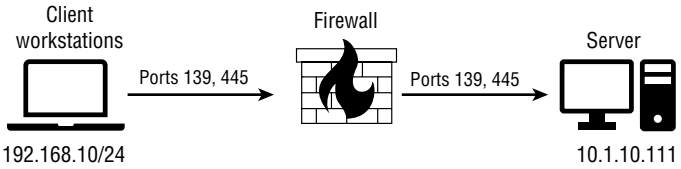
Chapter 2

Architecture and Design

THE COMPTIA SECURITY+ EXAM SY0-601 TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **2.1 Explain the importance of security concepts in an enterprise environment**
- ✓ **2.2 Summarize virtualization and cloud computing concepts**
- ✓ **2.3 Summarize secure application development, deployment, and automation concepts**
- ✓ **2.4 Summarize authentication and authorization design concepts**
- ✓ **2.5 Given a scenario, implement cybersecurity resilience**
- ✓ **2.6 Explain the security implications of embedded and specialized systems**
- ✓ **2.7 Explain the importance of physical security controls**
- ✓ **2.8 Summarize the basics of cryptographic concepts**

1. Ben is reviewing configuration management documentation for his organization and finds the following diagram in his company's document repository. What key information is missing from the diagram that a security professional would need to build firewall rules based on the diagram?



   A. The subnet mask
   B. The service name
   C. The protocol the traffic uses
   D. The API key

2. You are responsible for network security at an e-commerce company. You want to ensure that you are using best practices for the e-commerce website your company hosts. What standard would be the best for you to review?
   A. OWASP
   B. NERC
   C. Trusted Foundry
   D. ISA/IEC

3. Cheryl is responsible for cybersecurity at a mid-sized insurance company. She has decided to use a different vendor for network antimalware than she uses for host antimalware. Is this a recommended action, and why or why not?
   A. This is not recommended; you should use a single vendor for a particular security control.
   B. This is recommended; this is described as vendor diversity.
   C. This is not recommended; this is described as vendor forking.
   D. It is neutral. This does not improve or detract from security.

4. Scott wants to back up the contents of a network-attached storage (NAS) device used in a critical department in his company. He is concerned about how long it would take to restore the device if a significant failure happened, and he is less concerned about the ability to recover in the event of a natural disaster. Given these requirements, what type of backup should he use for the NAS?
   A. A tape-based backup with daily full backups
   B. A second NAS device with a full copy of the primary NAS
   C. A tape-based backup with nightly incremental backups
   D. A cloud-based backup service that uses high durability near-line storage

5. Yasmine is responding to a full datacenter outage, and after referencing the documentation for the systems in the datacenter she brings the network back up, then focuses on the storage area network (SAN), followed by the database servers. Why does her organization list systems for her to bring back online in a particular series?
   - **A.** The power supply for the building cannot handle all the devices starting at once.
   - **B.** The organization wants to ensure that a second outage does not occur due to failed systems.
   - **C.** The organization wants to ensure that systems are secure and have the resources they need by following a restoration order.
   - **D.** The fire suppression system may activate due to the sudden change in heat, causing significant damage to the systems.

6. Enrique is concerned about backup data being infected by malware. The company backs up key servers to digital storage on a backup server. Which of the following would be most effective in preventing the backup data being infected by malware?
   - **A.** Place the backup server on a separate VLAN.
   - **B.** Air-gap the backup server.
   - **C.** Place the backup server on a different network segment.
   - **D.** Use a honeynet.

7. What type of attribute is a Windows picture password?
   - **A.** Somewhere you are
   - **B.** Something you exhibit
   - **C.** Something you can do
   - **D.** Someone you know

8. Which of the following is not a critical characteristic of a hash function?
   - **A.** It converts variable-length input into a fixed-length output.
   - **B.** Multiple inputs should not hash to the same output.
   - **C.** It must be reversible.
   - **D.** It should be fast to compute.

9. Naomi wants to hire a third-party secure data destruction company. What process is most frequently used to ensure that third parties properly perform data destruction?
   - **A.** Manual on-site inspection by federal inspectors
   - **B.** Contractual requirements and a csertification process
   - **C.** Requiring pictures of every destroyed document or device
   - **D.** All of the above

10. Olivia wants to ensure that the code executed as part of her application is secure from tampering and that the application itself cannot be tampered with. Which of the following solutions should she use and why?

A. Server-side execution and validation, because it prevents data and application tampering

B. Client-side validation and server-side execution to ensure client data access

C. Server-side validation and client-side execution to prevent data tampering

D. Client-side execution and validation, because it prevents data and application tampering

11. Trevor wants to use an inexpensive device to build a custom embedded system that can monitor a process. Which of the following options is best suited for this if he wants to minimize expense and maximize simplicity while avoiding the potential for system or device compromise?

A. A Raspberry Pi

B. A custom FPGA

C. A repurposed desktop PC

D. An Arduino

12. Amanda wants to use a digital signature on an email she is sending to Maria. Which key should she use to sign the email?

A. Maria's public key

B. Amanda's public key

C. Maria's private key

D. Amanda's private key

13. Nick wants to make an encryption key harder to crack, and he increases the key length by one bit from a 128-bit encryption key to a 129-bit encryption key as an example to explain the concept. How much more work would an attacker have to do to crack the key using brute force if no other attacks or techniques could be applied?

A. One more

B. 129 more

C. Twice as much

D. Four times as much

14. Gurvinder knows that the OpenSSL passwd file protects passwords by using 1,000 rounds of MD5 hashing to help protect password information. What is this technique called?

A. Spinning the hash

B. Key rotation

C. Key stretching

D. Hash iteration

15. Fred wants to make it harder for an attacker to use rainbow tables to attack the hashed password values he stores. What should he add to every password before it is hashed to make it impossible for the attacker to simply use a list of common hashed passwords to reveal the passwords Fred has stored if they gain access to them?

A. A salt

B. A cipher

C. A spice

D. A trapdoor

16. Ian wants to send an encrypted message to Michelle using public key cryptography. What key does he need to encrypt the message?

