1. Alyssa is responsible for her organization's security awareness program. She is concerned that changes in technology may make the content outdated. What control can she put in place to protect against this risk?
   - **A.** Gamification
   - **B.** Computer-based training
   - **C.** Content reviews
   - **D.** Live training

2. Gavin is creating a report to management on the results of his most recent risk assessment. In his report, he would like to identify the remaining level of risk to the organization after adopting security controls. What term best describes this current level of risk?
   - **A.** Inherent risk
   - **B.** Residual risk
   - **C.** Control risk
   - **D.** Mitigated risk

3. Francine is a security specialist for an online service provider in the United States. She recently received a claim from a copyright holder that a user is storing information on her service that violates the third party's copyright. What law governs the actions that Francine must take?
   - **A.** Copyright Act
   - **B.** Lanham Act
   - **C.** Digital Millennium Copyright Act
   - **D.** Gramm Leach Bliley Act

4. FlyAway Travel has offices in both the European Union (EU) and the United States and transfers personal information between those offices regularly. They have recently received a request from an EU customer requesting that their account be terminated. Under the General Data Protection Regulation (GDPR), which requirement for processing personal information states that individuals may request that their data no longer be disseminated or processed?
   - **A.** The right to access
   - **B.** Privacy by design
   - **C.** The right to be forgotten
   - **D.** The right of data portability

5. After conducting a qualitative risk assessment of her organization, Sally recommends purchasing cybersecurity breach insurance. What type of risk response behavior is she recommending?
   - **A.** Accept
   - **B.** Transfer
   - **C.** Reduce
   - **D.** Reject

6. Which one of the following elements of information is not considered personally identifiable information that would trigger most United States (U.S.) state data breach laws?
   - **A.** Student identification number
   - **B.** Social Security number
   - **C.** Driver's license number
   - **D.** Credit card number

7. Renee is speaking to her board of directors about their responsibilities to review cybersecurity controls. What rule requires that senior executives take personal responsibility for information security matters?
   - **A.** Due diligence rule
   - **B.** Personal liability rule
   - **C.** Prudent man rule
   - **D.** Due process rule

8. Henry recently assisted one of his co-workers in preparing for the CISSP exam. During this process, Henry disclosed confidential information about the content of the exam, in violation of Canon IV of the Code of Ethics: "Advance and protect the profession." Who may bring ethics charges against Henry for this violation?
   - **A.** Anyone may bring charges.
   - **B.** Any certified or licensed professional may bring charges.
   - **C.** Only Henry's employer may bring charges.
   - **D.** Only the affected employee may bring charges.

9. Wanda is working with one of her organization's European Union business partners to facilitate the exchange of customer information. Wanda's organization is located in the United States. What would be the best method for Wanda to use to ensure GDPR compliance?
   - **A.** Binding corporate rules
   - **B.** Privacy Shield
   - **C.** Standard contractual clauses
   - **D.** Safe harbor

10. Yolanda is the chief privacy officer for a financial institution and is researching privacy requirements related to customer checking accounts. Which one of the following laws is most likely to apply to this situation?
    - **A.** GLBA
    - **B.** SOX
    - **C.** HIPAA
    - **D.** FERPA

11. Tim's organization recently received a contract to conduct sponsored research as a government contractor. What law now likely applies to the information systems involved in this contract?

A. FISMA

B. PCI DSS

C. HIPAA

D. GISRA

12. Chris is advising travelers from his organization who will be visiting many different countries overseas. He is concerned about compliance with export control laws. Which of the following technologies is most likely to trigger these regulations?

A. Memory chips

B. Office productivity applications

C. Hard drives

D. Encryption software

13. Bobbi is investigating a security incident and discovers that an attacker began with a normal user account but managed to exploit a system vulnerability to provide that account with administrative rights. What type of attack took place under the STRIDE threat model?

A. Spoofing

B. Repudiation

C. Tampering

D. Elevation of privilege

14. You are completing your business continuity planning effort and have decided that you want to accept one of the risks. What should you do next?

A. Implement new security controls to reduce the risk level.

B. Design a disaster recovery plan.

C. Repeat the business impact assessment.

D. Document your decision-making process.

15. You are completing a review of the controls used to protect a media storage facility in your organization and would like to properly categorize each control that is currently in place. Which of the following control categories accurately describe a fence around a facility? (Select all that apply.)

A. Physical

B. Detective

C. Deterrent

D. Preventive

16. Tony is developing a business continuity plan and is having difficulty prioritizing resources because of the difficulty of combining information about tangible and intangible assets. What would be the most effective risk assessment approach for him to use?

A. Quantitative risk assessment

B. Qualitative risk assessment

C. Neither quantitative nor qualitative risk assessment

D. Combination of quantitative and qualitative risk assessment

17. Vincent believes that a former employee took trade secret information from his firm and brought it with him to a competitor. He wants to pursue legal action. Under what law could he pursue charges?

A. Copyright law

B. Lanham Act

C. Glass-Steagall Act

D. Economic Espionage Act

18. Which one of the following principles imposes a standard of care upon an individual that is broad and equivalent to what one would expect from a reasonable person under the circumstances?

A. Due diligence

B. Separation of duties

C. Due care

D. Least privilege

19. Brenda's organization recently completed the acquisition of a competitor firm. Which one of the following tasks would be LEAST likely to be part of the organizational processes addressed during the acquisition?

A. Consolidation of security functions

B. Integration of security tools

C. Protection of intellectual property

D. Documentation of security policies

20. Kelly believes that an employee engaged in the unauthorized use of computing resources for a side business. After consulting with management, she decides to launch an administrative investigation. What is the burden of proof that she must meet in this investigation?

A. Preponderance of the evidence

B. Beyond a reasonable doubt

C. Beyond the shadow of a doubt

D. There is no standard

21. Keenan Systems recently developed a new manufacturing process for microprocessors. The company wants to license the technology to other companies for use but wants to prevent unauthorized use of the technology. What type of intellectual property protection is best suited for this situation?

A. Patent

B. Trade secret

C. Copyright

D. Trademark

22. Which one of the following actions might be taken as part of a business continuity plan?

A. Restoring from backup tapes

B. Implementing RAID

C. Relocating to a cold site

D. Restarting business operations

23. When developing a business impact analysis, the team should first create a list of assets. What should happen next?

A. Identify vulnerabilities in each asset.

B. Determine the risks facing the asset.

C. Develop a value for each asset.

D. Identify threats facing each asset.

24. Mike recently implemented an intrusion prevention system designed to block common network attacks from affecting his organization. What type of risk management strategy is Mike pursuing?

A. Risk acceptance

B. Risk avoidance

C. Risk mitigation

D. Risk transference

25. Laura has been asked to perform an SCA. What type of organization is she most likely in?

A. Higher education

B. Banking

C. Government

D. Healthcare

26. Carl is a federal agent investigating a computer crime case. He identified an attacker who engaged in illegal conduct and wants to pursue a case against that individual that will lead to imprisonment. What standard of proof must Carl meet?

A. Beyond the shadow of a doubt

B. Preponderance of the evidence

C. Beyond a reasonable doubt

D. Majority of the evidence

27. The International Information Systems Security Certification Consortium uses the logo shown here to represent itself online and in a variety of forums. What type of intellectual property protection may it use to protect its rights in this logo?

A. Copyright

B. Patent

C. Trade secret

D. Trademark

28. Mary is helping a computer user who sees the following message appear on his computer screen. What type of attack has occurred?

A. Availability
B. Confidentiality
C. Disclosure
D. Distributed

29. Which one of the following organizations would not be automatically subject to the privacy and security requirements of HIPAA if they engage in electronic transactions?
A. Healthcare provider
B. Health and fitness application developer
C. Health information clearinghouse
D. Health insurance plan

30. John's network begins to experience symptoms of slowness. Upon investigation, he realizes that the network is being bombarded with TCP SYN packets and believes that his organization is the victim of a denial-of-service attack. What principle of information security is being violated?
A. Availability
B. Integrity
C. Confidentiality
D. Denial

31. Renee is designing the long-term security plan for her organization and has a three- to five-year planning horizon. Her primary goal is to align the security function with the broader plans and objectives of the business. What type of plan is she developing?
A. Operational
B. Tactical
C. Summary
D. Strategic

32. Gina is working to protect a logo that her company will use for a new product they are launching. She has questions about the intellectual property protection process for this logo. What U.S. government agency would be best able to answer her questions?
A. USPTO
B. Library of Congress
C. NSA
D. NIST

33. The Acme Widgets Company is putting new controls in place for its accounting department. Management is concerned that a rogue accountant may be able to create a new false vendor and then issue checks to that vendor as payment for services that were never rendered. What security control can best help prevent this situation?
A. Mandatory vacation
B. Separation of duties
C. Defense in depth
D. Job rotation

34. Which one of the following categories of organizations is most likely to be covered by the provisions of FISMA?

A. Banks

B. Defense contractors

C. School districts

D. Hospitals

35. Robert is responsible for securing systems used to process credit card information. What security control framework should guide his actions?

A. HIPAA

B. PCI DSS

C. SOX

D. GLBA

36. Which one of the following individuals is normally responsible for fulfilling the operational data protection responsibilities delegated by senior management, such as validating data integrity, testing backups, and managing security policies?

A. Data custodian

B. Data owner

C. User

D. Auditor

37. Alan works for an e-commerce company that recently had some content stolen by another website and republished without permission. What type of intellectual property protection would best preserve Alan's company's rights?

A. Trade secret

B. Copyright

C. Trademark

D. Patent

38. Florian receives a flyer from a U.S. federal government agency announcing that a new administrative law will affect his business operations. Where should he go to find the text of the law?

A. United States Code

B. Supreme Court rulings

C. Code of Federal Regulations

D. Compendium of Laws

39. Tom enables an application firewall provided by his cloud infrastructure as a service provider that is designed to block many types of application attacks. When viewed from a risk management perspective, what metric is Tom attempting to lower by implementing this countermeasure?

A. Impact

B. RPO

C. MTO

D. Likelihood

40. Which one of the following individuals would be the most effective organizational owner for an information security program?

A. CISSP-certified analyst

B. Chief information officer (CIO)

C. Manager of network security

D. President and CEO

41. What important function do senior managers normally fill on a business continuity planning team?

A. Arbitrating disputes about criticality

B. Evaluating the legal environment

C. Training staff

D. Designing failure controls

42. You are the CISO for a major hospital system and are preparing to sign a contract with a software as a service (SaaS) email vendor and want to perform a control assessment to ensure that its business continuity planning measures are reasonable. What type of audit might you request to meet this goal?

A. SOC 1

B. FISMA

C. PCI DSS

D. SOC 2

43. Gary is analyzing a security incident and, during his investigation, encounters a user who denies having performed an action that Gary believes he did perform. What type of threat has taken place under the STRIDE model?

A. Repudiation

B. Information disclosure

C. Tampering

D. Elevation of privilege

44. Beth is the security administrator for a public school district. She is implementing a new student information system and is testing the code to ensure that students are not able to alter their own grades. What principle of information security is Beth enforcing?

A. Integrity

B. Availability

C. Confidentiality

D. Denial

45. Which one of the following issues is not normally addressed in a service-level agreement (SLA)?

A. Confidentiality of customer information

B. Failover time

C. Uptime

D. Maximum consecutive downtime

46. Joan is seeking to protect a piece of computer software that she developed under intellectual property law. Which one of the following avenues of protection would not apply to a piece of software?

A. Trademark

B. Copyright

C. Patent

D. Trade secret

For questions 47–49, please refer to the following scenario:

Juniper Content is a web content development company with 40 employees located in two offices: one in New York and a smaller office in the San Francisco Bay Area. Each office has a local area network protected by a perimeter firewall. The local area network (LAN) contains modern switch equipment connected to both wired and wireless networks.

Each office has its own file server, and the information technology (IT) team runs software every hour to synchronize files between the two servers, distributing content between the offices. These servers are primarily used to store images and other files related to web content developed by the company. The team also uses a SaaS-based email and document collaboration solution for much of their work.

You are the newly appointed IT manager for Juniper Content, and you are working to augment existing security controls to improve the organization's security.

47. Users in the two offices would like to access each other's file servers over the internet. What control would provide confidentiality for those communications?

A. Digital signatures

B. Virtual private network

C. Virtual LAN

D. Digital content management

48. You are also concerned about the availability of data stored on each office's server. You would like to add technology that would enable continued access to files located on the server even if a hard drive in a server fails. What control allows you to add robustness without adding additional servers?

A. Server clustering

B. Load balancing

C. RAID

D. Scheduled backups

49. Finally, there are historical records stored on the server that are extremely important to the business and should never be modified. You would like to add an integrity control that allows you to verify on a periodic basis that the files were not modified. What control can you add?

A. Hashing

B. ACLs

C. Read-only attributes

D. Firewalls

50. Beth is a human resources specialist preparing to assist in the termination of an employee. Which of the following is not typically part of a termination process?

A. An exit interview

B. Recovery of property

C. Account termination

D. Signing an NCA

51. Frances is reviewing her organization's business continuity plan documentation for completeness. Which one of the following is not normally included in business continuity plan documentation?

A. Statement of accounts

B. Statement of importance

C. Statement of priorities

D. Statement of organizational responsibility

52. An accounting employee at Doolittle Industries was recently arrested for participation in an embezzlement scheme. The employee transferred money to a personal account and then shifted funds around between other accounts every day to disguise the fraud for months. Which one of the following controls might have best allowed the earlier detection of this fraud?

A. Separation of duties

B. Least privilege

C. Defense in depth

D. Mandatory vacation

53. Jeff would like to adopt an industry-standard approach for assessing the processes his organization uses to manage risk. What maturity model would be most appropriate for his use?

A. CMM

B. SW-CMM

C. RMM

D. COBIT

54. Chris' organization recently suffered an attack that rendered their website inaccessible to paying customers for several hours. Which information security goal was most directly impacted?

A. Confidentiality

B. Integrity

C. Availability

D. Denial

55. Yolanda is writing a document that will provide configuration information regarding the minimum level of security that every system in the organization must meet. What type of document is she preparing?

A. Policy

B. Baseline

C. Guideline

D. Procedure

56. Who should receive initial business continuity plan training in an organization?

A. Senior executives

B. Those with specific business continuity roles

C. Everyone in the organization

D. First responders

57. James is conducting a risk assessment for his organization and is attempting to assign an asset value to the servers in his data center. The organization's primary concern is ensuring that it has sufficient funds available to rebuild the data center in the event it is damaged or destroyed. Which one of the following asset valuation methods would be most appropriate in this situation?

A. Purchase cost

B. Depreciated cost

C. Replacement cost

D. Opportunity cost

58. Roger's organization suffered a breach of customer credit card records. Under the terms of PCI DSS, what organization may choose to pursue an investigation of this matter?

A. FBI

B. Local law enforcement

C. Bank

D. PCI SSC

59. Rick recently engaged critical employees in each of his organization's business units to ask for their assistance with his security awareness program. They will be responsible for sharing security messages with their peers and answering questions about cybersecurity matters. What term best describes this relationship?

A. Security champion

B. Security expert

C. Gamification

D. Peer review

60. Frank discovers a keylogger hidden on the laptop of his company's chief executive officer. What information security principle is the keylogger most likely designed to disrupt?

A. Confidentiality

B. Integrity

C. Availability

D. Denial

61. Elise is helping her organization prepare to evaluate and adopt a new cloud-based human resource management (HRM) system vendor. What would be the most appropriate minimum security standard for her to require of possible vendors?

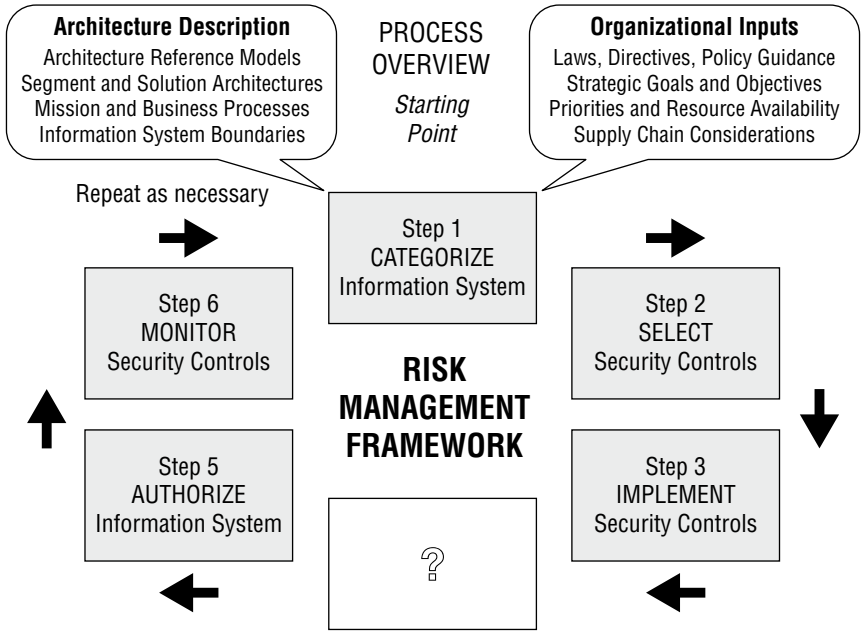
A. Compliance with all laws and regulations

B. Handling information in the same manner the organization would

C. Elimination of all identified security risks

D. Compliance with the vendor's own policies

62. The following graphic shows the NIST risk management framework with step 4 missing. What is the missing step?



A. Assess security controls.

B. Determine control gaps.

C. Remediate control gaps.

D. Evaluate user activity.

63. HAL Systems recently decided to stop offering public NTP services because of a fear that its NTP servers would be used in amplification DDoS attacks. What type of risk management strategy did HAL pursue with respect to its NTP services?

A. Risk mitigation

B. Risk acceptance

C. Risk transference

D. Risk avoidance

64. Susan is working with the management team in her company to classify data in an attempt to apply extra security controls that will limit the likelihood of a data breach. What principle of information security is Susan trying to enforce?

A. Availability

B. Denial

C. Confidentiality

D. Integrity

65. Which one of the following components should be included in an organization's emergency response guidelines?

A. List of individuals who should be notified of an emergency incident

B. Long-term business continuity protocols

C. Activation procedures for the organization's cold sites

D. Contact information for ordering equipment

66. Chas recently completed the development of his organization's business continuity plan. Who is the ideal person to approve an organization's business continuity plan?

A. Chief information officer

B. Chief executive officer

C. Chief information security officer

D. Chief operating officer

67. Which one of the following actions is not normally part of the project scope and planning phase of business continuity planning?

A. Structured analysis of the organization

B. Review of the legal and regulatory landscape

C. Creation of a BCP team

D. Documentation of the plan

68. Gary is implementing a new website architecture that uses multiple small web servers behind a load balancer. What principle of information security is Gary seeking to enforce?

A. Denial

B. Confidentiality

C. Integrity

D. Availability

69. Becka recently signed a contract with an alternate data processing facility that will provide her company with space in the event of a disaster. The facility includes HVAC, power, and communications circuits but no hardware. What type of facility is Becka using?

A. Cold site

B. Warm site

C. Hot site

D. Mobile site

70. Greg's company recently experienced a significant data breach involving the personal data of many of their customers. Which breach laws should they review to ensure that they are taking appropriate action?

A. The breach laws in the state where they are headquartered.

B. The breach laws of states they do business in.

C. Only federal breach laws.

D. Breach laws only cover government agencies, not private businesses.

71. Ben is seeking a control objective framework that is widely accepted around the world and focuses specifically on information security controls. Which one of the following frameworks would best meet his needs?

A. ITIL

B. ISO 27002

C. CMM

D. PMBOK Guide

72. Matt works for a telecommunications firm and was approached by a federal agent seeking assistance with wiretapping one of Matt's clients pursuant to a search warrant. Which one of the following laws requires that communications service providers cooperate with law enforcement requests?

A. ECPA

B. CALEA

C. Privacy Act

D. HITECH Act

73. Every year, Gary receives privacy notices in the mail from financial institutions where he has accounts. What law requires the institutions to send Gary these notices?

A. FERPA

B. GLBA

C. HIPAA

D. HITECH

74. Which one of the following agreements typically requires that a vendor not disclose confidential information learned during the scope of an engagement?

A. NCA

B. SLA

C. NDA

D. RTO

75. The (ISC)² Code of Ethics applies to all CISSP holders. Which of the following is not one of the four mandatory canons of the code?

A. Protect society, the common good, the necessary public trust and confidence, and the infrastructure.

B. Disclose breaches of privacy, trust, and ethics.

C. Provide diligent and competent service to the principles.

D. Advance and protect the profession.

76. Which one of the following stakeholders is not typically included on a business continuity planning team?

A. Core business function leaders

B. Information technology staff

C. CEO

D. Support departments

77. Ben is designing a messaging system for a bank and would like to include a feature that allows the recipient of a message to prove to a third party that the message did indeed come from the purported originator. What goal is Ben trying to achieve?

A. Authentication

B. Authorization

C. Integrity

D. Nonrepudiation

78. What principle of information security states that an organization should implement overlapping security controls whenever possible?

A. Least privilege

B. Separation of duties

C. Defense in depth

D. Security through obscurity

79. Ryan is a CISSP-certified cybersecurity professional working in a nonprofit organization. Which of the following ethical obligations apply to his work? (Select all that apply.)

A. (ISC)² Code of Ethics

B. Organizational code of ethics

C. Federal code of ethics

D. RFC 1087

80. Ben is responsible for the security of payment card information stored in a database. Policy directs that he remove the information from the database, but he cannot do this for operational reasons. He obtained an exception to policy and is seeking an appropriate compensating control to mitigate the risk. What would be his best option?

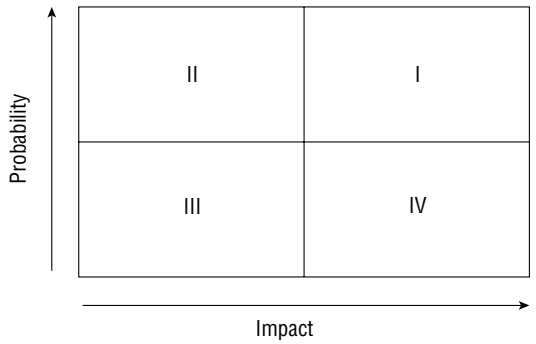
A. Purchasing insurance

B. Encrypting the database contents

C. Removing the data

D. Objecting to the exception

81. The Domer Industries risk assessment team recently conducted a qualitative risk assessment and developed a matrix similar to the one shown here. Which quadrant contains the risks that require the most immediate attention?



A. I

B. II

C. III

D. IV

82. Tom is planning to terminate an employee this afternoon for fraud and expects that the meeting will be somewhat hostile. He is coordinating the meeting with human resources and wants to protect the company against damage. Which one of the following steps is most important to coordinate in time with the termination meeting?

A. Informing other employees of the termination

B. Retrieving the employee's photo ID

C. Calculating the final paycheck

D. Revoking electronic access rights

83. Rolando is a risk manager with a large-scale enterprise. The firm recently evaluated the risk of California mudslides on its operations in the region and determined that the cost of responding outweighed the benefits of any controls it could implement. The company

chose to take no action at this time. What risk management strategy did Rolando's organization pursue?

A. Risk avoidance

B. Risk mitigation

C. Risk transference

D. Risk acceptance

84. Helen is the owner of a U.S. website that provides information for middle and high school students preparing for exams. She is writing the site's privacy policy and would like to ensure that it complies with the provisions of the Children's Online Privacy Protection Act (COPPA). What is the cutoff age below which parents must give consent in advance of the collection of personal information from their children under COPPA?

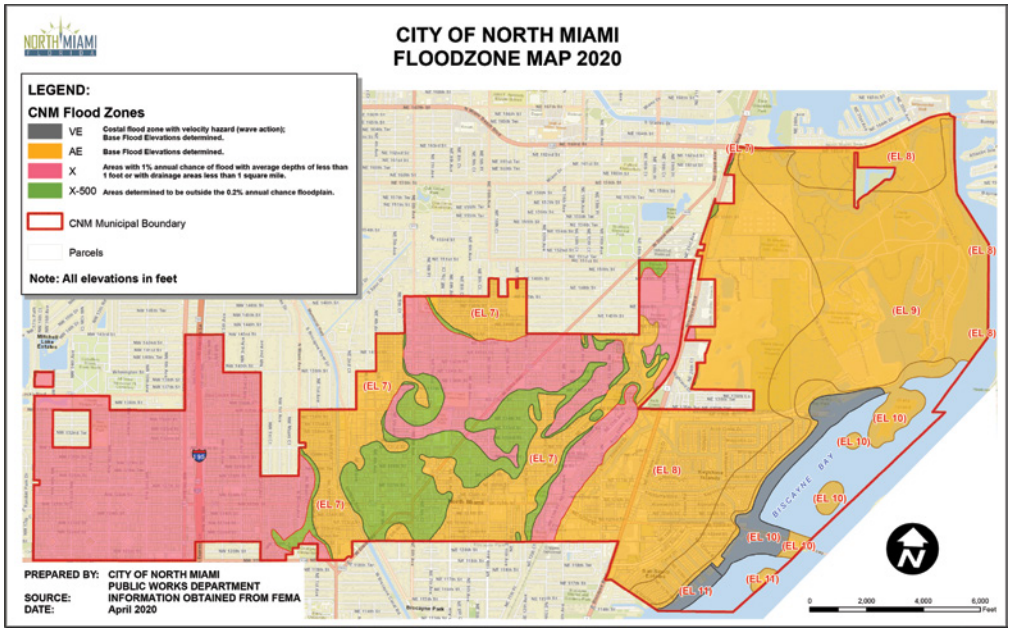
A. 13

B. 15

C. 17

D. 18

85. Tom is considering locating a business in the downtown area of Miami, Florida. He consults the FEMA flood plain map for the region, shown here, and determines that the area he is considering lies within a 100-year flood plain. What is the ARO of a flood in this area?



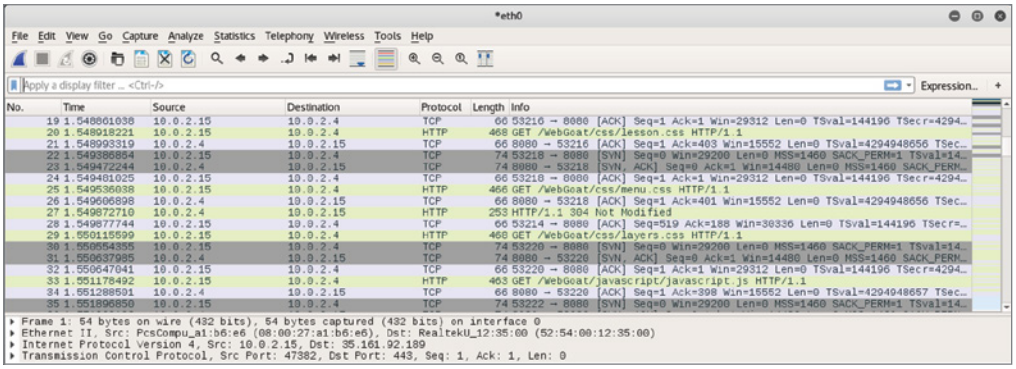
A. 100

B. 1

C. 0.1

D. 0.01

86. You discover that a user on your network has been using the Wireshark tool, as shown here. Further investigation revealed that he was using it for illicit purposes. What pillar of information security has most likely been violated?



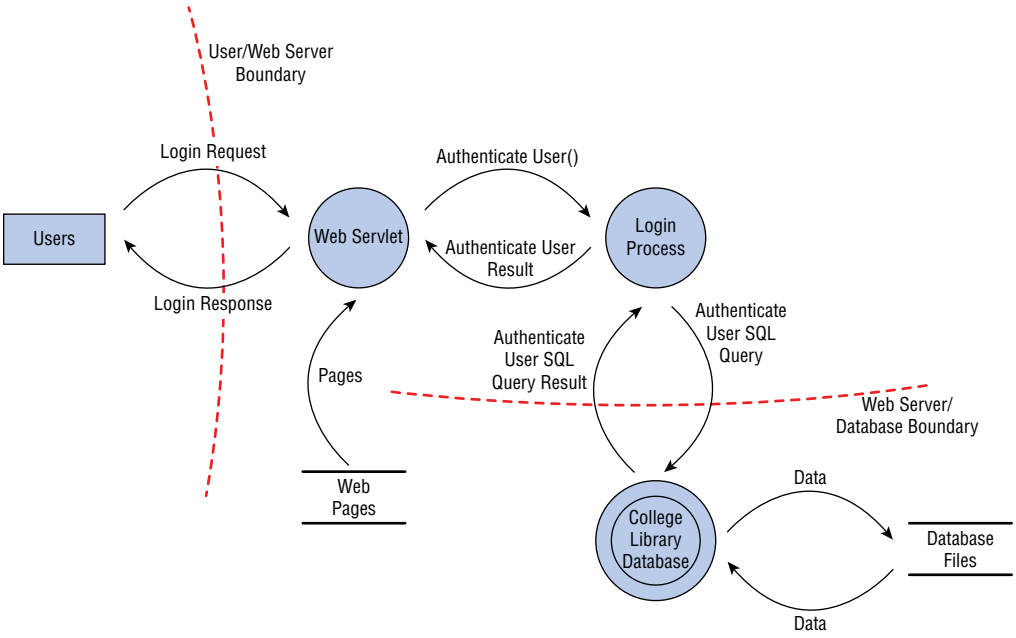
A. Integrity

B. Denial

C. Availability

D. Confidentiality

87. Alan is performing threat modeling and decides that it would be useful to decompose the system into the core elements shown here. What tool is he using?



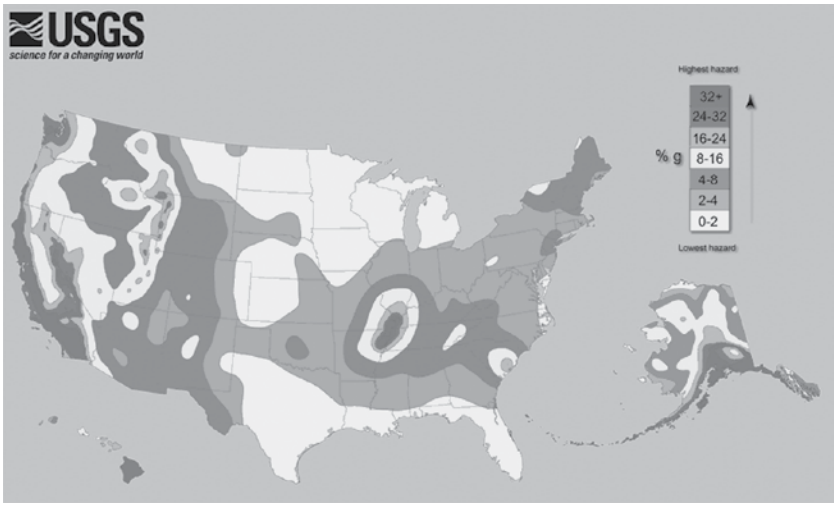
A. Vulnerability assessment

B. Fuzzing

C. Reduction analysis

D. Data modeling

88. Craig is selecting the site for a new data center and must choose a location somewhere within the United States. He obtained the earthquake risk map shown here from the United States Geological Survey. Which of the following would be the safest location to build his facility if he were primarily concerned with earthquake risk?



(Source: US Geological Survey)

A. New York

B. North Carolina

C. Indiana

D. Florida

89. Which type of business impact assessment tool is most appropriate when attempting to evaluate the impact of a failure on customer confidence?

A. Quantitative

B. Qualitative

C. Annualized loss expectancy

D. Reduction

90. Ryan is a security risk analyst for an insurance company. He is currently examining a scenario in which a malicious hacker might use a SQL injection attack to deface a web server due to a missing patch in the company's web application. In this scenario, what is the threat?

A. Unpatched web application

B. Web defacement

C. Malicious hacker

D. Operating system

For questions 91–93, please refer to the following scenario:

Henry is the risk manager for Atwood Landing, a resort community in the midwestern United States. The resort's main data center is located in northern Indiana in an area that is prone to tornados. Henry recently undertook a replacement cost analysis and determined that rebuilding and reconfiguring the data center would cost $10 million.

Henry consulted with tornado experts, data center specialists, and structural engineers. Together, they determined that a typical tornado would cause approximately $5 million of damage to the facility. The meteorologists determined that Atwood's facility lies in an area where they are likely to experience a tornado once every 200 years.

91. Based upon the information in this scenario, what is the exposure factor for the effect of a tornado on Atwood Landing's data center?

A. 10 percent

B. 25 percent

C. 50 percent

D. 75 percent

92. Based upon the information in this scenario, what is the annualized rate of occurrence for a tornado at Atwood Landing's data center?

A. 0.0025

B. 0.005

C. 0.01

D. 0.015

93. Based upon the information in this scenario, what is the annualized loss expectancy for a tornado at Atwood Landing's data center?

