it is done objectively. Programmers should test their code, but so should another party.

85、 C .Aggregation is the act of reviewing information at or below a specific security clearance and then deducing information that resides at a higher level that the user is not authorized to know.

86、 D .High-level and assembly language cannot be directly understood by a CPU; it must first be compiled into machine language, which is expressed in binary values.

87、 A .In object-oriented programming, objects have a clear set of interfaces that other objects interact with. The other objects only need to know how to communicate to these interfaces, which reduces the complexity. This means that objects do not need to know or understand how another object works internally to be able to communicate with it.

88、 D .Assemblers turn assembly language into machine code, interpreters translate single commands from source code into object code, and compilers turn an entire set of source code into object code. Source code is turned into an intermediate code (object code), which is then turned into machine code. Assemblers translate directly to machine code.

89、 A .Java's claim to fame is that when compiled, it can be run anywhere, assuming a Java Virtual Machine is available on the client.

90、 B .A smurf attack involves spoofing the source IP address in a packet header, and then using it to bombard the victim's network with ICMP ECHO REQUESTs. The victim's network works as the amplifying network to increase the power of the attack.

91、 A .Entity integrity is a rule in relational databases that dictates that each row must contain a unique primary key and that the primary key does not point to a null value.

92、 D .The three types of attacks that fall under the umbrella of timing attacks are between the lines, NAK, and line disconnect.

93、 B .An EICAR test is used to test the configurations of an antivirus software package. Most antivirus products come with a benign file that the product will identify as a virus, the administrator can verify that the correct configurations have been made to treat the virus as needed, and the product will properly carry out some type of notification.

94、 C .The CMM model provides policies, procedures, and best practices to allow companies to develop proper software development processes. It is made up of five different maturity levels, one of which the company achieves when it is audited and evaluated against this model.

95、 A .The code repository, which is typically a version control system, is used to ensure that code is not changed or altered in any fashion without strict control procedures. These procedures involve checking code out of the code repository, and formally checking it back in, as well as strict documentation and approval of changes.

96、 B .Air gapping the development, test, and production environments ensures that code is protected and separated from the different stages of development.

97、 D .During acceptance testing, the customer accepts or rejects the code base before it is implemented.

98、 D .While penetration testing is an effective means of determining if vulnerabilities can be exploited, it does not examine the overall security impact of acquired software in terms of risk to the organization.

99、 A .During the design phase, both attack surface analysis and threat modeling are used to further assess the security impact of developed software

100、 C .The application programming interface (API) specifies the manner in which a software component interacts and communicates with other software components or objects.