A. His public key

B. His private key

C. Her public key

D. Her private key

17. What key advantage does an elliptical curve cryptosystem have over an RSA-based cryptosystem?

A. It can use a smaller key length for the same resistance to being broken.

B. It requires only a single key to encrypt and decrypt.

C. It can run on older processors.

D. It can be used for digital signatures as well as encryption.

18. What cryptographic capability ensures that even if the server's private key is compromised, the session keys will not be compromised?

A. Perfect forward secrecy

B. Symmetric encryption

C. Quantum key rotation

D. Diffie-Hellman key modulation

19. Alaina is reviewing practices for her reception desk and wants to ensure that the reception desk's visitor log is accurate. What process should she add to the guard's check-in procedure?

A. Check the visitor's ID against their log book entry.

B. Perform a biometric scan to validate visitor identities.

C. Require two-person integrity control.

D. Replace the guard with a security robot.

20. In an attempt to observe hacker techniques, a security administrator configures a nonproduction network to be used as a target so that he can covertly monitor network attacks. What is this type of network called?

A. Active detection

B. False subnet

C. IDS

D. Honeynet

21. What type of system is used to control and monitor power plant power generation systems?

A. IPG

B. SEED

C. SCADA

D. ICD

22. What major technical component of modern cryptographic systems is likely to be susceptible to quantum attacks?

A. Key generation

B. Elliptical plot algorithms

C. Cubic root curve cryptography

D. Prime factorization algorithms

23. Geoff wants to establish a contract with a company to have datacenter space that is equipped and ready to go so that he can bring his data to the location in the event of a disaster. What type of disaster recovery site is he looking for?

A. A hot site

B. A cold site

C. A warm site

D. An RTO site

24. Olivia needs to ensure an IoT device does not have its operating system modified by third parties after it is sold. What solution should she implement to ensure that this does not occur?

A. Set a default password.

B. Require signed and encrypted firmware.

C. Check the MD5sum for new firmware versions.

D. Patch regularly.

25. What statement is expected to be true for a post-quantum cryptography world?

A. Encryption speed will be measured in qubits.

B. Nonquantum cryptosystems will no longer be secure.

C. Quantum encryption will no longer be relevant.

D. Key lengths longer than 4,096 bits using RSA will be required.

26. What function does counter mode perform in a cryptographic system?

A. It reverses the encryption process.

B. It turns a block cipher into a stream cipher.

C. It turns a stream cipher into a block cipher.

D. It allows public keys to unlock private keys.

27. Which of the following items is not included in a blockchain's public ledger?

A. A record of all genuine transactions between network participants

B. A record of cryptocurrency balances (or other data) stored in the blockchain

C. The identity of the blockchain participants

D. A token that identifies the authority under which the transaction was made

28. Suzan is responsible for application development in her company. She wants to have all web applications tested before they are deployed live. She wants to use a test system that is identical to the live server. What is this called?

A. A production server

B. A development server

C. A test server

D. A predeployment server

29. Alexandra is preparing to run automated security tests against the code that developers in her organization have completed. Which environment is she most likely to run them in if the next step is to deploy the code to production?

A. Development

B. Test

C. Staging

D. Production

30. Chris wants to limit who can use an API that his company provides and be able to log usage of the API uniquely to each organization that they provide access to. What solution is most often used to do this?

A. Firewalls with rules for each company's public IP address

B. User credentials for each company

C. API keys

D. API passwords

31. Derek has been assigned to assess the security of smart meters. Which of the following is not a common concern for an embedded system like a smart meter?

A. Eavesdropping

B. Denial of service

C. Remote disconnection

D. SQL injection

32. Selah wants to analyze real-world attack patterns against systems similar to what she already has deployed in her organization. She would like to see local commands on a compromised system and have access to any tools or other materials the attackers would normally deploy. What type of technology could she use to do this?

A. A honeypot

B. An IPS

C. An IDS

D. A WAF

33. Charles sets up a network with intentional vulnerabilities and then instruments it so that he can watch attackers and capture details of their attacks and techniques. What has Charles set up?

A. A black hole

B. A honeyhole

C. A spynet

D. A honeynet

34. Maria is a security engineer with a manufacturing company. During a recent investigation, she discovered that an engineer's compromised workstation was being used to connect to SCADA systems while the engineer was not logged in. The engineer is responsible for administering the SCADA systems and cannot be blocked from connecting to them. What should Maria do to mitigate this threat?

A. Install host-based antivirus software on the engineer's system.

B. Implement account usage auditing on the SCADA system.

C. Implement an NIPS on the SCADA system.

D. Use FDE on the engineer's system.

35. AES and DES are an example of what type of cipher?

A. Stream ciphers that encrypt groups of plain-text symbols all together

B. Block ciphers that encrypt groups of plain-text symbols all together

C. Stream ciphers that encrypt one plain-text symbol at a time

D. Block ciphers that encrypt one plain-text symbol at a time

36. Gerard is responsible for secure communications with his company's e-commerce server. All communications with the server use TLS. What is the most secure option for Gerard to store the private key on the e-commerce server?

A. HSM

B. FDE

C. SED

D. SDN

37. What purpose does a transit gateway serve in cloud services?

A. It connects systems inside of a cloud datacenter.

B. It connects virtual private clouds and on-premises networks.

C. It provides an API gateway between trust zones.

D. It allows multicloud infrastructure designs.

38. Web developers in your company currently have direct access to the production server and can deploy code directly to it. This can lead to unsecure code, or simply code flaws being deployed to the live system. What would be the best change you could make to mitigate this risk?

A. Implement sandboxing.

B. Implement virtualized servers.

C. Implement a staging server.

D. Implement deployment policies.

39. Ian is concerned about VoIP phones used in his organization due to the use of SMS as part of their multifactor authentication rollout. What type attack should he be concerned about?

A. A vishing attack

B. A voicemail hijack

C. An SMS token redirect

D. A weak multifactor code injection

40. Angela wants to ensure that IoT devices in her organization have a secure configuration when they are deployed and that they are ready for further configuration for their specific purposes. What term is used to describe these standard configurations used as part of her configuration management program?