A. $25,000

B. $50,000

C. $250,000

D. $500,000

94. John is analyzing an attack against his company in which the attacker found comments embedded in HTML code that provided the clues needed to exploit a software vulnerability. Using the STRIDE model, what type of attack did he uncover?

A. Spoofing

B. Repudiation

C. Information disclosure

D. Elevation of privilege

95. Chris is worried that the laptops that his organization has recently acquired were modified by a third party to include keyloggers before they were delivered. Where should he focus his efforts to prevent this?

A. His supply chain

B. His vendor contracts

C. His post-purchase build process

D. The original equipment manufacturer (OEM)

96. In her role as a developer for an online bank, Lisa is required to submit her code for testing and review. After it passes through this process and it is approved, another employee moves the code to the production environment. What security management does this process describe?

A. Regression testing

B. Code review

C. Change management

D. Fuzz testing

97. After completing the first year of his security awareness program, Charles reviews the data about how many staff completed training compared to how many were assigned the training to determine whether he hit the 95 percent completion rate he was aiming for. What is this type of measure called?

A. A KPI

B. A metric

C. An awareness control

D. A return on investment rate

98. Which of the following is not typically included in a prehire screening process?

A. A drug test

B. A background check

C. Social media review

D. Fitness evaluation

99. Which of the following would normally be considered a supply chain risk? (Select all that apply.)

A. Adversary tampering with hardware prior while being shipped to the end customer

B. Adversary hacking into a web server run by the organization in an IaaS environment

C. Adversary using social engineering to compromise an employee of a SaaS vendor to gain access to customer accounts

D. Adversary conducting a denial-of-service attack using a botnet

100. Match the following numbered laws or industry standards to their lettered description:

Laws and industry standards

1. GLBA A
2. PCI DSS C
3. HIPAA D
4. SOX B

Descriptions

A. A U.S. law that requires covered financial institutions to provide their customers with a privacy notice on a yearly basis

B. A U.S. law that requires internal controls assessments, including IT transaction flows for publicly traded companies

C. An industry standard that covers organizations that handle credit cards

D. A U.S. law that provides data privacy and security requirements for medical information

1. Angela is an information security architect at a bank and has been assigned to ensure that transactions are secure as they traverse the network. She recommends that all transactions use TLS. What threat is she most likely attempting to stop, and what method is she most likely using to protect against it?
   - **A.** Man-in-the-middle, VPN
   - **B.** Packet injection, encryption
   - **C.** Sniffing, encryption
   - **D.** Sniffing, TEMPEST

2. Control Objectives for Information and Related Technology (COBIT) is a framework for information technology (IT) management and governance. Which data management role is most likely to select and apply COBIT to balance the need for security controls against business requirements?
   - **A.** Business owners
   - **B.** Data processors
   - **C.** Data owners
   - **D.** Data stewards

3. Nadia's company is operating a hybrid cloud environment with some on-site systems and some cloud-based systems. She has satisfactory monitoring on-site, but needs to apply security policies to both the activities her users engage in and to report on exceptions with her growing number of cloud services. What type of tool is best suited to this purpose?
   - **A.** A NGFW
   - **B.** A CASB
   - **C.** An IDS
   - **D.** A SOAR

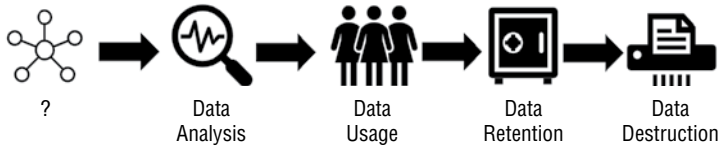
4. When media is labeled based on the classification of the data it contains, what rule is typically applied regarding labels?
   - **A.** The data is labeled based on its integrity requirements.
   - **B.** The media is labeled based on the highest classification level of the data it contains.
   - **C.** The media is labeled with all levels of classification of the data it contains.
   - **D.** The media is labeled with the lowest level of classification of the data it contains.

5. Which one of the following administrative processes assists organizations in assigning appropriate levels of security control to sensitive information?
   - **A.** Data classification
   - **B.** Remanence
   - **C.** Transmitting data
   - **D.** Clearing

6. How can a data retention policy help to reduce liabilities?
   - **A.** By ensuring that unneeded data isn't retained
   - **B.** By ensuring that incriminating data is destroyed
   - **C.** By ensuring that data is securely wiped so it cannot be restored for legal discovery
   - **D.** By reducing the cost of data storage required by law

7. Staff in an information technology (IT) department who are delegated responsibility for day-to-day tasks hold what data role?
   - **A.** Business owner
   - **B.** User
   - **C.** Data processor
   - **D.** Custodian

8. Helen's company uses a simple data lifecycle as shown in the figure here. What stage should come first in their data lifecycle?



   - **A.** Data policy creation
   - **B.** Data labeling
   - **C.** Data collection
   - **D.** Data analysis

9. Ben has been tasked with identifying security controls for systems covered by his organization's information classification system. Why might Ben choose to use a security baseline?
   - **A.** It applies in all circumstances, allowing consistent security controls.
   - **B.** They are approved by industry standards bodies, preventing liability.
   - **C.** They provide a good starting point that can be tailored to organizational needs.
   - **D.** They ensure that systems are always in a secure state.

10. Megan wants to prepare media to allow for its reuse in an environment operating at the same sensitivity level. Which of the following is the best option to meet her needs?
    - **A.** Clearing
    - **B.** Erasing
    - **C.** Purging
    - **D.** Sanitization

11. Mikayla wants to identify data that should be classified that already exists in her environment. What type of tool is best suited to identifying data like Social Security numbers, credit card numbers, and similar well-understood data formats?

A. Manual searching

B. A sensitive data scanning tool

C. An asset metadata search tool

D. A data loss prevention system (DLP)

12. What issue is common to spare sectors and bad sectors on hard drives as well as overprovisioned space on modern SSDs?

A. They can be used to hide data.

B. They can only be degaussed.

C. They are not addressable, resulting in data remanence.

D. They may not be cleared, resulting in data remanence.

13. Naomi knows that commercial data is typically classified based on different criteria than government data. Which of the following is not a common criterion for commercial data classification?

A. Useful lifespan

B. Data value

C. Impact to national security

D. Regulatory or legal requirements

For questions 14–16, please refer to the following scenario:

Your organization regularly handles three types of data: information that it shares with customers, information that it uses internally to conduct business, and trade secret information that offers the organization significant competitive advantages. Information shared with customers is used and stored on web servers, while both the internal business data and the trade secret information are stored on internal file servers and employee workstations.

14. What term best describes data that is resident in system memory?

A. Data at rest

B. Buffered data

C. Data in use

D. Data in motion

15. What technique could you use to mark your trade secret information in case it was released or stolen and you need to identify it?

A. Classification

B. Symmetric encryption

C. Watermarks

D. Metadata

16. What type of encryption is best suited for use on the file servers for the proprietary data, and how might you secure the data when it is in motion?
    - **A.** TLS at rest and AES in motion
    - **B.** AES at rest and TLS in motion
    - **C.** VPN at rest and TLS in motion
    - **D.** DES at rest and AES in motion

17. What does labeling data allow a DLP system to do?
    - **A.** The DLP system can detect labels and apply appropriate protections based on rules.
    - **B.** The DLP system can adjust labels based on changes in the classification scheme.
    - **C.** The DLP system can modify labels to permit requested actions.
    - **D.** The DLP system can delete unlabeled data.

18. Why is it cost effective to purchase high-quality media to contain sensitive data?
    - **A.** Expensive media is less likely to fail.
    - **B.** The value of the data often far exceeds the cost of the media.
    - **C.** Expensive media is easier to encrypt.
    - **D.** More expensive media typically improves data integrity.

19. Chris is responsible for workstations throughout his company and knows that some of the company's workstations are used to handle both proprietary information and highly sensitive trade secrets. Which option best describes what should happen at the end of their life (EOL) for workstations he is responsible for?
    - **A.** Erasing
    - **B.** Clearing
    - **C.** Sanitization
    - **D.** Destruction

20. Fred wants to classify his organization's data using common labels: private, sensitive, public, and proprietary. Which of the following should he apply to his highest classification level based on common industry practices?
    - **A.** Private
    - **B.** Sensitive
    - **C.** Public
    - **D.** Proprietary

21. What scenario describes data at rest?
    - **A.** Data in an IPsec tunnel
    - **B.** Data in an e-commerce transaction
    - **C.** Data stored on a hard drive
    - **D.** Data stored in RAM

22. If you are selecting a security standard for a Windows 10 system that processes credit cards, what security standard is your best choice?
    - **A.** Microsoft's Windows 10 security baseline
    - **B.** The CIS Windows 10 baseline
    - **C.** PCI DSS
    - **D.** The NSA Windows 10 Secure Host Baseline

For questions 23–25, please refer to the following scenario:

The Center for Internet Security (CIS) works with subject matter experts from a variety of industries to create lists of security controls for operating systems, mobile devices, server software, and network devices. Your organization has decided to use the CIS benchmarks for your systems. Answer the following questions based on this decision.

23. The CIS benchmarks are an example of what practice?
    - **A.** Conducting a risk assessment
    - **B.** Implementing data labeling
    - **C.** Proper system ownership
    - **D.** Using security baselines

24. Adjusting the CIS benchmarks to your organization's mission and your specific IT systems would involve what two processes?
    - **A.** Scoping and selection
    - **B.** Scoping and tailoring
    - **C.** Baselining and tailoring
    - **D.** Tailoring and selection

25. How should you determine which controls from the baseline should be applied to a given system or software package?
    - **A.** Consult the custodians of the data.
    - **B.** Select based on the data classification of the data it stores or handles.
    - **C.** Apply the same controls to all systems.
    - **D.** Consult the business owner of the process the system or data supports.

26. The company that Henry works for operates in the EU and collects data about their customers. They send that data to a third party to analyze and provide reports to help the company make better business decisions. What term best describes the third-party analysis company?
    - **A.** The data controller
    - **B.** The data owner
    - **C.** The data subject
    - **D.** The data processor

27. The government defense contractor that Selah works for has recently shut down a major research project and is planning on reusing the hundreds of thousands of dollars of systems and data storage tapes used for the project for other purposes. When Selah reviews the company's internal processes, she finds that she can't reuse the tapes and that the manual says they should be destroyed. Why isn't Selah allowed to degauss and then reuse the tapes to save her employer money?
    - **A.** Data permanence may be an issue.
    - **B.** Data remanence is a concern.
    - **C.** The tapes may suffer from bitrot.
    - **D.** Data from tapes can't be erased by degaussing.

28. Information maintained about an individual that can be used to distinguish or trace their identity is known as what type of information?
    - **A.** Personally identifiable information (PII)
    - **B.** Personal health information (PHI)
    - **C.** Social Security number (SSN)
    - **D.** Secure identity information (SII)

29. Which of the following information security risks to data at rest would result in the greatest reputational impact on an organization?
    - **A.** Improper classification
    - **B.** Data breach
    - **C.** Decryption
    - **D.** An intentional insider threat

30. Full disk encryption like Microsoft's BitLocker is used to protect data in what state?
    - **A.** Data in transit
    - **B.** Data at rest
    - **C.** Unlabeled data
    - **D.** Labeled data

31. The company that Katie works for provides its staff with mobile phones for employee use, with new phones issued every two years. What scenario best describes this type of practice when the phones themselves are still usable and receiving operating system updates?
    - **A.** EOL
    - **B.** Planned obsolescence
    - **C.** EOS
    - **D.** Device risk management

32. What is the primary purpose of data classification?
    - **A.** It quantifies the cost of a data breach.
    - **B.** It prioritizes IT expenditures.
    - **C.** It allows compliance with breach notification laws.
    - **D.** It identifies the value of the data to the organization.

33. Fred's organization allows downgrading of systems for reuse after projects have been finished and the systems have been purged. What concern should Fred raise about the reuse of the systems from his Top Secret classified project for a future project classified as Secret?

A. The Top Secret data may be commingled with the Secret data, resulting in a need to relabel the system.

B. The cost of the sanitization process may exceed the cost of new equipment.

C. The data may be exposed as part of the sanitization process.

D. The organization's DLP system may flag the new system due to the difference in data labels.

34. Which of the following concerns should not be part of the decision when classifying data?

A. The cost to classify the data

B. The sensitivity of the data

C. The amount of harm that exposure of the data could cause

D. The value of the data to the organization

35. Which of the following is the least effective method of removing data from media?

A. Degaussing

B. Purging

C. Erasing

D. Clearing

For questions 36–38, please refer to the following scenario:

The healthcare company that Amanda works for handles HIPAA data as well as internal business data, protected health information, and day-to-day business communications. Its internal policy uses the following requirements for securing HIPAA data at rest and in transit.

Classification	Handling Requirements
Confidential (HIPAA)	Encrypt at rest and in transit.
	Full disk encryption is required for all workstations.
	Files can only be sent in encrypted form, and passwords must be transferred under separate cover.
	Printed documents must be labeled with "HIPAA handling required."
Private (PHI)	Encrypt at rest and in transit.
	PHI must be stored on secure servers, and copies should not be kept on local workstations.
	Printed documents must be labeled with "Private."
Sensitive (business confidential)	Encryption is recommended but not required.
Public	Information can be sent unencrypted.

36. What encryption technology would be appropriate for HIPAA documents in transit?

A. BitLocker

B. DES

C. TLS

D. SSL

37. Amanda's employer asks Amanda to classify patient X-ray data that has an internal patient identifier associated with it but does not have any way to directly identify a patient. The company's data owner believes that exposure of the data could cause damage (but not exceptional damage) to the organization. How should Amanda classify the data?

A. Public

B. Sensitive

C. Private

D. Confidential

38. What technology could Amanda's employer implement to help prevent confidential data from being emailed out of the organization?

A. DLP

B. IDS

C. A firewall

D. UDP

39. Jacob's organization uses the US government's data classification system, which includes Top Secret, Secret, Confidential, and Unclassified ratings (from most sensitive to least). Jacob encounters a system that contains Secret, Confidential, and Top Secret data. How should it be classified?

A. Top Secret

B. Confidential

C. Secret

D. Mixed classification

40. Elle is planning her organization's asset retention efforts and wants to establish when the company will remove assets from use. Which of the following is typically the last event in a manufacturer or software provider's lifecycle?

A. End of life

B. End of support

C. End of sales

D. General availability

41. Amanda has been asked to ensure that her organization's controls assessment procedures match the specific systems that the company uses. What activity best matches this task?

A. Asset management

B. Compliance

C. Scoping

D. Tailoring

42. Chris is responsible for his organization's security standards and has guided the selection and implementation of a security baseline for Windows PCs in his organization. How can Chris most effectively make sure that the workstations he is responsible for are being checked for compliance and that settings are being applied as necessary?

A. Assign users to spot-check baseline compliance.

B. Use Microsoft Group Policy.

C. Create startup scripts to apply policy at system start.

D. Periodically review the baselines with the data owner and system owners.

43. Frank is reviewing his company's data lifecycle and wants to place appropriate controls around the data collection phase. Which of the following ensures that data subjects agree to the processing of their data?

A. Retention

B. Consent

C. Certification

D. Remanence

44. As a DBA, Amy's data role in her organization includes technical implementations of the data policies and standards, as well as managing the data structures that the data is stored in. What data role best fits what Amy does?

A. Data custodian

B. Data owner

C. Data processor

D. Data user

45. The company Jim works for suffered from a major data breach in the past year and now wants to ensure that it knows where data is located and if it is being transferred, is being copied to a thumb drive, or is in a network file share where it should not be. Which of the following solutions is best suited to tagging, monitoring, and limiting where files are transferred to?

A. DRM

B. DLP

C. A network IPS

D. Antivirus

46. What security measure can provide an additional security control in the event that backup tapes are stolen or lost?

A. Keep multiple copies of the tapes.

B. Replace tape media with hard drives.

C. Use appropriate security labels.

D. Use AES-256 encryption.

47. Joe works at a major pharmaceutical research and development company and has been tasked with writing his organization's data retention policy. As part of its legal requirements, the organization must comply with the US Food and Drug Administration's Code of Federal Regulations Title 21. To do so, it is required to retain records with electronic signatures. Why would a signature be part of a retention requirement?

A. It ensures that someone has reviewed the data.

B. It provides confidentiality.

C. It ensures that the data has been changed.

D. It validates who approved the data.

48. Susan wants to manage her data's lifecycle based on retention rules. What technique can she use to ensure that data that has reached the end of its lifecycle can be identified and disposed of based on her organization's disposal processes?

A. Rotation

B. DRM

C. DLP

D. Tagging

49. Ben has been asked to scrub data to remove data that is no longer needed by his organization. What phase of the data lifecycle is Ben most likely operating in?

A. Data retention

B. Data maintenance

C. Data remanence

D. Data collection

50. Steve is concerned about the fact that employees leaving his organization were often privy to proprietary information. Which one of the following controls is most effective against this threat?

A. Sanitization

B. NDAs

C. Clearing

D. Encryption

51. Alex works for a government agency that is required to meet US federal government requirements for data security. To meet these requirements, Alex has been tasked with making sure data is identifiable by its classification level when it is created. What should Alex do to the data?

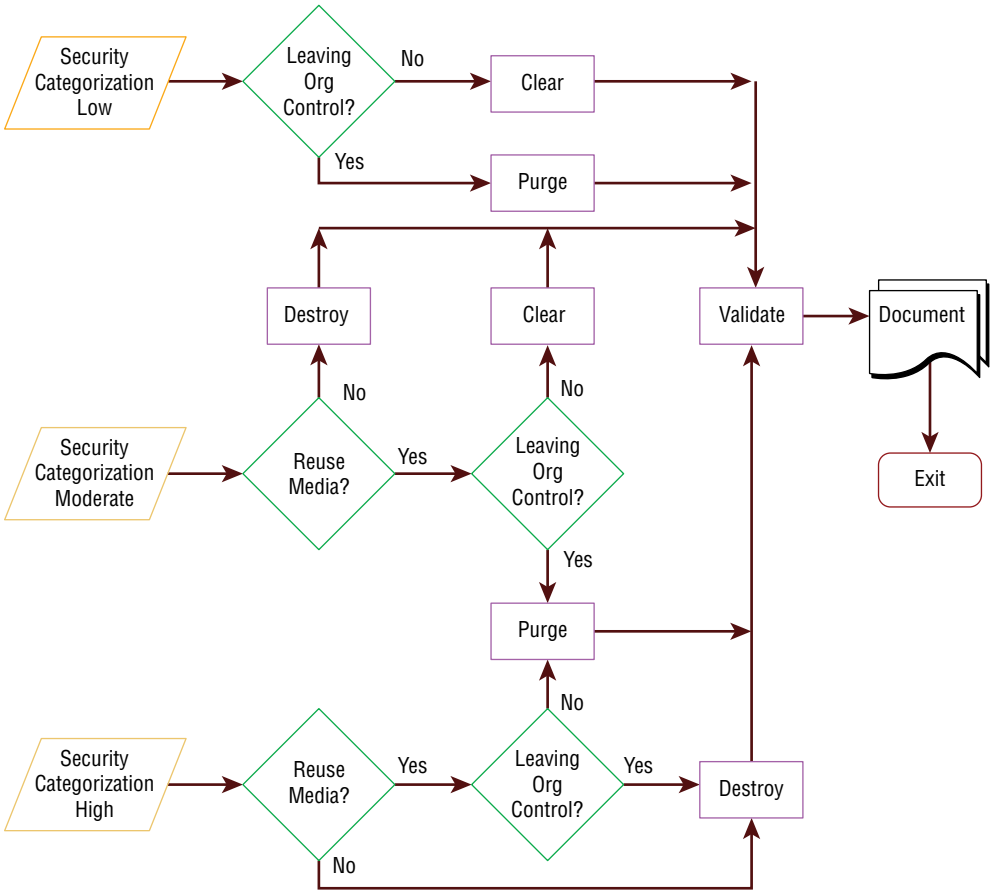
A. Classify the data.

B. Encrypt the data.

C. Label the data.

D. Apply DRM to the data.

52. Ben is following the National Institute of Standards and Technology (NIST) Special Publication 800-88 guidelines for sanitization and disposition as shown here. He is handling information that his organization classified as sensitive, which is a moderate security categorization in the NIST model. If the media is going to be sold as surplus, what process does Ben need to follow?



Source: NIST SP 800-88.

A. Destroy, validate, document

B. Clear, purge, document

C. Purge, document, validate

D. Purge, validate, document

53. What methods are often used to protect data in transit?

A. Telnet, ISDN, UDP

B. BitLocker, FileVault

C. AES, Serpent, IDEA

D. TLS, VPN, IPsec

54. Which one of the following data roles bears ultimate organizational responsibility for data?

A. System owners

B. Business owners

C. Data owners

D. Mission owners

55. Shandra wants to secure an encryption key. Which location would be the most difficult to protect, if the key was kept and used in that location?

A. On a local network

B. On disk

C. In memory

D. On a public network

For questions 56–58, please refer to the following scenario:

Chris has recently been hired into a new organization. The organization that Chris belongs to uses the following classification process:

1. Criteria are set for classifying data.
2. Data owners are established for each type of data.
3. Data is classified.
4. Required controls are selected for each classification.
5. Baseline security standards are selected for the organization.
6. Controls are scoped and tailored.
7. Controls are applied and enforced.
8. Access is granted and managed.

56. If Chris is one of the data owners for the organization, what steps in this process is he most likely responsible for?

A. He is responsible for steps 3, 4, and 5.

B. He is responsible for steps 1, 2, and 3.

C. He is responsible for steps 5, 6, and 7.

D. All of the steps are his direct responsibility.

57. Chris manages a team of system administrators. What data role are they fulfilling if they conduct steps 6, 7, and 8 of the classification process?

A. They are system owners and administrators.

B. They are administrators and custodians.

C. They are data owners and administrators.

D. They are custodians and users.

58. If Chris's company operates in the European Union and has been contracted to handle the data for a third party, what role is his company operating in when it uses this process to classify and handle data?

A. Business owners

B. Mission owners

C. Data processors

D. Data administrators

For questions 59–62, please refer to the following scenario:

Chris has been put in charge of his organization's IT service management effort, and part of that effort includes creating an inventory of both tangible and intangible assets. As a security professional, you have been asked to provide Chris with security-related guidance on each of the following topics. Your goal is to provide Chris with the best answer from each of the options, knowing that in some cases more than one of the answers could be acceptable.

59. Chris needs to identify all of the active systems and devices on the network. Which of the following techniques will give him the most complete list of connected devices?

A. Query Active Directory for a list of all computer objects.

B. Perform a port scan of all systems on the network.

C. Ask all staff members to fill out a form listing all of their systems and devices.

D. Use network logs to identify all connected devices and track them down from there.

60. Chris knows that his inventory is only accurate at the moment it was completed. How can he best ensure that it remains up-to-date?

A. Perform a point-in-time query of network connected devices and update the list based on what is found.

B. Ensure that procurement and acquisition processes add new devices to the inventory before they are deployed.

C. Require every employee to provide an updated inventory of devices they are responsible for on a quarterly basis.

D. Manually verify every device in service at each organizational location on a yearly basis.

61. Chris knows that his organization has more than just physical assets. In fact, his organization's business involves significant intellectual property assets, including designs and formulas. Chris needs to track and inventory those assets as well. How can he most effectively ensure that he can identify and manage data throughout his organization based on its classification or type?

A. Track file extensions for common data types.

B. Ensure that data is collected in specific network share locations based on the data type and group that works with it.

C. Use metadata tagging based on data type or security level.

D. Automatically tag data by file extension type.

62. Chris has been tasked with identifying intangible assets but needs to provide his team with a list of the assets they will be inventorying. Which of the following is not an example of an intangible asset?

A. Patents

B. Databases

C. Formulas

D. Employees

63. Which of the following is not a common requirement for the collection of data under data privacy laws and statutes?

A. Only data that is needed is collected.

B. Data should be obtained lawfully and via fair methods.

C. Data should only be collected with the consent of the individual whose data is being collected.

D. Data should be collected from all individuals equally.

64. Susan works in an organization that labels all removable media with the classification level of the data it contains, including public data. Why would Susan's employer label all media instead of labeling only the media that contains data that could cause harm if it was exposed?

A. It is cheaper to order all prelabeled media.

B. It prevents sensitive media from not being marked by mistake.

C. It prevents reuse of public media for sensitive data.

D. Labeling all media is required by HIPAA.

65. Data stored in RAM is best characterized as what type of data?

A. Data at rest

B. Data in use

C. Data in transit

D. Data at large

66. What issue is the validation portion of the NIST SP 800-88 sample certificate of sanitization (shown here) intended to help prevent?

CERTIFICATE OF SANITIZATION		
PERSON PERFORMING SANITIZATION		
Name:	Title:	
Organization:	Location:	Phone:
MEDIA INFORMATION		
Make/ Vendor:	Model Number:	
Serial Number:		
Media Property Number:		
Media Type:	Source *(ie user name or PC property number)*:	
Classification:	Data Backed Up: ☐ Yes ☐ No ☐ Unknown	
Backup Location:		
SANITIZATION DETAILS		
Method Type: ☐ Clear ☐ Purge ☐ Damage ☐ Destruct		
Method Used: ☐ Degauss ☐ Overwrite ☐ Block Erase ☐ Crypto Erase ☐ Other:		
Method Details:		
Tool Used *(include version)*:		
Verification Method: ☐ Full ☐ Quick Sampling ☐ Other:		
Post Sanitization Classification:		
Notes:		
MEDIA DESTINATION		
☐ Internal Reuse ☐ External Reuse ☐ Recycling Facility ☐ Manufacturer ☐ Other *(specify in details area)*		
Details:		
SIGNATURE		
I attest that the information provided on this statement is accurate to the best of my knowledge.		
Signature:		Date:
VALIDATION		
Name:	Title:	
Organization:	Location:	Phone:
Signature:		Date:

Source: Certificate of Sanitization.

A. Destruction

B. Reuse

C. Data remanence

D. Attribution

67. Why is declassification rarely chosen as an option for media reuse?

A. Purging is sufficient for sensitive data.

B. Sanitization is the preferred method of data removal.

C. It is more expensive than new media and may still fail.

D. Clearing is required first.

68. Incineration, crushing, shredding, and disintegration all describe what stage in the lifecycle of media?

A. Sanitization

B. Degaussing

C. Purging

D. Destruction

69. What term is used to describe information like prescriptions and X-rays?

A. PHI

B. Proprietary data

C. PID

D. PII

70. Why might an organization use unique screen backgrounds or designs on workstations that deal with data of different classification levels?

A. To indicate the software version in use

B. To promote a corporate message

C. To promote availability

D. To indicate the classification level of the data or system

71. Charles has been asked to downgrade the media used for storage of private data for his organization. What process should Charles follow?

A. Degauss the drives, and then relabel them with a lower classification level.

B. Pulverize the drives, and then reclassify them based on the data they contain.

C. Follow the organization's purging process, and then downgrade and replace labels.

D. Relabel the media, and then follow the organization's purging process to ensure that the media matches the label.

72. Which of the following tasks is not performed by a system owner per NIST SP 800-18?

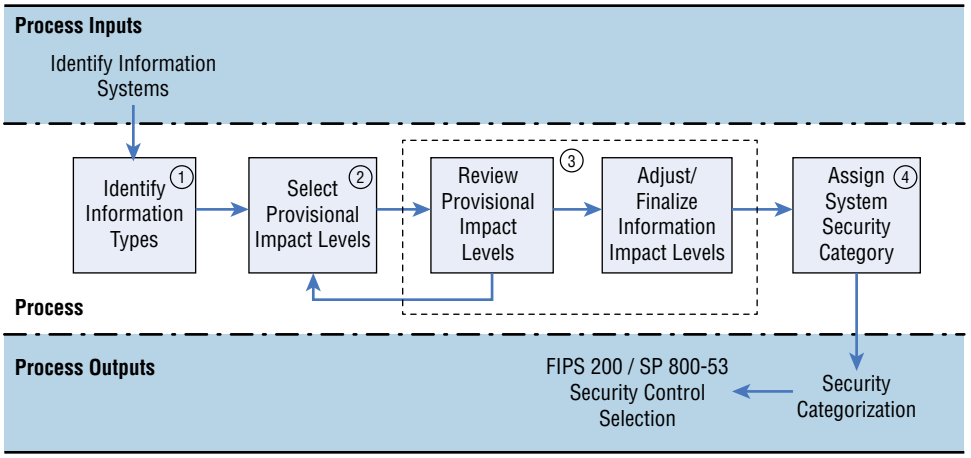
A. Develops a system security plan

B. Establishes rules for appropriate use and protection of data

C. Identifies and implements security controls

D. Ensures that system users receive appropriate security training

73. NIST SP 800-60 provides a process shown in the following diagram to assess information systems. What process does this diagram show?



Source: NIST SP 800-60.

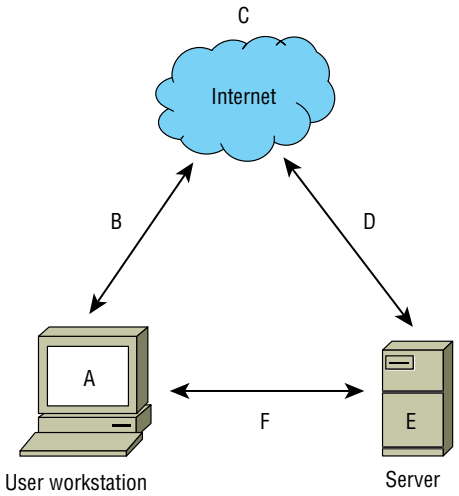
A. Selecting a standard and implementing it

B. Categorizing and selecting controls

C. Baselining and selecting controls

D. Categorizing and sanitizing

The following diagram shows a typical workstation and server and their connections to each other and the internet. For questions 74–76, please refer to this diagram.



74. Which letters on this diagram are locations where you might find data at rest?

A. A, B, and C

B. C and E

C. A and E

D. B, D, and F

75. What would be the best way to secure data at points B, D, and F?

A. AES-256

B. SSL

C. TLS

D. 3DES

76. What is the best way to secure files that are sent from workstation A via the internet service (C) to remote server E?

A. Use AES at rest at point A, and use TLS in transit via B and D.

B. Encrypt the data files and send them.

C. Use 3DES and TLS to provide double security.

D. Use full disk encryption at A and E, and use SSL at B and D.

77. Susan needs to provide a set of minimum security requirements for email. What steps should she recommend for her organization to ensure that the email remains secure?

A. All email should be encrypted.

B. All email should be encrypted and labeled.

C. Sensitive email should be encrypted and labeled.

D. Only highly sensitive email should be encrypted.

78. How can a data retention policy reduce liabilities?

A. By reducing the amount of storage in use

B. By limiting the number of data classifications

C. By reducing the amount of data that may need to be produced for lawsuits

D. By reducing the legal penalties for noncompliance

79. What data role does a system that is used to process data have?

A. Mission owner

B. Data owner

C. Data processor

D. Custodian

80. Which one of the following is not considered PII under US federal government regulations?

A. Name

B. Social Security number

C. Student ID number

D. ZIP code

81. What type of health information is the Health Insurance Portability and Accountability Act required to protect?

A. PII

B. PHI

C. SHI

D. HPHI

82. The system that Ian has built replaces data in a database field with a randomized string of characters that remains the same for each instance of that data. What technique has he used?

A. Data masking

B. Tokenization

C. Anonymization

D. DES

83. Juanita's company processes credit cards and wants to select appropriate data security standards. What data security standard is she most likely to need to use and comply with?

A. CC-Comply

B. PCI-DSS

C. GLBA

D. GDPR

84. What is the best method to sanitize a solid-state drive (SSD)?

A. Clearing

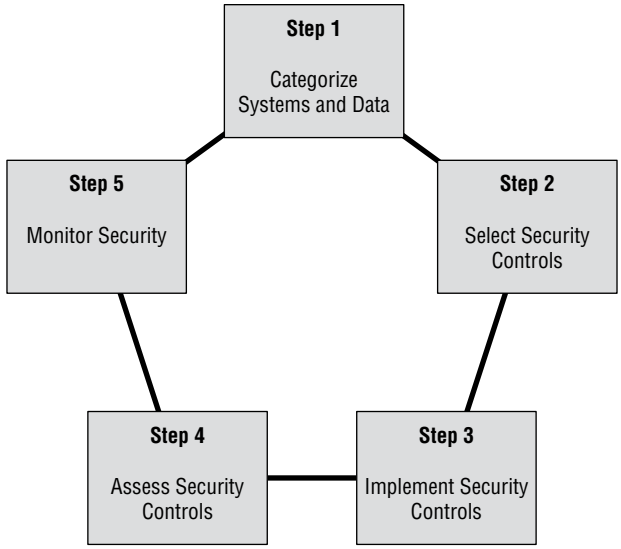
B. Zero fill

C. Disintegration

D. Degaussing

For questions 85–87, please refer to the following scenario:

As shown in the following security lifecycle diagram (loosely based on the NIST reference architecture), NIST uses a five-step process for risk management. Using your knowledge of data roles and practices, answer the following questions based on the NIST framework process.



