Questions

1. Candace suspects the Harvard diploma from the new employee is fake. What is her *BEST* next step to verify their background?

   A. Inspect the paper type of the diploma.

   B. Run a credit check.

   C. Contact the college verification department.

   D. Contact the employee's references.

2. Technical controls are a type of access control for organizations. What are two other access-control types?

   A. Physical

   B. Turnstile

   C. Firewall

   D. Administrative

3. Which of the following is considered the strongest form of authentication?

   A. Fingerprint scan

   B. Retinal scan

   C. Iris scan

   D. Password

4. Annie is a security engineer seeking to improve authentication from using just a password, to a password and a smartphone authenticator that uses a time-based one-time password (TOTP). What type of authentication is she implementing?

   A. Two-factor authentication (2FA)

   B. Something you know

   C. Three-factor authentication (3FA)

   D. MFA

5. Which type of communication connectors provide the *BEST* defense and security to leaky authentication vulnerabilities?

   A. Bayonet-Neill-Concelman (BNC)

   B. Standard connector (SC)

   C. **RJ-45**

   D. **RJ-11**

6. Aika, a security engineer, desires to set up secure authentication systems with the fewest vulnerabilities. Which of the following does she *AVOID*?

   A. Extensible Authentication Protocol (EAP)

   B. Challenge-Handshake Authentication Protocol (CHAP)

   C. Protected Extensible Authentication Protocol (PEAP)

   D. Password Authentication Protocol (PAP)

7. Of the following, which is the strongest password?

   A. **Partner**

   B. **C@t456789**

   C. **@b(D3?**

   D. **antiestablishmentarianism**

8. 4-foot fencing that surrounds an organization's parking lot would be of which control type and in which control category?

   A. Physical type and deterrent category

   B. Physical type and preventative category

   C. Technical type and deterrent category

   D. Administrative type and corrective category

9. Aika, a security analyst with *BARA Corp*, is made aware that electro-magnetic interference (EMI) is extending 100 meters outside of the building. What can she install to minimize EMI leakage?

A. AirHopper

B. Tempest filter

C. Van Eck radiation

D. Van Eck phreaking

10. An authentication system that connects via a dial-up modem and uses the User Datagram Protocol (UDP) protocol on ports **1812** and **1813** is known as what?

    A. Prodigy

    B. Terminal Access Control Access-Control System (TACACS)

    C. Kerberos

    D. Remote Authentication Dial-In User Service (RADIUS)

11. What are two critical issues with signature-based intrusion detection systems (IDSs)? (Choose 2)

    A. They cannot detect all malware.

    B. Encryption makes it difficult to detect malware.

    C. Zero-days.

    D. Signature-based IDSes are very expensive.

12. Corey is a security manager creating a corporate security document that states laptops must maintain the latest patches and use ClamAV malware detection, the LibreOffice suite, and the Thunderbird email client. This document *BEST* fits which category?

    A. Policy

    B. Standard

    C. Guidelines

    D. Procedures

13. Nneka receives an email that her email box is filling up. In the message is a link for her to click so that the issue can be resolved. The link is *MOST LIKELY* to activate which kind of attack?

A. Denial of service (DoS)

B. Pharming

C. Phishing

D. Social engineering

14. Kyrie is a security analyst that belongs to the LinkedIn group *Secure your Business*. He gets to know some of the others in the group and shares information about his corporate network. Within 2 weeks, his organization is hit with ransomware. Which attack did the hacker use?

    A. Spoofing

    B. Honeynet

    C. Watering hole

    D. Honeypot

15. Breanna is a systems administrator who ensures all systems are secured by not only making backup tapes but also testing backup tapes. What would make this process more secure?

    A. Implement separation of duties.

    B. Implement collusion.

    C. Implement job rotation.

    D. Restrict users from using computers while backups are being made.

16. Giannis is a network engineer setting up a firewall to separate the business' intranet from the internet. For initial setup just after power-on, which is the *BEST* default rule of the firewall?

    A. Allow all traffic.

    B. Deny all traffic.

    C. Allow all traffic except any related to sports, gambling, or pornography.

    D. Deny all traffic except any related to news and social networking.

17. A Linux feature known as SELinux enables which type of access control?

A. Discretionary access control (DAC)

B. Access-control list (ACL)

C. Role-based access control (RBAC)

D. MAC

18. Markizai is a barber seeking to visit his daughter at the Central Intelligence Agency (CIA). He's instructed to go through a door that locks behind him, and the door in front is also locked. While locked in the room, he hears over the speaker that metal is detected, and he is being detained. What is the name of this room?

    A. Panic room

    B. Mantrap

    C. Chroot jail

    D. Temporary lockup

19. Colt is an administrative assistant at *90 Days Corp* and needs to print his boss's schedule. Which *BEST* describes the relationship?

    A. Colt is the subject, the printer is the object

    B. Colt and the printer are subjects

    C. Colt and the printer are objects

    D. Colt is the object, the printer is the subject

20. Which system uses a series of distinguished names, common names, and domain components, as shown here?

    dn: cn=Ted Jordan,dc=jordanteam,dc=com

    A. Active Directory (AD)

    B. Lightweight Directory Access Protocol (LDAP)

    C. Domain Name System (DNS)

    D. Dynamic Host Configuration Protocol (DHCP)

21. Hillary, a grandmother, receives a phone call from *FlyWithMe Airlines* stating she has been granted 100,000 award miles. So that the miles can be added, she gladly provides her password to the *FlyWithMe* associate. What type of attack is this?

    A. Social engineering

    B. Pharming

    C. Phishing

    D. Vishing

22. Grant is a new employee of *DifQu Corp* and is provided his identity card to access the building, and login credentials to do his programming job. What is this process called?

    A. Enablement

    B. Bringing a new employee online

    C. Identity management

    D. Provisioning

23. Rina is a Navy Lieutenant and has secret access to all objects, including fighter jets. She requires top-secret access to complete a portion of her work but is not allowed. This is enforcing which policy?

    A. Least privilege

    B. Need to know

    C. SSO

    D. Federation

24. Landon is a security engineer analyzing biometric devices to access the security operations center (SOC). Device A has a crossover error rate (CER) of 3.5. Device B has a CER of 3.1. Which of the following is true for *BEST* security?

    A. He should use device A because the CER is higher.

    B. He should use device B because the CER is lower.

    C. Use both devices to simplify access to the SOC.

    D. Since the CERs are similar, he should use the lower-cost device.

25. Biometric systems, such as fingerprint scanners, do which of the following when enrolling a new user if designed in the *MOST* secure manner?

    A. Save an image of the user's fingerprint.

    B. Convert the user's fingerprint into a hash and encrypt the hash.

    C. Save an image of the user's fingerprint and encrypt the fingerprint.

    D. Convert the user's fingerprint into a hash.

26. Palm-vein scanners are highly accurate authentication systems because they capture millions of points from the palm, and they also do which of the following?

    A. Collect deoxyribonucleic acid (DNA).

    B. Collect a sweat sample.

    C. Detect keystroke dynamics.

    D. Perform a liveness test.

27. Which feature reduces the risk of attackers abusing privileged accounts because higher-level privileges are time-limited?

    A. Rule-based access control (RBAC)

    B. JIT access

    C. MFA

    D. Least privilege

28. A synchronous token device is utilized to aid in dual-factor authentication by providing what type of output?

    A. One-time password (OTP)

    B. Time

    C. Date

    D. User password

29. An authentication device that contains private keys, certificates, and even fingerprints would be which of the following?