A. A baseline configuration

B. An essential settings list

C. A preinstall checklist

D. A setup guide

41. Why is heating, ventilation, and air-conditioning (HVAC) part of organizational security planning?

A. Attackers often use HVAC systems as part of social engineering exercises.

B. HVAC systems are important for availability.

C. HVAC systems are a primary line of network defense.

D. None of the above

42. What advantage does symmetric encryption have over asymmetric encryption?

A. It is more secure.

B. It is faster.

C. It can use longer keys.

D. It simplifies key distributions.

43. Laura knows that predictability is a problem in pseudo-random number generators (PRNGs) used for encryption operations. What term describes the measure of uncertainty used to a PRNG?

A. Ellipses

B. Quantum flux

C. Entropy

D. Primeness

44. Which cloud service model gives the consumer the ability to use applications provided by the cloud provider over the Internet?

A. SaaS

B. PaaS

C. IaaS

D. Hybrid

45. Chris sets a resource policy in his cloud environment. What type of control does this allow him to exert?

A. It allows him to determine how much disk space can be used.

B. It allows him to determine how much bandwidth can be used.

C. It allows him to specify who has access to resources and what actions they can perform on it.

D. It allows him to specify what actions a resource can take on specific users.

46. Chris sets up SAN replication for his organization. What has he done?

A. He has enabled RAID 1 to ensure that the SAN cannot lose data if a drive fails because the drives are replicated.

B. He has set up backups to a tape library for the SAN to ensure data resilience.

C. He has built a second identical set of hardware for his SAN.

D. He has replicated the data on one SAN to another at the block or hardware level.

47. Mike is a security analyst and has just removed malware from a virtual server. What feature of virtualization would he use to return the virtual server to a last known good state?

A. Sandboxing

B. Hypervisor

C. Snapshot

D. Elasticity

48. Lisa is concerned about fault tolerance for her database server. She wants to ensure that if any single drive fails, it can be recovered. What RAID level would support this goal while using distributed parity bits?

A. RAID 0

B. RAID 1

C. RAID 3

D. RAID 5

49. Jarod is concerned about EMI affecting a key escrow server. Which method would be most effective in mitigating this risk?

A. VLAN

B. SDN

C. Trusted platform module

D. Faraday cage

50. John is responsible for physical security at his company. He is particularly concerned about an attacker driving a vehicle into the building. Which of the following would provide the best protection against this threat?

A. A gate

B. Bollards

C. A security guard on duty

D. Security cameras

51. Mark is responsible for cybersecurity at a small college. There are many computer labs that are open for students to use. These labs are monitored only by a student worker, who may or may not be very attentive. Mark is concerned about the theft of computers. Which of the following would be the best way for him to mitigate this threat?

A. Cable locks

B. FDE on the lab computers

C. Strong passwords on the lab computers

D. Having a lab sign-in sheet

52. Joanne is responsible for security at a power plant. The facility is very sensitive and security is extremely important. She wants to incorporate two-factor authentication with physical security. What would be the best way to accomplish this?

A. Smartcards

B. A mantrap with a smartcard at one door and a PIN keypad at the other door

C. A mantrap with video surveillance

D. A fence with a smartcard gate access

53. Which of the following terms refers to the process of establishing a standard for security?

A. Baselining

B. Security evaluation

C. Hardening

D. Normalization

54. Angela configures a honeypot to ongoing events like user logins and logouts, disk usage, program and script loads, and similar information. What is this type of deception called?

A. Fake telemetry

B. User emulation

C. Honeyfakes

D. Deepfakes

55. Which level of RAID is a "stripe of mirrors"?

A. RAID 1+0

B. RAID 6

C. RAID 0

D. RAID 1

56. Isabella is responsible for database management and security. She is attempting to remove redundancy in the database. What is this process called?

A. Integrity checking

B. Deprovisioning

C. Baselining

D. Normalization

57. Gary wants to implement an AAA service. Which of the following services should he implement?

A. OpenID

B. LDAP

C. RADIUS

D. SAML

58. Where does TLS/SSL inspection happen, and how does it occur?

A. On the client, using a proxy

B. On the server, using a protocol analyzer

C. At the certificate authority, by validating a request for a TLS certificate

D. Between the client and server by intercepting encrypted communications

59. Diana wants to prevent drones from flying over her organization's property. What can she do?

A. Deploy automated drone take-down systems that will shoot the drones down.

B. Deploy radio frequency jamming systems to disrupt the drone's control frequencies.

C. Contact the FAA to get her company's property listed as a no-fly zone.

D. None of the above

60. Isaac has configured an infrastructure-as-code-based cloud environment that relies on code-defined system builds to spin up new systems as the services they run need to scale horizontally. An attacker discovers a vulnerability and exploits a system in the cluster, but it is shut down and terminated before they can perform a forensic analysis. What term describes this type of environment?

A. Forensic-resistant

B. Nonpersistent

C. Live-boot

D. Terminate and stay resident

61. You are responsible for database security at your company. You are concerned that programmers might pass badly written SQL commands to the database, or that an attacker might exploit badly written SQL in applications. What is the best way to mitigate this threat?

A. Formal code inspection

B. Programming policies

C. Agile programming

D. Stored procedures

62. Joanna's company has adopted multiple software-as-a-service (SaaS) tools and now wants to better coordinate them so that the data that they each contain can be used in multiple services. What type of solution should she recommend if she wants to minimize the complexity of long-term maintenance for her organization?

A. Replace the SaaS service with a platform-as-a-service (PaaS) environment to move everything to a single platform.

B. Build API-based integrations using in-house expertise.

C. Adopt an integration platform to leverage scalability.

D. Build flat-file integrations using in-house expertise.

63. Farès is responsible for managing the many virtual machines on his company's networks. Over the past two years, the company has increased the number of virtual machines significantly. Farès is no longer able to effectively manage the large number of machines. What is the term for this situation?

A. VM overload

B. VM sprawl

C. VM spread

D. VM zombies

64. Mary is responsible for virtualization management in her company. She is concerned about VM escape. Which of the following methods would be the most effective in mitigating this risk?

A. Only share resources between the VM and host if absolutely necessary.

B. Keep the VM patched.

C. Use a firewall on the VM.

D. Use host-based antimalware on the VM.

65. Irene wants to use a cloud service for her organization that does not require her to do any coding or system administration, and she wants to do minimal configuration to perform the tasks that her organization needs to accomplish. What type of cloud service is she most likely looking for?