85. What data role will own responsibility for step 1, the categorization of information systems; to whom will they delegate step 2; and what data role will be responsible for step 3?

A. Data owners, system owners, custodians

B. Data processors, custodians, users

C. Business owners, administrators, custodians

D. System owners, business owners, administrators

86. If the systems that are being assessed all handle credit card information (and no other sensitive data), at what step would the PCI DSS first play an important role?

A. Step 1

B. Step 2

C. Step 3

D. Step 4

87. What data security role is primarily responsible for step 5?

A. Data owners

B. Data processors

C. Custodians

D. Users

88. Susan's organization performs a secure disk wipe process on hard drives before they are sent to a third-party organization to be shredded. What issue is her organization attempting to avoid?

A. Data retention that is longer than defined in policy

B. Mishandling of drives by the third party

C. Classification mistakes

D. Data permanence

89. Mike wants to track hardware assets as devices and equipment are moved throughout his organization. What type of system can help do this without requiring staff to individually check bar codes or serial numbers?

A. A visual inventory

B. WiFi MAC address tracking

C. RFID tags

D. Steganography

90. Retaining and maintaining information for as long as it is needed is known as what?

A. Data storage policy

B. Data storage

C. Asset maintenance

D. Record retention

91. Which of the following activities is not a consideration during data classification?

A. Who can access the data

B. What the impact would be if the data was lost or breached

C. How much the data cost to create

D. What protection regulations may be required for the data

92. What type of encryption is typically used for data at rest?

A. Asymmetric encryption

B. Symmetric encryption

C. DES

D. OTP

93. Which data role is tasked with apply rights that provide appropriate access to staff members?

A. Data processors

B. Business owners

C. Custodians

D. Administrators

94. What element of asset security is often determined by identifying an asset's owner?

A. It identifies the individual(s) responsible for protecting the asset.

B. It provides a law enforcement contact in case of theft.

C. It helps establish the value of the asset.

D. It determines the security classification of the asset.

95. Fred is preparing to send backup tapes off-site to a secure third-party storage facility. What steps should Fred take before sending the tapes to that facility?

A. Ensure that the tapes are handled the same way the original media would be handled based on their classification.

B. Increase the classification level of the tapes because they are leaving the possession of the company.

C. Purge the tapes to ensure that classified data is not lost.

D. Decrypt the tapes in case they are lost in transit.

96. Which of the following does not describe data in motion?

A. Data on a backup tape that is being shipped to a storage facility

B. Data in a TCP packet

C. Data in an e-commerce transaction

D. Data in files being copied between locations

97. A new law is passed that would result in significant financial harm to your company if the data that it covers was stolen or inadvertently released. What should your organization do about this?

A. Select a new security baseline.

B. Relabel the data.

C. Encrypt all of the data at rest and in transit.

D. Review its data classifications and classify the data appropriately.

98. Which of the following data roles are typically found inside of a company instead of as a third-party contracting relationship? (Select all that apply.)

A. Data owners

B. Data controllers

C. Data custodians

D. Data processors

99. What commercial data classification is most appropriate for data contained on corporate websites?

A. Private

B. Sensitive

C. Public

D. Proprietary

100. Match each of the numbered data elements shown here with one of the lettered categories. You may use the categories once, more than once, or not at all. If a data element matches more than one category, choose the one that is most specific.

Data elements

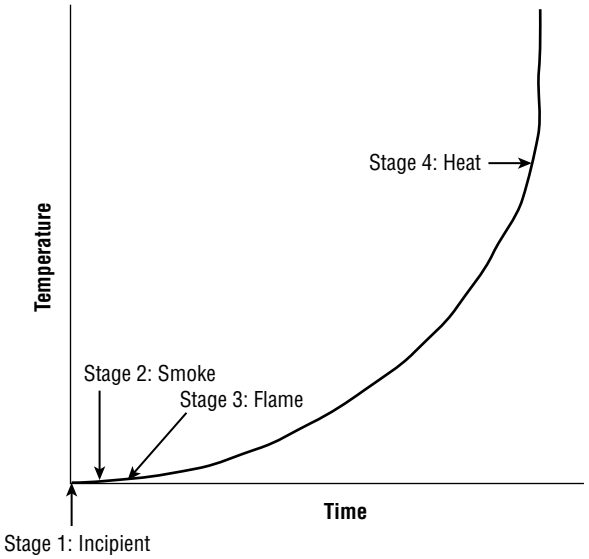
1. Medical records
2. Trade secrets
3. Social Security numbers
4. Driver's license numbers

Categories

A. Proprietary data
B. Protected health information
C. Personally identifiable information

1. Matthew is the security administrator for a consulting firm and must enforce access controls that restrict users' access based upon their previous activity. For example, once a consultant accesses data belonging to Acme Cola, a consulting client, they may no longer access data belonging to any of Acme's competitors. What security model best fits Matthew's needs?
   - **A.** Clark-Wilson
   - **B.** Biba
   - **C.** Bell-LaPadula
   - **D.** Brewer-Nash

2. Referring to the figure shown here, what is the earliest stage of a fire where it is possible to use detection technology to identify it?



   - **A.** Incipient
   - **B.** Smoke
   - **C.** Flame
   - **D.** Heat

3. Ralph is designing a physical security infrastructure for a new computing facility that will remain largely unstaffed. He plans to implement motion detectors in the facility but would also like to include a secondary verification control for physical presence. Which one of the following would best meet his needs?
   - **A.** CCTV
   - **B.** IPS
   - **C.** Turnstiles
   - **D.** Faraday cages

4. Harry would like to retrieve a lost encryption key from a database that uses m of n control, with m = 4 and n = 8. What is the minimum number of escrow agents required to retrieve the key?
   - **A.** 2
   - **B.** 4
   - **C.** 8
   - **D.** 12

5. Fran's company is considering purchasing a web-based email service from a vendor and eliminating its own email server environment as a cost-saving measure. What type of cloud computing environment is Fran's company considering?
   - **A.** SaaS
   - **B.** IaaS
   - **C.** CaaS
   - **D.** PaaS

6. Bob is a security administrator with the U.S. federal government and wants to choose a digital signature approach that is an approved part of the federal Digital Signature Standard under FIPS 186-4. Which one of the following encryption algorithms is not an acceptable choice for use in digital signatures?
   - **A.** DSA
   - **B.** HAVAL
   - **C.** RSA
   - **D.** ECDSA

7. Harry would like to access a document owned by Sally and stored on a file server. Applying the subject/object model to this scenario, who or what is the subject of the resource request?
   - **A.** Harry
   - **B.** Sally
   - **C.** Server
   - **D.** Document

8. Michael is responsible for forensic investigations and is investigating a medium-severity security incident that involved the defacement of a corporate website. The web server in question ran on a virtualization platform, and the marketing team would like to get the website up and running as quickly as possible. What would be the most reasonable next step for Michael to take?
   - **A.** Keep the website offline until the investigation is complete.
   - **B.** Take the virtualization platform offline as evidence.
   - **C.** Take a snapshot of the compromised system and use that for the investigation.
   - **D.** Ignore the incident and focus on quickly restoring the website.

9. Helen is a software engineer and is developing code that she would like to restrict to running within an isolated sandbox for security purposes. What software development technique is Helen using?

A. Bounds
B. Input validation
C. Confinement
D. TCB

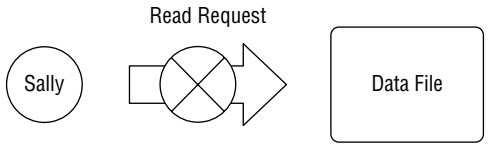
10. What concept describes the degree of confidence that an organization has that its controls satisfy security requirements?

A. Trust
B. Credentialing
C. Verification
D. Assurance

11. What type of security vulnerability are developers most likely to introduce into code when they seek to facilitate their own access, for testing purposes, to software they developed?

A. Maintenance hook
B. Cross-site scripting
C. SQL injection
D. Buffer overflow

12. In the figure shown here, Sally is blocked from reading the file due to the Biba integrity model. Sally has a Secret security clearance, and the file has a Confidential classification. What principle of the Biba model is being enforced?



A. Simple Security Property
B. Simple Integrity Property
C. *-Security Property
D. *-Integrity Property

13. Tom is responsible for maintaining the security of systems used to control industrial processes located within a power plant. What term is used to describe these systems?

A. POWER
B. SCADA
C. HAVAL
D. COBOL

14. Sonia recently removed an encrypted hard drive from a laptop and moved it to a new device because of a hardware failure. She is having difficulty accessing encrypted content on the drive despite the fact that she knows the user's password. What hardware security feature is likely causing this problem?

    A. TCB

    B. TPM

    C. NIACAP

    D. RSA

15. Chris wants to verify that a software package that he downloaded matches the original version. What hashing tool should he use if he believes that technically sophisticated attackers may have replaced the software package with a version containing a backdoor?

    A. MD5

    B. 3DES

    C. SHA1

    D. SHA 256

For questions 16–19, please refer to the following scenario:

Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

16. If Alice wants to send Bob a message that is encrypted for confidentiality, what key does she use to encrypt the message?

    A. Alice's public key

    B. Alice's private key

    C. Bob's public key

    D. Bob's private key

17. When Bob receives the encrypted message from Alice, what key does he use to decrypt the message's plaintext content?

    A. Alice's public key

    B. Alice's private key

    C. Bob's public key

    D. Bob's private key

18. Which one of the following keys would Bob not possess in this scenario?

    A. Alice's public key

    B. Alice's private key

    C. Bob's public key

    D. Bob's private key

19. Alice would also like to digitally sign the message that she sends to Bob. What key should she use to create the digital signature?
    - **A.** Alice's public key
    - **B.** Alice's private key
    - **C.** Bob's public key
    - **D.** Bob's private key

20. What name is given to the random value added to a password in an attempt to defeat rainbow table attacks?
    - **A.** Hash
    - **B.** Salt
    - **C.** Extender
    - **D.** Rebar

21. Which one of the following is not an attribute of a hashing algorithm?
    - **A.** They require a cryptographic key.
    - **B.** They are irreversible.
    - **C.** It is very difficult to find two messages with the same hash value.
    - **D.** They take variable-length input.

22. What type of fire suppression system fills with water after a valve opens when the initial stages of a fire are detected and then requires a sprinkler head heat activation before dispensing water?
    - **A.** Wet pipe
    - **B.** Dry pipe
    - **C.** Deluge
    - **D.** Preaction

23. Susan would like to configure IPsec in a manner that provides confidentiality for the content of packets. What component of IPsec provides this capability?
    - **A.** AH
    - **B.** ESP
    - **C.** IKE
    - **D.** ISAKMP

24. Which one of the following cryptographic goals protects against the risks posed when a device is lost or stolen?
    - **A.** Nonrepudiation
    - **B.** Authentication
    - **C.** Integrity
    - **D.** Confidentiality

25. Joanna wants to review the status of the industrial control systems her organization uses for building control. What type of systems should she inquire about access to?

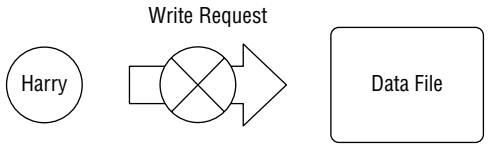
A. SCADA

B. DSS

C. BAS

D. ICS-CSS

26. In the figure shown here, Harry's request to write to the data file is blocked. Harry has a Secret security clearance, and the data file has a Confidential classification. What principle of the Bell-LaPadula model blocked this request?



A. Simple Security Property

B. Simple Integrity Property

C. *-Security Property

D. Discretionary Security Property

27. Florian and Tobias would like to begin communicating using a symmetric cryptosystem, but they have no prearranged secret and are not able to meet in person to exchange keys. What algorithm can they use to securely exchange the secret key?

A. IDEA

B. Diffie-Hellman

C. RSA

D. MD5

28. Carl's organization recently underwent a user access review. At the conclusion of the review, the auditors noted several cases of privilege creep. What security principle was violated?

A. Fail securely

B. Keep it simple

C. Trust but verify

D. Least privilege

29. Matt's organization recently adopted a zero-trust network architecture. Under this approach, which one of the following criteria would be LEAST appropriate to use when granting a subject access to resources?

A. Password

B. Two-factor authentication

C. IP address

D. Biometric scan

30. Colin is the chief privacy officer for a nonprofit organization and is assisting with the team's transition to a Privacy by Design approach. Under this approach, which of the following principles should the team embrace?

A. Proactive, not reactive

B. Privacy as the default setting

C. End-to-end security

D. Defense in depth

31. What cryptographic principle stands behind the idea that cryptographic algorithms should be open to public inspection?

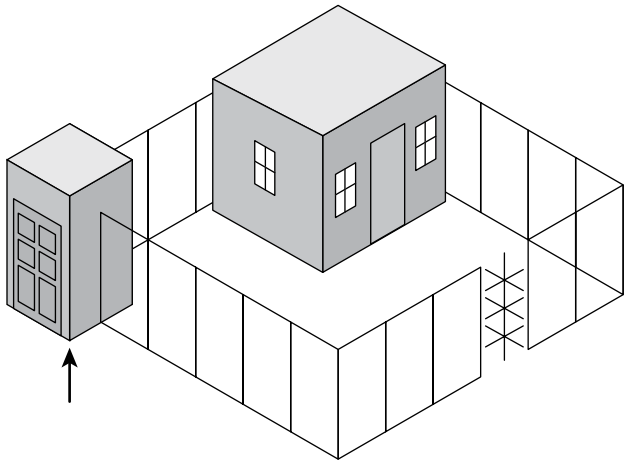
A. Security through obscurity

B. Kerckhoffs' principle

C. Defense in depth

D. Heisenburg principle

32. Ryan is developing a physical access plan for his organization's data center and wants to implement the security control indicated by the arrow in this diagram. What is the name of this control?



A. Mantrap

B. Turnstile

C. Intrusion prevention system

D. Portal

33. Which one of the following does not describe a standard physical security requirement for wiring closets?

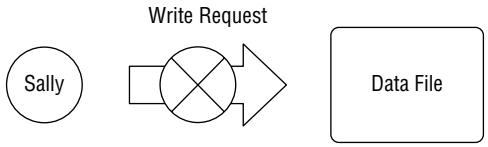
A. Place only in areas monitored by security guards.

B. Do not store flammable items in the closet.

C. Use sensors on doors to log entries.

D. Perform regular inspections of the closet.

34. In the figure shown here, Sally is blocked from writing to the data file by the Biba integrity model. Sally has a Secret security clearance, and the file is classified Top Secret. What principle is preventing her from writing to the file?



A. Simple Security Property

B. Simple Integrity Property

C. *-Security Property

D. *-Integrity Property

35. Lana recently implemented a new process in her organization where managers who are responsible for granting users access to a system are not permitted to participate in access reviews. What principle is she enforcing?

A. Two-person control

B. Least privilege

C. Privilege creep

D. Separation of duties

36. Which of the following statements about system development are correct? (Select all that apply.)

A. Systems should be designed to operate in a secure manner if the user performs no other configuration.

B. Systems should be designed to fall back to a secure state if they experience an error.

C. Systems should be designed to incorporate security as a design feature.

D. Systems should be designed in a manner that keeps their functionality as simple as possible.

37. Alan is reviewing a system that has been assigned the EAL1 evaluation assurance level under the Common Criteria. What is the degree of assurance that he may have about the system?

A. It has been functionally tested.

B. It has been structurally tested.

C. It has been formally verified, designed, and tested.

D. It has been methodically designed, tested, and reviewed.

38. Jake works for a research organization that is seeking to deploy a grid computing system that will perform cycle scavenging on user workstations to conduct research tasks that require high-performance computing. What is the most significant risk associated with this operation?

A. Data confidentiality

B. Isolation breach

C. Data integrity

D. Data availability

39. Eimear's software development team uses an approach that creates many discrete software objects and then binds them together using APIs. What term best describes this architecture?

A. Microservices

B. Function-as-a-service

C. Containerization

D. Virtualization

40. Adam recently configured permissions on an NTFS filesystem to describe the access that different users may have to a file by listing each user individually. What did Adam create?

A. An access control list

B. An access control entry

C. Role-based access control

D. Mandatory access control

41. Betty is concerned about the use of buffer overflow attacks against a custom application developed for use in her organization. What security control would provide the strongest defense against these attacks?

A. Firewall

B. Intrusion detection system

C. Parameter checking

D. Vulnerability scanning

42. Which one of the following combinations of controls best embodies the defense in depth principle?

A. Encryption of email and network intrusion detection

B. Cloud access security brokers (CASB) and security awareness training

C. Data loss prevention and multifactor authentication

D. Network firewall and host firewall

43. James is working with a Department of Defense system that is authorized to simultaneously handle information classified at the Secret and Top Secret levels. What type of system is he using?

A. Single state

B. Unclassified

C. Compartmented

D. Multistate

44. Kyle is being granted access to a military computer system that uses System High mode. What is not true about Kyle's security clearance requirements?

A. Kyle must have a clearance for the highest level of classification processed by the system, regardless of his access.

B. Kyle must have access approval for all information processed by the system.

C. Kyle must have a valid need to know for all information processed by the system.

D. Kyle must have a valid security clearance.

45. Gary intercepts a communication between two individuals and suspects that they are exchanging secret messages. The content of the communication appears to be the image shown here. What type of technique may the individuals use to hide messages inside this image?

A. Visual cryptography

B. Steganography

C. Cryptographic hashing

D. Transport layer security

46. Philip is developing a new security tool that will be used by individuals in many different subsidiaries of his organization. He chooses to use Docker to deploy the tool to simplify configuration. What term best describes this approach?

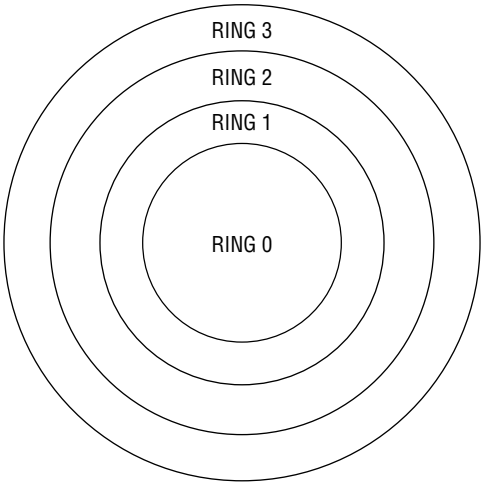
A. Virtualization

B. Abstraction

C. Simplification

D. Containerization

47. In the ring protection model shown here, what ring contains the operating system's kernel?



A. Ring 0

B. Ring 1

C. Ring 2

D. Ring 3

48. In an infrastructure as a service (IaaS) environment where a vendor supplies a customer with access to storage services, who is normally responsible for removing sensitive data from drives that are taken out of service?

A. Customer's security team

B. Customer's storage team

C. Customer's vendor management team

D. Vendor

49. During a system audit, Casey notices that the private key for her organization's web server has been stored in a public Amazon S3 storage bucket for more than a year. Which one of the following actions should she take first?

A. Remove the key from the bucket.

B. Notify all customers that their data may have been exposed.

C. Request a new certificate using a new key.

D. Nothing, because the private key should be accessible for validation.

50. Which one of the following systems assurance processes provides an independent third-party evaluation of a system's controls that may be trusted by many different organizations?

A. Certification

B. Definition

C. Verification

D. Accreditation

51. Darcy's organization is deploying serverless computing technology to better meet the needs of developers and users. In a serverless model, who is normally responsible for configuring operating system security controls?

A. Software developer

B. Cybersecurity professional

C. Cloud architect

D. Vendor

52. Harold is assessing the susceptibility of his environment to hardware failures and would like to identify the expected lifetime of a piece of hardware. What measure should he use for this?

A. MTTR

B. MTTF

C. RTO

D. MTO

53. Chris is designing a cryptographic system for use within his company. The company has 1,000 employees, and they plan to use an asymmetric encryption system. They would like the system to be set up so that any pair of arbitrary users may communicate privately. How many total keys will they need?

A. 500

B. 1,000

C. 2,000

D. 4,950

54. Gary is concerned about applying consistent security settings to the many mobile devices used throughout his organization. What technology would best assist with this challenge?

A. MDM

B. IPS

C. IDS

D. SIEM

55. Alice sent a message to Bob. Bob would like to demonstrate to Charlie that the message he received definitely came from Alice. What goal of cryptography is Bob attempting to achieve?

A. Authentication
B. Confidentiality
C. Nonrepudiation
D. Integrity

56. Rhonda is considering the use of new identification cards for physical access control in her organization. She comes across a military system that uses the card shown here. What type of card is this?

A. Smart card
B. Proximity card
C. Magnetic stripe card
D. Phase three card

57. Gordon is concerned about the possibility that hackers may be able to use the Van Eck radiation phenomenon to remotely read the contents of computer monitors in a restricted work area within his facility. What technology would protect against this type of attack?

A. TCSEC
B. SCSI
C. GHOST
D. TEMPEST

58. Jorge believes that an attacker has obtained the hash of the Kerberos service account from one of his organization's Active Directory servers. What type of attack would this enable?

A. Golden ticket

B. Kerberoasting

C. Pass the ticket

D. Brute force

59. Sherry conducted an inventory of the cryptographic technologies in use within her organization and found the following algorithms and protocols in use. Which one of these technologies should she replace because it is no longer considered secure?

A. MD5

B. AES

C. PGP

D. WPA3

60. Robert is investigating a security breach and discovers the Mimikatz tool installed on a system in his environment. What type of attack has likely taken place?

A. Password cracking

B. Pass the hash

C. MAC spoofing

D. ARP poisoning

61. Tom is a cryptanalyst and is working on breaking a cryptographic algorithm's secret key. He has a copy of an intercepted message that is encrypted, and he also has a copy of the decrypted version of that message. He wants to use both the encrypted message and its decrypted plaintext to retrieve the secret key for use in decrypting other messages. What type of attack is Tom engaging in?

A. Chosen ciphertext

B. Chosen plaintext

C. Known plaintext

D. Brute force

62. A hacker recently violated the integrity of data in James's company by modifying a file using a precise timing attack. The attacker waited until James verified the integrity of a file's contents using a hash value and then modified the file between the time that James verified the integrity and read the contents of the file. What type of attack took place?

A. Social engineering

B. TOCTOU

C. Data diddling

D. Parameter checking

63. Carl is deploying a set of video sensors that will be placed in remote locations as part of a research project. Due to connectivity limitations, he would like to perform as much image processing and computation as possible on the device itself before sending results back to the cloud for further analysis. What computing model would best meet his needs?

A. Serverless computing

B. Edge computing

C. IaaS computing

D. SaaS computing

64. What action can you take to prevent accidental data disclosure due to wear leveling on an SSD device before reusing the drive?

A. Reformatting

B. Disk encryption

C. Degaussing

D. Physical destruction

65. Johnson Widgets strictly limits access to total sales volume information, classifying it as a competitive secret. However, shipping clerks have unrestricted access to order records to facilitate transaction completion. A shipping clerk recently pulled all of the individual sales records for a quarter from the database and totaled them up to determine the total sales volume. What type of attack occurred?

A. Social engineering

B. Inference

C. Aggregation

D. Data diddling

66. What physical security control broadcasts false emanations constantly to mask the presence of true electromagnetic emanations from computing equipment?

A. Faraday cage

B. Copper-infused windows

C. Shielded cabling

D. White noise

67. In a software as a service cloud computing environment, who is normally responsible for ensuring that appropriate firewall controls are in place to protect the application?

A. Customer's security team

B. Vendor

C. Customer's networking team

D. Customer's infrastructure management team

68. Alice has read permissions on an object, and she would like Bob to have those same rights. Which one of the rules in the Take-Grant protection model would allow her to complete this operation?

A. Create rule

B. Remove rule

C. Grant rule

D. Take rule

69. As part of his incident response process, Charles securely wipes the drive of a compromised machine and reinstalls the operating system (OS) from original media. Once he is done, he patches the machine fully and applies his organization's security templates before reconnecting the system to the network. Almost immediately after the system is returned to service, he discovers that it has reconnected to the same botnet it was part of before. Where should Charles look for the malware that is causing this behavior?

A. The operating system partition

B. The system BIOS or firmware

C. The system memory

D. The installation media

70. Lauren implements ASLR to help prevent system compromises. What technique has she used to protect her system?

A. Encryption

B. Mandatory access control

C. Memory address randomization

D. Discretionary access control

71. Alan intercepts an encrypted message and wants to determine what type of algorithm was used to create the message. He first performs a frequency analysis and notes that the frequency of letters in the message closely matches the distribution of letters in the English language. What type of cipher was most likely used to create this message?

A. Substitution cipher

B. AES

C. Transposition cipher

D. 3DES

72. The Double DES (2DES) encryption algorithm was never used as a viable alternative to the original DES algorithm. What implementation attack is 2DES vulnerable to that does not exist for the DES or 3DES approach?

A. Chosen ciphertext

B. Brute force

C. Man-in-the-middle

D. Meet-in-the-middle

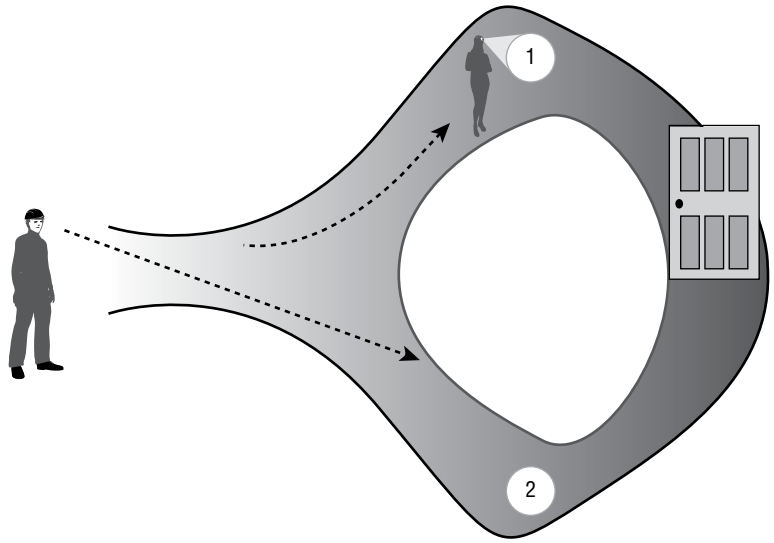
73. Grace would like to implement application control technology in her organization. Users often need to install new applications for research and testing purposes, and she does not want to interfere with that process. At the same time, she would like to block the use of known malicious software. What type of application control would be appropriate in this situation?

A. Blacklisting
B. Graylisting
C. Whitelisting
D. Bluelisting

74. Warren is designing a physical intrusion detection system for use in a sensitive media storage facility and wants to include technology that issues an alert if the communications lines for the alarm system are unexpectedly cut. What technology would meet this requirement?

A. Heartbeat sensor
B. Emanation security
C. Motion detector
D. Faraday cage

75. John and Gary are negotiating a business transaction, and John must demonstrate to Gary that he has access to a system. He engages in an electronic version of the "magic door" scenario shown here. What technique is John using?



A. Split-knowledge proof
B. Zero-knowledge proof
C. Logical proof
D. Mathematical proof

76. After scanning all of the systems on his wireless network, Mike notices that one system is identified as an iOS device running a massively out-of-date version of Apple's mobile operating system. When he investigates further, he discovers that the device is an original iPad and that it cannot be updated to a current secure version of the operating system. What would be the best option for handling this device?

A. Retire or replace the device.

B. Isolate the device on a dedicated wireless network.

C. Install a firewall on the tablet.

D. Reinstall the OS.

77. Tonya believes that an attacker was able to eavesdrop on legitimate HTTPS communications between her users and remote web servers by engaging in a DNS poisoning attack. After conducting DNS poisoning, what technique would an attacker likely use to conduct this eavesdropping?

A. Man-in-the-middle

B. Brute-force

C. Timing

D. Meet-in-the-middle

78. Howard is choosing a cryptographic algorithm for his organization, and he would like to choose an algorithm that supports the creation of digital signatures. Which one of the following algorithms would meet his requirement?

A. RSA

B. 3DES

C. AES

D. Blowfish

79. Laura is responsible for securing her company's web-based applications and wants to conduct an educational program for developers on common web application security vulnerabilities. Where can she turn for a concise listing of the most common web application issues?

A. CVE

B. NSA

C. OWASP

D. CSA

80. The Bell-LaPadula and Biba models implement state machines in a fashion that uses what specific state machine model?

A. Information flow

B. Noninterference

C. Cascading

D. Feedback

81. During a third-party vulnerability scan and security test, Danielle's employer recently discovered that the embedded systems that were installed to manage her company's new buildings have a severe remote access vulnerability. The manufacturer has gone out of business, and there is no patch or update for the devices. What should Danielle recommend that her employer do about the hundreds of devices that are vulnerable?

A. Identify a replacement device model and replace every device.

B. Turn off all of the devices.

C. Move the devices to a secure and isolated network segment.

D. Reverse engineer the devices and build an in-house patch.

82. What type of motion detector senses changes in the electromagnetic fields in monitored areas?

A. Infrared

B. Wave pattern

C. Capacitance

D. Photoelectric

83. Mike has been tasked with preventing an outbreak of malware like Mirai, a botnet that targeted IP-based cameras and routers. What type of systems should be protected in his organization?

A. Servers

B. SCADA

C. Mobile devices

D. Internet of Things (IoT) devices

84. Which one of the following statements is correct about the Biba model of access control?

A. It addresses confidentiality and integrity.

B. It addresses integrity and availability.

C. It prevents covert channel attacks.

D. It focuses on protecting objects from integrity threats.

85. In Transport Layer Security, what type of key is used to encrypt the actual content of communications between a web server and a client?

A. Ephemeral session key

B. Client's public key

C. Server's public key

D. Server's private key

86. Beth would like to include technology in a secure area of her data center to protect against unwanted electromagnetic emanations. What technology would assist her with this goal?

A. Heartbeat sensor

B. Faraday cage

C. Piggybacking

D. WPA2

87. In a virtualized computing environment, what component is responsible for enforcing separation between guest machines?

A. Guest operating system

B. Hypervisor

C. Kernel

D. Protection manager

88. Rick is an application developer who works primarily in Python. He recently decided to evaluate a new service where he provides his Python code to a vendor who then executes it on their server environment. What type of cloud computing environment is this service?

A. SaaS

B. PaaS

C. IaaS

D. CaaS

89. A component failure in the primary HVAC system leads to a high temperature alarm in the data center that Kim manages. After resolving the issue, what should Kim consider to prevent future issues like this?

A. A closed loop chiller

B. Redundant cooling systems

C. Swamp coolers

D. Relocating the data center to a colder climate

90. Tommy is planning to implement a power conditioning UPS for a rack of servers in his data center. Which one of the following conditions will the UPS be unable to protect against if it persists for an extended period of time?

A. Fault

B. Blackout

C. Sag

D. Noise

91. Which one of the following humidity values is within the acceptable range for a data center operation?

A. 0 percent

B. 10 percent

C. 25 percent

D. 40 percent

92. Kristen's organization suffered a ransomware infection and has lost access to critical business data. She is considering paying the ransom to regain access to her data. Which of the following statements about this payment are correct? (Select all that apply.)

A. Payment of the ransom may be illegal.

B. Payment of the ransom may result in further demands for payments.

C. Payment of the ransom guarantees access to the decryption key.

D. Payment of the ransom may cause a data breach.

93. Alex's employer creates most of their work output as PDF files. Alex is concerned about limiting the audience for the PDF files to those individuals who have paid for them. What technology can he use to most effectively control the access to and distribution of these files?

A. EDM

B. Encryption

C. Digital signatures

D. DRM

94. As part of his team's forensic investigation process, Matt signs out drives and other evidence from an evidence storage facility before working with them. What type of documentation is he creating?

A. Criminal

B. Chain of custody

C. Civil

D. CYA

95. Todd believes that a digital certificate used by his organization has been compromised and he wants to add it to the certificate revocation list (CRL). What element of the certificate goes on the CRL?

A. Serial number

B. Public key

C. Digital signature

D. Private key

96. Alison is examining a digital certificate presented to her by her bank's website. Which one of the following requirements is not necessary for her to trust the digital certificate?

A. She knows that the server belongs to the bank.

B. She trusts the certificate authority.

C. She verifies that the certificate is not listed on a CRL.

D. She verifies the digital signature on the certificate.

97. Which one of the following is an example of a covert timing channel when used to exfiltrate information from an organization?

A. Sending an electronic mail message

B. Posting a file on a peer-to-peer file sharing service

C. Typing with the rhythm of Morse code

D. Writing data to a shared memory space

98. Which one of the following would be a reasonable application for the use of self-signed digital certificates?

A. Digital commerce website

B. Banking application

C. Internal scheduling application

D. Customer portal

99. Ron is investigating a security incident that took place at a highly secure government facility. He believes that encryption keys were stolen during the attack and finds evidence that the attackers used dry ice to freeze an encryption component. What type of attack was likely attempted?