A. Token

B. Smart card

C. Automated teller machine (ATM) card

D. Memory dual inline memory module (DIMM)

30. Security devices used to protect packaged goods or clothing from shrinkage or loss prevention are called what?

A. ATM cards

B. Smart cards

C. Memory cards

D. Radio-frequency identification (RFID) tags

31. Sergei is a hacker who enjoys taking train rides for free. He does this by tricking the ticketing system into thinking he has money on his card. Which attack does he use to recharge the card and simulate it has money?

A. Differential power analysis

B. Side-channel attack

C. Electromagnetic analysis

D. Timing analysis

32. Won Kim just gave Sameeha access to a file so that they can work together on a project. Sameeha can view the file but cannot make modifications. What is the problem?

A. Won Kim did not grant Sameeha read authorization.

B. Won Kim did not grant Sameeha write authorization.

C. Won Kim did not grant Sameeha delete authorization.

D. Won Kim did not grant Sameeha copy authorization.

33. Ilhan is a systems administrator finishing setup on a new server. After testing, her users cannot access any files on the system. Why is that?

A. The users are using incorrect passwords.

B. The users do not have login credentials for the system.

C. The system is set up as default-to-no-access until access policies are defined.

D. She is limiting access to monitor authorization creep and need-to-know.

34. SSO systems have which characteristics?

A. Provide a single username and password to access each system.

B. Provide a single username with various passwords to access resources.

C. Provide multiple usernames and passwords to access resources.

D. Provide a single username and password to access the entire network.

35. Which two of the following are *NOT* virtual private network (VPN) protocols?

A. TACACS+

B. Layer Two Tunneling Protocol (L2TP)

C. TACACS

D. Point-to-Point Tunneling Protocol (PPTP)

36. After a user completes authentication with their secret key, the user is allowed access to a service with which of the following?

A. Service Provisioning Markup Language (SPML)

B. A session key

C. Security Assertion Markup Language (SAML)

D. A secret key

37. A user's digital identity is composed of three parts. These are which of the following?

A. Passwords, personal identification number (PIN), mother's maiden name

B. Cards, tokens, office key

C. Fingerprint, iris, palm vein

D. Attributes, entitlements, and traits

38. Kenhap is a traveling sales rep who often uses hotel computers to email expense reports. He receives an urgent phone call from tech support that *only* his account has been compromised and he is forced to create a new password. What *MOST LIKELY* occurred?

    A. He fell victim to a phishing attack.

    B. A keylogger compromised his credentials.

    C. He was the victim of a social engineering attack.

    D. His password was compromised in a mantrap.

39. Extensible Markup Language (XML) is often used for the federation of identities. Which two of the following take advantage of XML features?

    A. TACACS

    B. Simple Object Access Protocol (SOAP)

    C. Information Systems Audit and Control Association (ISACA)

    D. eXtensible Access Control Markup Language (XACML)

40. Marta is seeking to access photos that she's uploaded to the cloud. She's given the option to authenticate with her Google, Facebook, or Yahoo account. This is using features of which protocol?

    A. SAML

    B. OpenID

    C. Open Authentication (OAuth)

    D. Online Certificate Status Protocol (OCSP)

41. A type of RBAC that allows for defining a subset of roles based on a superset role is named which of the following?

    A. Superuser

    B. Subset-based

    C. Superset-based

    D. Hierarchical

42. Anna is a network security engineer, and her manager recognizes an overwhelming amount of phishing attacks coming from a remote country. Which access-control model is *BEST* used to deny these attacks?

    A. MAC

    B. Role-based access control (RBAC)

    C. Attribute-based access control (ABAC)

    D. Rule-based access control

43. Blake is a security engineer taking the Linux+ exam. The screen opens with a Bash shell interface in which he is allowed to *only* use the **ls**, **pwd**, **cd**, **touch**, **rm**, **chmod**, and **sudo** commands. Which type of user interface (UI) is this?

    A. Viewing

    B. Constrained

    C. Read-only

    D. Menu

44. Lionel is told by his manager to open a specific email only if he doesn't receive a package that afternoon and to otherwise delete the email without reading it. This is an example of which type of access control?

    A. Context-dependent

    B. Rule-based

    C. Package-based

    D. Content-dependent

45. Which of the following would *NOT* be considered an SSO system?

    A. Kerberos

    B. Diameter

    C. RADIUS

    D. Circumference

46. An audit finds that Danielle's access card is used to enter a building at 4:55 P.M. 10 minutes later. she's accessing a building 50 miles (100 kilometers) from the first location. What *MOST LIKELY* occurred?

    A. She successfully accessed both buildings at different times.

    B. Her manager's card is often misread as hers because they are in the same department.

    C. The time is improperly set on one of the buildings.

    D. Her card was cloned.

47. Pascal retired from *SMR Corp* 6 months ago. He realizes there are personal photos on the corporate computer that he would like to download. To his surprise, he is able to log in and download his photos. What could have *BEST* prevented this access?

    A. Disabling remote logon capability

    B. Proper deprovisioning

    C. Automatically disabling the account if the wrong password is used three times

    D. Enforcing password changes every 30 days

48. Which of the following is *NOT* true of TACACS+ over RADIUS?

    A. Communicates using the UDP protocol.

    B. Separates authentication, authorization, and accounting procedures.

    C. Encrypts username, password, and accounting messages.

    D. MFA is available.

49. Which of the following is an example of technical control?

    A. Computer usage policy

    B. Proxy firewall

    C. Bollard

    D. Internet use policy

50. *MLP Corp* is under a widespread phishing attack stating that users' email boxes are full and they must click a link to fix the problem. Which is the *BEST* solution?

A. Program a packet filtering firewall.

B. Install software-based firewalls on each personal computer.

C. Install and program a circuit-level gateway within the corporate local area network (LAN).

D. Security-awareness training and phish auditing.

51. What does geo-velocity mean when it comes to SSO?

A. A user's password is so simple, they can authenticate within microseconds.

B. A user is authenticating from locations far from where they last logged in.

C. A SSO system allows users to authenticate from more locations than the average system.

D. A user's current location can be determined from where they authenticate.

52. Luis, a systems engineer, gets called in daily to reboot the accounting server because it crashes every afternoon. Which solution does he put in place to resolve this issue?

A. Luis replaces the motherboard, network cards, and memory cards.

B. Luis implements log rotations, automated backups, and the removal of old log files.

C. Luis doubles the hard-drive size.

D. Luis makes no change because rebooting the server daily is the normal operating procedure.

53. One way to mitigate hackers attempting to cover their tracks by clearing logs is to do which of the following?

A. Immediately write logs to Redundant Array of Inexpensive Disks (RAID) 0 or RAID 10 systems.

B. Immediately write logs to RAID 1 or RAID 5 systems.

C. Immediately write logs to write once, read many (WORM) media.

D. Save changes by doing incremental backups.

54. Eden is a security engineer seeking methods to mitigate data loss and prevent password compromise by keyloggers. Which is her *BEST* solution?

A. Have users sign a data loss-prevention document.

B. Automatically prevent passwords that are too short and dictionary words.

C. Disable Universal Serial Bus (USB) ports.

D. Install trojan horses on user systems known to use poor passwords.

55. Istvan is a new security manager and is pretty certain that a backup tape missing yesterday was there today. What can he *BEST* do to mitigate his discomfort?

A. Put backup tapes in a locked cabinet that only he has control over.

B. Check recent surveillance of the area.

C. Ensure that backups are encrypted.

D. Hold a meeting with his immediate staff and ask who is removing backup tapes.

56. Sniffers are utilities that can listen to network traffic and can collect data, usernames, and passwords. What are two examples of sniffing tools?