A. SaaS

B. PaaS

C. IaaS

D. IDaaS

66. Which of the following is not an advantage of a serverless architecture?

A. It does not require a system administrator.

B. It can scale as function call frequency increases.

C. It can scale as function call frequency decreases.

D. It is ideal for complex applications.

67. You are responsible for server room security for your company. You are concerned about physical theft of the computers. Which of the following would be best able to detect theft or attempted theft?

A. Motion sensor–activated cameras

B. Smartcard access to the server rooms

C. Strong deadbolt locks for the server rooms

D. Logging everyone who enters the server room

68. Alexandra wants to prevent systems that are infected with malware from connecting to a botnet controller that she knows the hostnames for. What type of solution can she implement to prevent the systems from reaching the controller?

A. An IDS

B. A round-robin DNS

C. A DNS sinkhole

D. A WAF

69. Hector is using infrared cameras to verify that servers in his datacenter are being properly racked. Which of the following datacenter elements is he concerned about?

A. EMI blocking

B. Humidity control

C. Hot and cold aisles

D. UPS failover

70. Gerald is concerned about unauthorized people entering the company's building. Which of the following would be most effective in preventing this?

A. Alarm systems

B. Fencing

C. Cameras

D. Security guards

71. Which of the following is the most important benefit from implementing SDN?

A. It will stop malware.

B. It provides scalability.

C. It will detect intrusions.

D. It will prevent session hijacking.

72. Mark is an administrator for a health care company. He has to support an older, legacy application. He is concerned that this legacy application might have vulnerabilities that would affect the rest of the network. What is the most efficient way to mitigate this?

A. Use an application container.

B. Implement SDN.

C. Run the application on a separate VLAN.

D. Insist on an updated version of the application.

73. Charles is performing a security review of an internally developed web application. During his review, he notes that the developers who wrote the application have made use of third-party libraries. What risks should he note as part of his review?

A. Code compiled with vulnerable third-party libraries will need to be recompiled with patched libraries.

B. Libraries used via code repositories could become unavailable, breaking the application.

C. Malicious code could be added without the developers knowing it.

D. All of the above

74. Valerie is considering deploying a cloud access security broker. What sort of tool is she looking at?

A. A system that implements mandatory access control on cloud infrastructure

B. A tool that sits between cloud users and applications to monitor activity and enforce policies

C. A tool that sits between cloud application providers and customers to enforce web application security policies

D. A system that implements discretionary access control on cloud infrastructure

75. Derek has been asked to implement his organization's service-oriented architecture as a set of microservices. What does he need to implement?

A. A set of loosely coupled services with specific purposes

B. A set of services that run on very small systems

C. A set of tightly coupled services with custom-designed protocols to ensure continuous operation

D. A set of services using third-party applications in a connected network enabled with industry standard protocols

76. Abigail is responsible for datacenters in a large, multinational company. She has to support multiple datacenters in diverse geographic regions. What would be the most effective way for her to manage these centers consistently across the enterprise?

A. Hire datacenter managers for each center.

B. Implement enterprise-wide SDN.

C. Implement infrastructure as code (IaC).

D. Automate provisioning and deprovisioning.

77. Elizabeth wants to implement a cloud-based authorization system. Which of the following protocols is she most likely to use for that purpose?

A. OpenID

B. Kerberos

C. SAML

D. OAuth

78. Greg is assessing an organization and finds that they have numerous multifunction printers (MFPs) that are accessible from the public Internet. What is the most critical security issue he should identify?

A. Third parties could print to the printers, using up the supplies.

B. The printers could be used as part of a DDoS attack.

C. The printers may allow attackers to access other parts of the company network.

D. The scanners may be accessed to allow attackers to scan documents that are left in them.

79. Keith has deployed computers to users in his company that load their resources from a central server environment rather than from their own hard drives. What term describes this model?

A. Thick clients

B. Client-as-a-server

C. Cloud desktops

D. Thin clients

80. Henry notices that a malware sample he is analyzing downloads a file from `imgur.com` and then executes an attack using Mimikatz, a powerful Windows password account theft tool. When he analyzes the image, he cannot identify any recognizable code. What technique has most likely been used in this scenario?

A. The image is used as decryption key.

B. The code is hidden in the image using steganography.

C. The code is encoded as text in the image.

D. The image is a control command from a malware command and control network.

81. Molly wants to advise her organization's developers on secure coding techniques to avoid data exposure. Which of the following is not a common technique used to prevent sensitive data exposure?

A. Store data in plain text.

B. Require HTTPs for all authenticated pages.

C. Ensure tokens are not disclosed in public source code.

D. Hash passwords using a salt.

82. Naomi wants to secure a real-time operating system (RTOS). Which of the following techniques is best suited to providing RTOS security?

A. Disable the web browser.

B. Install a host firewall.

C. Use secure firmware.

D. Install antimalware software.

83. John is examining the logs for his company's web applications. He discovers what he believes is a breach. After further investigation, it appears as if the attacker executed code from one of the libraries the application uses, code that is no longer even used by the application. What best describes this attack?

A. Buffer overflow

B. Code reuse attack

C. DoS attack

D. Session hijacking

84. Chris is designing an embedded system that needs to provide low-power, peer-to-peer communications. Which of the following technologies is best suited to this purpose?

A. Baseband radio

B. Narrowband radio

C. Zigbee

D. Cellular

85. What term is used to describe encryption that can permit computations to be conducted on ciphertext, with the results matching what would have occurred if the same computations were performed on the original plain text?

A. Identity-preserving encryption

B. Homomorphic encryption

C. Replicable encryption

D. None of the above

86. Tony wants to implement a biometric system for entry access in his organization. Which of the following systems is likely to be most accepted by members of his organization's staff?

A. Fingerprint

B. Retina

C. Iris

D. Voice

87. Nathan wants to implement off-site cold backups. What backup technology is most commonly used for this type of need?

A. SAN

B. Disk

C. Tape

D. NAS

88. Allan is considering implementing off-site storage. When he does, his datacenter manager offers four solutions. Which of these solutions will best ensure resilience and why?

A. Back up to a second datacenter in another building nearby, allowing reduced latency for backups.

B. Back up to an off-site location at least 90 miles away to ensure that a natural disaster does not destroy both copies.