A. Side channel attack

B. Brute-force attack

C. Timing attack

D. Fault injection attack

100. Match the following numbered security models with the appropriate lettered security descriptions:

Security models

1. Clark-Wilson
2. Graham-Denning
3. Bell-LaPadula
4. Biba

Descriptions

A. This model blocks lower-classified objects from accessing higher-classified objects, thus ensuring confidentiality.

B. The * property of this model can be summarized as "no write-up."

C. This model uses security labels to grant access to objects via transformation procedures and a restricted interface model.

D. This model focuses on the secure creation and deletion of subjects and objects using eight primary protection rules or actions.

101. Match each of these following numbered architecture security concepts with the appropriate lettered description:

Architectural security concepts

1. Time of check
2. Covert channel

3. Time of use
4. Maintenance hooks
5. Parameter checking
6. Race condition

Descriptions

A. A method used to pass information over a path not normally used for communication

B. The exploitation of the reliance of a system's behavior on the sequence of events that occur externally

C. The time at which the subject checks whether an object is available

D. The time at which a subject can access an object

E. An access method known only to the developer of the system

F. A method that can help prevent buffer overflow attacks

1. Gary wants to distribute a large file and prefers a peer-to-peer CDN. Which of the following is the most common example of this type of technology?
   - **A.** CloudFlare
   - **B.** BitTorrent
   - **C.** Amazon CloudFront
   - **D.** Akamai Edge

2. During a security assessment of a wireless network, Jim discovers that LEAP is in use on a network using WPA. What recommendation should Jim make?
   - **A.** Continue to use LEAP. It provides better security than TKIP for WPA networks.
   - **B.** Use an alternate protocol like PEAP or EAP-TLS and implement WPA2 if supported.
   - **C.** Continue to use LEAP to avoid authentication issues, but move to WPA2.
   - **D.** Use an alternate protocol like PEAP or EAP-TLS, and implement Wired Equivalent Privacy to avoid wireless security issues.

3. Ben has connected his laptop to his tablet PC using an 802.11ac connection. What wireless network mode has he used to connect these devices?
   - **A.** Infrastructure mode
   - **B.** Wired extension mode
   - **C.** Ad hoc mode
   - **D.** Standalone mode

4. Selah's and Nick's PCs simultaneously send traffic by transmitting at the same time. What network term describes the range of systems on a network that could be affected by this same issue?
   - **A.** The subnet
   - **B.** The supernet
   - **C.** A collision domain
   - **D.** A broadcast domain

5. Sarah is manually reviewing a packet capture of TCP traffic and finds that a system is setting the RST flag in the TCP packets it sends repeatedly during a short period of time. What does this flag mean in the TCP packet header?
   - **A.** RST flags mean "Rest." The server needs traffic to briefly pause.
   - **B.** RST flags mean "Relay-set." The packets will be forwarded to the address set in the packet.
   - **C.** RST flags mean "Resume Standard." Communications will resume in their normal format.
   - **D.** RST means "Reset." The TCP session will be disconnected.

6. Gary is deploying a wireless network and wants to deploy the fastest possible wireless technology. Which one of the following wireless networking standards should he use?
   - **A.** 802.11a
   - **B.** 802.11g
   - **C.** 802.11n
   - **D.** 802.11ac

7. Michele wants to replace FTP traffic with a secure replacement. What secure protocol should she select instead?
   - **A.** TFTP
   - **B.** HFTPS
   - **C.** SecFTP
   - **D.** SFTP

8. Jake has been told that there is a layer 3 problem with his network. Which of the following is associated with layer 3 in the OSI model?
   - **A.** IP addresses
   - **B.** TCP and UDP protocols
   - **C.** MAC addresses
   - **D.** Sending and receiving bits via hardware

9. Frank is responsible for ensuring that his organization has reliable, supported network hardware. Which of the following is not a common concern for network administrators as they work to ensure their network continues to be operational?
   - **A.** If the devices have vendor support
   - **B.** If the devices are under warranty
   - **C.** If major devices support redundant power supplies
   - **D.** If all devices support redundant power supplies

10. Brian is selecting an authentication protocol for a PPP connection. He would like to select an option that encrypts both usernames and passwords and protects against replay using a challenge/response dialog. He would also like to reauthenticate remote systems periodically. Which protocol should he use?
    - **A.** PAP
    - **B.** CHAP
    - **C.** EAP
    - **D.** LEAP

11. Which one of the following protocols is commonly used to provide back-end authentication services for a VPN?
    - **A.** HTTPS
    - **B.** RADIUS

C. ESP

D. AH

12. Isaac wants to ensure that his VoIP session initialization is secure. What protocol should he ensure is enabled and required?

A. SVOIP

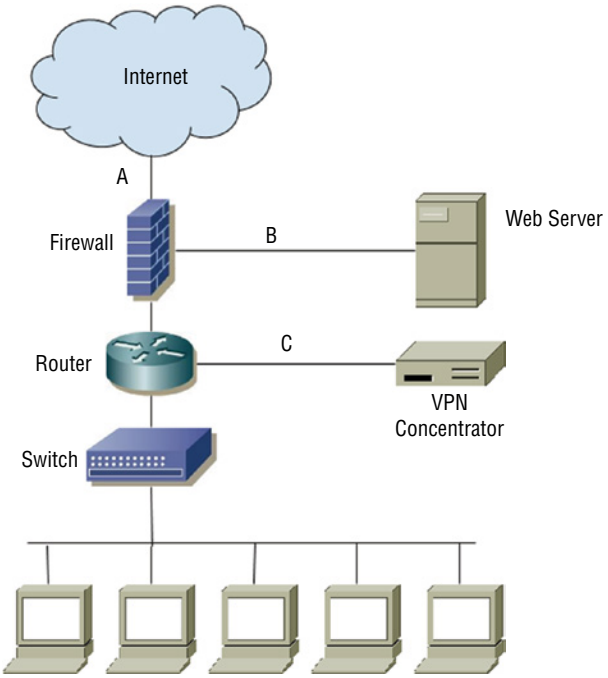
B. PBSX

C. SIPS

D. SRTP

For questions 13–15, please refer to the following scenario and diagram:

Chris is designing layered network security for his organization.



13. What type of firewall design is shown in the diagram?

A. A single-tier firewall

B. A two-tier firewall

C. A three-tier firewall

D. A four-tier firewall

14. If the VPN grants remote users the same access to network and system resources as local workstations have, what security issue should Chris raise?

A. VPN users will not be able to access the web server.

B. There is no additional security issue; the VPN concentrator's logical network location matches the logical network location of the workstations.

C. Web server traffic is not subjected to stateful inspection.

D. VPN users should only connect from managed PCs.

15. If Chris wants to stop cross-site scripting attacks against the web server, what is the best device for this purpose, and where should he put it?

A. A firewall, location A

B. An IDS, location A

C. An IPS, location B

D. A WAF, location C

16. Susan is deploying a routing protocol that maintains a list of destination networks with metrics that include the distance in hops to them and the direction traffic should be sent to them. What type of protocol is she using?

A. A link-state protocol

B. A link-distance protocol

C. A destination metric protocol

D. A distance-vector protocol

17. Ben has configured his network to not broadcast an SSID. Why might Ben disable SSID broadcast, and how could his SSID be discovered?

A. Disabling SSID broadcast prevents attackers from discovering the encryption key. The SSID can be recovered from decrypted packets.

B. Disabling SSID broadcast hides networks from unauthorized personnel. The SSID can be discovered using a wireless sniffer.

C. Disabling SSID broadcast prevents issues with beacon frames. The SSID can be recovered by reconstructing the BSSID.

D. Disabling SSID broadcast helps avoid SSID conflicts. The SSID can be discovered by attempting to connect to the network.

18. What network tool can be used to protect the identity of clients while providing Internet access by accepting client requests, altering the source addresses of the requests, mapping requests to clients, and sending the modified requests out to their destination?

A. A switch

B. A proxy

C. A router

D. A firewall

19. Susan wants to secure her communications traffic via multiple internet service providers as it is sent to her company's second location. What technology should she use to protect the traffic for an always on, always connected link between the sites?

A. FCoE

B. SDWAN

C. A point-to-point IPsec VPN

D. Zigbee

20. Melissa wants to combine multiple physical networks in her organization in a way that is transparent to users but allows the resources to be allocated as needed for networked services. What type of network should she deploy?

A. iSCSI

B. A virtual network

C. SDWAN

D. A CDN

21. Which email security solution provides two major usage modes: (1) signed messages that provide integrity, sender authentication, and nonrepudiation; and (2) an enveloped message mode that provides integrity, sender authentication, and confidentiality?

A. S/MIME

B. MOSS

C. PEM

D. DKIM

22. During a security assessment, Jim discovers that the organization he is working with uses a multilayer protocol to handle SCADA systems and recently connected the SCADA network to the rest of the organization's production network. What concern should he raise about serial data transfers carried via TCP/IP?

A. SCADA devices that are now connected to the network can now be attacked over the network.

B. Serial data over TCP/IP cannot be encrypted.

C. Serial data cannot be carried in TCP packets.

D. TCP/IP's throughput can allow for easy denial-of-service attacks against serial devices.

23. Ben provides networking and security services for a small chain of coffee shops. The coffee shop chain wants to provide secure, free wireless for customers. Which of the following is the best option available to Ben to allow customers to connect securely to his wireless network without needing a user account if Ben does not need to worry about protocol support issues?

A. Use WPA2 in PSK mode.

B. Use WPA3 in SAE mode.

C. Use WPA2 in Enterprise mode.

D. Use a captive portal.

24. Alicia's company has implemented multifactor authentication using SMS messages to provide a numeric code. What is the primary security concern that Alicia may want to express about this design?

A. SMS messages are not encrypted.

B. SMS messages can be spoofed by senders.

C. SMS messages may be received by more than one phone.

D. SMS messages may be stored on the receiving phone.

25. What speed and frequency range are used by 802.11n?

A. 5 GHz only

B. 900 MHz and 2.4 GHz

C. 2.4 GHz and 5 GHz

D. 2.4 GHz only

26. The Address Resolution Protocol (ARP) and the Reverse Address Resolution Protocol (RARP) operate at what layer of the OSI model?

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 4

27. Which of the following is a converged protocol that allows storage mounts over TCP, and which is frequently used as a lower-cost alternative to Fibre Channel?

A. MPLS

B. SDN

C. VoIP

D. iSCSI

28. Chris is building an Ethernet network and knows that he needs to span a distance of more than 150 meters with his 1000BaseT network. What network technology should he use to help with this?

A. Install a repeater, a switch, or a concentrator before 100 meters.

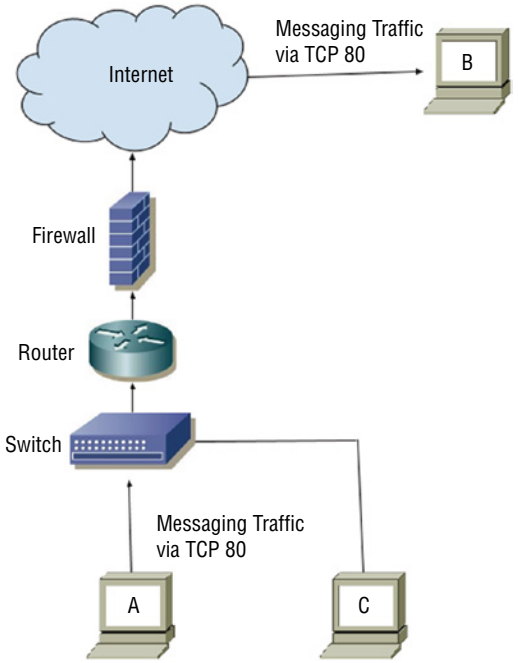
B. Use Category 7 cable, which has better shielding for higher speeds.

C. Install a gateway to handle the distance.

D. Use STP cable to handle the longer distance at high speeds.

For questions 29–31, please refer to the following scenario and diagram:

Selah's organization has used a popular messaging service for a number of years. Recently, concerns have been raised about the use of messaging.



29. What protocol is the messaging traffic most likely to use based on the diagram?

A. SLACK

B. HTTP

C. SMTP

D. HTTPS

30. What security concern does sending internal communications from A to B raise?

A. The firewall does not protect system B.

B. System C can see the broadcast traffic from system A to B.

C. It is traveling via an unencrypted protocol.

D. Messaging does not provide nonrepudation.

31. How could Selah's company best address a desire for secure messaging for users of internal systems A and C?

A. Use a third-party messaging service.

B. Implement and use a locally hosted service.

C. Use HTTPS.

D. Discontinue use of messaging and instead use email, which is more secure.

32. Which of the following drawbacks is a concern when multilayer protocols are allowed?

A. A range of protocols may be used at higher layers.

B. Covert channels are allowed.

C. Filters cannot be bypassed.

D. Encryption can't be incorporated at multiple layers.

33. Which of the following is not an example of a converged protocol?

A. MIME

B. FCoE

C. iSCSI

D. VoIP

34. Chris uses a cellular hot spot to provide internet access when he is traveling. If he leaves the hot spot connected to his PC while his PC is on his organization's corporate network, what security issue might he cause?

A. Traffic may not be routed properly, exposing sensitive data.

B. His system may act as a bridge from the internet to the local network.

C. His system may be a portal for a reflected DDoS attack.

D. Security administrators may not be able to determine his IP address if a security issue occurs.

35. In her role as an information security professional, Susan has been asked to identify areas where her organization's wireless network may be accessible even though it isn't intended to be. What should Susan do to determine where her organization's wireless network is accessible?

A. A site survey

B. Warwalking

C. Wardriving

D. A design map

36. What features can IPsec provide for secure communication?

A. Encryption, access control, nonrepudiation and message authentication

B. Protocol convergence, content distribution, micro-segmentation, and network virtualization

C. Encryption, authorization, nonrepudiation, and message integrity checking

D. Micro-segmentation, network virtualization, encryption, and message authentication

37. Casey has been asked to determine if Zigbee network traffic can be secured in transit. What security mechanism does Zigbee use to protect data traffic?

A. 3DES encryption

B. AES encryption

C. ROT13 encryption

D. Blowfish encryption

38. Sue modifies her MAC address to one that is allowed on a network that uses MAC filtering to provide security. What is the technique Sue used, and what nonsecurity issue could her actions cause?

A. Broadcast domain exploit, address conflict

B. Spoofing, token loss

C. Spoofing, address conflict

D. Sham EUI creation, token loss

39. Joanna wants to deploy 4G LTE as an out-of-band management solution for devices at remote sites. Which of the following security capabilities is not commonly available from 4G service providers?

A. Encryption capabilities

B. Device-based authentication

C. Dedicated towers and antennas for secure service subscribers

D. SIM-based authentication

40. SMTP, HTTP, and SNMP all occur at what layer of the OSI model?

A. Layer 4

B. Layer 5

C. Layer 6

D. Layer 7

41. Melissa uses the ping utility to check whether a remote system is up as part of a penetration testing exercise. If she does not want to see her own ping packets, what protocol should she filter out from her packet sniffer's logs?

A. UDP

B. TCP

C. IP

D. ICMP

42. Selah wants to provide port-based authentication on her network to ensure that clients must authenticate before using the network. What technology is an appropriate solution for this requirement?

A. 802.11a

B. 802.3

C. 802.15.1

D. 802.1x

43. Ben has deployed a 1000BaseT gigabit network and needs to run a cable across a large building. If Ben is running his link directly from a switch to another switch in that building, what is the maximum distance Ben can cover according to the 1000BaseT specification?

A. 2 kilometers

B. 500 meters

C. 185 meters

D. 100 meters

44. What security control does MAC cloning attempt to bypass for wired networks?

A. Port security

B. VLAN hopping

C. 802.1q trunking

D. Etherkiller prevention

45. The company that Kathleen works for has moved to remote work for most employees and wants to ensure that the multimedia collaboration platform that they use for voice, video, and text-based collaboration is secure. Which of the following security options will provide the best user experience while providing appropriate security for communications?

A. Require software-based VPN to the corporate network for all use of the collaboration platform.

B. Require the use of SIPS and SRTP for all communications.

C. Use TLS for all traffic for the collaboration platform.

D. Deploy secure VPN endpoints to each remote location and use a point-to-point VPN for communications.

46. Chris wants to use a low-power, personal area network wireless protocol for a device he is designing. Which of the following wireless protocols is best suited to creating small, low-power devices that can connect to each other at relatively short distances across buildings or rooms?

A. WiFi

B. Zigbee

C. NFC

D. Infrared

47. Which of the following options includes standards or protocols that exist in layer 6 of the OSI model?

A. NFS, SQL, and RPC

B. TCP, UDP, and TLS

C. JPEG, ASCII, and MIDI

D. HTTP, FTP, and SMTP

48. Cameron is worried about distributed denial-of-service attacks against his company's primary web application. Which of the following options will provide the most resilience against large-scale DDoS attacks?

A. A CDN

B. Increasing the number of servers in the web application server cluster

C. Contract for DDoS mitigation services via the company's ISP

D. Increasing the amount of bandwidth available from one or more ISPs

49. There are four common VPN protocols. Which group listed contains all of the common VPN protocols?

A. PPTP, LTP, L2TP, IPsec

B. PPP, L2TP, IPsec, VNC

C. PPTP, L2F, L2TP, IPsec

D. PPTP, L2TP, IPsec, SPAP

50. Wayne wants to deploy a secure voice communication network. Which of the following techniques should he consider? (Select all that apply.)

A. Use a dedicated VLAN for VoIP phones and devices.

B. Require the use of SIPS and SRTP.

C. Require the use of VPN for all remote VoIP devices.

D. Implement a VoIP IPS.

51. Which OSI layer includes electrical specifications, protocols, and interface standards?

A. The Transport layer

B. The Device layer

C. The Physical layer

D. The Data Link layer

52. Ben is designing a WiFi network and has been asked to choose the most secure option for the network. Which wireless security standard should he choose?

A. WPA2

B. WPA

C. WEP

D. WPA3

53. Kathleen has two primary locations in a town and wants the two environments to appear like the same local network. Each location has a router, switches, and wireless access points deployed to them. What technology would best work to allow her to have the two facilities appear to be on the same network segment?

A. SDWAN

B. VXLAN

C. VMWAN

D. iSCSI

54. Segmentation, sequencing, and error checking all occur at what layer of the OSI model that is associated with SSL, TLS, and UDP?

A. The Transport layer

B. The Network layer

C. The Session layer

D. The Presentation layer

55. The Windows `ipconfig` command displays the following information:

BC-5F-F4-7B-4B-7D

What term describes this, and what information can usually be gathered from it?

A. The IP address, the network location of the system

B. The MAC address, the network interface card's manufacturer

C. The MAC address, the media type in use

D. The IPv6 client ID, the network interface card's manufacturer

56. Chris has been asked to choose between implementing PEAP and LEAP for wireless authentication. What should he choose, and why?

A. LEAP, because it fixes problems with TKIP, resulting in stronger security

B. PEAP, because it implements CCMP for security

C. LEAP, because it implements EAP-TLS for end-to-end session encryption

D. PEAP, because it can provide a TLS tunnel that encapsulates EAP methods, protecting the entire session

57. Ben is troubleshooting a network and discovers that the NAT router he is connected to has the 192.168.x.x subnet as its internal network and that its external IP is 192.168.1.40. What problem is he encountering?

A. 192.168.x.x is a nonroutable network and will not be carried to the internet.

B. 192.168.1.40 is not a valid address because it is reserved by RFC 1918.

C. Double NATing is not possible using the same IP range.

D. The upstream system is unable to de-encapsulate his packets, and he needs to use PAT instead.

58. What is the default subnet mask for a Class B network?

A. 255.0.0.0

B. 255.255.0.0

C. 255.254.0.0

D. 255.255.255.0

59. Jim's organization uses a traditional PBX for voice communication. What is the most common security issue that its internal communications are likely to face, and what should he recommend to prevent it?

A. Eavesdropping, encryption

B. Man-in-the-middle attacks, end-to-end encryption

C. Eavesdropping, physical security

D. Wardialing, deploy an IPS

60. What technical difference separates wireless communication via WiFi and LiFi?

A. LiFi is not susceptible to electromagnetic interference.

B. LiFi cannot be used to deliver broadband speeds.

C. WiFi is not susceptible to electromagnetic interference.

D. WiFi cannot be used to deliver broadband speeds.

61. Selah's organization has deployed VoIP phones on the same switches that the desktop PCs are on. What security issue could this create, and what solution would help?

A. VLAN hopping; use physically separate switches.

B. VLAN hopping; use encryption.

C. Caller ID spoofing; MAC filtering.

D. Denial-of-service attacks; use a firewall between networks.

For questions 62–65, please refer to the following scenario:

Susan is designing her organization's new network infrastructure for a branch office.

62. Susan wants to use a set of nonroutable IP addresses for the location's internal network addresses. Using your knowledge of secure network design principles and IP networking, which of the following IP ranges are usable for that purpose? (Select all that apply.)

A. 172.16.0.0/12

B. 192.168.0.0/16

C. 128.192.0.0/24

D. 10.0.0.0/8

63. Susan knows that she will need to implement a WiFi network for her customers and wants to gather information about the customers, such as their email address, without having to provide them with a wireless network password or key. What type of solution would provide this combination of features?

A. NAC

B. A captive portal

C. Pre-shared keys

D. WPA3's SAE mode

64. With her wireless network set up, Susan moves on to ensuring that her network will remain operational even if disruptions occur. What is the simplest way she can ensure that her network devices, including her router, access points, and network switches, stay on if a brownout or other temporary power issue occurs?

A. Purchase and install a generator with an automatic start.

B. Deploy dual power supplies for all network devices.

C. Install UPS systems to cover all network devices that must remain online.

D. Contract with multiple different power companies for redundant power.

65. Susan wants to provide 10 gigabit network connections to devices in the facility where the new branch will operate. What connectivity options does she have for structured wiring that can meet those speeds? (Select all that apply.)

A. Cat5e

B. Fiber

C. Cat6

D. Coaxial cable

66. Data streams occur at what three layers of the OSI model?

A. Application, Presentation, and Session

B. Presentation, Session, and Transport

C. Physical, Data Link, and Network

D. Data Link, Network, and Transport

67. Lucca wants to protect endpoints that are in production use but that are no longer supported and cannot be patched from network attacks. What should he do to best protect these devices?

A. Install a firewall on the device.

B. Disable all services and open ports on the devices.

C. Place a hardware network security device in front of the devices.

D. Unplug the devices from the network because they cannot be properly secured.

68. Selah's networking team has been asked to identify a technology that will allow them to dynamically change the organization's network by treating the network like code. What type of architecture should she recommend?

A. A network that follows the 5-4-3 rule

B. A converged network

C. A software-defined network

D. A hypervisor-based network

69. Jason knows that protocols using the OSI model rely on encapsulation as data moves from layer to layer. What is added at each layer as data flows up the OSI layers?

A. Information is added to the header.

B. Information is added to the main body of the data.

C. The data is encrypted with a new secret key.

D. A security envelope that provides perfect forward secrecy

70. During a troubleshooting process, the support technician that Alyssa is talking to states that the problem is a layer 3 problem. Which of the following possible issues is not a layer 3 problem?

A. A TTL mismatch

B. An MTU mismatch

C. An incorrect ACL

D. A broken network cable

71. During a review of her organization's network, Angela discovered that it was suffering from broadcast storms and that contractors, guests, and organizational administrative staff were on the same network segment. What design change should Angela recommend?

A. Require encryption for all users.

B. Install a firewall at the network border.

C. Enable spanning tree loop detection.

D. Segment the network based on functional requirements.

72. ICMP, RIP, and network address translation all occur at what layer of the OSI model?

A. Layer 1

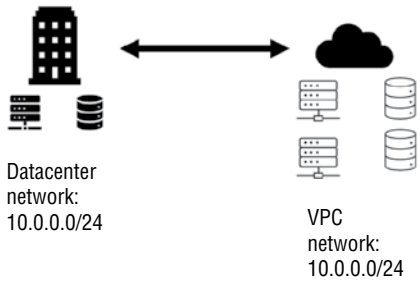
B. Layer 2

C. Layer 3

D. Layer 4

For questions 73–75, please refer to the following scenario:

Ben is an information security professional at an organization that is replacing its physical servers with cloud-hosted virtual machines. As the organization builds its virtual environment, it is moving toward a hybrid cloud operational model with some systems and services remaining in its local data center and others hosted in the cloud. The following diagram shows the local data center and cloud VPC's network IP ranges, which you should consider as you answer the questions.



73. Ben wants to ensure that the instance-to-instance (system-to-system) traffic in his cloud-hosted infrastructure as a service environment is secure. What can he do to fully ensure that the virtualized network traffic is not being captured and analyzed?

A. Prevent the installation of a packet sniffer on all hosts.

B. Disable promiscuous mode for all virtual network interfaces.

C. Disallow the use of any virtual taps.

D. Encrypt all traffic between hosts.

74. What issue is most likely to occur due to the subnets configured for the data center and VPC?

A. IP address conflicts

B. Routing loops

C. MAC address conflicts

D. All of the above

75. Ben wants to use multiple internet service providers (ISPs) to connect to his cloud VPC to ensure reliable access and bandwidth. What technology can he use to manage and optimize those connections?

A. FCoE

B. VXLAN

C. SDWAN

D. LiFi

76. WPA2's Counter Mode Cipher Block Chaining Message Authentication Mode Protocol (CCMP) is based on which common encryption scheme?

A. DES

B. 3DES

C. AES

D. TLS

77. When a host on an Ethernet network detects a collision and transmits a jam signal, what happens next?
    - **A.** The host that transmitted the jam signal is allowed to retransmit while all other hosts pause until that transmission is received successfully.
    - **B.** All hosts stop transmitting, and each host waits a random period of time before attempting to transmit again.
    - **C.** All hosts stop transmitting, and each host waits a period of time based on how recently it successfully transmitted.
    - **D.** Hosts wait for the token to be passed and then resume transmitting data as they pass the token.

78. Mark is concerned about the physical security of his network cables. What type of network connection would be the hardest to tap without specialized equipment?
    - **A.** WiFi
    - **B.** Bluetooth
    - **C.** Cat5/Cat6 twisted pair
    - **D.** Fiber optic

79. Rich wants to connect his network to a building a half-mile away from his current location. There are trees and terrain features along the way, but a road passes between the trees to the other location. What type of transmission media is best suited to this type of deployment?
    - **A.** Ethernet cable with repeaters every 200 to 300 yards
    - **B.** A WiFi directional antenna
    - **C.** Fiber-optic cable
    - **D.** A LiFi system

80. What challenge is most common for endpoint security system deployments?
    - **A.** Compromises
    - **B.** The volume of data
    - **C.** Monitoring encrypted traffic on the network
    - **D.** Handling non-TCP protocols

81. What type of address is 127.0.0.1?
    - **A.** A public IP address
    - **B.** An RFC 1918 address
    - **C.** An APIPA address
    - **D.** A loopback address

82. Susan is writing a best practices statement for her organizational users who need to use Bluetooth. She knows that there are many potential security issues with Bluetooth and wants to provide the best advice she can. Which of the following sets of guidance should Susan include?

A. Use Bluetooth's built-in strong encryption, change the default PIN on your device, turn off discovery mode, and turn off Bluetooth when it's not in active use.

B. Use Bluetooth only for those activities that are not confidential, change the default PIN on your device, turn off discovery mode, and turn off Bluetooth when it's not in active use.

C. Use Bluetooth's built-in strong encryption, use extended (eight digits or longer) Bluetooth PINs, turn off discovery mode, and turn off Bluetooth when it's not in active use.

D. Use Bluetooth only for those activities that are not confidential, use extended (eight digits or longer) Bluetooth PINs, turn off discovery mode, and turn off Bluetooth when it's not in active use.

83. What type of networking device is most commonly used to assign endpoint systems to VLANs?

A. Firewall

B. Router

C. Switch

D. Hub

84. Steve has been tasked with implementing a network storage protocol over an IP network. What storage-centric converged protocol is he likely to use in his implementation?

A. MPLS

B. FCoE

C. SDN

D. VoIP

85. Michelle is told that the organization that she is joining uses an SD-WAN controller architecture to manage their WAN connections. What can she assume about how the network is managed and controlled? (Select all that apply.)

A. The network uses predefined rules to optimize performance.

B. The network conducts continuous monitoring to support better performance.

C. The network uses self-learning techniques to respond to changes in the network.

D. All connections are managed by the organization's primary internet service provider.

86. Which of the following shows the layers of the OSI model in correct order, from layer 1 to layer 7? Place the layers of the OSI model shown here in the appropriate order, from layer 1 to layer 7.

A. Layer 1 = Data Link; Layer 2 = Physical; Layer 3 = Network; Layer 4 = Transport; Layer 5 = Session; Layer 6 = Presentation; Layer 7 = Applications

B. Layer 1 = Physical; Layer 2 = Data Link; Layer 3 = Network; Layer 4 = Transport; Layer 5 = Session; Layer 6 = Presentation; Layer 7 = Applications

C. Layer 1 = Physical; Layer 2 = Data Link; Layer 3 = Network; Layer 4 = Transport; Layer 5 = Session; Layer 6 = Applications; Layer 7 = Presentation

D. Layer 1 = Physical; Layer 2 = Data Link; Layer 3 = Network; Layer 4 = Session; Layer 5 = Transport; Layer 6 = Presentation; Layer 7 = Applications

87. Valerie enables port security on the switches on her network. What type of attack is she most likely trying to prevent?

A. IP spoofing

B. MAC aggregation

C. CAM table flooding

D. VLAN hopping

88. Alaina wants to ensure that systems are compliant with her network security settings before they are allowed on the network and wants to ensure that she can test and validate system settings as possible. What type of NAC system should she deploy?

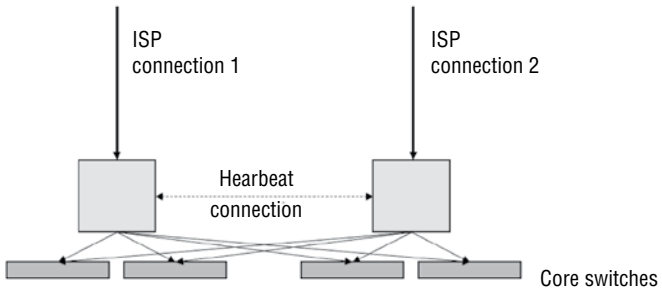
A. A pre-admit, clientless NAC system

B. A postadmission, client-based NAC system

C. A pre-admit, client-based NAC system

D. A postadmission, clientless NAC system

89. Derek wants to deploy redundant core routers, as shown in the diagram. What model of high availability clustering will provide him with the greatest throughput?



A. Active/active

B. Line interactive

C. Active/passive

D. Nearline

90. Angela needs to choose between the following protocols for secure authentication and doesn't want to create unneeded technical complexity. Which authentication protocol should she choose and why?

A. EAP, because it provides strong encryption by default

B. LEAP, because it provides frequent reauthentication and changing of WEP keys

C. PEAP, because it provides encryption and doesn't suffer from the same vulnerabilities that LEAP does

D. EAP-TLS

91. What is a frequent concern for systems that require high-performing internet connectivity when satellite internet is the only available option?

A. Security

B. Compatibility with protocols like LiFi

C. Compatibility with protocols like Zigbee

D. Latency

92. What layer of an SDN implementation uses programs to communicate needs for resources via APIs?

A. The data plane

B. The control plane

C. The application plane

D. The monitoring plane

93. Which of the following is not a drawback of multilayer protocols?

A. They can allow filters and rules to be bypassed.

B. They can operate at higher OSI levels.

C. They can allow covert channels.

D. They can allow network segment boundaries to be bypassed.

94. Place the following layers of the TCP/IP model in order, starting with the Application layer and moving down the stack.

1. Application layer
2. Network Access layer
3. Internet layer
4. Transport layer

A. 1, 2, 3, 4

B. 1, 4, 2, 3

C. 1, 4, 3, 2

D. 4, 1, 3, 2

95. What is the maximum speed that Category 5e cable is rated for?

A. 5 Mbps

B. 10 Mbps

C. 100 Mbps

D. 1000 Mbps

96. What are two primary advantages that 5G networks have over 4G networks? (Select all that apply.)

A. Anti-jamming features

B. Enhanced subscriber identity protection

C. Mutual authentication capabilities

D. Multifactor authentication

97. What function does VXLAN perform in a data center environment?

A. It removes limitations due to maximum distance for Ethernet cables.

B. It allows multiple subnets to exist in the same IP space with hosts using the same IP addresses.

C. It tunnels layer 2 connections over a layer 3 network, stretching them across the underlying layer 3 network.

D. All of the above

98. Chris is setting up a hotel network and needs to ensure that systems in each room or suite can connect to each other, but systems in other suites or rooms cannot. At the same time, he needs to ensure that all systems in the hotel can reach the internet. What solution should he recommend as the most effective business solution?