A. John the Ripper

B. Wireshark

C. Tcpdump

D. Snort

57. Amandine contacts her corporate help desk because an app she installed on her computer is not functioning normally. The manager of tech support steps in and states they cannot help her with the app. What is the *MOST LIKELY* reason?

A. The application is too difficult a problem for the help desk to resolve.

B. Amandine has not installed the latest patch for the app.

C. Amandine is using a Linux computer instead of a Windows one.

D. She is using some form of shadow Information Technology (IT).

58. Jacqueline, a systems administrator, has just completed installing the Kerberos system into the corporate network. Which is her *BEST* next step?

A. Create user accounts and create passwords.

B. Test the system.

C. Notify users the system is ready for use.

D. Employ an MFA system.

59. Mobile device management (MDM) helps system administrators manage the security features of smartphones. Which three of the following are features that are managed using MDM?

A. Remote wipe

B. Encryption

C. Patch updates

D. Contact list updates

60. Neymar is a network engineer and suspects a new switch appearing on the network is fraudulent. What is one step he can take to test whether it is legitimate?

A. Use the **ping** command to validate the switch.

B. Use the inventory management system to validate the certificate.

C. Log in to the switch using the default login name and password.

D. Run a hardware inventory to verify the model number is consistent with company policy.

61. Which of the following would be considered an administrative control?

A. Encryption

B. Perimeter security

C. Data backups

D. Non-disclosure agreement (NDA)

62. Jasmin is an administrative assistant for *LHW Corp* and has access to all client data except for social security numbers and information regarding medical conditions. This is an example of what type of access control?

A. People-based

B. Rule-based

C. Context-dependent

D. Content-dependent

63. Mursel is a network engineer who is programming a wireless access point to allow only **05:06:11:aa:a1:88** and **22:11:de:dd:af:fe:23** Media Access Control (MAC) addresses. Which access control model *BEST* describes this?

A. DAC

B. RBAC

C. ABAC

D. MAC

64. Emily is scanning and saving her tax records to her thumb drive using the convenient multifunctional device at her hotel. Months later, she discovers her identity has been stolen. What *MOST LIKELY* occurred?

A. A hacker attacked the multifunction device.

B. A hacker launched a man-in-the-middle (MITM) attack on the network.

C. A hacker planted a phishing attack on the multifunction device.

D. A hacker recovered her documents using a dumpster dive attack.

65. A public key infrastructure (PKI) offers which type of trust to users?

A. Peer-to-peer

B. Transitive

C. Coaching

D. Trust metrics

66. Sasha is an engineer with *EBL Energy*, a regulated industry. He learns at an industry seminar that outsourcing their identity management (IDM) could save them time and money. What is his next *BEST* step?

A. Find the identity-as-a-service (IDaaS) vendor that presented at the seminar and schedule installation.

B. Contact three IDaaS vendors, select the one with the best value, and schedule installation.

C. Work with his manager to construct a statement of work (SOW) and a request for proposal (RFP) to various IDaaS vendors.

D. Determine if IDaaS fits with EBL Energy's security policy.

67. Leida is using a customer relationship management (CRM) application that requests access to her Google address book. Which protocol is this *MOST LIKELY* using?

A. Registry Authority (RA)

B. OAuth

C. Key Distribution Center (KDC)

D. Ticket Granting Ticket (TGT)

68. Which are two protocols that use XML for the federation of identities?

A. SPML

B. RADIUS

C. Kerberos

D. SAML

69. Devante is part of an intern rotation program where he works in four departments in 12 months. Which risk should be *MOST* considered by the security team?

A. Non-compete agreement

B. Need to know

C. NDA

D. Authorization creep

70. Jamaun is a network engineer who installs a new firewall for the organization. Unfortunately, it does not work because all traffic is blocked. What should he do?

A. Return the firewall for a full refund and use a different manufacturer and model.

B. Reboot the firewall.

C. Reboot the gateway system.

D. Write ACL rules because firewalls are set up as deny by default.

71. Lisa attempts to withdraw $500 from her bank using her ATM card, but she is denied access to her money, even after verifying that there is enough money in her account. What is the *MOST LIKELY* reason that she cannot withdraw her money?

A. She is using a foreign ATM that does not accept her card.

B. She has a transaction-type restriction that allows her to withdraw no more than $300.

C. She used the wrong PIN to access her account.

D. She needs to clean the magnetic strip on her ATM card and try again.

72. Reesie and Carl have the same role that allows them to add hard drives and printers, but not networks or filesystems. Reesie has full access to files that belong to the security team, but Carl only has read access to those files in the DAC system. Why doesn't Carl have full access to the security team's files?

A. There is a bug in the access-control system and it requires a patch update.

B. Even though he and Reesie share a security role, he is not part of the security group.

C. Carl could access the files if he were in the right location.

D. Reesie has secret access, but Carl only has confidential rights.

73. Russell frequently logs in as root to access Secure Shell (SSH) servers across the internet. The security team hears about this and asks him to log in remotely as a regular user and then use **sudo** if he needs elevated privileges. Why does the security team recommend this?

A. Complexity makes it harder for hackers to break into systems.

B. To reduce the risk of Russell's privileges being compromised.

C. To reduce the risk of the root password being compromised.

D. The security team is usually bullied; making such claims helps them keep their power.

74. An example of a device that blocks cars from entering, but allows people through, is known as which kind of device?

A. Fence

B. Mantrap

C. Bollard

D. Turnstile

75. Eric is a security specialist who needs some administrative rights to add printers and modify networks. Which the *BEST* security control for him in this case?

A. Role-based access control (RBAC)

B. Rule-based access control

C. MAC

D. ABAC

76. Which utility assures that an application is interacting with a human?

A. GOTCHA

B. CAPTCHA

C. SaveYa

D. Blockchain

77. Kalani, a security administrator, suspects that many users are using poor passwords after overhearing a conversation that the best passwords to use are favorite dogs or flowers. What is her next *BEST* step?

A. Immediately launch a password audit.

B. Change her password.

C. Inform each department head to conduct password audits.

D. Ask management for approval to conduct a password audit.

78. Linux systems have a feature that allows a user to elevate their privilege temporarily, *without* knowing the root password. Which command performs this function?

A. **su**

B. **sudo**

C. **sudoers**

D. **administrator**

79. Asuelu is a systems administrator training a summer intern to assist with creating new user accounts. He needs the intern to provision 10 new accounts, so he provides the intern temporary rights with which type of account?

    A. Ephemeral account

    B. Superuser account

    C. Standard account

    D. Root account

80. Which of the following biometric authentication devices is the *MOST* intrusive to users, having the ability to collect protected health information (PHI)?

    A. Palm-vein scan

    B. Retina scan

    C. Iris scan

    D. Facial scan

81. Mimi has just received a call from the help desk that her password needs to be updated. A few days later, she notices her account has been compromised. Which kind of attack *MOST LIKELY* occurred?

    A. A hacker impersonated tech support.

    B. Tech support asked Mimi for her password.

    C. The password request was done by phone instead of using a self-service password reset.

    D. Social engineering attack.

82. Yung enjoys using social media and answering all the fun questions about himself. His credit union account was recently hacked and money was stolen from his account. What *MOST LIKELY* occurred?

    A. His credentials and other private data were stolen during a credit union hack.

B. Hackers launched a DOS attack on the credit union to obtain his login credentials.

C. Hackers obtained his credentials by launching a Structured Query Language (SQL) injection attack on his computer.

D. Hackers used information from social media to discover his credentials and his mother's maiden name.

83. Renee is notified that she has just made a purchase of $120 from Walmart that she does not recognize. Her email reports several messages of bad login attempts to other online stores. What is *MOST LIKELY* occurring?