C. Back up to a second datacenter in another building nearby to ensure that the data will be accessible if the power fails to the primary building.

D. Back up to an off-site location at least 10 miles away to balance latency and resilience due to natural disaster.

89. Ben has been asked to explain the security implications for an embedded system that his organization is considering building and selling. Which of the following is not a typical concern for embedded systems?

A. Limited processor power

B. An inability to patch

C. Lack of authentication capabilities

D. Lack of bulk storage

90. You are concerned about the security of new devices your company has implemented. Some of these devices use SoC technology. What would be the best security measure you could take for these?

A. Using a TPM

B. Ensuring each has its own cryptographic key

C. Using SED

D. Using BIOS protection

91. Vincent works for a company that manufactures portable medical devices, such as insulin pumps. He is concerned about ensuring these devices are secure. Which of the following is the most important step for him to take?

A. Ensure all communications with the device are encrypted.

B. Ensure the devices have FDE.

C. Ensure the devices have individual antimalware.

D. Ensure the devices have been fuzz-tested.

92. Emile is concerned about securing the computer systems in vehicles. Which of the following vehicle types has significant cybersecurity vulnerabilities?

A. UAV

B. Automobiles

C. Airplanes

D. All of the above

93. What additional security control can Amanda implement if she uses compiled software that she cannot use if she only has software binaries?

A. She can review the source code.

B. She can test the application in a live environment.

C. She can check the checksums provided by the vendor.

D. None of the above

94. Greta wants to understand how a protocol works, including what values should be included in packets that use that protocol. Where is this data definitively defined and documented?

A. An RFC

B. Wikipedia

C. The Internet Archive

D. None of the above

95. Using standard naming conventions provides a number of advantages. Which of the following is not an advantage of using a naming convention?

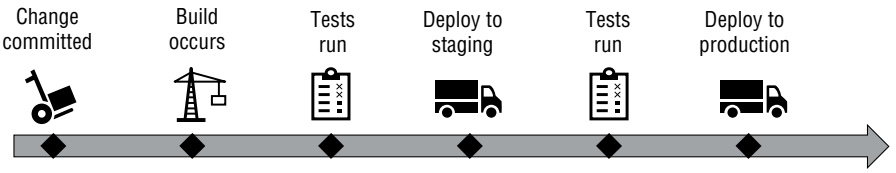
A. It can help administrators determine the function of a system.

B. It can help administrators identify misconfigured or rogue systems.

C. It can help conceal systems from attackers.

D. It can make scripting easier.

96. What process is shown in the following figure?



A. A continuous monitoring environment

B. A CI/CD pipeline

C. A static code analysis system

D. A malware analysis process

97. Keith wants to identify a subject from camera footage from a train station. What biometric technology is best suited to this type of identification?

A. Vein analysis

B. Voiceprint analysis

C. Fingerprint analysis

D. Gait analysis

98. Your company is interested in keeping data in the cloud. Management feels that public clouds are not secure but is concerned about the cost of a private cloud. What is the solution you would recommend?

A. Tell them there are no risks with public clouds.

B. Tell them they will have to find a way to budget for a private cloud.

C. Suggest that they consider a community cloud.

D. Recommend against a cloud solution at this time.

99. Your development team primarily uses Windows, but they need to develop a specific solution that will run on Linux. What is the best solution to get your programmers access to Linux systems for development and testing if you want to use a cloud solution where you could run the final systems in production as well?

A. Set their machines to dual-boot Windows and Linux.

B. Use PaaS.

C. Set up a few Linux machines for them to work with as needed.

D. Use IaaS.

100. Corrine has been asked to automate security responses, including blocking IP addresses from which attacks are detected using a series of scripts. What critical danger should she consider while building the scripts for her organization?

A. The scripts could cause an outage.

B. The scripts may not respond promptly to private IP addresses.

C. Attackers could use the scripts to attack the organization.

D. Auditors may not allow the scripts.

101. Madhuri has configured a backup that will back up all of the changes to a system since the last time that a full backup occurred. What type of backup has she set up?

A. A snapshot

B. A full backup

C. An incremental backup

D. A differential

102. You are the CIO for a small company. The company wants to use cloud storage for some of its data, but cost is a major concern. Which of the following cloud deployment models would be best?

A. Community cloud

B. Private cloud

C. Public cloud

D. Hybrid cloud

103. What is the point where false acceptance rate and false rejection rate cross over in a biometric system?

A. CRE

B. FRE

C. CER

D. FRR

104. Devin is building a cloud system and wants to ensure that it can adapt to changes in its workload by provisioning or deprovisioning resources automatically. His goal is to ensure that the environment is not overprovisioned or underprovisioned and that he is efficiently spending money on his infrastructure. What concept describes this?

A. Vertical scalability

B. Elasticity

C. Horizontal scalability

D. Normalization

105. Nathaniel wants to improve the fault tolerance of a server in his datacenter. If he wants to ensure that a power outage does not cause the server to lose power, what is the first control he should deploy from the following list?

A. A UPS

B. A generator

C. Dual power supplies

D. Managed power units (PDUs)

106. Which of the following is the best description for VM sprawl?

A. When VMs on your network outnumber physical machines

B. When there are more VMs than IT can effectively manage

C. When a VM on a computer begins to consume too many resources

D. When VMs are spread across a wide area network

107. Which of the following is the best description of a stored procedure?

A. Code that is in a DLL, rather than the executable

B. Server-side code that is called from a client

C. SQL statements compiled on the database server as a single procedure that can be called

D. Procedures that are kept on a separate server from the calling application, such as in middleware

108. Farès is responsible for security at his company. He has had bollards installed around the front of the building. What is Farès trying to accomplish?

A. Gated access for people entering the building

B. Video monitoring around the building

C. Protecting against EMI

D. Preventing a vehicle from being driven into the building

109. The large company that Selah works at uses badges with a magnetic stripe for entry access. Which threat model should Selah be concerned about with badges like these?

A. Cloning of badges

B. Tailgating

C. Use by unauthorized individuals

D. All of the above

110. You are concerned about VM escape attacks causing a significant data breach. Which of the following would provide the most protection against this?