A. Per-room VPNs

B. VLANs

C. Port security

D. Firewalls

99. During a forensic investigation, Charles is able to determine the Media Access Control (MAC) address of a system that was connected to a compromised network. Charles knows that MAC addresses are tied back to a manufacturer or vendor and are part of the fingerprint of the system. To which OSI layer does a MAC address belong?

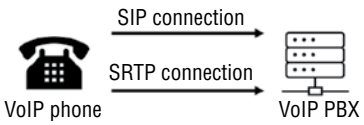
A. The Application layer

B. The Session layer

C. The Physical layer

D. The Data Link layer

100. Mikayla is reviewing her organization's VoIP environment configuration and finds a diagram that shows the following design. What concern should she express?



A. The voice connection is unencrypted and could be listened to.

B. There are no security issues in this diagram.

C. The session initialization connection is unencrypted and could be viewed.

D. Both the session initialization and voice data connection are unencrypted and could be captured and analyzed.

1. Which of the following is best described as an access control model that focuses on subjects and identifies the objects that each subject can access?
   - **A.** An access control list
   - **B.** An implicit denial list
   - **C.** A capability table
   - **D.** A rights management matrix

2. Jim's organization-wide implementation of IDaaS offers broad support for cloud-based applications. Jim's company does not have internal identity management staff and does not use centralized identity services. Instead, they rely upon Active Directory for AAA services. Which of the following options should Jim recommend to best handle the company's on-site identity needs?
   - **A.** Integrate on-site systems using OAuth.
   - **B.** Use an on-premises third-party identity service.
   - **C.** Integrate on-site systems using SAML.
   - **D.** Design an internal solution to handle the organization's unique needs.

3. Which of the following is not a weakness in Kerberos?
   - **A.** The KDC is a single point of failure.
   - **B.** Compromise of the KDC would allow attackers to impersonate any user.
   - **C.** Authentication information is not encrypted.
   - **D.** It is susceptible to password guessing.

4. Voice pattern recognition is what type of authentication factor?
   - **A.** Something you know
   - **B.** Something you have
   - **C.** Something you are
   - **D.** Somewhere you are

5. If Susan's organization requires her to log in with her username, a PIN, a password, and a retina scan, how many distinct authentication factor types has she used?
   - **A.** One
   - **B.** Two
   - **C.** Three
   - **D.** Four

6. Charles wants to deploy a credential management system (CMS). He wants to keep the keys as secure as possible. Which of the following is the best design option for his CMS implementation?
   - **A.** Use AES-256 instead of 3DES.
   - **B.** Use long keys.

C. Use an HSM.

D. Change passphrases regularly.

7. Brian is a researcher at a major university. As part of his research, he logs into a computing cluster hosted at another institution using his own university's credentials. Once logged in, he is able to access the cluster and use resources based on his role in a research project, as well as using resources and services in his home organization. What has Brian's home university implemented to make this happen?

A. Domain stacking

B. Federated identity management

C. Domain nesting

D. Hybrid login

8. Place the following steps in the order in which they occur during the Kerberos authentication process.

1. Client/server ticket generated
2. TGT generated
3. Client/TGS key generated
4. User accesses service
5. User provides authentication credentials

A. 5, 3, 2, 1, 4

B. 5, 4, 2, 1, 3

C. 3, 5, 2, 1, 4

D. 5, 3, 1, 2, 4

9. What major issue often results from decentralized access control?

A. Access outages may occur.

B. Control is not consistent.

C. Control is too granular.

D. Training costs are high.

10. Callback to a landline phone number is an example of what type of factor?

A. Something you know

B. Somewhere you are

C. Something you have

D. Something you are

11. Kathleen needs to set up an Active Directory trust to allow authentication with an existing Kerberos K5 domain. What type of trust does she need to create?

A. A shortcut trust

B. A forest trust

C. An external trust

D. A realm trust

12. Which of the following AAA protocols is the most commonly used?

A. TACACS

B. TACACS+

C. XTACACS

D. Super TACACS

13. Which of the following is not a single sign-on implementation?

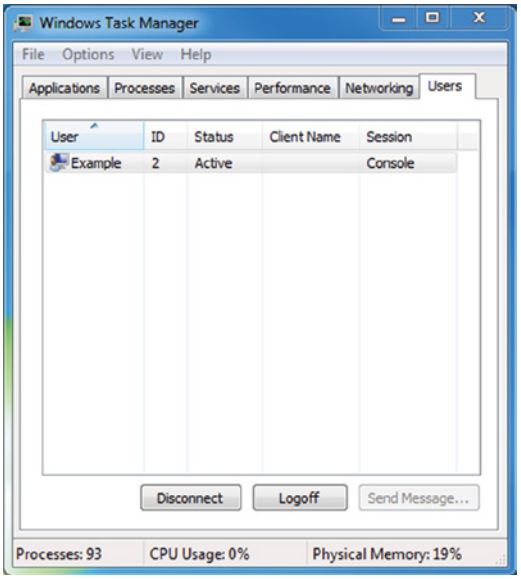
A. Kerberos

B. ADFS

C. CAS

D. RADIUS

14. As shown in the following image, a user on a Windows system is not able to use the Send Message functionality. What access control model best describes this type of limitation?



A. Least privilege

B. Need to know

C. Constrained interface

D. Separation of duties

15. What type of access controls allow the owner of a file to grant other users access to it using an access control list?

A. Role-based

B. Nondiscretionary

C. Rule-based

D. Discretionary

16. Alex's job requires him to see protected health information (PHI) to ensure proper treatment of patients. His access to their medical records does not provide access to patient addresses or billing information. What access control concept best describes this control?

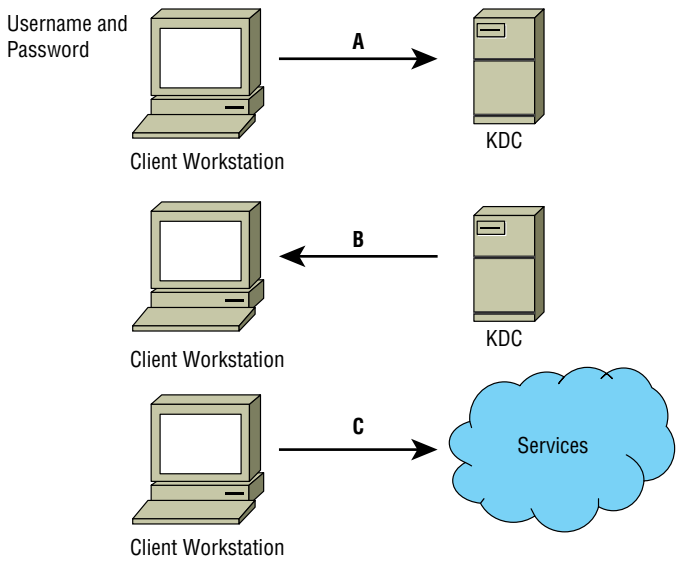
A. Separation of duties

B. Constrained interfaces

C. Context-dependent control

D. Need to know

For questions 17–19, please use your knowledge of the Kerberos logon process and refer to the following diagram:



17. At point A in the diagram, the client sends the username and password to the KDC. How is the username and password protected?

A. 3DES encryption

B. TLS encryption

C. SSL encryption

D. AES encryption

18. At point B in the diagram, what two important elements does the KDC send to the client after verifying that the username is valid?

A. An encrypted TGT and a public key

B. An access ticket and a public key

C. An encrypted, time-stamped TGT and a symmetric key encrypted with a hash of the user's password

D. An encrypted, time-stamped TGT and an access token

19. What tasks must the client perform before it can use the TGT?

A. It must generate a hash of the TGT and decrypt the symmetric key.

B. It must accept the TGT and decrypt the symmetric key.

C. It must decrypt the TGT and the symmetric key.

D. It must send a valid response using the symmetric key to the KDC and must install the TGT.

20. Jacob is planning his organization's biometric authentication system and is considering retina scans. What concern may be raised about retina scans by others in his organization?

A. Retina scans can reveal information about medical conditions.

B. Retina scans are painful because they require a puff of air in the user's eye.

C. Retina scanners are the most expensive type of biometric device.

D. Retina scanners have a high false positive rate and will cause support issues.

21. Mandatory access control is based on what type of model?

A. Discretionary

B. Group-based

C. Lattice-based

D. Rule-based

22. Greg wants to control access to iPads used throughout his organization as point-of-sale terminals. Which of the following methods should he use to allow logical access control for the devices in a shared environment?

A. Use a shared PIN for all point-of-sale terminals to make them easier to use.

B. Use OAuth to allow cloud logins for each user.

C. Issue a unique PIN to each user for the iPad they are issued.

D. Use Active Directory and user accounts for logins to the iPads using the AD userID and password.

23. What is the best way to provide accountability for the use of identities?

A. Logging

B. Authorization

C. Digital signatures

D. Type 1 authentication

24. Jim has worked in human relations, payroll, and customer service roles in his company over the past few years. What type of process should his company perform to ensure that he has appropriate rights?

A. Re-provisioning

B. Account review

C. Privilege creep

D. Account revocation

25. Biba is what type of access control model?

A. MAC

B. DAC

C. Role BAC

D. ABAC

26. Which of the following is a client/server protocol designed to allow network access servers to authenticate remote users by sending access request messages to a central server?

A. Kerberos

B. EAP

C. RADIUS

D. OAuth

27. Henry is working with a web application development team on their authentication and authorization process for his company's new application. The team wants to make session IDs as secure as possible. Which of the following is not a best practice that Henry should recommend?

A. The session ID token should be predictable.

B. The session ID should have at least 64 bits of entropy.

C. The session length should be at least 128 bits.

D. The session ID should be meaningless.

28. Angela uses a sniffer to monitor traffic from a RADIUS server configured with default settings. What protocol should she monitor, and what traffic will she be able to read?

A. UDP, none. All RADIUS traffic is encrypted.

B. TCP, all traffic but the passwords, which are encrypted.

C. UDP, all traffic but the passwords, which are encrypted.

D. TCP, none. All RADIUS traffic is encrypted.

29. What type of access control best describes NAC's posture assessment capability?

A. A mandatory access control

B. A risk-based access control

C. A discretionary access control

D. A role-based access control

30. When an application or system allows a logged-in user to perform specific actions, it is an example of what?

A. Roles

B. Group management

C. Logins

D. Authorization

31. Alex has been employed by his company for more than a decade and has held a number of positions in the company. During an audit, it is discovered that he has access to shared folders and applications because of his former roles. What issue has Alex's company encountered?

A. Excessive provisioning

B. Unauthorized access

C. Privilege creep

D. Account review

32. Geoff wants to prevent privilege escalation attacks in his organization. Which of the following practices is most likely to prevent horizontal privilege escalation?

A. Multifactor authentication

B. Limiting permissions for groups and accounts

C. Disabling unused ports and services

D. Sanitizing user inputs to applications

33. Jim's Microsoft Exchange environment includes servers that are located in local data centers at multiple business offices around the world as well as an Office 365 deployment for employees who are not located at one of those offices. Identities are created and used in both environments and will work in both. What type of federated system is Jim running?

A. A primary cloud system

B. A primary on-premise system

C. A hybrid system

D. A multitenant system

34. What type of access control scheme is shown in the following table?

Highly Sensitive	Red	Blue	Green
Confidential	Purple	Orange	Yellow
Internal Use	Black	Gray	White
Public	Clear	Clear	Clear

A. RBAC

B. DAC

C. MAC

D. TBAC

35. Michelle's company is creating a new division by splitting the marketing and communications departments into two separate groups. She wants to create roles that provide access to resources used by each group. What should she do to maintain the appropriate security and rights for each group?

A. Put both the marketing and communications teams into the existing group because they will have similar access requirements.

B. Keep the marketing team in the existing group and create a new communications group based on their specific needs.

C. Keep the communications team in the existing group and create a new marketing group based on their specific needs.

D. Create two new groups, assess which rights they need to perform their roles, and then add additional rights if required.

36. When a subject claims an identity, what process is occurring?

A. Login

B. Identification

C. Authorization

D. Token presentation

37. Dogs, guards, and fences are all common examples of what type of control?

A. Detective

B. Recovery

C. Administrative

D. Physical

38. Susan's organization is updating its password policy and wants to use the strongest possible passwords. What password requirement will have the highest impact in preventing brute-force attacks?

A. Change maximum age from 1 year to 180 days.

B. Increase the minimum password length from 8 characters to 16 characters.

C. Increase the password complexity so that at least three character classes (such as uppercase, lowercase, numbers, and symbols) are required.

D. Retain a password history of at least four passwords to prevent reuse.

39. Alaina is performing a regularly scheduled review for service accounts. Which of the following events should she be most concerned about?

A. An interactive login for the service account

B. A password change for the service account

C. Limitations placed on the service account's rights

D. Local use of the service account

40. When might an organization using biometrics choose to allow a higher FRR instead of a higher FAR?

A. When security is more important than usability

B. When false rejection is not a concern due to data quality

C. When the CER of the system is not known

D. When the CER of the system is very high

41. After recent reports of undesired access to workstations after hours, Derek has been asked to find a way to ensure that maintenance staff cannot log in to workstations in business offices. The maintenance staff members do have systems in their break rooms and their offices for the organization, which they still need access to. What should Derek do to meet this need?

A. Require multifactor authentication and only allow office staff to have multifactor tokens.

B. Use rule-based access control to prevent logins after hours in the business area.

C. Use role-based access control by setting up a group that contains all maintenance staff and then give that group rights to log into only the designated workstations.

D. Use geofencing to only allow logins in maintenance areas.

42. Nick wants to do session management for his web application. Which of the following are common web application session management techniques or methods? (Select all that apply.)

A. IP tracking

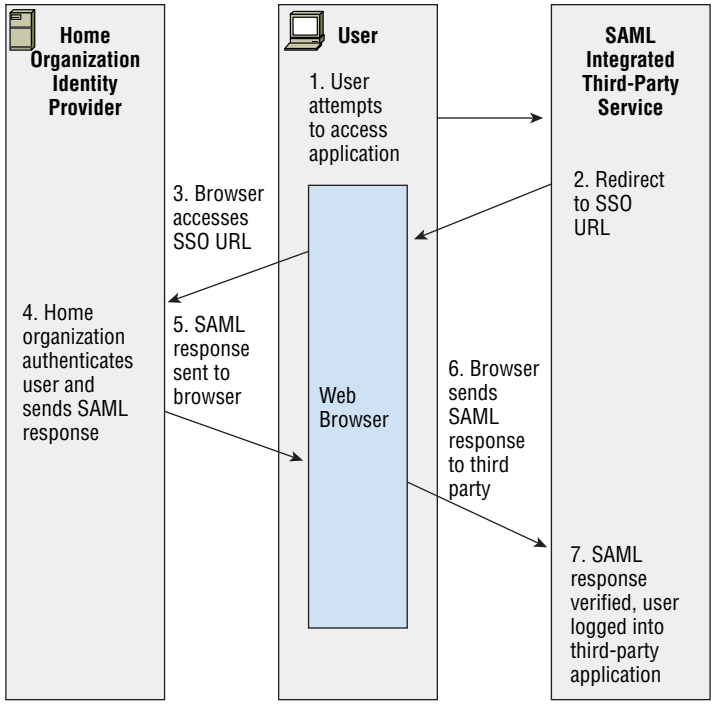
B. Cookies

C. URL rewriting

D. TLS tokens

For questions 43–45, please use your knowledge of SAML integrations and security architecture design and refer to the following scenario and diagram:

Alex is in charge of SAML integration with a major third-party partner that provides a variety of business productivity services for his organization.



43. Alex is concerned about eavesdropping on the SAML traffic and also wants to ensure that forged assertions will not be successful. What should he do to prevent these potential attacks?

A. Use SAML's secure mode to provide secure authentication.

B. Implement TLS using a strong cipher suite, which will protect against both types of attacks.

C. Implement TLS using a strong cipher suite and use digital signatures.

D. Implement TLS using a strong cipher suite and message hashing.

44. If Alex's organization is one that is primarily made up of off-site, traveling users, what availability risk does integration of critical business applications to on-site authentication create, and how could he solve it?

A. Third-party integration may not be trustworthy; use SSL and digital signatures.

B. If the home organization is offline, traveling users won't be able to access third-party applications; implement a hybrid cloud/local authentication system.

C. Local users may not be properly redirected to the third-party services; implement a local gateway.

D. Browsers may not properly redirect; use host files to ensure that issues with redirects are resolved.

45. What solution can best help address concerns about third parties that control SSO redirects as shown in step 2 in the diagram?

A. An awareness campaign about trusted third parties

B. TLS

C. Handling redirects at the local site

D. Implementing an IPS to capture SSO redirect attacks

46. Susan has been asked to recommend whether her organization should use a MAC scheme or a DAC scheme. If flexibility and scalability are important requirements for implementing access controls, which scheme should she recommend and why?

A. MAC, because it provides greater scalability and flexibility because you can simply add more labels as needed

B. DAC, because allowing individual administrators to make choices about the objects they control provides scalability and flexibility

C. MAC, because compartmentalization is well suited to flexibility and adding compartments will allow it to scale well

D. DAC, because a central decision process allows quick responses and will provide scalability by reducing the number of decisions required and flexibility by moving those decisions to a central authority

47. Which of the following tools is not typically used to verify that a provisioning process was followed in a way that ensures that the organization's security policy is being followed?

A. Log review

B. Manual review of permissions

C. Signature-based detection

D. Review the audit trail

48. Jessica needs to send information about services she is provisioning to a third-party organization. What standards-based markup language should she choose to build the interface?

A. SAML

B. SOAP

C. SPML

D. XACML

49. During a penetration test, Chris recovers a file containing hashed passwords for the system he is attempting to access. What type of attack is most likely to succeed against the hashed passwords?

A. A brute-force attack

B. A pass-the-hash attack

C. A rainbow table attack

D. A salt recovery attack

50. Google's identity integration with a variety of organizations and applications across domains is an example of which of the following?

A. PKI

B. Federation

C. Single sign-on

D. Provisioning

51. Amanda starts at her new job and finds that she has access to a variety of systems that she does not need to accomplish her job. What problem has she encountered?

A. Privilege creep

B. Rights collision

C. Least privilege

D. Excessive privileges

52. When Chris verifies an individual's identity and adds a unique identifier like a user ID to an identity system, what process has occurred?

A. Identity proofing

B. Registration

C. Directory management

D. Session management

53. Selah wants to provide accountability for actions performed via her organization's main line of business application. What controls are most frequently used to provide accountability in a situation like this? (Select all that apply.)

A. Enable audit logging.

B. Provide every staff member with a unique account and enable multifactor authentication.

C. Enable time- and location-based login requirements.

D. Provide every staff member with a unique account and require a self-selected password.

54. Charles wants to provide authorization services as part of his web application. What standard should he use if he wants to integrate easily with other web identity providers?

A. OpenID

B. TACACS+

C. RADIUS

D. OAuth

55. The company that Cameron works for uses a system that allows users to request privileged access to systems when necessary. Cameron requests access, and the request is pre-approved due to his role. He is then able to access the system to perform the task. Once he is done, the rights are removed. What type of system is he using?

A. Zero trust

B. Federated identity management

C. Single sign-on

D. Just-in-time access

56. Elle is responsible for building a banking website. She needs proof of the identity of the users who register for the site. How should she validate user identities?

A. Require users to create unique questions that only they will know.

B. Require new users to bring their driver's license or passport in person to the bank.

C. Use information that both the bank and the user have such as questions pulled from their credit report.

D. Call the user on their registered phone number to verify that they are who they claim to be.

57. Susan's organization is part of a federation that allows users from multiple organizations to access resources and services at other federated sites. When Susan wants to use a service at a partner site, which identity provider is used?

A. Susan's home organization's identity provider

B. The service provider's identity provider

C. Both their identity provider and the service provider's identity provider

D. The service provider creates a new identity

58. A new customer at a bank that uses fingerprint scanners to authenticate its users is surprised when he scans his fingerprint and is logged in to another customer's account. What type of biometric factor error occurred?

A. A registration error

B. A Type 1 error

C. A Type 2 error

D. A time of use, method of use error

59. What type of access control is typically used by firewalls?

A. Discretionary access controls

B. Rule-based access controls

C. Task-based access control

D. Mandatory access controls

60. When you input a user ID and password, you are performing what important identity and access management activity?

A. Authorization

B. Validation

C. Authentication

D. Login

61. Kathleen works for a data center hosting facility that provides physical data center space for individuals and organizations. Until recently, each client was given a magnetic-strip-based keycard to access the section of the facility where their servers are located, and they were also given a key to access the cage or rack where their servers reside. In the past month, a number of servers have been stolen, but the logs for the passcards show only valid IDs. What is Kathleen's best option to make sure that the users of the passcards are who they are supposed to be?

A. Add a reader that requires a PIN for passcard users.

B. Add a camera system to the facility to observe who is accessing servers.

C. Add a biometric factor.

D. Replace the magnetic stripe keycards with smartcards.

62. Theresa wants to allow her staff to securely store and manage passwords for systems including service accounts and other rarely used administrative credentials. What type of tool should she implement to enable this?

A. Single sign-on

B. A federated identity system

C. A password manager

D. A multifactor authentication system

63. Olivia wants to limit the commands that a user can run via `sudo` to limit the potential for privilege escalation attacks. What Linux file should she modify to allow this?

A. The bash `.bin` configuration file

B. The `sudoers` file

C. The bash `.allowed` configuration file

D. The `sudont` file

64. Which objects and subjects have a label in a MAC model?

A. Objects and subjects that are classified as Confidential, Secret, or Top Secret have a label.

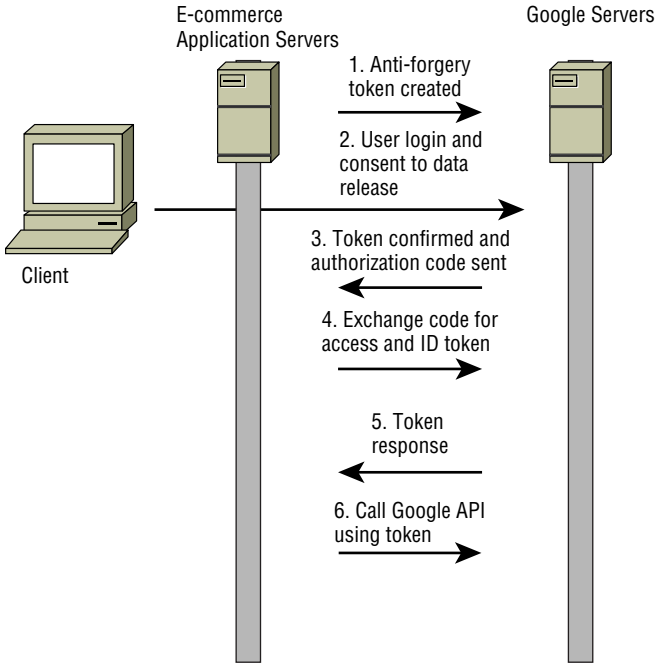
B. All objects have a label, and all subjects have a compartment.

C. All objects and subjects have a label.

D. All subjects have a label and all objects have a compartment.

For questions 65–67, please refer to the following scenario and diagram:

Chris is the identity architect for a growing e-commerce website that wants to leverage social identity. To do this, he and his team intend to allow users to use their existing Google accounts as their primary accounts when using the e-commerce site. This means that when a new user initially connects to the e-commerce platform, they are given the choice between using their Google account using OAuth 2.0 or creating a new account on the platform using their own email address and a password of their choice.



65. When the e-commerce application creates an account for a Google user, where should that user's password be stored?

A. The password is stored in the e-commerce application's database.

B. The password is stored in memory on the e-commerce application's server.

C. The password is stored in Google's account management system.

D. The password is never stored; instead, a salted hash is stored in Google's account management system.

66. Which of the following is responsible for user authentication for Google users?

A. The e-commerce application.

B. Both the e-commerce application and Google servers.

C. Google servers.

D. The diagram does not provide enough information to determine this.

67. What type of attack is the creation and exchange of state tokens intended to prevent?

A. XSS

B. CSRF

C. SQL injection

D. XACML

68. Questions like "What is your pet's name?" are examples of what type of identity proofing?

A. Knowledge-based authentication

B. Dynamic knowledge-based authentication

C. Out-of-band identity proofing

D. A Type 3 authentication factor

69. Madhuri creates a table that includes assigned privileges, objects, and subjects to manage access control for the systems she is responsible for. Each time a subject attempts to access an object, the systems check the table to ensure that the subject has the appropriate rights to the objects. What type of access control system is Madhuri using?

A. A capability table

B. An access control list

C. An access control matrix

D. A subject/object rights management system

70. During a review of support tickets, Ben's organization discovered that password changes accounted for more than a quarter of its help desk's cases. Which of the following options would be most likely to decrease that number significantly?

A. Two-factor authentication

B. Biometric authentication

C. Self-service password reset

D. Passphrases

71. Brian's large organization has used RADIUS for AAA services for its network devices for years and has recently become aware of security issues with the unencrypted information transferred during authentication. How should Brian implement encryption for RADIUS?

A. Use the built-in encryption in RADIUS.

B. Implement RADIUS over its native UDP using TLS for protection.

C. Implement RADIUS over TCP using TLS for protection.

D. Use an AES256 pre-shared cipher between devices.

72. Jim wants to allow cloud-based applications to act on his behalf to access information from other sites. Which of the following tools can allow that?

A. Kerberos

B. OAuth

C. OpenID

D. LDAP

73. Ben's organization has had an issue with unauthorized access to applications and workstations during the lunch hour when employees aren't at their desk. What are the best types of session management solutions for Ben to recommend to help prevent this type of access?

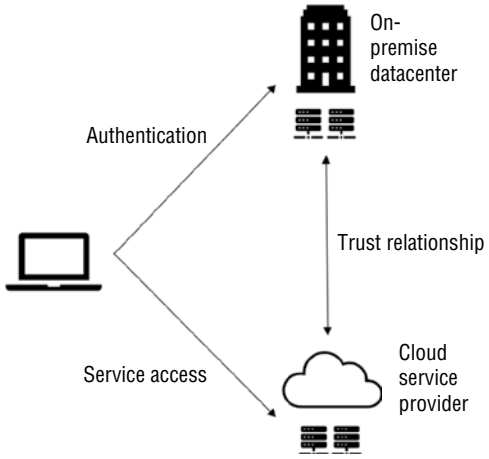
A. Use session IDs for all access and verify system IP addresses of all workstations.

B. Set session timeouts for applications and use password-protected screensavers with inactivity timeouts on workstations.

C. Use session IDs for all applications, and use password-protected screensavers with inactivity timeouts on workstations.

D. Set session timeouts for applications and verify system IP addresses of all workstations.

74. What type of authentication scenario is shown in the following diagram?



A. Hybrid federation

B. On-premise federation

C. Cloud federation

D. Kerberos federation

75. Chris wants to control access to his facility while still identifying individuals. He also wants to ensure that the individuals are the people who are being admitted without significant ongoing costs. Which solutions from the following options would meet all of these requirements? (Select all that apply.)

A. Security guards and photo identification badges

B. RFID badges and readers with PIN pads

C. Magstripe badges and readers with PIN pads

D. Security guards and magstripe readers

76. A device like Yubikey or Titan Security Key is what type of Type 2 authentication factor?

A. A token

B. A biometric identifier

C. A smart card

D. A PIV

77. What authentication technology can be paired with OAuth to perform identity verification and obtain user profile information using a RESTful API?

A. SAML

B. Shibboleth

C. OpenID Connect

D. Higgins

78. Jim wants to implement an access control scheme that will ensure that users cannot delegate access. He also wants to enforce access control at the operating system level. What access control mechanism best fits these requirements?

A. Role-based access control

B. Discretionary access control

C. Mandatory access control

D. Attribute-based access control

79. The security administrators at the company that Susan works for have configured the workstation she uses to allow her to log in only during her work hours. What type of access control best describes this limitation?

A. Constrained interface

B. Context-dependent control

C. Content-dependent control

D. Least privilege

80. Ben uses a software-based token that changes its code every minute. What type of token is he using?

A. Asynchronous

B. Smart card

C. Synchronous

D. Static

81. Firewalls are an example of what type of access control mechanism?

A. Mandatory access control

B. Attribute-based access control

C. Discretionary access control

D. Rule-based access control

82. Michelle works for a financial services company and wants to register customers for her web application. What type of authentication mechanism could she use for the initial login if she wants to quickly and automatically verify that the person is who they claim to be without having a previous relationship with them?

A. Request their Social Security number.

B. Use knowledge-based authentication.

C. Perform manual identity verification.

D. Use a biometric factor.

83. Megan's company wants to use Google accounts to allow users to quickly adopt their web application. What common cloud federation technologies will Megan need to implement? (Select all that apply.)

A. Kerberos

B. OpenID

C. OAuth

D. RADIUS

84. Session ID length and session ID entropy are both important to prevent what type of attack?

A. Denial of service

B. Cookie theft

C. Session guessing

D. Man-in-the-middle attacks

85. The access control system for Naomi's organization checks if her computer is fully patched, if it has a successful clean anti-malware scan, and if the firewall is turned on among other security validations before it allows her to connect to the network. If there are potential issues, she is not permitted to connect and must contact support. What type of access control scheme best describes this type of process?

A. MAC

B. Rule-based access control

C. Role-based access control

D. Risk-based access control

86. Isabelle wants to prevent privilege escalation attacks via her organization's service accounts. Which of the following security practices is best suited to this?

A. Remove unnecessary rights.

B. Disable interactive login for service accounts.

C. Limit when accounts can log in.

D. Use meaningless or randomized names for service accounts.

87. What danger is created by allowing the OpenID relying party to control the connection to the OpenID provider?

A. It may cause incorrect selection of the proper OpenID provider.

B. It creates the possibility of a phishing attack by sending data to a fake OpenID provider.

C. The relying party may be able to steal the client's username and password.

D. The relying party may not send a signed assertion.

88. Jim is implementing a cloud identity solution for his organization. What type of technology is he putting in place?

A. Identity as a service

B. Employee ID as a service

C. Cloud-based RADIUS

D. OAuth

89. Kristen wants to control access to an application in her organization based on a combination of staff member's job titles, the permissions each group of titles need for the application, and the time of day and location. What type of control scheme should she select?

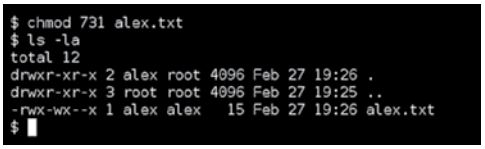
A. ABAC

B. DAC

C. MAC

D. Role BAC

90. When Alex sets the permissions shown in the following image as one of many users on a Linux server, what type of access control model is he leveraging?



A. Role-based access control

B. Rule-based access control

C. Mandatory access control (MAC)

D. Discretionary access control (DAC)

91. Joanna leads her organization's identity management team and wants to ensure that roles are properly updated when staff members change to new positions. What issue should she focus on for those staff members to avoid future issues with role definition?

A. Registration

B. Privilege creep

C. Deprovisioning

D. Accountability

92. What type of authorization mechanism is shown in the following chart?

Group	Privileges
System administrators	Superuser on a desktop, domain administrator
Application administrators	Sudo privileges on application servers
Database administrators	Sudo privileges on database servers
Users	User rights on desktop workstations

A. RBAC
B. ABAC
C. MAC
D. DAC

93. Susan is troubleshooting Kerberos authentication problems with symptoms including TGTs that are not accepted as valid and an inability to receive new tickets. If the system she is troubleshooting is properly configured for Kerberos authentication, her username and password are correct, and her network connection is functioning, what is the most likely issue?

A. The Kerberos server is offline.
B. There is a protocol mismatch.
C. The client's TGTs have been marked as compromised and de-authorized.
D. The Kerberos server and the local client's time clocks are not synchronized.

94. Brian wants to explain the benefits of an on-premise federation approach for identity to his organization's leadership. Which of the following is not a common benefit of a federated identity system?

A. Ease of account management
B. Single sign-on
C. Prevention of brute-force attacks
D. Increased productivity

95. The bank that Aaron works for wants to allow customers to use a new add-on application from a third-party partner they are working with. Since not every customer will want or need an account, Aaron has suggested that the bank use a SAML-based workflow that creates an account when a user downloads the app and tries to log in. What type of provisioning system has he suggested?

A. JIT
B. OpenID
C. OAuth
D. Kerberos

96. What authentication protocol does Windows use by default for Active Directory systems?

A. RADIUS

B. Kerberos

C. OAuth

D. TACACS+

97. Valerie needs to control access to applications that are deployed to mobile devices in a BYOD environment. What type of solution will best allow her to exercise control over the applications while ensuring that they do not leave remnant data on the devices used by her end users?

A. Deploy the applications to the BYOD devices and require unique PINs on every device.

B. Deploy the application to desktop systems and require users to use remote desktop to access them using enterprise authentication.