A. A hacker broke into her computer and stole all her online store credentials.

B. Her Walmart credentials were discovered on **pastebin**, and hackers are attempting to use these elsewhere.

C. Walmart sent her the message in error.

D. There is no issue because she simply forgot about the purchase.

84. Which two of the following statements are true?

A. A false negative is the same as a Type I error.

B. A false positive is the same as a Type II error.

C. A false negative is the same as a Type II error.

D. A false positive is the same as a Type I error.

85. Larissa is a security auditor who has borrowed someone's ID card. She uses the card to access the office building because the guard allows her to after viewing the card. This access would be described as what?

A. True positive

B. False positive

C. True negative

D. False negative

86. Which are two examples of biometric controls for authentication?

A. Keystroke dynamics

B. Birthday

C. Height

D. Thumbprint

87. Which of the following is the *BEST* process for a user to access a resource?

A. Identification > Authorization

B. Identification > Authentication > Authorization > Accounting

C. Identification > Authorization > Authentication > Accounting

D. Identification > Authentication > Accounting > Authorization

88. Which two of the following are administrative control types?

A. Acceptable use policy (AUP)

B. ACL

C. Exchange Online Protection (EOP)

D. SSO

89. TACACS+ uses which communication protocol to support authentication, authorization, and accounting?

A. UDP

B. TCP

C. Internet Control Message Protocol (ICMP)

D. Assessment & Protection (A&P)

90. Toffin is a virtual reality (VR) artist at *Fakeia Corp*. His manager suspects he is giving away software licenses every Monday to a secret contact that sells them online, and they split the money. On Monday morning, Toffin is told to leave and not return for a week. This is known as _____?

A. Voluntary vacation

B. Expulsion

C. Suspension

D. Mandatory vacation

91. Maya is a security engineer assigned the task of installing a Debian-based online shopping cart that is improperly set up and unpatched for research purposes. What type of computer is she installing?

    A. Web server

    B. Honeypot

    C. Shopping cart

    D. Linux server

92. Which two of the following transmits username and password information in plain text across the network?

    A. Secure Copy Protocol (SCP)

    B. Telnet

    C. SSH

    D. File Transfer Protocol (FTP)

93. Leosel is an inexperienced hacker who performs this type of attack and gets caught by the authorities. Which attack did she run?

    A. Offline rainbow attack

    B. MITM attack

    C. Online brute-force attack

    D. Passive sniffing attack

94. Which access-control system uses a series of layers to distinguish rights—for example, top-secret versus secret—and only allows users with the proper authorization to access those documents?

    A. RBAC

    B. ACL

C. MAC

D. DAC

95. Uhura, a security engineer, has installed a biometric system to authenticate users. The device has a relatively high false accept rate (FAR). Which result can she expect?

A. Too many unauthorized users will be granted access.

B. Unauthorized users will be blocked.

C. The FAR will be equal to the CER.

D. The false reject rate (FRR) will be relatively high.

96. Scotty has just joined DAP Products as a new employee and his accounts must be set up through identity proofing and enrollment. What is the correct order for providing his credentials?

A. Resolution, verification, validation, authentication

B. Resolution, validation, verification, authentication

C. Validation, verification, authentication, resolution

D. Verification, validation, authentication, resolution

97. Which of the following lists five of the seven control types?

A. Deterrent, monitoring, access, recovery, authentication

B. Authentication, corrective, detective, logging, monitoring

C. Deterrent, corrective, logging, compensating, authorization

D. Deterrent, detective, corrective, compensating, recovery

98. Which SSO system uses a concept called *tickets* to manage authentication?

A. RADIUS

B. Kerberos

C. SAML

D. TACACS

99. Greer is a security engineer seeking authentication solutions. Which of the following would be the *MOST IMPORTANT* for her to consider?

A. Impact and the likelihood of an attack

B. Threats and vulnerabilities

C. Single Loss Expectancy (SLE) and Annual Loss Expectancy (ALE)

D. Which biometric system to consider

100. Which of the following is the *BEST* example of 2FA?

A. Fingerprint scanner

B. Bank ATM card

C. The Global Positioning System (GPS)

D. Logging in to your bank with a password, and they also request your birth city

Quick answer key

h

1. C	16. B	31. B	46. D	61. D	76. B	91. B
2. A D	17. D	32. B	47. B	62. D	77. D	92. B D
3. B	18. B	33. C	48. A	63. B	78. B	93. C
4. A	19. A	34. D	49. B	64. A	79. A	94. C
5. B	20. B	35. A C	50. D	65. B	80. B	95. A
6. D	21. D	36. B	51. B	66. D	81. D	96. B
7. B	22. D	37. D	52. B	67. B	82. D	97. D
8. A	23. A	38. B	53. C	68. A D	83. B	98. B
9. B	24. B	39. B D	54. C	69. D	84. A B	99. A
10. D	25. B	40. B	55. A	70. D	85. B	100. B
11. B C	26. D	41. D	56. B C	71. B	86. A D	
12. B	27. B	42. D	57. D	72. B	87. B	
13. C	28. A	43. B	58. B	73. C	88. A C	
14. C	29. B	44. A	59. A B C	74. C	89. B	
15. A	30. D	45. D	60. B	75. A	90. D	

Answers with explanations

1. **Answer: C** Candace's best next step is to contact Harvard's verification department. Information required is the student's name and—often—their tax ID number. References may be friends from college, but they could also be catfish accounts. Most employers never physically touch a new employee's diploma but get the information from their resume. Most credit checks do not contain college graduation information.
2. **Answer: A and D** Administrative controls (which some call operational) include policies, contracts, agreements, and so on. A firewall is an example of technical control (also known as logical control), and this includes devices such as switches, SSO, and so on. Physical controls limit people or vehicles, such as fences, gates, turnstiles, and so on.
3. **Answer: B** A retinal scanner is a biometric type of control that is very accurate—so accurate that it can detect if people carry some disease or ailment, such as cancer or **Acquired Immunodeficiency Syndrome** (**AIDS**), so because of privacy concerns, it is not often used. Iris scanners just look at iris details, not blood vessels, so they are not as accurate as retinal scanners.
4. **Answer: A** This is an example of something you know (password) and something you have (TOTP). This is tough because MFA is a correct answer, but when given the option, choose the more specific answer.