A. Separate VM hosts by data type or sensitivity.

B. Install a host-based antivirus on both the VM and the host.

C. Implement FDE on both the VM and the host.

D. Use a TPM on the host.

111. Teresa is the network administrator for a small company. The company is interested in a robust and modern network defense strategy but lacks the staff to support it. What would be the best solution for Teresa to use?

A. Implement SDN.

B. Use automated security.

C. Use an MSSP.

D. Implement only the few security controls they have the skills to implement.

112. Dennis is trying to set up a system to analyze the integrity of applications on his network. He wants to make sure that the applications have not been tampered with or Trojaned. What would be most useful in accomplishing this goal?

A. Implement NIPS.

B. Use cryptographic hashes.

C. Sandbox the applications in question.

D. Implement NIDS.

113. George is a network administrator at a power plant. He notices that several turbines had unusual ramp-ups in cycles last week. After investigating, he finds that an executable was uploaded to the system control console and caused this. Which of the following would be most effective in preventing this from affecting the SCADA system in the future?

A. Implement SDN.

B. Improve patch management.

C. Place the SCADA system on a separate VLAN.

D. Implement encrypted data transmissions.

114. Gordon knows that regression testing is important but wants to prevent old versions of code from being re-inserted into new releases. What process should he use to prevent this?

A. Continuous integration

B. Version numbering

C. Continuous deployment

D. Release management

115. Mia is a network administrator for a bank. She is responsible for secure communications with her company's customer website. Which of the following would be the best for her to implement?

A. SSL

B. PPTP

C. IPSec

D. TLS

116. Which of the following is not a common challenge with smartcard-based authentication s ystems?

A. Weak security due to the limitations of the smartcard's encryption support

B. Added expense due to card readers, distribution, and software installation

C. Weaker user experience due to the requirement to insert the card for every authentication

D. Lack of security due to possession of the card being the only factor used

117. Susan's secure building is equipped with alarms that go off if specific doors are opened. As part of a penetration test, Susan wants to determine if the alarms are effective. What technique is used by penetration testers to make alarms less effective?

A. Setting off the alarms as part of a preannounced test

B. Disabling the alarms and then opening doors to see if staff report the opened doors

C. Asking staff members to open the doors to see if they will set the alarm off

D. Setting off the alarms repeatedly so that staff become used to hearing them go off

118. What term is used to describe the general concept of "anything as a service"?

A. AaaS

B. ATaaS

C. XaaS

D. ZaaS

119. What role does signage play in building security?

A. It is a preventive control warning unauthorized individuals away from secured areas.

B. It can help with safety by warning about dangerous areas, materials, or equipment.

C. It can provide directions for evacuation and general navigation.

D. All of the above

120. Nora has rented a building with access to bandwidth and power in case her organization ever experiences a disaster. What type of site has she established?

A. A hot site

B. A cold site

C. A warm site

D. A MOU site

121. Matt is patching a Windows system and wants to have the ability to revert to a last known good configuration. What should he set?

A. A system restore point

B. A reversion marker

C. A nonpersistent patch point

D. A live boot marker

122. Which multifactor authentication can suffer from problems if the system or device's time is not correct?

A. TOTP

B. SMS

C. HOTP

D. MMAC

123. The company that Nina works for has suffered from recent thefts of packages from a low-security delivery area. What type of camera capability can they use to ensure that a recently delivered package is properly monitored?

A. Infrared image capture

B. Motion detection

C. Object detection

D. Facial recognition

124. Which of the following is not a common organizational security concern for wearable devices?

A. GPS location data exposure

B. Data exposure

C. User health data exposure

D. Insecure wireless connectivity

125. Tim is building a Faraday cage around his server room. What is the primary purpose of a Faraday cage?

A. To regulate temperature

B. To regulate current

C. To block intrusions

D. To block EMI

126. You are working for a large company. You are trying to find a solution that will provide controlled physical access to the building and record every employee who enters the building. Which of the following would be the best for you to implement?

A. A security guard with a sign-in sheet

B. Smartcard access using electronic locks

C. A camera by the entrance

D. A sign-in sheet by the front door

127. What concern causes organizations to choose physical locks over electronic locks?

A. They provide greater security.

B. They are resistant to bypass attempts.

C. They are harder to pick.

D. They do not require power.

128. Kara has been asked to include IP schema management as part of her configuration management efforts. Which of the following is a security advantage of IP schema configuration management?

A. Detecting rogue devices

B. Using IP addresses to secure encryption keys

C. Preventing denial-of-service attacks

D. Avoiding IP address exhaustion

129. Carole is concerned about security for her server room. She wants the most secure lock she can find for the server room door. Which of the following would be the best choice for her?

A. Combination lock

B. Key-in-knob

C. Deadbolt

D. Padlock

130. Melissa wants to implement NIC teaming for a server in her datacenter. What two major capabilities will this provide for her?

A. Lower latency and greater throughput

B. Greater throughput and fault tolerance

C. Higher latency and fault tolerance

D. Fault tolerance and lower latency

131. Molly is implementing biometrics in her company. Which of the following should be her biggest concern?

A. FAR

B. FRR

C. CER

D. EER

132. Mike is concerned about data sovereignty for data that his organization captures and maintains. What best describes his concern?

A. Who owns the data that is captured on systems hosted in a cloud provider's infrastructure?

B. Can Mike's organization make decisions about data that is part of its service, or does it belong to users?

C. Is the data located in a country subject to the laws of the country where it is stored?

D. Does data have rights on its own, or does the owner of the data determine what rights may apply to it?

133. What are the key limiting factors for cryptography on low-power devices?

A. There are system limitations on memory, CPU, and storage.

B. The devices cannot support public key encryption due to an inability to factor prime numbers.

C. There is a lack of chipset support for encryption.

D. Legal limitations for low-power devices prevent encryption from being supported.

134. Fred is responsible for physical security in his company. He wants to find a good way to protect the USB thumb drives that have BitLocker keys stored on them. Which of the following would be the best solution for this situation?

A. Store the drives in a secure cabinet or safe.

B. Encrypt the thumb drives.

C. Don't store BitLocker keys on these drives.

D. Lock the thumb drives in desk drawers.

135. Juanita is responsible for servers in her company. She is looking for a fault-tolerant solution that can handle two drives failing. Which of the following should she select?