C. Deploy the applications to the BYOD devices using application containers and require unique PINs on every device.

D. Use a virtual hosted application environment that requires authentication using enterprise credentials.

98. Match the following authorization mechanisms with their descriptions:

1. Role-BAC

2. Rule BAC

3. DAC

4. ABAC

5. MAC

A. An access control model enforced by the operating system.

B. Permissions or rights are granted based on parameters like an IP address, time, or other specific details that match requirements.

C. Sometimes called policy-based access control, this model uses information about the subject to assign permissions.

D. A model where subjects with the proper rights can assign or pass those rights to other subjects.

E. Used to assign permissions based on job or function.

99. Match each of the numbered authentication techniques with the appropriate lettered category. Each technique should be matched with exactly one category. Each category may be used once, more than once, or not at all.

Authentication technique

1. Password

2. ID card

3. Retinal scan
4. Smartphone token
5. Fingerprint analysis

Category

A. Something you have
B. Something you know
C. Something you are

100. Match the following identity and access controls with the asset type they are best suited to protect. Each only has one option.

1. Information assets A
2. Systems E
3. Mobile devices D
4. Facilities B
5. Partner applications C

A. Discretionary access controls
B. Badge readers
C. Federated identity management
D. Biometric authentication
E. User accounts with multifactor authentication

1. During a port scan, Susan discovers a system running services on TCP and UDP 137–139 and TCP 445, as well as TCP 1433. What type of system is she likely to find if she connects to the machine?
   - **A.** A Linux email server
   - **B.** A Windows SQL server
   - **C.** A Linux file server
   - **D.** A Windows workstation

2. Which of the following is a method used to automatically design new software tests and to ensure the quality of tests?
   - **A.** Code auditing
   - **B.** Static code analysis
   - **C.** Regression testing
   - **D.** Mutation testing

3. During a port scan, Naomi found TCP port 443 open on a system. Which tool is best suited to scanning the service that is most likely running on that port?
   - **A.** zzuf
   - **B.** Nikto
   - **C.** Metasploit
   - **D.** sqlmap

4. What message logging standard is commonly used by network devices, Linux and Unix systems, and many other enterprise devices?
   - **A.** Syslog
   - **B.** Netlog
   - **C.** Eventlog
   - **D.** Remote Log Protocol (RLP)

5. Alex wants to use an automated tool to fill web application forms to test for format string vulnerabilities. What type of tool should he use?
   - **A.** A black box
   - **B.** A brute-force tool
   - **C.** A fuzzer
   - **D.** A static analysis tool

6. Susan needs to scan a system for vulnerabilities, and she wants to use an open source tool to test the system remotely. Which of the following tools will meet her requirements and allow vulnerability scanning?
   - **A.** Nmap
   - **B.** OpenVAS
   - **C.** MBSA
   - **D.** Nessus

7. Morgan is implementing a vulnerability management system that uses standards-based components to score and evaluate the vulnerabilities it finds. Which of the following is most commonly used to provide a severity score for vulnerabilities?
   - **A.** CCE
   - **B.** CVSS
   - **C.** CPE
   - **D.** OVAL

8. Jim has been contracted to perform a penetration test of a bank's primary branch. To make the test as real as possible, he has not been given any information about the bank other than its name and address. What type of penetration test has Jim agreed to perform?
   - **A.** A crystal-box penetration test
   - **B.** A gray-box penetration test
   - **C.** A black-box penetration test
   - **D.** A white-box penetration test

9. In a response to a request for proposal, Susan receives an SSAE 18 SOC report. If she wants a report that includes operating effectiveness detail, what should Susan ask for as follow-up and why?
   - **A.** A SOC 2 Type II report, because Type I does not cover operating effectiveness
   - **B.** A SOC 1 Type I report, because SOC 2 does not cover operating effectiveness
   - **C.** A SOC 2 Type I report, because SOC 2 Type II does not cover operating effectiveness
   - **D.** A SOC 3 report, because SOC 1 and SOC 2 reports are outdated

10. During a wireless network penetration test, Susan runs aircrack-ng against the network using a password file. What might cause her to fail in her password-cracking efforts?
    - **A.** Using WPA2 encryption
    - **B.** Running WPA2 in Enterprise mode
    - **C.** Using WEP encryption
    - **D.** Running WPA2 in PSK mode

11. A zero-day vulnerability is announced for the popular Apache web server in the middle of a workday. In Jacob's role as an information security analyst, he needs to quickly scan his network to determine what servers are vulnerable to the issue. What is Jacob's best route to quickly identify vulnerable systems?
    - **A.** Immediately run Nessus against all of the servers to identify which systems are vulnerable.
    - **B.** Review the CVE database to find the vulnerability information and patch information.
    - **C.** Create a custom IDS or IPS signature.
    - **D.** Identify affected versions and check systems for that version number using an automated scanner.

12. What type of testing is used to ensure that separately developed software modules properly exchange data?
    - **A.** Fuzzing
    - **B.** Dynamic testing
    - **C.** Interface testing
    - **D.** API checksums

13. Selah wants to provide security assessment information to customers who want to use her organization's cloud services. Which of the following options should she select to ensure that the greatest number of customers are satisfied with the assessment information?
    - **A.** Use an internal audit team to self-assess against internal metrics.
    - **B.** Use a third-party auditor.
    - **C.** Use internal technical staff who know the systems.
    - **D.** Use an internal audit team to self-assess against a common standard like COBIT.

14. Yasmine has been asked to consider a breach and attack simulation system. What type of system should she look for?
    - **A.** A ticket and change management system designed to help manage incidents
    - **B.** A system that runs incident response simulations for blue teams to test their skills
    - **C.** A system that combines red and blue team techniques with automation
    - **D.** A security operations and response (SOAR) system

15. Monica wants to gather information about security awareness in her organization. What technique is most frequently used to assess security awareness?
    - **A.** Phishing simulators
    - **B.** Gamified applications
    - **C.** Assessment tests
    - **D.** Surveys

16. Jim has been contracted to conduct a gray-box penetration test, and his clients have provided him with the following information about their networks so that he can scan them:

    Data center: 10.10.10.0/24

    Sales: 10.10.11.0/24

    Billing: 10.10.12.0/24

    Wireless: 192.168.0.0/16

    What problem will Jim encounter if he is contracted to conduct a scan from off-site?
    - **A.** The IP ranges are too large to scan efficiently.
    - **B.** The IP addresses provided cannot be scanned.
    - **C.** The IP ranges overlap and will cause scanning issues.
    - **D.** The IP addresses provided are RFC 1918 addresses.

17. Mark's company has been notified that there is a flaw in their web application. The anonymous individual has notified them that they have two weeks to fix it before the details of the flaw are published along with example exploit code. What industry norm is the individual who contacted Mark's company violating?

A. Zero-day reporting

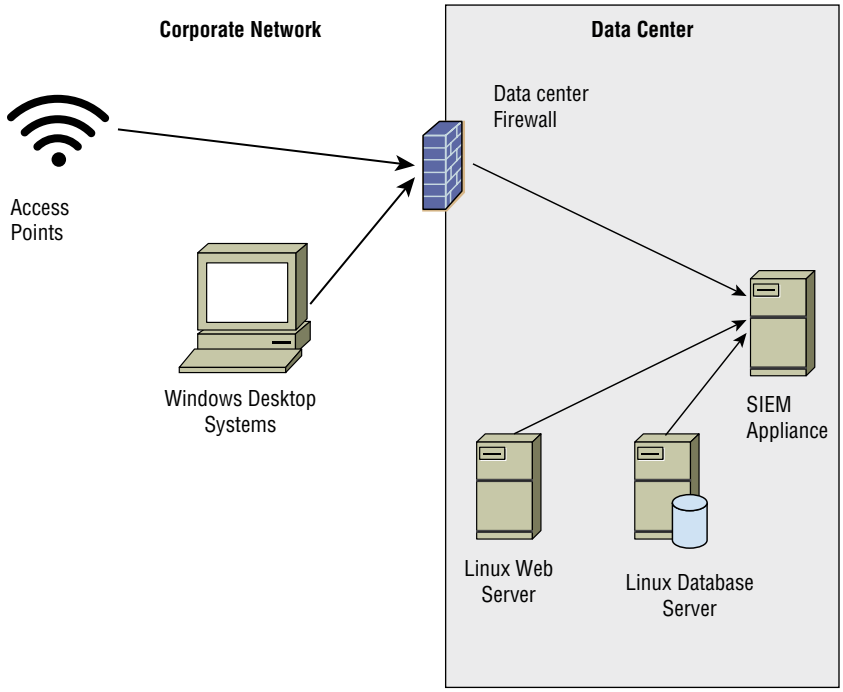
B. Ethical disclosure

C. Ethical hacking

D. The (ISC)² vulnerability disclosure ethics statement

For questions 18–20, please refer to the following scenario:

The company that Jennifer works for has implemented a central logging infrastructure, as shown in the following image. Use this diagram and your knowledge of logging systems to answer the following questions.



18. Jennifer needs to ensure that all Windows systems provide identical logging information to the SIEM. How can she best ensure that all Windows desktops have the same log settings?

A. Perform periodic configuration audits.

B. Use Group Policy.

C. Use Local Policy.

D. Deploy a Windows syslog client.

19. During normal operations, Jennifer's team uses the SIEM appliance to monitor for exceptions received via syslog. What system shown does not natively have support for syslog events?

A. Enterprise wireless access points

B. Windows desktop systems

C. Linux web servers

D. Enterprise firewall devices

20. What technology should an organization use for each of the devices shown in the diagram to ensure that logs can be time sequenced across the entire infrastructure?

A. Syslog

B. NTP

C. Logsync

D. SNAP

21. During a penetration test, Michelle needs to identify systems, but she hasn't gained sufficient access on the system she is using to generate raw packets. What type of scan should she run to verify the most open services?

A. A TCP connect scan

B. A TCP SYN scan

C. A UDP scan

D. An ICMP scan

22. During a port scan using nmap, Joseph discovers that a system shows two ports open that cause him immediate worry:

21/open

23/open

What services are likely running on those ports?

A. SSH and FTP

B. FTP and Telnet

C. SMTP and Telnet

D. POP3 and SMTP

23. Aaron wants to validate his compliance with PCI-DSS. His company is a large commercial organization with millions of dollars in transactions a year. What is the most common method of conducting this type of testing for large organizations?

A. Self-assessment

B. To conduct a thirty-party assessment using COBIT

C. To partner with another company and trade assessments between the organizations

D. To conduct a third-party assessment using a qualified security assessor

24. What method is commonly used to assess how well software testing covered the potential uses of an application?

A. A test coverage analysis

B. A source code review

C. A fuzz analysis

D. A code review report

25. Testing that is focused on functions that a system should not allow is an example of what type of testing?

A. Use case testing

B. Manual testing

C. Misuse case testing

D. Dynamic testing

26. What type of monitoring uses simulated traffic to a website to monitor performance?

A. Log analysis

B. Synthetic monitoring

C. Passive monitoring

D. Simulated transaction analysis

27. Derek wants to ensure that his organization tracks all changes to accounts through their lifecycle. What type of tool should he invest in for his organization?

A. A directory service like LDAP

B. An IAM system

C. An SIEM

D. An EDR system

28. Jim uses a tool that scans a system for available services and then connects to them to collect banner information to determine what version of the service is running. It then provides a report detailing what it gathers, basing results on service fingerprinting, banner information, and similar details it gathers combined with CVE information. What type of tool is Jim using?

A. A port scanner

B. A service validator

C. A vulnerability scanner

D. A patch management tool

29. Emily builds a script that sends data to a web application that she is testing. Each time the script runs, it sends a series of transactions with data that fits the expected requirements of the web application to verify that it responds to typical customer behavior. What type of transactions is she using, and what type of test is this?
    - **A.** Synthetic, passive monitoring
    - **B.** Synthetic, use case testing
    - **C.** Actual, dynamic monitoring
    - **D.** Actual, fuzzing

30. What passive monitoring technique records all user interaction with an application or website to ensure quality and performance?
    - **A.** Client/server testing
    - **B.** Real user monitoring
    - **C.** Synthetic user monitoring
    - **D.** Passive user recording

31. Earlier this year, the information security team at Jim's employer identified a vulnerability in the web server that Jim is responsible for maintaining. He immediately applied the patch and is sure that it installed properly, but the vulnerability scanner has continued to incorrectly flag the system as vulnerable. To deal with the issue so that it does not continue to be flagged incorrectly?
    - **A.** Uninstall and reinstall the patch.
    - **B.** Ask the information security team to flag the system as patched and not vulnerable to that particular flaw.
    - **C.** Update the version information in the web server's configuration.
    - **D.** Review the vulnerability report and use alternate remediation options.

32. Angela wants to test a web browser's handling of unexpected data using an automated tool. What tool should she choose?
    - **A.** Nmap
    - **B.** zzuf
    - **C.** Nessus
    - **D.** Nikto

33. STRIDE, which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, is useful in what part of application threat modeling?
    - **A.** Vulnerability assessment
    - **B.** Misuse case testing
    - **C.** Threat categorization
    - **D.** Penetration test planning

34. Why should passive scanning be conducted in addition to implementing wireless security technologies like wireless intrusion detection systems?

A. It can help identify rogue devices.

B. It can test the security of the wireless network via scripted attacks.

C. Their short dwell time on each wireless channel can allow them to capture more packets.

D. They can help test wireless IDS or IPS systems.

35. Paul is reviewing the approval process for a penetration test and wants to ensure that it has appropriate management review. Who should he ensure has approved the request for a penetration test for a business system?

A. The change advisory board

B. Senior management

C. The systems administrator for the system

D. The service owner

36. What term describes software testing that is intended to uncover new bugs introduced by patches or configuration changes?

A. Nonregression testing

B. Evolution testing

C. Smoke testing

D. Regression testing

37. Which of the following tools cannot identify a target's operating system for a penetration tester?

A. Nmap

B. Nessus

C. Nikto

D. sqlmap

38. Susan needs to predict high-risk areas for her organization and wants to use metrics to assess risk trends as they occur. What should she do to handle this?

A. Perform yearly risk assessments.

B. Hire a penetration testing company to regularly test organizational security.

C. Identify and track key risk indicators.

D. Monitor logs and events using a SIEM device.

39. What major difference separates synthetic and passive monitoring?

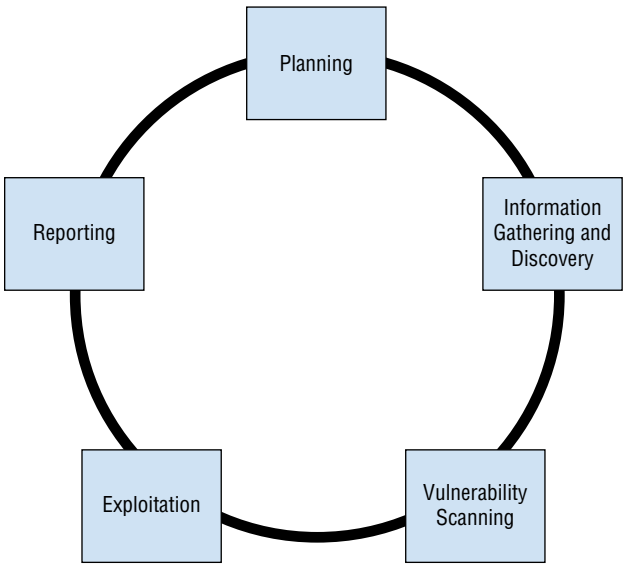
A. Synthetic monitoring works only after problems have occurred.

B. Passive monitoring cannot detect functionality issues.

C. Passive monitoring works only after problems have occurred.

D. Synthetic monitoring cannot detect functionality issues.

For questions 40–42, please refer to the following scenario. Chris uses the standard penetration testing methodology shown here. Use this methodology and your knowledge of penetration testing to answer questions about tool usage during a penetration test.



40. What task is the most important during Phase 1, Planning?

A. Building a test lab

B. Getting authorization

C. Gathering appropriate tools

D. Determining if the test is white, black, or gray box

41. Which of the following tools is most likely to be used during discovery?

A. Nessus

B. john

C. Nmap

D. Nikto

42. Which of these concerns is the most important to address during planning to ensure that the reporting phase does not cause problems?

A. Which CVE format to use

B. How the vulnerability data will be stored and sent

C. Which targets are off-limits

D. How long the report should be

43. What four types of coverage criteria are commonly used when validating the work of a code testing suite?

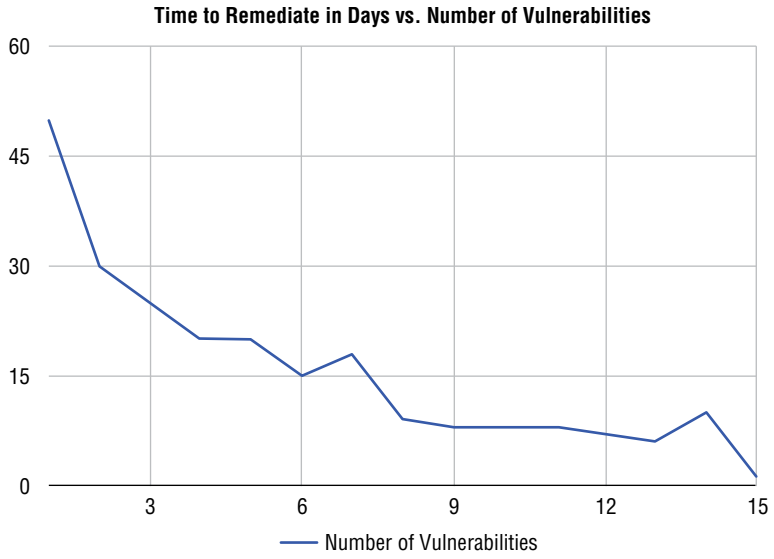
A. Input, statement, branch, and condition coverage

B. Function, statement, branch, and condition coverage

C. API, branch, bounds, and condition coverage

D. Bounds, branch, loop, and condition coverage

44. As part of his role as a security manager, Jacob provides the following chart to his organization's management team. What type of measurement is he providing for them?



A. A coverage rate measure

B. A key performance indicator

C. A time to live metric

D. A business criticality indicator

45. What does using unique user IDs for all users provide when reviewing logs?

A. Confidentiality

B. Integrity

C. Availability

D. Accountability

46. Which of the following is not an interface that is typically tested during the software testing process?

A. APIs

B. Network interfaces

C. UIs

D. Physical interfaces

47. Alan's organization uses the Security Content Automation Protocol (SCAP) to standardize its vulnerability management program. Which component of SCAP can Alan use to reconcile the identity of vulnerabilities generated by different security assessment tools?

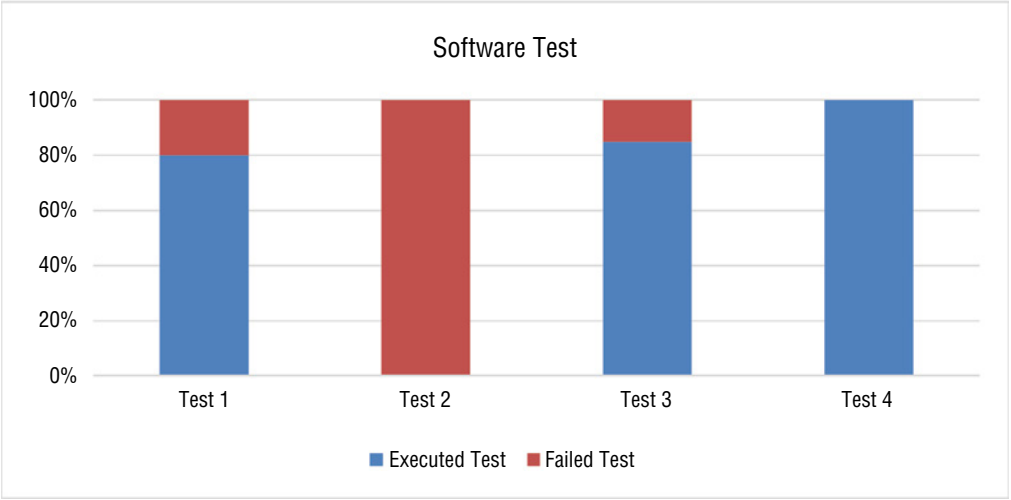
A. OVAL

B. XCCDF

C. CVE

D. SCE

48. Susan is reviewing software testing coverage data and sees the information shown in the following figure. What can she determine about this testing process? (Select all answers that apply.)



A. The testing does not have full coverage.

B. Test 4 completed with no failures.

C. Test 2 failed to run successfully.

D. The testing needs to be run a fifth time.

49. Which of the following strategies is not a reasonable approach for remediating a vulnerability identified by a vulnerability scanner?

A. Install a patch.

B. Use a workaround fix.

C. Update the banner or version number.

D. Use an application layer firewall or IPS to prevent attacks against the identified vulnerability.

50. During a penetration test, Selah calls her target's help desk claiming to be the senior assistant to an officer of the company. She requests that the help desk reset the officer's password because of an issue with his laptop while traveling and persuades them to do so. What type of attack has she successfully completed?

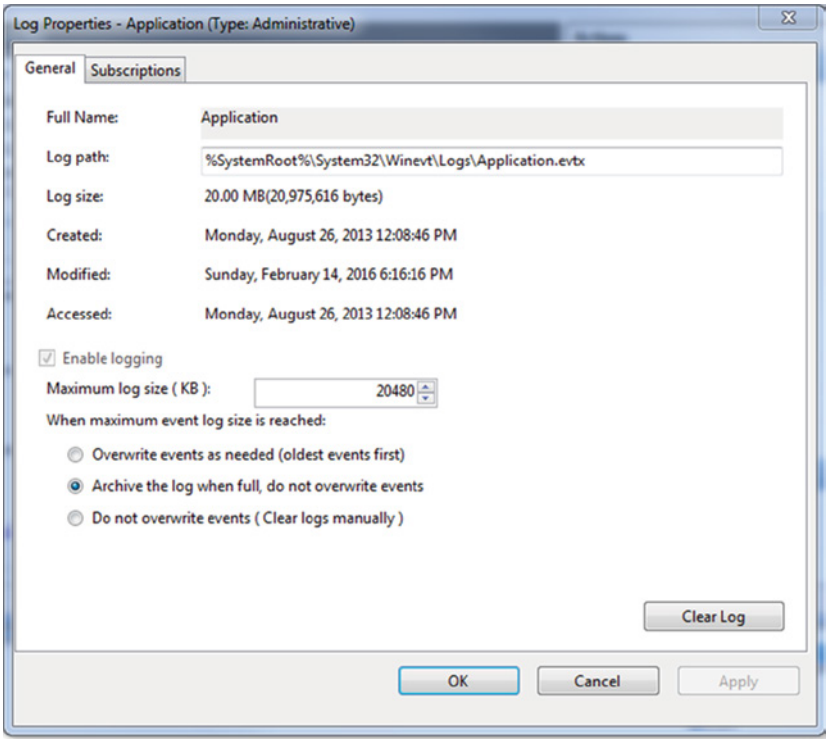
A. Zero knowledge

B. Help desk spoofing

C. Social engineering

D. Black box

51. In this image, what issue may occur due to the log handling settings?



A. Log data may be lost when the log is archived.

B. Log data may be overwritten.

C. Log data may not include needed information.

D. Log data may fill the system disk.

52. Which of the following is not a hazard associated with penetration testing?

A. Application crashes

B. Denial of service

C. Blackouts

D. Data corruption

53. Which NIST special publication covers the assessment of security and privacy controls?

A. 800-12

B. 800-53A

C. 800-34

D. 800-86

54. Michelle is conducting a quantitative business impact assessment and wants to collect data to determine the dollar cost of downtime. What information would she need from outages during the previous year to calculate the cost of those outages to the business? (Select all that apply.)

A. The total amount of time the business was down

B. The number of personnel hours worked to recover from the outage

C. The business lost during the outage per hour in dollars

D. The average employee wage per hour

55. If Kara's primary concern is preventing eavesdropping attacks, which port should she block?

A. 22

B. 80

C. 443

D. 1433

56. If Kara's primary concern is preventing administrative connections to the server, which port should she block?

A. 22

B. 80

C. 443

D. 1433

57. During a third-party audit, Jim's company receives a finding that states, "The administrator should review backup success and failure logs on a daily basis and take action in a timely manner to resolve reported exceptions." What potential problem does this finding indicate?

A. Administrators will not know if the backups succeeded or failed.

B. The backups may not be properly logged.

C. The backups may not be usable.

D. The backup logs may not be properly reviewed.

58. Jim is helping his organization decide on audit standards for use throughout their international organization. Which of the following is not an IT standard that Jim's organization is likely to use as part of its audits?

A. COBIT

B. SSAE-18

C. ITIL

D. ISO 27001

59. Nicole wants to conduct a standards-based audit of her organization. Which of the following is commonly used to describe common requirements for information systems?

A. IEC

B. COBIT

C. FISA

D. DMCA

60. Kelly's team conducts regression testing on each patch that they release. What key performance measure should they maintain to measure the effectiveness of their testing?

A. Time to remediate vulnerabilities

B. A measure of the rate of defect recurrence

C. A weighted risk trend

D. A measure of the specific coverage of their testing

61. Which of the following types of code review is not typically performed by a human?

A. Software inspections

B. Pair programming

C. Static program analysis

D. Software walk-throughs

For questions 62–64, please refer to the following scenario:

Susan is the lead of a quality assurance team at her company. The team has been tasked with the testing for a major release of their company's core software product.

62. Susan's team of software testers are required to test every code path, including those that will only be used when an error condition occurs. What type of testing environment does her team need to ensure complete code coverage?

A. White box

B. Gray box

C. Black box

D. Dynamic

63. As part of the continued testing of their new application, Susan's quality assurance team has designed a set of test cases for a series of black-box tests. These functional tests are then run, and a report is prepared explaining what has occurred. What type of report is typically generated during this testing to indicate test metrics?

A. A test coverage report

B. A penetration test report

C. A code coverage report

D. A line coverage report

64. As part of their code coverage testing, Susan's team runs the analysis in a nonproduction environment using logging and tracing tools. Which of the following types of code issues is most likely to be missed during testing due to this change in the operating environment?

A. Improper bounds checking

B. Input validation

C. A race condition

D. Pointer manipulation

65. Robin recently conducted a vulnerability scan and found a critical vulnerability on a server that handles sensitive information. What should Robin do next?

A. Patching

B. Reporting

C. Remediation

D. Validation

66. The automated code testing and integration that Andrea ran as part of her organization's CI/CD pipeline errored out. What should Andrea do with the code if the company needs the code to go live immediately?

A. Manually bypass the test.

B. Review error logs to identify the problem.

C. Rerun the test to see if it works.

D. Send the code back to the developer for a fix.

67. Michelle wants to compare vulnerabilities she has discovered in her data center based on how exploitable they are, if exploit code exists, and how hard they are to remediate. What scoring system should she use to compare vulnerability metrics like these?

A. CSV

B. NVD

C. VSS

D. CVSS

68. During a port scan of his network, Alex finds that a number of hosts respond on TCP ports 80, 443, 515, and 9100 in offices throughout his organization. What type of devices is Alex likely discovering?

A. Web servers

B. File servers

C. Wireless access points

D. Printers

69. Nikto, Burp Suite, and Wapiti are all examples of what type of tool?

A. Web application vulnerability scanners

B. Code review tools

C. Vulnerability scanners

D. Port scanners

70. Frank's team is testing a new API that his company's developers have built for their application infrastructure. Which of the following is not a common API issue that you would expect Frank's team to find?

A. Improper encryption

B. Object-level authorization issues

C. User authentication issues

D. Lack of rate limiting

71. Jim is working with a penetration testing contractor who proposes using Metasploit as part of her penetration testing effort. What should Jim expect to occur when Metasploit is used?

A. Systems will be scanned for vulnerabilities.

B. Systems will have known vulnerabilities exploited.

C. Services will be probed for buffer overflow and other unknown flaws.

D. Systems will be tested for zero-day exploits.

72. Susan needs to ensure that the interactions between the components of her e-commerce application are all handled properly. She intends to verify communications, error handling, and session management capabilities throughout her infrastructure. What type of testing is she planning to conduct?

A. Misuse case testing

B. Fuzzing

C. Regression testing

D. Interface testing

73. Jim is designing his organization's log management systems and knows that he needs to carefully plan to handle the organization's log data. Which of the following is not a factor that Jim should be concerned with?

A. The volume of log data

B. A lack of sufficient log sources

C. Data storage security requirements

D. Network bandwidth

74. Ryan's organization wants to ensure that proper account management is occurring but does not have a central identity and access management tool in place. Ryan has a limited amount of time to do his verification process. What is his best option to test the account management process as part of an internal audit?

A. Validate all accounts changed in the past 90 days.

B. Select high-value administrative accounts for validation.

C. Validate all account changes in the past 180 days.

D. Validate a random sample of accounts.

75. When a Windows system is rebooted, what type of log is generated?

A. Error

B. Warning

C. Information

D. Failure audit

76. During a review of access logs, Alex notices that Michelle logged into her workstation in New York at 8 a.m. daily but that she was recorded as logging into her department's main web application shortly after 3 a.m. daily. What common logging issue has Alex likely encountered?

A. Inconsistent log formatting

B. Modified logs

C. Inconsistent timestamps

D. Multiple log sources

77. What type of vulnerability scan accesses configuration information from the systems it is run against as well as information that can be accessed via services available via the network?

A. Authenticated scans

B. Web application scans

C. Unauthenticated scans

D. Port scans

For questions 78–80, please refer to the following scenario:

Ben's organization has begun to use STRIDE to assess its software and has identified threat agents and the business impacts that these threats could have. Now they are working to identify appropriate controls for the issues they have identified.

78. Ben's development team needs to address an authorization issue, resulting in an elevation of privilege threat. Which of the following controls is most appropriate to this type of issue?

A. Auditing and logging are enabled.

B. Role-based access control is used for specific operations.

C. Data type and format checks are enabled.

D. User input is tested against a whitelist.

79. Ben's team is attempting to categorize a transaction identification issue that is caused by use of a symmetric key shared by multiple servers. What STRIDE category should this fall into?

A. Information disclosure

B. Denial of service

C. Tampering

D. Repudiation

80. Ben wants to use a third-party service to help assess denial-of-service attack vulnerabilities due the amount of traffic during denial-of-service attacks. What type of engagement should he suggest to his organization?

A. A social engineering engagement

B. A penetration test

C. Load or stress testing

D. Testing using a fuzzer

81. Chris is troubleshooting an issue with his organization's SIEM reporting. After analyzing the issue, he believes that the timestamps on log entries from different systems are inconsistent. What protocol can he use to resolve this issue?

A. SSH

B. FTP

C. TLS

D. NTP

82. Ryan is considering the use of fuzz testing in his web application testing program. Which one of the following statements about fuzz testing should Ryan consider when making his decision?

A. Fuzzers only find complex faults.

B. Testers must manually generate input.

C. Fuzzers may not fully cover the code.

D. Fuzzers can't reproduce errors.

83. Ken is designing a testing process for software developed by his team. He is designing a test that verifies that every line of code was executed during the test. What type of analysis is Ken performing?

A. Branch coverage

B. Condition coverage

C. Function coverage

D. Statement coverage

For questions 84–86, please refer to the following scenario. During a port scan, Ben uses nmap's default settings and sees the following results.

```
Nmap scan report for 192.168.184.130
Host is up (1.0s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 54.69 seconds
```

84. If Ben is conducting a penetration test, what should his next step be after receiving these results?

A. Connect to the web server using a web browser.

B. Connect via Telnet to test for vulnerable accounts.

C. Identify interesting ports for further scanning.

D. Use sqlmap against the open databases.

85. Based on the scan results, what operating system (OS) was the system that was scanned most likely running?

A. Windows Desktop

B. Linux

C. Network device

D. Windows Server

86. Ben's manager expresses concern about the coverage of his scan. Why might his manager have this concern?

A. Ben did not test UDP services.

B. Ben did not discover ports outside the "well-known ports."

C. Ben did not perform OS fingerprinting.

D. Ben tested only a limited number of ports.

87. Lucca is reviewing his organization's disaster recovery process data and notes that the MTD for the business's main website is two hours. What does he know about the RTO for the site when he does testing and validation?

A. It needs to be less than two hours.

B. It needs to be at least two hours.

C. The MTD is too short and needs to be longer.

D. The RTO is too short and needs to be longer.

88. Diana has engaged third-party auditors and wants to release an audit attestation to third parties without including details of the audit. What type of SSAE 18 SOC report should she request?

A. SOC 1

B. SOC 2

C. SOC 3

D. SOC 4

89. While reviewing the software testing output for her organization's new application, Madhuri notices that the application has produced errors that included directory and file information shown to the web application tester. What issue should she include in her report about the application?