5. **Answer: B Standard connector** (**SC**) for fiber optic cable, which does not give off EMI, making it much less vulnerable to MITM attacks. BNC connectors are designed for coaxial cables, which emit EMI. RJ-45 is used for Ethernet and twisted-pair cables, and RJ-11 is for telephone modem cables, which also emits EMI.
6. **Answer: D** PAP does not encrypt username and password information. The others do. PEAP and EAP can also accept certificates.
7. **Answer: B** Hackers first test for simple passwords that come from the dictionary, so A and D are out. Then, they start with shorter-length passwords, using brute-force methods by trying all possible characters; in other words, after dictionary words, length is more important than complexity. (See https://www.grc.com/haystack.htm for more information.)
8. **Answer: A** Physical types control whether people or vehicles are allowed or denied access. For example, turnstiles and K-rated fencing are physical controls. Categories include deterrents, detective, and so on. Deterrents discourage criminal activity. Detective categories, such as alarm systems, detect activity.
9. **Answer: B** An EMI contains meaningful data that a hacker can decipher. AirHopper is an attack that collects emissions from mobile phones. Van Eck phreaking, also known as Van Eck radiation, is a form of eavesdropping that tempest filters mitigate.
10. **Answer: D** Prodigy is a distractor. Kerberos and TACACS are SSO systems, but neither uses dial-up access; they use the TCP protocol for better reliability and do not use ports **1812** and **1813**.
11. **Answer: B and C** Signature-based IDSes rely on matching malware *signatures* to label it as an attack or not. When signatures are encrypted, no match can be detected. Since zero-days are known exploits without solutions, they are undetectable by IDSes.
12. **Answer: B** Policies are higher-level, visionary documents with few details of how the policy is achieved. Procedures discuss how updates are accomplished and how software is installed. Guidelines are non-mandatory recommendations.
13. **Answer: C** Emails that appear to be from system administrators are cleverly spoofed to hide the identity of the hacker. These are technically social engineering attacks, but in the CISSP exam, if there is a more specific option, select that answer. Pharming is an attack on the DNS—when putting a **Uniform Resource Locator** (**URL**) into a browser, the user is redirected to the hacker's domain.
14. **Answer: C** Honeypots and honeynets are tools to attract hackers to conduct malware studies. Spoofing is pretending to be someone or something else. Watering-hole attacks build trust through public newsgroups.
15. **Answer: A** For best security, another worker should test the backups to mitigate the possibility of internal threats. Job rotations would help because this mitigates collusion, but only after implementing separation of duties. Snapshots allow users to work while backups are being made.
16. **Answer: B** After all traffic is blocked (by default), then program the trusted traffic into the firewall. To allow or deny traffic initiated by your users, use a proxy server to allow or deny specific types of traffic.
17. **Answer: D** MAC enforces access depending on the object level (for example, top-secret, secret, confidential, and so on).
18. **Answer: B** A mantrap locks a person in a room if they appear to be an offender. A panic room is a safe room where people can hide while their primary area is under attack. A

chroot jail limits where users can maneuver in a filesystem after logging in to a computer. Temporary lockup is an area in local jails to detain suspects.

19. **Answer: A** Subjects are the users actively accessing some device, file, or another user. The resource is the object.
20. **Answer: B** LDAP is similar to Microsoft's AD but runs on all hardware. In this example, Ted Jordan is one of the namespaces for LDAP.
21. **Answer: D** A couple of close possibilities, but social engineering is too general, so choose the more specific answer for the real exam.
22. **Answer: D** Identity management is a system in place to maintain the identities of staff but bringing the employee online, and modifications as staff change jobs are known as provisioning.
23. **Answer: A** Need to know is similar to least privilege but contains the user's rights based on their role. SSO grants a user access to the network with a single username and password. Federation grants a user additional services; for example, a user logs in to their bank, and then the user's credentials are *federated* to the check-printing company, and not entered again.
24. **Answer: B** CER is where the false-acceptance rate meets the false-rejection rate. Since the question asks for the *best security*, option **B** is your only possibility.
25. **Answer: B** This is the best option because if a hacker is able to attack the saved credentials, they have to first decrypt them, and then determine which pattern made the hash.
26. **Answer: D** Palm-vein scanners mitigate spoofing by examining blood flow.
27. **Answer: B** Privileged accounts are those that have some or all administrator rights. For JIT accounts, users only use the privilege when needed, and usually for some limited period.
28. **Answer: A** A synchronous token generates an OTP that expires and regenerates every 30 seconds (for most devices). The user password is a *something-you-know* type authentication that combines with the *something-you-have* token to complete dual-factor authentication.
29. **Answer: B** A token provides an OTP and does not contain private keys, certificates, or fingerprints. An ATM card contains a PIN. Memory DIMMs are not authentication devices but are the computer's **random-access memory** (**RAM**).
30. **Answer: D** Shrinkage is a term used in the retail industry that defines loss, usually due to shoplifting. RFID tags attached to items assist with inventory management and sound an alarm if someone is taking it without paying.
31. **Answer: B** Differential, side-channel, and timing analysis are all side-channel type attacks that can be used against smart cards.
32. **Answer: B** Write authorizations allow Sameeha to modify the contents of the file. The other options have nothing to do with changing file contents.
33. **Answer: C** On the real exam, look for answers related to policy because it is very important to follow management decisions in the real world.
34. **Answer: D** A SSO system allows a user to access network resources with one login name and password, easing usability.
35. **Answer: A and C** L2TP is a recommended VPN protocol because it uses **IP Security** (**IPsec**) for encryption. TACACS and TACACS+ are SSO systems.

36. **Answer: B** When the user authenticates with the **KDC**, a secret key connects to the **ticket-granting service** (**TGS**). Access to a service, such as printing or email, is secured with a session key. SPML and SGML are markup languages used to federate identities across different vendors.
37. **Answer: D** Attributes include job titles, clearance levels, and so on. Entitlements include rights to files or services, and so on. Traits include biometric information.
38. **Answer: B** A phishing attack is carried out by the user clicking on a malformed link in an email (this was not mentioned in the question). Keyloggers are common in hotel computers because of all of the vast **personally identifiable information** (**PII**) to be collected. Social engineering attacks are non-technical by definition. Mantraps lock a person in a room if they appear to be a threat.
39. **Answer: B and D** TACACS is for corporate environments and is not designed for identity federation. ISACA is an organization that competes with the developer of the CISSP exam called **International Information System Security Certification Consortium** (**ISC2**) and offers cybersecurity certifications.
40. **Answer: B** SAML uses XML to help federate identities between business organizations. OAuth authorizes applications to obtain data from other vendors. OCSP is used as a more efficient **certificate revocation list** (**CRL**).
41. **Answer: D** The superuser has all privileges, similar to an administrator account.
42. **Answer: D** Application firewall rules permit and deny emails based on data within messages and use rule-based access control to watch for specific keywords, patterns, and heuristics.
43. **Answer: B** Constrained interfaces limit which user's command can run and where they can maneuver through the filesystem.
44. **Answer: A** There is no such system as a package-based system. The access control does not depend on the content of a package or email, but on whether a package is received. **Rule-based access control** (**RBAC**) is found in firewalls and switches.
45. **Answer: D** SSO allows a user access and authorizations for all of the resources on the network with a single username and password. SSO systems include RADIUS, Diameter, Kerberos, TACACS, TACACS+, and more.
46. **Answer: D** If there were faulty equipment or a faulty card, the system would be giving off dozens of alerts daily for everyone. Since this is a singular issue, it is most likely her card was cloned.
47. **Answer: B** Proper deprovisioning would back up and remove the account altogether. The other options keep the account opened.
48. **Answer: A** All of the others are true of TACACS+ over RADIUS. TACACS+ communicates via the more stable TCP protocol, and RADIUS uses UDP. Neither of them is compatible with TACACS.
49. **Answer: B** Policies (for example, a computer usage policy and an internet usage policy) are administrative controls, and bollards (which are devices that block vehicles from entering, but not people) are physical controls.
50. **Answer: D** Technical solutions can help to minimize spam and phishing attacks, but staff training to recognize and not click links is the most effective way for the few messages that get through.
51. **Answer: B** Option D is an example of geo-location, and is the ability to determine the location of a device when the user authenticates. Geo-velocity validates authentication

also based on *when* the user logged in, and asks, for example, *can the user log in from Canada, and then two minutes later log in from Nigeria?*. A user cannot travel 5000 miles in two minutes, so the second authentication would be denied. The others options are distractors.