A. RAID 3

B. RAID 0

C. RAID 5

D. RAID 6

136. Maria's organization uses a CCTV monitoring system in their main office building, which is occupied and in use 24-7. The system uses cameras connected to displays to provide real-time monitoring. What additional feature is the most likely to receive requests to ensure that her organization can effectively use the CCTV system to respond to theft and other issues?

A. Motion activation

B. Infrared cameras

C. DVR

D. Facial recognition

137. What is the primary threat model against static codes used for multifactor authentication?

A. Brute force

B. Collisions

C. Theft

D. Clock mismatch

138. Dennis needs a cryptographic algorithm that provides low latency. What type of cryptosystem is most likely to meet this performance requirement?

A. Hashing

B. Symmetric encryption

C. Asymmetric encryption

D. Electronic one-time pad

139. The company that Devin works for has selected a nondescript building and does not use exterior signage to advertise that the facility belongs to them. What physical security term describes this type of security control?

A. Industrial camouflage

B. Demilitarized zone

C. Industrial obfuscation

D. Disruptive coloration

140. Ed knows that TLS sessions start using asymmetric encryption, and then move to use symmetric keys. What limitation of asymmetric cryptography drives this design decision?

A. Speed and computational overhead

B. Key length limitations

C. Lifespan (time) to brute force it

D. Key reuse for asymmetric algorithms

141. When you are concerned about application security, what is the most important issue in memory management?

A. Never allocate a variable any larger than is needed.

B. Always check bounds on arrays.

C. Always declare a variable where you need it (i.e., at function or file level if possible).

D. Make sure you release any memory you allocate.

142. Bart wants to ensure that the files he encrypts remain secure for as long as possible. What should Bart do to maximize the longevity of his encrypted file's security?

A. Use a quantum cipher.

B. Use the longest key possible.

C. Use an anti-quantum cipher.

D. Use a rotating symmetric key.

143. Nadine's organization stores and uses sensitive information, including Social Security numbers. After a recent compromise, she has been asked to implement technology that can help prevent this sensitive data from leaving the company's systems and networks. What type of technology should Nadine implement?

A. Stateful firewalls

B. OEM

C. DLP

D. SIEM

144. What form is the data used for quantum key distribution sent in?

A. Bytes

B. Bits

C. Qubits

D. Nuquants

145. Alicia needs to ensure that a process cannot be subverted by a single employee. What security control can she implement to prevent this?

A. Biometric authentication

B. Two-person control

C. Robotic sentries

D. A DMZ

146. Social login, the ability to use an existing identity from a site like Google, Facebook, or a Microsoft account, is an example of which of the following concepts?

A. Federation

B. AAA

C. Privilege creep

D. Identity and access management

147. Michelle is traveling and wants to plug her phone into the charger in her hotel room. What security precaution can she use to ensure that her phone is not attacked by a malicious device built into the charger in her room?

A. A USB data blocker

B. A parallel USB cable

C. A data circuit breaker

D. An HOTP interrogator

148. Which cloud service model provides the consumer with the infrastructure to create applications and host them?

A. SaaS

B. PaaS

C. IaaS

D. IDaaS

149. Why is avoiding initialization vector and key reuse recommended to ensure secure encryption?

A. It makes it impossible to brute force.

B. It means a single successful attack will not expose multiple messages.

C. It means a single successful attack will not expose any messages.

D. It makes brute force easier.

150. Dan knows that his Linux system generates entropy that is used for multiple functions, including encryption. Which of the following is a source of entropy for the Linux kernel?

A. Time of day

B. User login events

C. Keystrokes and mouse movement

D. Network packet timing

151. Mike knows that computational overheads are a concern for cryptographic systems. What can he do to help limit the computational needs of his solution?

A. Use hashes instead.

B. Use short keys.

C. Use elliptic curve encryption.

D. Use the RSA algorithm.

152. What is the primary role of lighting in a physical security environment?

A. It acts as a detective control.

B. It acts as a reactive control.

C. It acts as a deterrent control.

D. It acts as a compensating control.

153. Dennis has deployed servers and storage to each of the facilities his organization runs to ensure that scientific equipment can send and receive data at the speed that it needs to function. What computational design concept describes this?

A. Hybrid cloud

B. Mist computing

C. Edge computing

D. Local cloud

154. Ben replaces sensitive data in his database with unique identifiers. The identifiers allow him to continue to take actions on the data without exposing the data itself. What type of solution has he deployed?

A. Masking

B. Encryption

C. Hashing

D. Tokenization

155. Dana wants to discourage potential malicious actors from accessing her facility. Which of the following is both a deterrent and a physical control?

A. A visitor log

B. A motion detector

C. A security camera

D. Fences

156. What additional capabilities does adding a digital signature to an encrypted message provide?

A. Integrity and nonrepudiation

B. Confidentiality and integrity

C. Availability and nonrepudiation

D. Confidentiality and availability

157. Megan has been asked to set up a periodic attestation process for accounts in her organization. What has she been asked to do?

A. Validate that the users are still employed.

B. Validate that the user's rights and permissions are still correct.

C. Require users to provide proof of identity.

D. Validate security controls as part of a test.

158. Elaine wants to adopt appropriate response and recovery controls for natural disasters. What type of control should she use to prepare for a multihour power outage caused by a tornado?

A. A hot site

B. A generator

C. A PDU

D. A UPS

159. What does a message authentication code (MAC) do when used as part of a cryptographic system?

A. It validates the message's integrity and authenticity.

B. It validates the message's confidentiality and authenticity.

C. It protects the message's confidentiality and integrity.

D. None of the above

160. Charles wants to put a fire suppression system in place in an area where highly sensitive electronics are in use. What type of fire suppression system is best suited to this type of environment if Charles is concerned about potential harm to first responders or on-site staff?

A. Pre-charge

B. Dry pipe

C. Inert gas

D. Carbon dioxide

161. What technology is typically used for proximity card readers?

A. Magnetic stripe

B. Biometrics

C. RFID

D. Infrared

162. How does asymmetric encryption support nonrepudiation?

A. Using digital signatures

B. Using longer keys

C. Using reversible hashes

D. Using the recipient's public key

163. Olivia knows that she needs to consider geography as part of her security considerations. Which of the following is a primary driver of geographical considerations for security?