A. It does not perform proper exception handling.

B. The software does not handle misuse case testing properly.

C. Debugging statements need to be removed.

D. The code was not fully tested due to errors.

90. What is the first step that should occur before a penetration test is performed?

A. Data gathering

B. Port scanning

C. Getting permission

D. Planning

91. The president of Josh's company is concerned about a significant increase in cryptographic malware that is impacting other companies in their industry. She has asked John to ensure that the company's data will be recoverable if malware strikes and encrypts their production systems. What process does Josh need to undertake to be able to tell her that the company is covered?

A. Encrypt all sensitive data.

B. Hash all of the organization's data to detect cryptographic malware.

C. Perform backup verification.

D. Use anti-encryption technology to prevent the malware from encrypting drives.

92. Joanna is her organization's CISO, and in her security operations oversight role she wants to ensure that management oversight is happening for security-related changes. What system should she focus on to track this type of data in most organizations?

A. The SIEM system

B. The IPS system

C. The CMS tool

D. The ITSM tool

93. Henry wants to validate that his backups are working. Which of the following options is the best way for him to ensure that the backups will be useful in a true disaster recovery scenario?

A. Periodically restore a random file to ensure that the backups are working.

B. Review configurations and settings on a regular schedule to validate backup settings.

C. Review the backup logs to ensure no errors are occurring.

D. Regularly perform full restores from backups to validate their success.

94. What type of vulnerabilities will not be found by a vulnerability scanner?

A. Local vulnerabilities

B. Service vulnerabilities

C. Zero-day vulnerabilities

D. Vulnerabilities that require authentication

95. Jacinda wants to measure the effectiveness of her security training as one of her security metrics. Which of the following measures are the most useful for assessing the effectiveness of security awareness training? (Select all that apply.)

A. How many people took the training

B. The level of security awareness before and after the training

C. The length of the training in hours

D. The number of training events each individual attended this year

96. Elaine has discovered a previously unknown critical vulnerability in a product that her organization uses. Her organization has a strong commitment to ethical disclosure, and Elaine wants to follow common ethical disclosure practices. What should she do first?

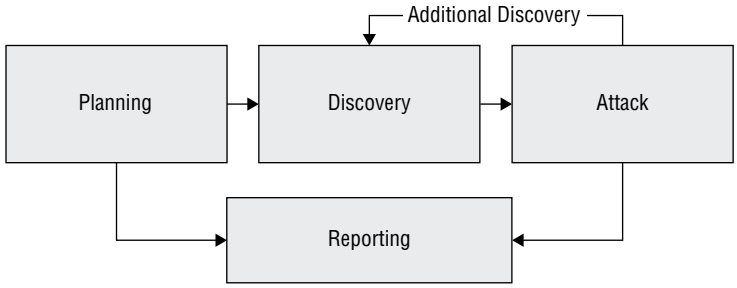
A. Build an in-house remediation or control and then publicly disclosure the vulnerability to prompt the vendor to patch it quickly.

B. Build an in-house remediation or control and then notify the vendor of the issue.

C. Notify the vendor and give them a reasonable amount of time to fix the issue.

D. Publicly disclose the vulnerability so that the vendor will patch it in an appropriate amount of time.

For questions 97–99, please refer to the following scenario. NIST Special Publication 800-115, the Technical Guide to Information Security Testing and Assessment, provides NIST's process for penetration testing. Use this image as well as your knowledge of penetration testing to answer the questions.



Source: NIST SP 800-115.

97. Which of the following is not a part of the discovery phase?

A. Hostname and IP address information gathering

B. Service information capture

C. Dumpster diving

D. Privilege escalation

98. NIST specifies four attack phase steps: gaining access, escalating privileges, system browsing, and installing additional tools. Once attackers install additional tools, what phase will a penetration tester typically return to?

A. Discovery

B. Gaining access

C. Escalating privileges

D. System browsing

99. Which of the following is not a typical part of a penetration test report?

A. A list of identified vulnerabilities

B. All sensitive data that was gathered during the test

C. Risk ratings for each issue discovered

D. Mitigation guidance for issues identified

100. Alex is using nmap to perform port scanning of a system, and he receives three different port status messages in the results. Match each of the numbered status messages with the appropriate lettered description. You should use each item exactly once.

Status message

1. Open

2. Closed

3. Filtered

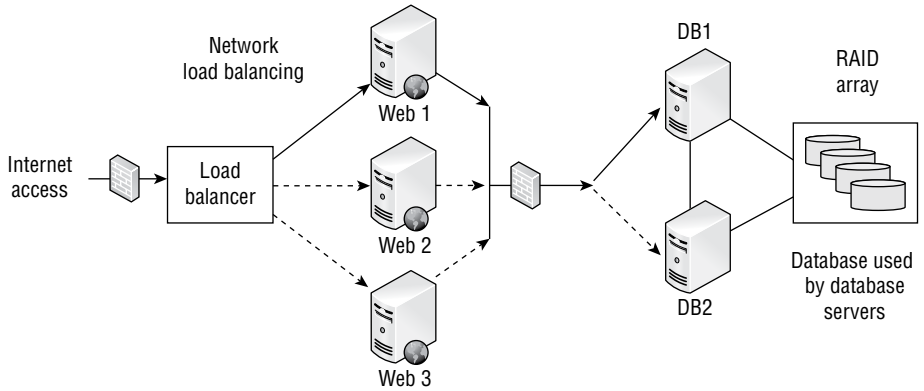
Description

A. The port is accessible on the remote system, but no application is accepting connections on that port.

B. The port is not accessible on the remote system.

C. The port is accessible on the remote system, and an application is accepting connections on that port.

1. Mary is reviewing the availability controls for the system architecture shown here. What technology is shown that provides fault tolerance for the database servers?



   A. Failover cluster
   B. UPS
   C. Tape backup
   D. Cold site

2. Joe is the security administrator for an ERP system. He is preparing to create accounts for several new employees. What default access should he give to all of the new employees as he creates the accounts?
   A. Read only
   B. Editor
   C. Administrator
   D. No access

3. Tim is configuring a privileged account management solution for his organization. Which one of the following is not a privileged administrative activity that should be automatically sent to a log of superuser actions?
   A. Purging log entries
   B. Restoring a system from backup
   C. Logging into a workstation
   D. Managing user accounts

4. When one of the employees of Alice's company calls in for support, she uses a code word that the company agreed to use if employees were being forced to perform an action. What is this scenario called?
   A. Social engineering
   B. Duress

C. Force majeure

D. Stockholm syndrome

5. Jordan is preparing to bring evidence into court after a cybersecurity incident investigation. He is responsible for preparing the physical artifacts, including affected servers and mobile devices. What type of evidence consists entirely of tangible items that may be brought into a court of law?

A. Documentary evidence

B. Parol evidence

C. Testimonial evidence

D. Real evidence

6. Lauren wants to ensure that her users only run software that her organization has approved. What technology should she deploy?

A. Blacklisting

B. Configuration management

C. Whitelisting

D. Graylisting

7. Colin is responsible for managing his organization's use of cybersecurity deception technologies. Which one of the following should he use on a honeypot system to consume an attacker's time while alerting administrators?

A. Honeynet

B. Pseudoflaw

C. Warning banner

D. Darknet

8. Toni responds to the desk of a user who reports slow system activity. Upon checking outbound network connections from that system, Toni notices a large amount of social media traffic originating from the system. The user does not use social media, and when Toni checks the accounts in question, they contain strange messages that appear encrypted. What is the most likely cause of this traffic?

A. Other users are relaying social media requests through the user's computer.

B. The user's computer is part of a botnet.

C. The user is lying about her use of social media.

D. Someone else is using the user's computer when she is not present.

9. John deploys his website to multiple regions using load balancers around the world through his cloud infrastructure as a service provider. What availability concept is he using?

A. Multiple processing sites

B. Warm sites

C. Cold sites

D. A honeynet

10. Jim would like to identify compromised systems on his network that may be participating in a botnet. He plans to do this by watching for connections made to known command-and-control servers. Which one of the following techniques would be most likely to provide this information if Jim has access to a list of known servers?

A. NetFlow records

B. IDS logs

C. Authentication logs

D. RFC logs

For questions 11–15, please refer to the following scenario:

Gary was recently hired as the first chief information security officer (CISO) for a local government agency. The agency recently suffered a security breach and is attempting to build a new information security program. Gary would like to apply some best practices for security operations as he is designing this program.

11. As Gary decides what access permissions he should grant to each user, what principle should guide his decisions about default permissions?

A. Separation of duties

B. Least privilege

C. Aggregation

D. Separation of privileges

12. As Gary designs the program, he uses the matrix shown here. What principle of information security does this matrix most directly help enforce?

Roles/Tasks	Application Programmer	Security Administrator	Database Administrator	Database Server Administrator	Budget Analyst	Accounts Receivable	Accounts Payable	Deploy Patches	Verify Patches
Application Programmer		X	X	X					
Security Administrator	X		X	X	X	X	X	X	
Database Administrator	X	X		X					
Database Server Administrator	X	X	X						
Budget Analyst		X				X	X		
Accounts Receivable		X			X		X		
Accounts Payable		X			X	X			
Deploy Patches		X							X
Verify Patches								X	
	Potential Areas of Conflict								

A. Segregation of duties
B. Aggregation
C. Two-person control
D. Defense in depth

13. Gary is preparing to create an account for a new user and assign privileges to the HR database. What two elements of information must Gary verify before granting this access?
A. Credentials and need to know
B. Clearance and need to know
C. Password and clearance
D. Password and biometric scan

14. Gary is preparing to develop controls around access to root encryption keys and would like to apply a principle of security designed specifically for very sensitive operations. Which principle should he apply?
A. Least privilege
B. Defense in depth
C. Security through obscurity
D. Two-person control

15. How often should Gary and his team conduct a review of the privileged access that a user has to sensitive systems? (Select all that apply.)
A. On a periodic basis
B. When a user leaves the organization
C. When a user changes roles
D. On a daily basis

16. Which one of the following terms is often used to describe a collection of unrelated patches released in a large collection?
A. Hotfix
B. Update
C. Security fix
D. Service pack

17. Tonya is collecting evidence from a series of systems that were involved in a cybersecurity incident. A colleague suggests that she use a forensic disk controller for the collection process. What is the function of this device?
A. Masking error conditions reported by the storage device
B. Transmitting write commands to the storage device
C. Intercepting and modifying or discarding commands sent to the storage device
D. Preventing data from being returned by a read operation sent to the device

18. Lydia is processing access control requests for her organization. She comes across a request where the user does have the required security clearance, but there is no business justification for the access. Lydia denies this request. What security principle is she following?

A. Need to know

B. Least privilege

C. Separation of duties

D. Two-person control

19. Helen is tasked with implementing security controls in her organization that might be used to deter fraudulent insider activity. Which one of the following mechanisms would be LEAST useful to her work?

A. Job rotation

B. Mandatory vacations

C. Incident response

D. Two-person control

20. Matt wants to ensure that critical network traffic from systems throughout his company is prioritized over web browsing and social media use at this company. What technology can he use to do this?

A. VLANs

B. QoS

C. VPN

D. ISDN

21. Tom is responding to a recent security incident and is seeking information on the approval process for a recent modification to a system's security settings. Where would he most likely find this information?

A. Change log

B. System log

C. Security log

D. Application log

22. Staff from Susan's company often travel internationally and require connectivity to corporate systems for their work. Susan believes that these users may be targeted for corporate espionage activities because of the technologies that her company is developing and wants to include advice in the security training provided to international travelers. What practice should Susan recommend that they adopt for connecting to networks while they travel?

A. Only connect to public WiFi.

B. Use a VPN for all connections.

C. Only use websites that support TLS.

D. Do not connect to networks while traveling.

23. Ricky is seeking a list of information security vulnerabilities in applications, devices, and operating systems. Which one of the following threat intelligence sources would be most useful to him?

A. OWASP

B. Bugtraq

C. Microsoft Security Bulletins

D. CVE

24. Which of the following would normally be considered an example of a disaster when performing disaster recovery planning? (Select all that apply.)

A. Hacking incident

B. Flood

C. Fire

D. Terrorism

25. Glenda would like to conduct a disaster recovery test and is seeking a test that will allow a review of the plan with no disruption to normal information system activities and as minimal a commitment of time as possible. What type of test should she choose?

A. Tabletop exercise

B. Parallel test

C. Full interruption test

D. Checklist review

26. Which one of the following is not an example of a backup tape rotation scheme?

A. Grandfather/Father/Son

B. Meet in the middle

C. Tower of Hanoi

D. Six Cartridge Weekly

27. Helen is implementing a new security mechanism for granting employees administrative privileges in the accounting system. She designs the process so that both the employee's manager and the accounting manager must approve the request before the access is granted. What information security principle is Helen enforcing?

A. Least privilege

B. Two-person control

C. Job rotation

D. Separation of duties

28. Frank is considering the use of different types of evidence in an upcoming criminal matter. Which one of the following is not a requirement for evidence to be admissible in court?

A. The evidence must be relevant.

B. The evidence must be material.

C. The evidence must be tangible.

D. The evidence must be competently acquired.

29. Harold recently completed leading the postmortem review of a security incident. What documentation should he prepare next?

A. A lessons learned document

B. A risk assessment

C. A remediation list

D. A mitigation checklist

30. Beth is creating a new cybersecurity incident response team (CSIRT) and would like to determine the appropriate team membership. Which of the following groups would she normally include? (Select all that apply.)

A. Information security

B. Law enforcement

C. Senior management

D. Public affairs

31. Sam is responsible for backing up his company's primary file server. He configured a backup schedule that performs full backups every Monday evening at 9 p.m. and differential backups on other days of the week at that same time. Files change according to the information shown in the following figure. How many files will be copied in Wednesday's backup?

File Modifications
Monday 8 a.m. - File 1 created
Monday 10 a.m. - File 2 created
Monday 11 a.m. - File 3 created
Monday 4 p.m. - File 1 modified
Monday 5 p.m. - File 4 created
Tuesday 8 a.m. - File 1 modified
Tuesday 9 a.m. - File 2 modified
Tuesday 10 a.m. - File 5 created
Wednesday 8 a.m. - File 3 modified
Wednesday 9 a.m. - File 6 created

A. 2

B. 3

C. 5

D. 6

32. Which one of the following security tools is not capable of generating an active response to a security event?

A. IPS

B. Firewall

C. IDS

D. Antivirus software

33. Scott is responsible for disposing of disk drives that have been pulled from his company's SAN as they are retired. Which of the following options should he avoid if the data on the SAN is considered highly sensitive by his organization?

A. Destroy them physically.

B. Sign a contract with the SAN vendor that requires appropriate disposal and provides a certification process.

C. Reformat each drive before it leaves the organization.

D. Use a secure wipe tool like DBAN.

34. What term is used to describe the default set of privileges assigned to a user when a new account is created?

A. Aggregation

B. Transitivity

C. Baseline

D. Entitlement

35. Which one of the following types of agreements is the most formal document that contains expectations about availability and other performance parameters between a service provider and a customer?

A. Service-level agreement (SLA)

B. Operational-level agreement (OLA)

C. Memorandum of understanding (MOU)

D. Statement of work (SOW)

36. As the CIO of a large organization, Clara would like to adopt standard processes for managing IT activities. Which one of the following frameworks focuses on IT service management and includes topics such as change management, configuration management, and service-level agreements?

A. ITIL

B. PMBOK

C. PCI DSS

D. TOGAF

37. Richard is experiencing issues with the quality of network service on his organization's network. The primary symptom is that packets are consistently taking too long to travel from their source to their destination. What term describes the issue Richard is facing?

A. Jitter
B. Packet loss
C. Interference
D. Latency

38. Joe wants to test a program he suspects may contain malware. What technology can he use to isolate the program while it runs?

A. ASLR
B. Sandboxing
C. Clipping
D. Process isolation

39. Which one of the following is an example of a non-natural disaster?

A. Hurricane
B. Flood
C. Mudslide
D. Transformer explosion

40. Anne wants to gather information about security settings as well as build an overall view of her organization's assets by gathering data about a group of Windows 10 workstations spread throughout her company. What Windows tool is best suited to this type of configuration management task?

A. SCCM
B. Group Policy
C. SCOM
D. A custom PowerShell script

41. Javier is verifying that only IT system administrators have the ability to log on to servers used for administrative purposes. What principle of information security is he enforcing?

A. Need to know
B. Least privilege
C. Two-person control
D. Transitive trust

42. Which one of the following is not a basic preventative measure that you can take to protect your systems and applications against attack?

A. Implement intrusion detection and prevention systems.
B. Maintain current patch levels on all operating systems and applications.
C. Remove unnecessary accounts and services.
D. Conduct forensic imaging of all systems.

43. Tim is a forensic analyst who is attempting to retrieve information from a hard drive. It appears that the user attempted to erase the data, and Tim is trying to reconstruct it. What type of forensic analysis is Tim performing?

A. Software analysis

B. Media analysis

C. Embedded device analysis

D. Network analysis

44. Which one of the following is an example of a computer security incident? (Select all that apply.)

A. Failure of a backup to complete properly

B. System access recorded in a log

C. Unauthorized vulnerability scan of a file server

D. Update of antivirus signatures

45. Roland is a physical security specialist in an organization that has a large amount of expensive lab equipment that often moves around the facility. Which one of the following technologies would provide the most automation of an inventory control process in a cost-effective manner?

A. IPS

B. WiFi

C. RFID

D. Ethernet

46. Connor's company recently experienced a denial-of-service attack that Connor believes came from an inside source. If true, what type of event has the company experienced?

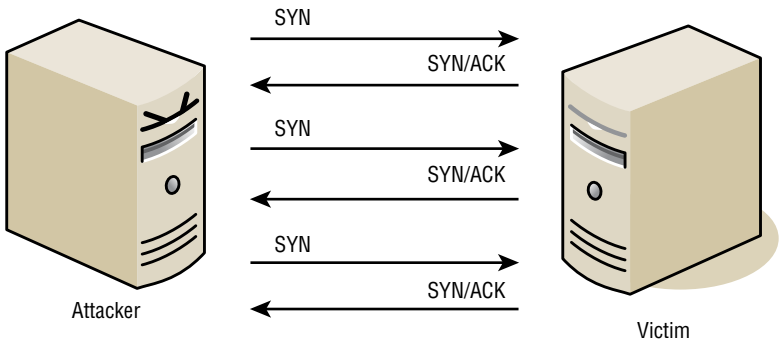
A. Espionage

B. Confidentiality breach

C. Sabotage

D. Integrity breach

47. Evan detects an attack against a server in his organization and examines the TCP flags on a series of packets, shown in the following diagram. What type of attack most likely took place?



A. SYN flood
B. Ping flood
C. Smurf
D. Fraggle

48. Florian is building a disaster recovery plan for his organization and would like to determine the amount of time that a particular IT service may be down without causing serious damage to business operations. What variable is Florian calculating?
A. RTO
B. MTD
C. RPO
D. SLA

49. Which of the following would normally be classified as zero-day attacks? (Select all that apply.)
A. An attacker who is new to the world of hacking
B. A database attack that places the date 00/00/0000 in data tables in an attempt to exploit flaws in business logic
C. An attack previously unknown to the security community
D. An attack that sets the operating system date and time to 00/00/0000 and 00:00:00

50. Grant is collecting records as part of the preparation for a possible lawsuit and is worried that his team may be spending too much time collecting information that may be irrelevant. What concept from the Federal Rules of Civil Procedure (FCRP) helps to ensure that additional time and expense are not incurred as part of electronic discovery when the benefits do not outweigh the costs?
A. Tool-assisted review
B. Cooperation
C. Spoilation
D. Proportionality

51. During an incident investigation, investigators meet with a system administrator who may have information about the incident but is not a suspect. What type of conversation is taking place during this meeting?
A. Interview
B. Interrogation
C. Both an interview and an interrogation
D. Neither an interview nor an interrogation

52. What technique has been used to protect the intellectual property in the following image?

A. Steganography
B. Clipping
C. Sampling
D. Watermarking

53. You are working to evaluate the risk of flood to an area as part of a business continuity planning (BCP) effort. You consult the flood maps from the Federal Emergency Management Agency (FEMA). According to those maps, the area lies within a 200-year flood plain. What is the annualized rate of occurrence (ARO) of a flood in that region?

A. 200
B. 0.01
C. 0.02
D. 0.005

54. Which one of the following individuals poses the greatest risk to security in most well-defended organizations?

A. Political activist
B. Malicious insider
C. Script kiddie
D. Thrill attacker

55. Veronica is considering the implementation of a database recovery mechanism recommended by a consultant. In the recommended approach, an automated process will move database backups from the primary facility to an off-site location each night. What type of database recovery technique is the consultant describing?

A. Remote journaling

B. Remote mirroring

C. Electronic vaulting

D. Transaction logging

56. When designing an access control scheme, Hilda set up roles so that the same person does not have the ability to provision a new user account and assign superuser privileges to an account. What information security principle is Hilda following?

A. Least privilege

B. Separation of duties

C. Job rotation

D. Security through obscurity

57. Patrick was charged with implementing a threat hunting program for his organization. Which one of the following is the basic assumption of a threat hunting program that he should use as he plans his work?

A. Security controls were designed using a defense-in-depth strategy.

B. Audits may uncover control deficiencies.

C. Attackers may already be present on the network.

D. Defense mechanisms may contain unpatched vulnerabilities.

58. Brian is developing the training program for his organization's disaster recovery program and would like to make sure that participants understand when disaster activity concludes. Which one of the following events marks the completion of a disaster recovery process?

A. Securing property and life safety

B. Restoring operations in an alternate facility

C. Restoring operations in the primary facility

D. Standing down first responders

59. Melanie suspects that someone is using malicious software to steal computing cycles from her company. Which one of the following security tools would be in the best position to detect this type of incident?

A. NIDS

B. Firewall

C. HIDS

D. DLP

60. Brandon observes that an authorized user of a system on his network recently misused his account to exploit a system vulnerability against a shared server that allowed him to gain root access to that server. What type of attack took place?

A. Denial-of-service

B. Privilege escalation

C. Reconnaissance

D. Brute-force

61. Carla has worked for her company for 15 years and has held a variety of different positions. Each time she changed positions, she gained new privileges associated with that position, but no privileges were ever taken away. What concept describes the sets of privileges she has accumulated?

A. Entitlement

B. Aggregation

C. Transitivity

D. Isolation

62. During what phase of the incident response process do administrators take action to limit the effect or scope of an incident?

A. Detection

B. Response

C. Mitigation

D. Recovery

For questions 63–66, please refer to the following scenario:

Ann is a security professional for a midsize business and typically handles log analysis and security monitoring tasks for her organization. One of her roles is to monitor alerts originating from the organization's intrusion detection system. The system typically generates several dozen alerts each day, and many of those alerts turn out to be false alarms after her investigation.

This morning, the intrusion detection system alerted because the network began to receive an unusually high volume of inbound traffic. Ann received this alert and began looking into the origin of the traffic.

63. At this point in the incident response process, what term best describes what has occurred in Ann's organization?

A. Security occurrence

B. Security incident

C. Security event

D. Security intrusion

64. Ann continues her investigation and realizes that the traffic generating the alert is abnormally high volumes of inbound UDP traffic on port 53. What service typically uses this port?

A. DNS

B. SSH/SCP

C. SSL/TLS

D. HTTP

65. As Ann analyzes the traffic further, she realizes that the traffic is coming from many different sources and has overwhelmed the network, preventing legitimate uses. The inbound packets are responses to queries that she does not see in outbound traffic. The responses are abnormally large for their type. What type of attack should Ann suspect?

A. Reconnaissance

B. Malicious code

C. System penetration

D. Denial-of-service

66. Now that Ann understands that an attack has taken place that violates her organization's security policy, what term best describes what has occurred in Ann's organization?

A. Security occurrence

B. Security incident

C. Security event

D. Security intrusion

67. Frank is seeking to introduce a hacker's laptop in court as evidence against the hacker. The laptop does contain logs that indicate the hacker committed the crime, but the court ruled that the search of the apartment that resulted in police finding the laptop was unconstitutional. What admissibility criteria prevents Frank from introducing the laptop as evidence?

A. Materiality

B. Relevance

C. Hearsay

D. Competence

68. Gordon suspects that a hacker has penetrated a system belonging to his company. The system does not contain any regulated information, and Gordon wants to conduct an investigation on behalf of his company. He has permission from his supervisor to conduct the investigation. Which of the following statements is true?

A. Gordon is legally required to contact law enforcement before beginning the investigation.

B. Gordon may not conduct his own investigation.

C. Gordon's investigation may include examining the contents of hard disks, network traffic, and any other systems or information belonging to the company.

D. Gordon may ethically perform "hack back" activities after identifying the perpetrator.

69. Which one of the following tools provides an organization with the greatest level of protection against a software vendor going out of business?

A. Service-level agreement

B. Escrow agreement

C. Mutual assistance agreement

D. PCI DSS compliance agreement

70. Fran is considering new human resources policies for her bank that will deter fraud. She plans to implement a mandatory vacation policy. What is typically considered the shortest effective length of a mandatory vacation?

A. Two days

B. Four days

C. One week

D. One month

71. Which of the following events would constitute a security incident? (Select all that apply.)

A. An attempted network intrusion

B. A successful database intrusion

C. A malware infection

D. A successful attempt to access a file

E. A violation of a confidentiality policy

F. An unsuccessful attempt to remove information from a secured area

72. Amanda is configuring her organization's firewall to implement egress filtering. Which one of the following traffic types should not be blocked by her organization's egress filtering policy? (Select all that apply.)

A. Traffic rapidly scanning many IP addresses on port 22

B. Traffic with a broadcast destination

C. Traffic with a source address from an external network

D. Traffic with a destination address on an external network

73. Allie is responsible for reviewing authentication logs on her organization's network. She does not have the time to review all logs, so she decides to choose only records where there have been four or more invalid authentication attempts. What technique is Allie using to reduce the size of the pool?

A. Sampling

B. Random selection

C. Clipping

D. Statistical analysis

74. You are performing an investigation into a potential bot infection on your network and want to perform a forensic analysis of the information that passed between different systems on your network and those on the internet. You believe that the information was likely encrypted. You are beginning your investigation after the activity concluded. What would be the best and easiest way to obtain the source of this information?

A. Packet captures

B. NetFlow data

C. Intrusion detection system logs

D. Centralized authentication records

75. Which one of the following tools helps system administrators by providing a standard, secure template of configuration settings for operating systems and applications?

A. Security guidelines

B. Security policy

C. Baseline configuration

D. Running configuration

76. What type of disaster recovery test activates the alternate processing facility and uses it to conduct transactions but leaves the primary site up and running?

A. Full interruption test

B. Parallel test

C. Checklist review

D. Tabletop exercise

77. During which phase of the incident response process would an analyst receive an intrusion detection system alert and verify its accuracy?

A. Response

B. Mitigation

C. Detection

D. Reporting

78. Kevin is developing a continuous security monitoring strategy for his organization. Which one of the following is not normally used when determining assessment and monitoring frequency?

A. Threat intelligence

B. System categorization/impact level

C. Security control operational burden

D. Organizational risk tolerance

79. Hunter is reviewing his organization's monitoring strategy and identifying new technologies that they might deploy. His assessment reveals that the firm is not doing enough to monitor employee activity on endpoint devices. Which one of the following technologies would best meet his needs?

A. EDR

B. IPS

C. IDS

D. UEBA

80. Bruce is seeing quite a bit of suspicious activity on his network. After consulting records in his SIEM, it appears that an outside entity is attempting to connect to all of his systems using a TCP connection on port 22. What type of scanning is the outsider likely engaging in?

A. FTP scanning

B. Telnet scanning

C. SSH scanning

D. HTTP scanning

81. Dylan believes that a database server in his environment was compromised using a SQL injection attack. Which one of the following actions would Dylan most likely take during the remediation phase of the attack?

A. Rebuilding the database from backups

B. Adding input validation to a web application

C. Reviewing firewall logs

D. Reviewing database logs

82. Roger recently accepted a new position as a security professional at a company that runs its entire IT infrastructure within an IaaS environment. Which one of the following would most likely be the responsibility of Roger's firm?

A. Configuring the network firewall

B. Applying hypervisor updates

C. Patching operating systems

D. Wiping drives prior to disposal

83. What technique can application developers use to test applications in an isolated virtualized environment before allowing them on a production network?

A. Penetration testing

B. Sandboxing

C. White-box testing

D. Black-box testing

84. Gina is the firewall administrator for a small business and recently installed a new firewall. After seeing signs of unusually heavy network traffic, she checked the intrusion detection system, which reported that a SYN flood attack was underway. What firewall configuration change can Gina make to most effectively prevent this attack?

A. Block SYN from known IPs.

B. Block SYN from unknown IPs.

C. Enable SYN-ACK spoofing at the firewall.

D. Disable TCP.

85. Nancy is leading an effort to modernize her organization's antimalware protection and would like to add endpoint detection and response (EDR) capabilities. Which of the following actions are normally supported by EDR systems? (Select all that apply.)

A. Analyzing endpoint memory, filesystem, and network activity for signs of malicious activity

B. Automatically isolating possible malicious activity to contain the potential damage

C. Conducting simulated phishing campaigns

D. Integration with threat intelligence sources

86. Alan is assessing the potential for using machine learning and artificial intelligence in his cybersecurity program. Which of the following activities is most likely to benefit from this technology?

A. Intrusion detection

B. Account provisioning

C. Firewall rule modification

D. Media sanitization

87. Timber Industries recently got into a dispute with a customer. During a meeting with his account representative, the customer stood up and declared, "There is no other solution. We will have to take this matter to court." He then left the room. When does Timber Industries have an obligation to begin preserving evidence?

A. Immediately

B. Upon receipt of a notice of litigation from opposing attorneys

C. Upon receipt of a subpoena

D. Upon receipt of a court order

88. Candace is designing a backup strategy for her organization's file server. She would like to perform a backup every weekday that has the smallest possible storage footprint. What type of backup should she perform?

A. Incremental backup

B. Full backup

C. Differential backup

D. Transaction log backup

89. Darcy is a computer security specialist who is assisting with the prosecution of a hacker. The prosecutor requests that Darcy give testimony in court about whether, in her opinion, the logs and other records in a case are indicative of a hacking attempt. What type of evidence is Darcy being asked to provide?

A. Expert opinion

B. Direct evidence

C. Real evidence

D. Documentary evidence

90. Which one of the following techniques is not commonly used to remove unwanted remnant data from magnetic tapes?

A. Physical destruction

B. Degaussing

C. Overwriting

D. Reformatting

91. Sally is building a new server for use in her environment and plans to implement RAID level 1 as a storage availability control. What is the minimum number of physical hard disks that she needs to implement this approach?

A. One

B. Two

C. Three

D. Five

92. Jerome is conducting a forensic investigation and is reviewing database server logs to investigate query contents for evidence of SQL injection attacks. What type of analysis is he performing?

A. Hardware analysis

B. Software analysis

C. Network analysis

D. Media analysis

93. Quigley Computing regularly ships tapes of backup data across the country to a secondary facility. These tapes contain confidential information. What is the most important security control that Quigley can use to protect these tapes?

A. Locked shipping containers

B. Private couriers

C. Data encryption

D. Media rotation

94. Carolyn is concerned that users on her network may be storing sensitive information, such as Social Security numbers, on their hard drives without proper authorization or security controls. What third-party security service can she implement to best detect this activity?

A. IDS

B. IPS

C. DLP

D. TLS

95. Gavin is the disaster recovery team leader for his organization, which is currently in the response phase of an incident that has severe customer impact. Gavin just received a phone call from a reporter asking for details on the root cause and an estimated recovery time. Gavin has this information at his fingertips. What should he do?

A. Provide the information to the reporter.

B. Request a few minutes to gather the information and return the call.

C. Refer the matter to the public relations department.

D. Refuse to provide any information.

96. Pauline is reviewing her organization's emergency management plans. What should be the highest priority when creating these plans?

A. Protection of mission-critical data

B. Preservation of operational systems

C. Collection of evidence

D. Preservation of safety

97. Barry is the CIO of an organization that recently suffered a serious operational issue that required activation of the disaster recovery plan. He would like to conduct a lessons learned session to review the incident. Who would be the best facilitator for this session?

A. Barry, as chief information officer

B. Chief information security officer

C. Disaster recovery team leader

D. External consultant

98. Brent is reviewing the controls that will protect his organization in the event of a sustained period of power loss. Which one of the following solutions would best meet his needs?