52. **Answer: B** This is an example of another issue that occurs in the real world when log files start growing, eventually filling the hard drive and causing the server to crash. Increasing hard-drive size only delays the issue.
53. **Answer: C** Writing logs to WORM systems makes the data undeletable or immutable. RAID systems and backups still allow data to be altered on the hard drive.
54. **Answer: C** USB downloaders and USB keyloggers are common hacker tools, and even installing *audit-based* trojans will not help a password from getting stolen with a USB keylogger.
55. **Answer: A** If there is an insider threat, they will not reveal themselves at a meeting, and they have access to encryption keys. Surveillance can often be unclear.
56. **Answer: B and C** John the Ripper is a password-cracking tool, and Snort is an IDS.
57. **Answer: D** Shadow IT is when staff use unsupported software or conduct unsupported activities. Companies provide a whitelist of allowed applications they support; otherwise, the user is on their own.
58. **Answer: B** Before notifying users and provisioning accounts, make sure the system works.
59. **Answer: A, B, and C** Users maintain their contact lists, but MDM features can handle doing remote backups of a user's contacts.
60. **Answer: B** One way to authenticate devices within the network is with certificates. The other methods verify there is a switch but do not validate that the switch is authorized.
61. **Answer: D** Encryption is a technical control. Perimeter security and backups are physical controls.
62. **Answer: D** People-based does not exist. Context-dependent depends more on the situation, such as the hour or location. Rule-based is used as part of ACLs.
63. **Answer: B Rule-based access control** (**RBAC**) is used commonly in switches and routers permitting and denying access based on MAC addresses, IP addresses, geographic location, and more.
64. **Answer: A** Emily did not make hard copies, so dumpster diving is out. Phishing cannot be done on a multifunction device. MITM would possibly work if she were emailing the documents. Many multifunction devices save copies of records on an internal hard drive.
65. **Answer: B** A PKI uses a **relying party** (**RP**) that has collected privacy details from an individual or vendor, and because of this, users trust the website they're visiting. Peer-to-peer is available with **pretty good privacy** (**PGP**) where each party trusts the others implicitly.
66. **Answer: D** Always follow the policy. There may be security and regulatory issues that make it impossible to outsource **IDM** through an IDaaS organization. If management gives the okay, then an SOW and an RFP can be generated.
67. **Answer: B** A **registry authority** (**RA**) is part of a PKI for registering owners of internet domains. The **KDC** issues session keys or tickets as part of Kerberos, using a **TGT**.
68. **Answer: A and D** SAML and SPML both use XML for **federated identity management** (**FIM**).

69. **Answer: D** Authorization creep could happen as Devante moves from department to department, and administrators neglect to remove rights and privileges from previous departments.
70. **Answer: D** ACL rules will allow Jamaun to select which traffic to allow into the corporate network.
71. **Answer: B** The question states that she is at her bank, so it is not a foreign ATM, and if she had forgotten her PIN, she would not be able to see her balance.
72. **Answer: B** Secret and confidential access only make sense on) MAC systems. The question states that they are using DAC. The location may make sense if the system were an ABAC system.
73. **Answer: C** When Russell follows the security team's standard, the root login and password are never used on the Linux or Unix systems, making it impossible for hackers to decrypt the information through an MITM attack.
74. **Answer: C** Fencing, mantraps, and turnstiles all deny people access, but vehicles can storm through those devices.
75. **Answer: A Role-based access control** (**RBAC**) allows administrative rights to specific functions and allows junior administrators to perform functions without knowing the administrator or root password.
76. **Answer: B** CAPTCHA is either skewed characters that a user has to type, a puzzle to be solved, or item recognition to assure that a human is interacting with the application or website and that it is not a robot or synthetic transaction.
77. **Answer: D** Before launching a password audit, make sure to obtain management approval; otherwise, it could be that the auditor is a hacker. Training staff would also be an important component.
78. **Answer: B** The **su** command allows the temporary elevation of privileges but requires knowing the root password. The **sudoers** file is a database of users allowed to use **sudo**, and which elevated commands they can run.
79. **Answer: A** An ephemeral account is a JIT access feature that sets up a one-time-use account that performs some administrator function, and then the account is deleted. Superuser and root accounts are the same and would allow the intern to have all privileges with no time limit. A standard account cannot add new users.
80. **Answer: B** Retinal scanners can detect medical conditions such as cancer or AIDS, and therefore can be considered a **Health Insurance Portability and Accountability Act** (**HIPAA**) violation.
81. **Answer: D** When taking the CISSP exam, this is as close as you will get to a "choose all of the above" question. Here, options A, B, and C represent social engineering. Also, the question asks for the *type of attack*.
82. **Answer: D** Options B and C are out because SQL injection attacks would be done on the credit union server, not the user's system, and DOS attacks make systems unavailable. Option A is a possibility, but for a question such as this, use what is given; so, when taking the CISSP exam, focus on the question, and here they mention social media, which leads to D.
83. **Answer: B** If the hacker had stolen all of her credentials, there would be no bad login attempts at other online stores because they would have the correct passwords. It is more likely that Walmart was hacked, and user credentials were discovered there.

84. **Answer: A and B** A Type I error is also known as a false rejection, and Type II is also known as a false acceptance.
85. **Answer: B** For authentication systems, a true positive means *good (person) allowed*, therefore positive means *allow*, and negative means *disallow*. Since she used a false ID card to gain entry, this triggers a false-positive response. When an employee uses their access card but are denied access, this triggers a false-negative response. A true-negative response is when a threat is denied entry. Learn more on this here: https://youtu.be/lTNWAiFROrA?t=12.
86. **Answer: A and D** Height is too inexact for biometric controls. There would be too many false acceptance errors because many people are the same height. There is no biometric device that knows the exact date someone was born; birthdays are something-you-know authentication, not something-you-are authentication.
87. **Answer: B** The process is also known as **Identification and Authorization, Authorization, and Accountability** (**IAAA**). The user identifies themselves with their username. Authentication can be done with a password, which confirms the user. Authorization is the rights or privileges the user has been granted by the administrator. Accounting is a record of their activity.
88. **Answer: A and C** An AUP is a document detailing what users can do on the corporate network; an EOP is a policy stating the organization will be fair to all employees regardless of race, sex, color, religion, and so on; an ACL is a *technical-type* authentication system that contains rules to allow or deny access to devices such as firewalls, switches, and so on; SSO is a *technical-type* authentication system allowing users to access multiple services with the same user ID and password.
89. **Answer: B** TACACS (pronounced *Tak-as*) uses port **49** to handle authentication requests to the TACACS authentication server. A&P was a popular grocery store chain in the 1970s.
90. **Answer: D** Expulsion and suspension occur as punishment for a misdeed. In this case, Toffin is only suspected. Voluntary vacation occurs when Toffin requests time off, not when he is being told to take time off. With mandatory vacations, the organization can investigate activities while the internal threat is gone.
91. **Answer: B** There are distractors in the questions and answers. When taking the real exam, focus on the most *secure* answer or the answer that speaks the most to security, so even though all of the responses are true, she is setting up a honeypot to distract hackers.
92. **Answer: B and D** Telnet and FTP were created before encryption was popular. For remote logons today, use SSH instead of Telnet, and SCP or SFTP instead of FTP.
93. **Answer: C** Online attacks send multiple alerts to IDSs. Brute-force attacks, attempting every possible password, collect all the information needed to locate the offender. All of the other attacks help hackers hide from their targets because they are offline. Rainbow tables contain password hashes with matching plain-text passwords.
94. **Answer: C Role-based access control** (**RBAC**) provides access to objects based on a user's job title or position. If they are a junior administrator, for example, they are allowed to mount hard drives and set up printers but have no rights to reboot computers. ACLs are a feature of **rule-based access control** (**RBAC**), where a defined rule grants whether users are allowed access, for example. MAC separates objects into different layers, and DAC allows users to set whatever rights they want on files they own.