A. MTR

B. Natural disasters

C. Service integration

D. Sprawl avoidance

164. Scott wants to limit the impact of potential threats from UAVs. What physical security control is best suited to this purpose?

A. Adding more fences

B. Moving sensitive areas to the interior of a building

C. Deploying biometric sensors

D. Moving sensitive areas to Faraday cages

165. Derek wants to explain the concept of resource constraints driving security constraints when using encryption. Which of the following descriptions best explains the trade-offs that he should explain to his management?

A. Stronger encryption requires more space on drives, meaning that the harder it is to break, the more storage you'll need, driving up cost.

B. Stronger encryption is faster, which means that using strong encryption will result in lower latency.

C. Stronger encryption requires more entropy. This may reduce the overall security of the system when entropy is exhausted.

D. Stronger encryption requires more computational resources, requiring a balance between speed and security.

166. Amanda wants to ensure that the message she is sending remains confidential. What should she do to ensure this?

A. Hash the messages.

B. Digitally sign the message.

C. Encrypt the message.

D. Use a quantum encryption algorithm.

167. What security advantage do cloud service providers like Amazon, Google, and Microsoft have over local staff and systems for most small to mid-sized organizations?

A. Better understanding of the organization's business practices

B. Faster response times

C. More security staff and budget

D. None of the above

168. Tim wants to ensure that his web servers can scale horizontally during traffic increases, while also allowing them to be patched or upgraded without causing outages. What type of network device should he deploy?

A. A firewall

B. A switch

C. A horizontal scaler

D. A network load balancer

169. Gabby wants to ensure that sensitive data can be transmitted in unencrypted form by using physical safeguards. What type of solution should she implement?

A. Shielded cables

B. Armored cables

C. Distribution lockdown

D. Protected cable distribution

170. Maureen conceals information she wants to transmit surreptitiously by modifying an MP3 file in a way that does not noticeably change how it sounds. What is this technique called?

A. MP3crypt

B. Audio steganography

C. Audio hashing

D. Honey MP3s

171. Nicole is assessing risks to her multifactor authentication system. Which of the following is the most likely threat model against short message service (SMS) push notifications to cell phones for her environment?

A. Attacks on VoIP systems

B. SIM cloning

C. Brute-force attacks

D. Rainbow tables

172. John wants to protect data at rest so that he can process it and use it as needed in its original form. What solution from the following list is best suited to this requirement?

A. Hashing

B. TLS

C. Encryption

D. Tokenization

173. Nathaniel has deployed the control infrastructure for his manufacturing plant without a network connection to his other networks. What term describes this type of configuration?

A. DMZ

B. Air gap

C. Vaulting

D. A hot aisle

174. Naomi hides the original data in a Social Security number field to ensure that it is not exposed to users of her database. What data security technique does this describe?

A. Masking

B. Encryption

C. Hashing

D. Tokenization

175. Isaac wants to use on-premises cloud computing. What term describes this type of cloud computing solution?

A. Infrastructure as a service

B. Hybrid cloud

C. Private cloud

D. Platform as a service

176. What is the primary threat model against physical tokens used for multifactor authentication?

A. Cloning

B. Brute force

C. Theft

D. Algorithm failure

177. Maria is a security administrator for a large bank. She is concerned about malware, particularly spyware that could compromise customer data. Which of the following would be the best approach for her to mitigate the threat of spyware?

A. Computer usage policies, network antimalware, and host antimalware

B. Host antimalware and network antimalware

C. Host and network antimalware, computer usage policies, and website whitelisting

D. Host and network antimalware, computer usage policies, and employee training

178. Charles has configured his multifactor system to require both a PIN and a password. How many effective factors does he have in place once he presents both of these and his username?

A. One

B. Two

C. Three

D. Four

179. Fred adds the value 89EA443CCDA16B89 to every password as a salt. What issue might this cause?

A. The salt is too long.

B. The salt is alphanumeric.

C. The salt is reused.

D. The salt is too short.

180. Alaina needs to physically secure the root encryption keys for a certificate authority. What type of security device should she use to maintain local control and security for them?

A. A USB thumb drive

B. A vault or safe

C. An air-gapped system

D. None of the above

181. Angela wants to help her organization use APIs more securely and needs to select three API security best practices. Which of the following options is not a common API security best practice?

A. Use encryption throughout the API's request/response cycle.

B. Authorize before authenticating.

C. Do not trust input strings and validate parameters.

D. Enable auditing and logging.

182. Frank uses a powerful magnet to wipe tapes before they are removed from his organization's inventory. What type of secure data destruction technique has he used?

A. Tape burning

B. Data shredding

C. Degaussing

D. Pulping

183. Angela has been asked to deploy 5G cellular inside her organization. What concern should she raise with her management about the effort to implement it?

A. 5G requires high levels of antenna density for full coverage.

B. 5G signals should only be used in exterior deployments.

C. 5G is not widely available and cannot be deployed yet.

D. 5G signals cannot coexist with traditional Wi-Fi.

184. Chris is reviewing the rights that staff in his organization have to data stored in a group of departmental file shares. He is concerned that rights management practices have not been followed and that employees who have been with the company he works for have not had their privileges removed after they switched jobs. What type of issue has Chris encountered?

A. Privilege creep

B. IAM inflation

C. Masking issues

D. Privilege escalation

185. Isaac has been asked to set up a honeyfile. What should he configure?

A. A list of tasks to accomplish

B. A list of potentially valuable data

C. A bait file for attackers to access

D. A vulnerable Word file

186. Yasmine wants to ensure that she has met a geographic dispersal requirement for her datacenters. How far away should she place her datacenter based on common best practices for dispersal?

A. 5 miles

B. 45 miles

C. 90 miles

D. 150 miles

187. What term describes extending cloud computing to the edge of an enterprise network?

A. Local cloud

B. Fog computing

C. Managed cloud

D. Blade computing

188. Which of the following algorithms is a key stretching algorithm?

A. bcrypt

B. ncrypt

C. MD5

D. SHA1

189. Jocelyn has been asked to implement a directory service. Which of the following technologies should she deploy?

A. SAML

B. OAuth

C. LDAP

D. 802.1x