A. Redundant servers

B. Uninterruptible power supply (UPS)

C. Generator

D. RAID

99. Match each of the numbered terms with its correct lettered definition:

Terms

1. Honeypot C
2. Honeynet B
3. Pseudoflaw A
4. Darknet D

Definitions

A. An intentionally designed vulnerability used to lure in an attacker

B. A network set up with intentional vulnerabilities

C. A system set up with intentional vulnerabilities

D. A monitored network without any hosts

100. Match each of the numbered types of recovery capabilities to their correct lettered definition:

Terms

1. Hot site B
2. Cold site D
3. Warm site C
4. Service bureau A

Definitions

A. An organization that can provide on-site or off-site IT services in the event of a disaster

B. A site with dedicated storage and real-time data replication, often with shared equipment that allows restoration of service in a very short time

C. A site that relies on shared storage and backups for recovery

D. A rented space with power, cooling, and connectivity that can accept equipment as part of a recovery effort

1. Susan provides a public RESTful API for her organization's data but wants to limit its use to trusted partners. She intends to use API keys. What other recommendation would you give Susan to limit the potential abuse of the service?
   - **A.** Limit request rates
   - **B.** Force HTTP-only requests
   - **C.** Avoid tokens due to bandwidth constraints
   - **D.** Blacklist HTTP methods such as GET, POST, and PUT

2. Darren is conducting a threat hunting exercise and would like to look for botnet indicators of compromise. Which of the following are common ways that attackers leverage botnets? (Select all that apply.)
   - **A.** Mining cryptocurrency
   - **B.** Conducting brute-force attacks
   - **C.** Scanning for vulnerable systems
   - **D.** Conducting man-in-the-middle attacks

3. Which one of the following statements is not true about code review?
   - **A.** Code review should be a peer-driven process that includes multiple developers.
   - **B.** Code review may be automated.
   - **C.** Code review occurs during the design phase.
   - **D.** Code reviewers may expect to review several hundred lines of code per hour.

4. Kathleen is reviewing the Ruby code shown here. What security technique is this code using?

```
insert_new_user = db.prepare "INSERT INTO users (name, userid, gender,
usertype) VALUES (?, ? ,?,?)"
insert_new_user.execute 'davids', '194567', 'male', 'admin'
```

   - **A.** Parameterization
   - **B.** Typecasting
   - **C.** Gem cutting
   - **D.** Stored procedures

5. Jessica is reviewing her organization's change management process and would like to verify that changes to software include acceptance testing. Which process is responsible for achieving this goal?
   - **A.** Request control
   - **B.** Change control
   - **C.** Release control
   - **D.** Configuration control

6. Ashley is investigating an attack that compromised an account of one of her users. In the attack, the attacker forced the submission of an authenticated request to a third-party site by exploiting trust relationships in the user's browser. What type of attack most likely took place?
   - **A.** XSS
   - **B.** CSRF
   - **C.** SQL injection
   - **D.** Session hijacking

7. Arnold is creating a new software package and is making use of the OpenSSL library. What term best describes the library he is using?
   - **A.** Open source
   - **B.** COTS
   - **C.** Third-party
   - **D.** Managed

8. Jaime is a technical support analyst and is asked to visit a user whose computer is displaying the error message shown here. What state has this computer entered?

   - **A.** Fail open
   - **B.** Irrecoverable error
   - **C.** Memory exhaustion
   - **D.** Fail secure

9. Joshua is developing a software threat modeling program for his organization. Which of the following are appropriate goals for the program? (Select all that apply.)

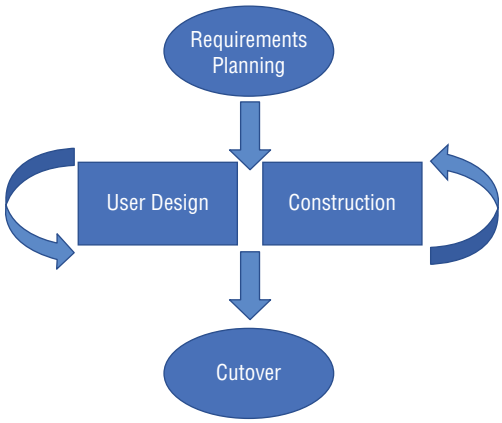
A. To reduce the number of security-related design flaws
B. To reduce the number of security-related coding flaws
C. To reduce the severity of non-security-related flaws
D. To reduce the number of threat vectors

10. In the diagram shown here, which is an example of a method?

Account
Balance: currency = 0 Owner: string
AddFunds(deposit: currency) RemoveFunds(withdrawal: currency)

A. `Account`
B. `Owner`
C. `AddFunds`
D. `Balance`

11. Wanda is reviewing the application development documentation used by her organization and finds the lifecycle illustration shown here. What application development method is her organization using?



A. Waterfall
B. Spiral
C. Agile
D. RAD

12. Which one of the following testing methodologies typically works without access to source code?
    A. Dynamic testing
    B. Static testing
    C. White-box testing
    D. Code review

13. Lucca is analyzing a web application that his organization acquired from a third-party vendor. Lucca determined that the application contains a flaw that causes users who are logged in to be able to take actions they should not be able to in their role. What type of security vulnerability should this be classified as?
    A. Data validation
    B. Session management
    C. Authorization
    D. Error handling

14. Bobby is investigating how an authorized database user is gaining access to information outside his normal clearance level. Bobby believes that the user is making use of a type of function that summarizes data. What term describes this type of function?
    A. Inference
    B. Polymorphic
    C. Aggregate
    D. Modular

15. Taylor would like to better protect the applications developed by her organization against buffer overflow attacks. Which of the following controls would best provide this protection?
    A. Encryption
    B. Input validation
    C. Firewall
    D. Intrusion prevention system

16. Kayla recently completed a thorough risk analysis and mitigation review of the software developed by her team and identified three persistent issues:

    1. Cross-site scripting
    2. SQL injection
    3. Buffer overflows

    What is the most significant deficiency in her team's work identified by these issues?
    A. Lack of API security
    B. Improper error handling
    C. Improper or missing input validation
    D. Source code design issues

For questions 17–20, please refer to the following scenario:

Robert is a consultant who helps organizations create and develop mature software development practices. He prefers to use the Software Capability Maturity Model (SW-CMM) to evaluate the current and future status of organizations using both independent review and self-assessments. He is currently working with two different clients.

Acme Widgets is not very well organized with its software development practices. It does have a dedicated team of developers who do "whatever it takes" to get software out the door, but it does not have any formal processes.

Beta Particles is a company with years of experience developing software using formal, documented software development processes. It uses a standard model for software development but does not have quantitative management of those processes.

17. What phase of the SW-CMM should Robert report as the current status of Acme Widgets?

A. Defined

B. Repeatable

C. Initial

D. Managed

18. Robert is working with Acme Widgets on a strategy to advance their software development practices. What SW-CMM stage should be their next target milestone?

A. Defined

B. Repeatable

C. Initial

D. Managed

19. What phase of the SW-CMM should Robert report as the current status of Beta Particles?

A. Defined

B. Repeatable

C. Optimizing

D. Managed

20. Robert is also working with Beta Particles on a strategy to advance their software development practices. What SW-CMM stage should be their next target milestone?

A. Defined

B. Repeatable

C. Optimizing

D. Managed

21. Which one of the following database keys is used to enforce referential integrity relationships between tables?

A. Primary key

B. Candidate key

C. Foreign key

D. Master key

22. Brynn believes that a system in her organization may have been compromised by a macro virus. Which one of the following files is most likely to be the culprit?

A. `projections.doc`

B. `command.com`

C. `command.exe`

D. `loopmaster.exe`

23. Victor created a database table that contains information on his organization's employees. The table contains the employee's user ID, three different telephone number fields (home, work, and mobile), the employee's office location, and the employee's job title. There are 16 records in the table. What is the degree of this table?

A. 3

B. 4

C. 6

D. 16

24. Carrie is analyzing the application logs for her web-based application and comes across the following string:

```
../../../../../../../../../etc/passwd
```

What type of attack was likely attempted against Carrie's application?

A. Command injection

B. Session hijacking

C. Directory traversal

D. Brute-force

25. When should a design review take place when following an SDLC approach to software development?

A. After the code review

B. After user acceptance testing

C. After the development of functional requirements

D. After the completion of unit testing

26. Tracy is preparing to apply a patch to her organization's enterprise resource planning system. She is concerned that the patch may introduce flaws that did not exist in prior versions, so she plans to conduct a test that will compare previous responses to input with those produced by the newly patched application. What type of testing is Tracy planning?

A. Unit testing

B. Acceptance testing

C. Regression testing

D. Vulnerability testing

27. What term is used to describe the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner?

A. Validation

B. Accreditation

C. Confidence interval

D. Assurance

28. Victor recently took a new position at an online dating website and is responsible for leading a team of developers. He realized quickly that the developers are having issues with production code because they are working on different projects that result in conflicting modifications to the production code. What process should Victor invest in improving?

A. Request control

B. Release control

C. Change control

D. Configuration control

29. Tom is assessing security risks related to a database he manages. Examining user access controls, he determines that users have access to individual records in a table that match their clearances, but if they pull multiple records, that collection of facts has a higher classification than the classification of any of those facts standing alone and exceeds the permitted access. What type of issue has Tom identified?

A. Inference

B. SQL injection

C. Multilevel security

D. Aggregation

30. Ron leads a team of software developers who find themselves often re-creating code that performs common functions. What software development tool could he use to best address this situation?

A. Code repositories

B. Code libraries

C. IDEs

D. DAST

31. Vivian would like to hire a software tester to come in and evaluate a new web application from a user's perspective. Which of the following tests best simulates that perspective?

A. Black box

B. Gray box

C. Blue box

D. White box

32. Referring to the database transaction shown here, what would happen if no account exists in the Accounts table with account number 1001?

```
BEGIN TRANSACTION

UPDATE accounts
SET balance = balance + 250
WHERE account_number = 1001;

UPDATE accounts
SET balance = balance - 250
WHERE account_number = 2002;

COMMIT TRANSACTION
```

A. The database would create a new account with this account number and give it a $250 balance.

B. The database would ignore that command and still reduce the balance of the second account by $250.

C. The database would roll back the transaction, ignoring the results of both commands.

D. The database would generate an error message.

33. Brandon is a software developer seeking to integrate his software with a popular social media site. The site provides him with software libraries that he can use to better integrate his code as well as other tools that make his work easier. What term best describes the service he is using?

A. SDK

B. DLP

C. IDE

D. API

34. Kim is troubleshooting an application firewall that serves as a supplement to the organization's network and host firewalls and intrusion prevention system, providing added protection against web-based attacks. The issue the organization is experiencing is that the firewall technology suffers somewhat frequent restarts that render it unavailable for 10 minutes at a time. What configuration might Kim consider to maintain availability during that period at the lowest cost to the company?

A. High availability cluster

B. Failover device

C. Fail open

D. Redundant disks

35. What type of security issue arises when an attacker can deduce a more sensitive piece of information by analyzing several pieces of information classified at a lower level?

A. SQL injection

B. Multilevel security

C. Parameterization

D. Inference

36. Greg is battling a malware outbreak in his organization. He used specialized malware analysis tools to capture samples of the malware from three different systems and noticed that the code is changing slightly from infection to infection. Greg believes that this is the reason that antivirus software is having a tough time defeating the outbreak. What type of malware should Greg suspect is responsible for this security incident?

A. Stealth virus

B. Polymorphic virus

C. Multipartite virus

D. Encrypted virus

For questions 37–40, please refer to the following scenario:

Linda is reviewing posts to a user forum on her company's website, and when she browses a certain post, a message pops up in a dialog box on her screen reading "Alert." She reviews the source code for the post and finds the following code snippet:

```
<script>alert('Alert');</script>
```

37. What vulnerability definitely exists on Linda's message board?

A. Cross-site scripting

B. Cross-site request forgery

C. SQL injection

D. Improper authentication

38. What was the likely motivation of the user who posted the message on the forum containing this code?

A. Reconnaissance

B. Theft of sensitive information

C. Credential stealing

D. Social engineering

39. Linda communicates with the vendor and determines that no patch is available to correct this vulnerability. Which one of the following devices would best help her defend the application against further attack?

A. VPN

B. WAF

C. DLP

D. IDS

40. In further discussions with the vendor, Linda finds that they are willing to correct the issue but do not know how to update their software. What technique would be most effective in mitigating the vulnerability of the application to this type of attack?

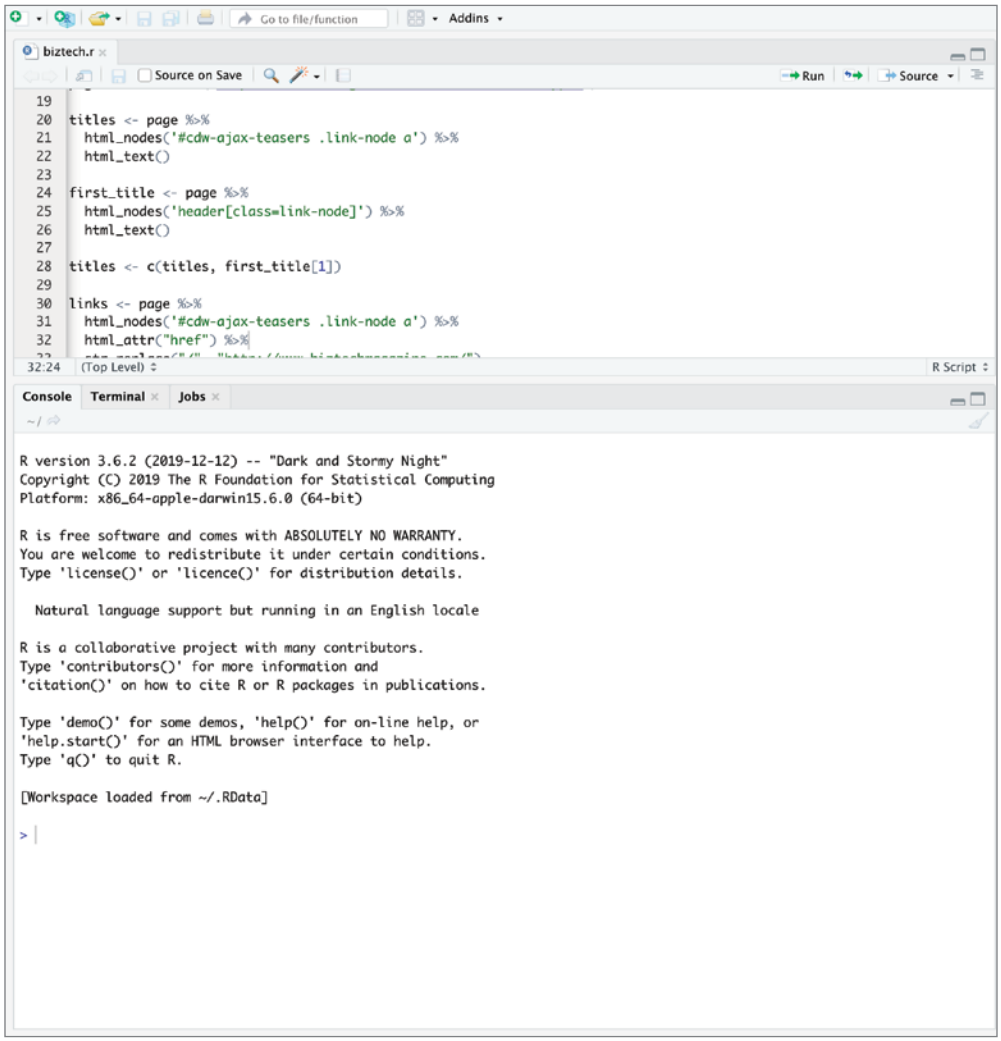
A. Bounds checking

B. Peer review

C. Input validation

D. OS patching

41. Hannah is a software developer working on creating statistical software using the R programming language. She uses the RStudio tool, shown here, to assist her in writing this code. What term best describes this tool?



A. SDK

B. IDE

C. API

D. DLP

42. Lauren wants to use a software review process for the application she is working on. Which of the following processes would work best if she is a remote worker who works different hours from the rest of her team?

A. Pass around

B. Pair programming

C. Team review

D. Fagan inspection

43. Alan is deploying Java code to a variety of machines in his environment and must install the JVM on those machines first. What term best describes the JVM in this case?

A. Repository

B. Change manager

C. Runtime

D. Sandbox

44. Christine is nearing the final stages of testing a new software package. Which one of the following types of software testing usually occurs last and is executed against test scenarios?

A. Unit testing

B. Integration testing

C. User acceptance testing

D. System testing

45. Alexis' organization recently moved to a CI/CD approach for software development where they intend to speed up the deployment of code supporting their website. What is the most reasonable frequency that they can expect to achieve using this type of approach?

A. Monthly deployments

B. Weekly deployments

C. Daily deployments

D. Hundreds of daily deployments

46. Amber is conducting a threat intelligence project and would like to find a source of information on threats to her organization's web applications. Which of the following organizations is widely considered as the definitive source for information on web-based attack vectors?

A. $(ISC)^2$

B. ISACA

C. OWASP

D. Mozilla Foundation

47. Chris is a software developer, and he is actively writing code for an application. What phase of the Agile process is he in?

A. Planning

B. Sprints

C. Deployment

D. Development

48. Alyssa's team recently implemented a new system that gathers information from a variety of different log sources, analyzes that information, and then triggers automated playbooks in response to security events. What term best describes this technology?

A. SIEM

B. Log repositories

C. IPS

D. SOAR

49. Chris is reviewing the code of an open source application that he is planning to use in his organization. He finds the code excerpt shown here:

```
int myarray[10];
myarray[10] = 8;
```

What type of attack is taking place?

A. Mismatched data types

B. Overflow

C. SQL injection

D. Covert channel

50. Which one of the following database issues occurs when one transaction writes a value to the database that overwrites a value that was needed by transactions with earlier precedence?

A. Dirty read

B. Incorrect summary

C. Lost update

D. SQL injection

51. Belinda would like to better protect users of her organization's web application from cookie stealing attacks. Which one of the following is the most effective control against this type of session hijacking attack?

A. TLS

B. Complex session cookies

C. SSL

D. Expiring cookies frequently

52. In a software configuration management program, what is the primary role of the CAB?

A. Approve the credentials of developers.

B. Facilitate lessons learned sessions.

C. Review and approve/reject code changes.

D. Prioritize software development efforts.

53. Which one of the following tools is commonly used by software developers to interact with and manage code that is stored in code repositories?

A. `grep`

B. `git`

C. `lsof`

D. `gcc`

54. While evaluating a potential security incident, Harry comes across a log entry from a web server request showing that a user entered the following input into a form field:

```
CARROT'&1=1;--
```

What type of attack was attempted?

A. Buffer overflow

B. Cross-site scripting

C. SQL injection

D. Cross-site request forgery

55. Which one of the following is not an effective control against SQL injection attacks?

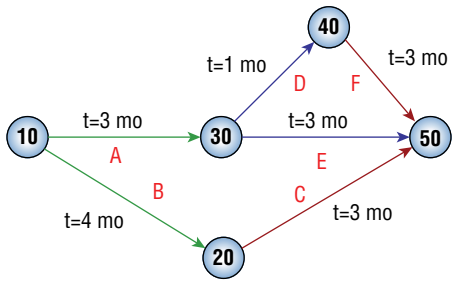
A. Escaping

B. Client-side input validation

C. Parameterization

D. Limiting database permissions

56. Jason is reviewing the documentation for a software development project and comes across the diagram shown here. What type of diagram is he examining?



A. WBS chart

B. PERT chart

C. Gantt chart

D. Wireframe diagram

57. In what software testing technique does the evaluator retest a large number of scenarios each time that the software changes to verify that the results are consistent with a standard baseline?

A. Orthogonal array testing

B. Pattern testing

C. Matrix testing

D. Regression testing

58. Haley is reviewing code created by her organization for its possible exposure to web application vulnerabilities. Which one of the following conditions may make an application most vulnerable to a cross-site scripting (XSS) attack?

A. Input validation

B. Reflected input

C. Unpatched server

D. Promiscuous firewall rules

59. Roger is conducting a software test for a tax preparation application developed by his company. End users will access the application over the web, but Roger is conducting his test on the back end, evaluating the source code on the web server. What type of test is Roger conducting?

A. White box

B. Gray box

C. Blue box

D. Black box

60. Which of the following statements is true about heuristic-based antimalware software?

A. It has a lower false positive rate than signature detection.

B. It requires frequent definition updates to detect new malware.

C. It has a higher likelihood of detecting zero-day exploits than signature detection.

D. It monitors systems for files with content known to be viruses.

61. Martin is inspecting a system where the user reported unusual activity, including disk activity when the system is idle and abnormal CPU and network usage. He suspects that the machine is infected by a virus, but scans come up clean. What malware technique might be in use here that would explain the clean scan results?

A. File infector virus

B. MBR virus

C. Service injection virus

D. Stealth virus

62. Tomas discovers a line in his application log that appears to correspond with an attempt to conduct a directory traversal attack. He believes the attack was conducted using URL encoding. The line reads as follows:

```
%252E%252E%252F%252E%252E%252Fetc/passwd
```

What character is represented by the %252E value?

A. .

B. ,

C. ;

D. /

63. An attacker posted a message to a public discussion forum that contains an embedded malicious script that is not displayed to the user but executes on the user's system when read. What type of attack is this?

A. Persistent XSRF

B. Nonpersistent XSRF

C. Persistent XSS

D. Nonpersistent XSS

64. Which one of the following is not a principle of the Agile software development process?

A. Welcome changing requirements, even late in the development process.

B. Maximizing the amount of work not done is essential.

C. Clear documentation is the primary measure of progress.

D. Build projects around motivated individuals.

65. Gavin is an internal auditor tasked with examining the change management practices of his organization. He would like to review a series of changes made to a software package to determine whether they were properly documented. Where should he turn for a description of each proposed change?

A. CAB

B. RFC

C. SOAR

D. SIEM

66. Neal is working with a DynamoDB database. The database is not structured like a relational database but allows Neal to store data using a key-value store. What type of database is DynamoDB?

A. Relational database

B. Graph database

C. Hierarchical database

D. NoSQL database

67. In the transaction shown here, what would happen if the database failed in between the first and second update statements?

```
BEGIN TRANSACTION

UPDATE accounts
SET balance = balance + 250
WHERE account_number = 1001;

UPDATE accounts
SET balance = balance - 250
WHERE account_number = 2002;

COMMIT TRANSACTION
```

A. The database would credit the first account with $250 in funds but then not reduce the balance of the second account.

B. The database would ignore the first command and only reduce the balance of the second account by $250.

C. The database would roll back the transaction, ignoring the results of both commands.

D. The database would successfully execute both commands.

68. Tareck's organization makes use of a significant amount of COTS software. He recently discovered a significant buffer overflow vulnerability in the code of a COTS software package that is crucial to his business. What is the most likely way that Tareck can get this corrected?

A. Work with his software development team to modify the code.

B. Notify the vendor and request a patch.

C. Deploy an intrusion prevention system.

D. Update firewall rules.

69. Which one of the following statements is true about software testing?

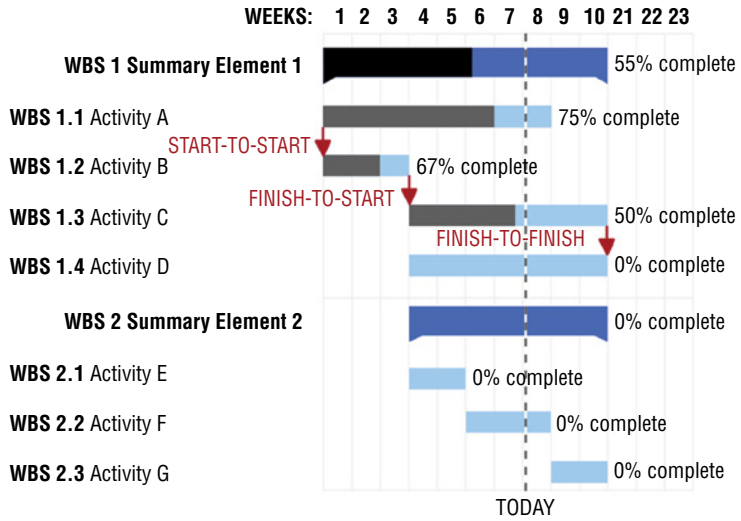
A. Static testing works on runtime environments.

B. Static testing performs code analysis.

C. Dynamic testing uses automated tools, but static testing does not.

D. Static testing is a more important testing technique than dynamic testing.

70. David is working on developing a project schedule for a software development effort, and he comes across the chart shown here. What type of chart is this?



A. Work breakdown structure

B. Functional requirements

C. PERT chart

D. Gantt chart

71. Barry is a software tester who is working with a new gaming application developed by his company. He is playing the game on a smartphone to conduct his testing in an environment that best simulates a normal end user, but he is referencing the source code as he conducts his test. What type of test is Barry conducting?

A. White box

B. Black box

C. Blue box

D. Gray box

72. Miguel recently completed a penetration test of the applications that his organization uses to handle sensitive information. During his testing, he discovered a condition where an attacker can exploit a timing condition to manipulate software into allowing him to perform an unauthorized action. Which one of the following attack types fits this scenario?

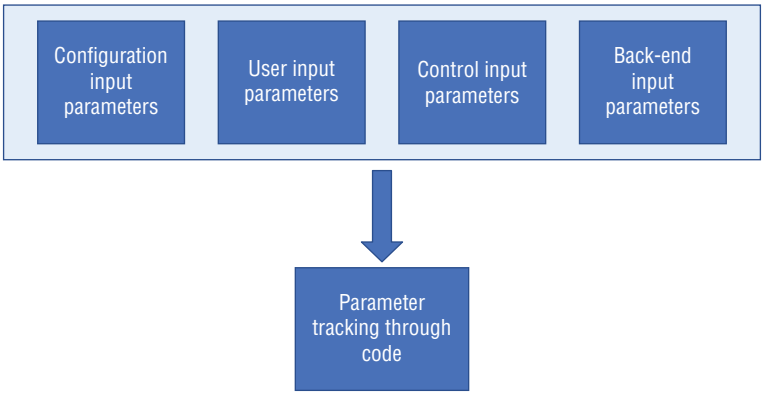
A. SQL injection

B. Cross-site scripting

C. Pass the hash

D. TOC/TOU

73. What part of the security review process are the input parameters shown in the diagram used for?



A. SQL injection review
B. Sprint review
C. Fagan inspection
D. Attack surface identification

74. What application security process can be described in these three major steps?

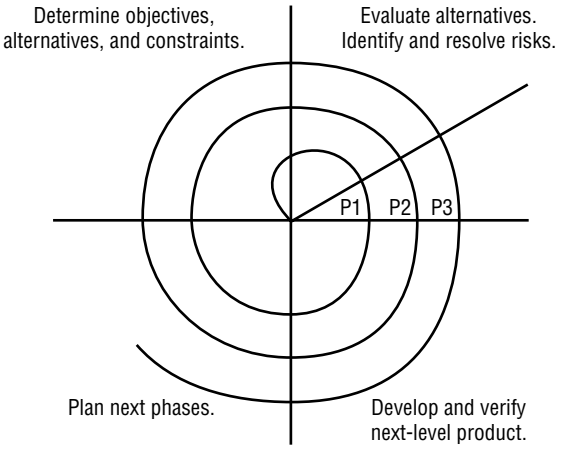
1. Decomposing the application
2. Determining and ranking threats
3. Determining countermeasures and mitigation

A. Fagan inspection
B. Threat modeling
C. Penetration testing
D. Code review

75. Which one of the following approaches to failure management is the most conservative from a security perspective?

A. Fail open
B. Fail mitigation
C. Fail clear
D. Fail closed

76. What software development model is shown in the figure?



A. Waterfall

B. Agile

C. Lean

D. Spiral

77. Mark is considering replacing his organization's customer relationship management (CRM) solution with a new product that is available in the cloud. This new solution is completely managed by the vendor, and Mark's company will not have to write any code or manage any physical resources. What type of cloud solution is Mark considering?

A. IaaS

B. CaaS

C. PaaS

D. SaaS

78. Which one of the following change management processes is initiated by users rather than developers?

A. Change request

B. Change control

C. Release control

D. Design review

79. Teagan would like to better protect his organization against database inference attacks. Which one of the following techniques is an effective countermeasure against these attacks?

A. Input validation

B. Parameterization

C. Polyinstantiation

D. Server-side validation

80. Ursula is a government web developer who recently created a public application that offers property records. She would like to make it available for other developers to integrate into their applications. What can Ursula create to make it easiest for developers to call her code directly and integrate the output into their applications?

A. Object model

B. Data dictionary

C. API

D. Primary key

81. Nathan recently completed a software development project where he integrated the organization's network operations stack with their development processes. As a result, developers can modify firewall rules from their code on an as-needed basis. What term best describes this ability?

A. Agile

B. IaC

C. SDS

D. DevOps

82. TJ is inspecting a system where the user reported a strange error message and the inability to access files. He sees the window shown in this figure. What type of malware should TJ suspect?

A. Service injection
B. Encrypted virus
C. SQL injection
D. Ransomware

83. Charles is developing a mission-critical application that has a direct impact on human safety. Time and cost are less important than correctly functioning software. Which of the following software development methodologies should he choose given these requirements?

A. Agile
B. DevOps
C. Spiral
D. Waterfall

84. Which one of the following types of artificial intelligence attempts to use complex computations to replicate the partial function of the human mind?

A. Decision support systems
B. Expert systems
C. Knowledge bank
D. Neural networks

85. At which level of the Software Capability Maturity Model (SW-CMM) does an organization introduce basic lifecycle management processes?

A. Initial
B. Repeatable
C. Defined
D. Managed

86. Lucas runs the accounting systems for his company. The morning after an essential was fired, systems began mysteriously losing information. Lucas suspects that the fired employee tampered with the systems prior to his departure. What type of attack should Lucas suspect?

A. Privilege escalation
B. SQL injection
C. Logic bomb
D. Remote code execution

87. Which one of the following principles would not be favored in an Agile approach to software development?

A. Processes and tools over individuals and interactions
B. Working software over comprehensive documentation
C. Customer collaboration over contract negotiations
D. Responding to change over following a plan

88. What technique do API developers most commonly use to limit access to an API to authorized individuals and applications?

A. Encryption

B. Input validation

C. API keys

D. IP filters

89. Reggie recently received a letter from his company's internal auditors scheduling the kickoff meeting for an assessment of his group. Which of the following should Reggie not expect to learn during that meeting?

A. Scope of the audit

B. Purpose of the audit

C. Expected timeframe

D. Expected findings

90. Which one of the following is the proper order of steps in the waterfall model of software development?

A. Requirements, Design, Testing, Coding, Maintenance

B. Requirements, Design, Coding, Testing, Maintenance

C. Design, Requirements, Coding, Testing, Maintenance

D. Design, Requirements, Testing, Coding, Maintenance

91. Renee is a software developer who writes code in Node.js for her organization. The company is considering moving from a self-hosted Node.js environment to one where Renee will run her code on application servers managed by a cloud vendor. What type of cloud solution is Renee's company considering?

A. IaaS

B. CaaS

C. PaaS

D. SaaS

92. Tom is writing a software program that calculates the sales tax for online orders placed from various jurisdictions. The application includes a user-defined field that allows the entry of the total sale amount. Tom would like to ensure that the data entered in this field is a properly formatted dollar amount. What technique should he use?

A. Limit check

B. Fail open

C. Fail secure

D. Input validation

93. Brian is helping implement a new software testing methodology for his organization and would like to review the completeness of his toolkit. Which of the following would be considered dynamic application security testing (DAST) tools? (Select all that apply.)

A. Code review

B. Fuzzing

C. Static analysis

D. Web application vulnerability scanning

94. What approach to technology management integrates the three components of technology management shown in this illustration?

A. Agile

B. Lean

C. DevOps

D. ITIL

95. Olivia is conducting a risk analysis of a web application that her organization obtained from a third party and is concerned that it might contain vulnerabilities. Which one of the following activities might she take to best mitigate the risk?

A. Deploy a WAF.

B. Implement strong encryption.

C. Purchase an insurance policy.

D. Discontinue use of the software.

96. Which one of the following database concurrency issues occurs when one transaction reads information that was written to a database by a second transaction that never committed?

A. Lost update

B. SQL injection

C. Incorrect summary

D. Dirty read

97. What software development concept was pioneered by the Defense Department in the 1990s as an effort to bring together diverse product development teams?

A. Integrated product team

B. Agile methodology

C. Scrum approach

D. User stories

98. Frank is working to select a new cloud service that will provide object storage for an application being developed by his team. What category of cloud service is Frank planning to use?

A. SaaS

B. IaaS

C. FaaS

D. PaaS

99. Match the numbered code testing methods to their lettered definition:

Code testing methods

1. Regression testing

2. Integration testing

3. Unit testing

4. System testing

Definitions

A. Testing on a complete integrated product

B. A testing method that focuses on modules or smaller sections of code for testing

C. A testing method that is used to verify that previously tested software performs the same way after changes are made

D. A testing method used to validate how software modules work together

100. Match the following numbered terms to their lettered definitions:

1. Session hijacking

2. Cross-site scripting

3. Cross-site request forgery

4. SQL injection

A. An attack that injects a malicious script into otherwise trusted websites

B. An attack that is designed to execute commands against a database via an insecure web application

C. An exploitation method that often involves cookies or keys to gain unauthorized access to a computer or service

D. An attack that forces a user to execute unwanted actions in a website or application they are currently logged into