95. **Answer: A** A FAR defines the percentage of unauthorized users granted access. An FRR defines the percentage of authorized users denied access. Where these values cross, this is known as the CER. The lower the CER, the better the biometric device.
96. **Answer: B** Scotty resolves and proves his identity by providing his government credentials, such as a driver's license. The **human resources** (**HR**) department ensures the credentials are valid, and can further validate Scotty by doing background checks. He can now receive his credentials and authenticate into computers or enter the building with his new badge.
97. **Answer: D** The seven control types include compensating, corrective, directive, deterrent, detective, preventative, recovery. Logging would be a detective type of control, and contracts and policies are considered directive controls. Fake cameras are considered deterrents that discourage threats.
98. **Answer: B** Kerberos tickets grant access to services and allow users to authenticate without passwords crossing the network, mitigating MITM attacks.
99. **Answer: A** Risk management starts with *risk assessment*, where event impact and likelihood occur. The next step is *risk response*, to determine whether to mitigate or avoid the risks. *Contingency planning* is next, as a backup plan if something goes wrong. Finally, *tracking and reporting* ensure the risk management plan stays current. Learn more about the risk management process here: http://www.phe.gov/about/amcg/contracts/documents/risk-management.pdf.
100. **Answer: B** The ATM card requires the user to have a card (something you have) and a PIN (something-you-know). Fingerprinting and GPS would be considered single-factor authentication. Logging in to your bank is requesting two items from one factor (something you know), so this is also considered single-factor authentication.

Chapter 5
Identity and Access Management (Domain 5)

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?
    1. An access control list
    2. An implicit denial list
    3. A capability table
    4. 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 in-house 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 onsite identity needs?
    1. Integrate onsite systems using OAuth.
    2. Use an on-premises third-party identity service.
    3. Integrate onsite systems using SAML.

4. Design an in-house solution to handle the organization's unique needs.

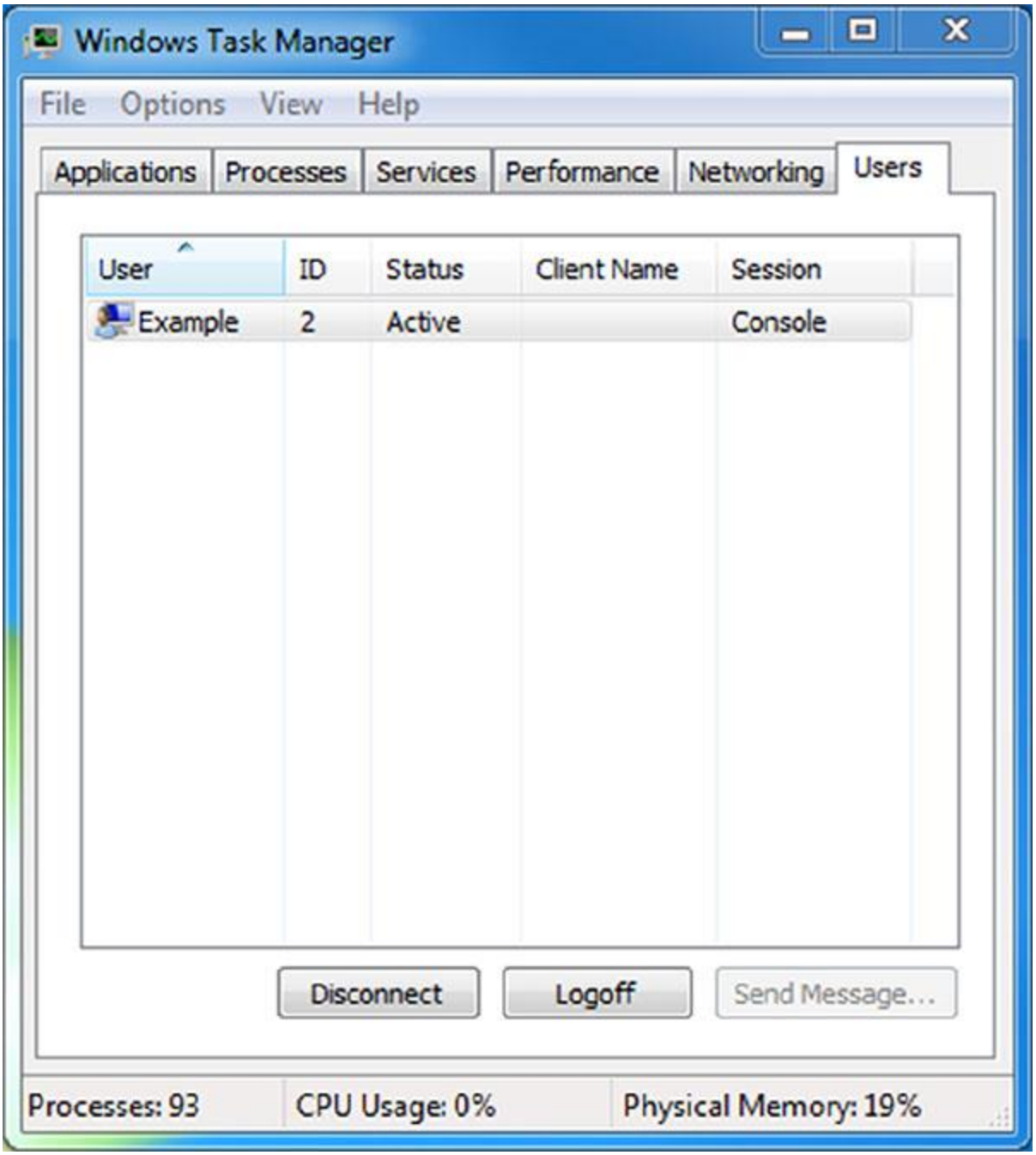
3. Which of the following is not a weakness in Kerberos?
    1. The KDC is a single point of failure.
    2. Compromise of the KDC would allow attackers to impersonate any user.
    3. Authentication information is not encrypted.
    4. It is susceptible to password guessing.
4. Voice pattern recognition is what type of authentication factor?
    1. Something you know
    2. Something you have
    3. Something you are
    4. 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?
    1. One
    2. Two
    3. Three
    4. Four
6. Which of the following items are not commonly associated with restricted interfaces?
    1. Shells
    2. Keyboards
    3. Menus
    4. Database views
7. During a log review, Saria discovers a series of logs that show login failures, as shown here:
    - Jan 31 11:39:12 ip-10-0-0-2 sshd[29092]: Invalid user admin from remotehost passwd=orange
    - Jan 31 11:39:20 ip-10-0-0-2 sshd[29098]: Invalid user admin from remotehost passwd=Orang3
    - Jan 31 11:39:23 ip-10-0-0-2 sshd[29100]: Invalid user admin from remotehost passwd=Orange93
    - Jan 31 11:39:31 ip-10-0-0-2 sshd[29106]: Invalid user admin from remotehost passwd=Orangutan1
    - Jan 31 20:40:53 ip-10-0-0-254 sshd[30520]: Invalid user admin from remotehost passwd=Orangemonkey

    What type of attack has Saria discovered?

    6. A brute-force attack
    7. A man-in-the-middle attack
    8. A dictionary attack
    9. A rainbow table attack
8. Place the following steps in the order in which they occur during the Kerberos authentication process.
    0. Client/server ticket generated
    1. TGT generated
    2. Client/TGS key generated

3. User accesses service
4. User provides authentication credentials

9. What major issue often results from decentralized access control?
    0. Access outages may occur.
    1. Control is not consistent.
    2. Control is too granular.
    3. Training costs are high.
10. Callback to a landline phone number is an example of what type of factor?
    0. Something you know
    1. Somewhere you are
    2. Something you have
    3. 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?
    0. A shortcut trust
    1. A forest trust
    2. An external trust
    3. A realm trust
12. Which of the following AAA protocols is the most commonly used?
    0. TACACS
    1. TACACS+
    2. XTACACS
    3. Super TACACS
13. Which of the following is not a single sign-on implementation?
    0. Kerberos
    1. ADFS
    2. CAS
    3. 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?



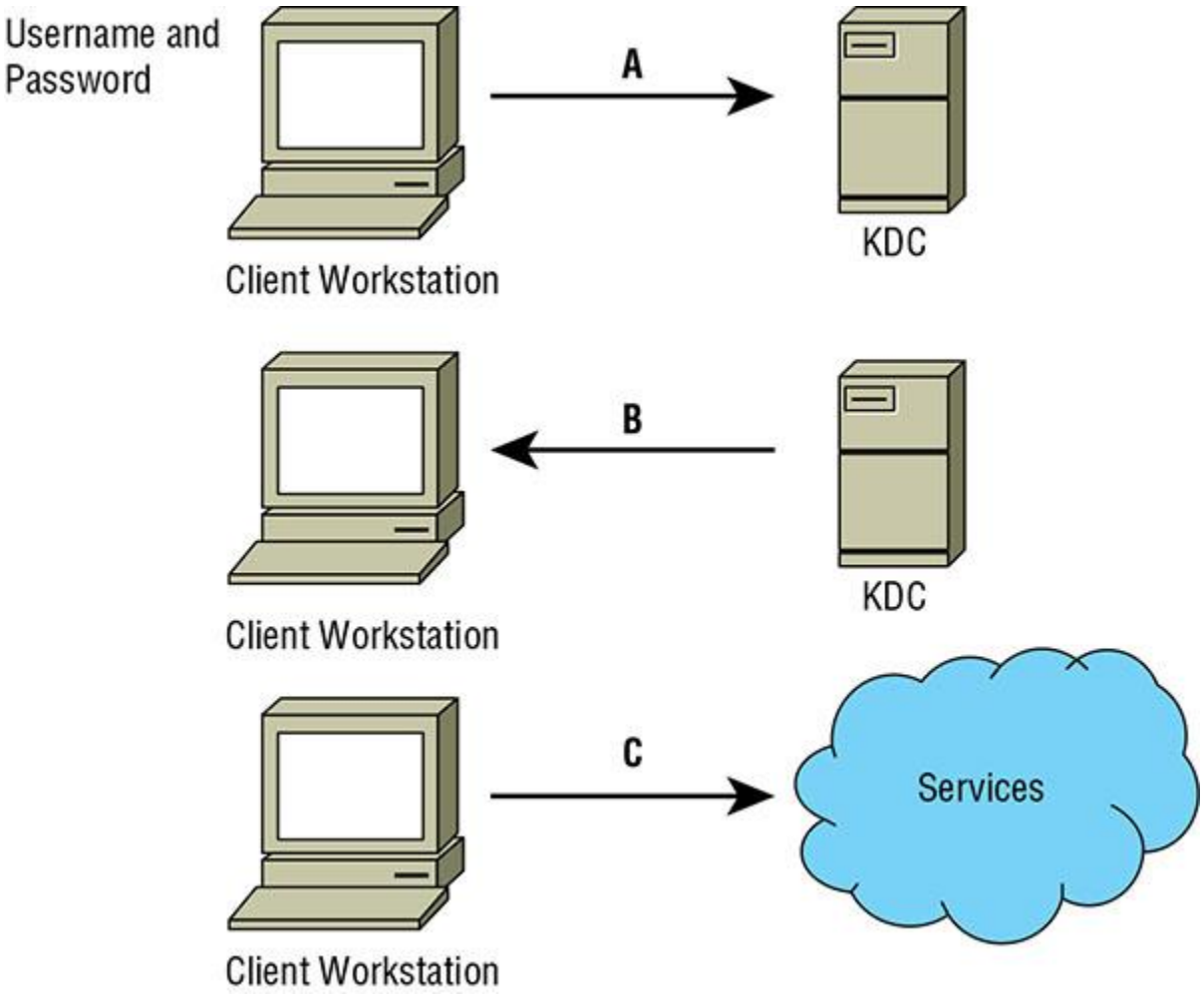
0. Least privilege
1. Need to know
2. Constrained interface
3. Separation of duties

15. What type of access controls allow the owner of a file to grant other users access to it using an access control list?
    0. Role based
    1. Nondiscretionary
    2. Rule based

3. 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?
    0. Separation of duties
    1. Constrained interfaces
    2. Context-dependent control
    3. Need to know

    Use your knowledge of the Kerberos logon process and the following diagram to answer questions 17–19.



17. At point A in the diagram, the client sends the username and password to the KDC. How is the username and password protected?
    0. 3DES encryption
    1. TLS encryption
    2. SSL encryption

3. 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?
    0. An encrypted TGT and a public key
    1. An access ticket and a public key
    2. An encrypted, time-stamped TGT and a symmetric key encrypted with a hash of the user's password
    3. An encrypted, time-stamped TGT and an access token
19. What tasks must the client perform before it can use the TGT?
    0. It must generate a hash of the TGT and decrypt the symmetric key.
    1. It must accept the TGT and decrypt the symmetric key.
    2. It must decrypt the TGT and the symmetric key.
    3. 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?
    0. Retina scans can reveal information about medical conditions.
    1. Retina scans are painful because they require a puff of air in the user's eye.
    2. Retina scanners are the most expensive type of biometric device.
    3. Retina scanners have a high false positive rate and will cause support issues.
21. Mandatory Access Control is based on what type of model?
    0. Discretionary
    1. Group based
    2. Lattice based
    3. Rule based
22. Which of the following is not a type of attack used against access controls?
    0. Dictionary attack
    1. Brute-force attack
    2. Teardrop
    3. Man-in-the-middle attack
23. What is the best way to provide accountability for the use of identities?
    0. Logging
    1. Authorization
    2. Digital signatures
    3. 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?
    0. Re-provisioning
    1. Account review
    2. Privilege creep
    3. Account revocation
25. Biba is what type of access control model?
    0. MAC
    1. DAC

2. Role BAC
3. 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?
    0. Kerberos
    1. EAP
    2. RADIUS
    3. OAuth
27. What type of access control is being used in the following permission listing:
    - Storage Device X
    - User1: Can read, write, list
    - User2: Can read, list
    - User3: Can read, write, list, delete
    - User4: Can list

    5. Resource-based access controls
    6. Role-based access controls
    7. Mandatory access controls
    8. Rule-based access controls
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?
    0. UDP, none. All RADIUS traffic is encrypted.
    1. TCP, all traffic but the passwords, which are encrypted.
    2. UDP, all traffic but the passwords, which are encrypted.
    3. TCP, none. All RADIUS traffic is encrypted.
29. Which of the following is not part of a Kerberos authentication system?
    0. KDC
    1. TGT
    2. AS
    3. TS
30. When an application or system allows a logged-in user to perform specific actions, it is an example of what?
    0. Roles
    1. Group management
    2. Logins
    3. 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?
    0. Excessive provisioning
    1. Unauthorized access
    2. Privilege creep
    3. Account review
32. Which of the following is not a common threat to access control mechanisms?
    0. Fake login pages

1. Phishing
2. Dictionary attacks
3. Man-in-the-middle attacks

33. What term properly describes what occurs when two or more processes require access to the same resource and must complete their tasks in the proper order for normal function?
    0. Collisions
    1. Race conditions
    2. Determinism
    3. Out-of-order execution
34. What type of access control scheme is shown in the following table?

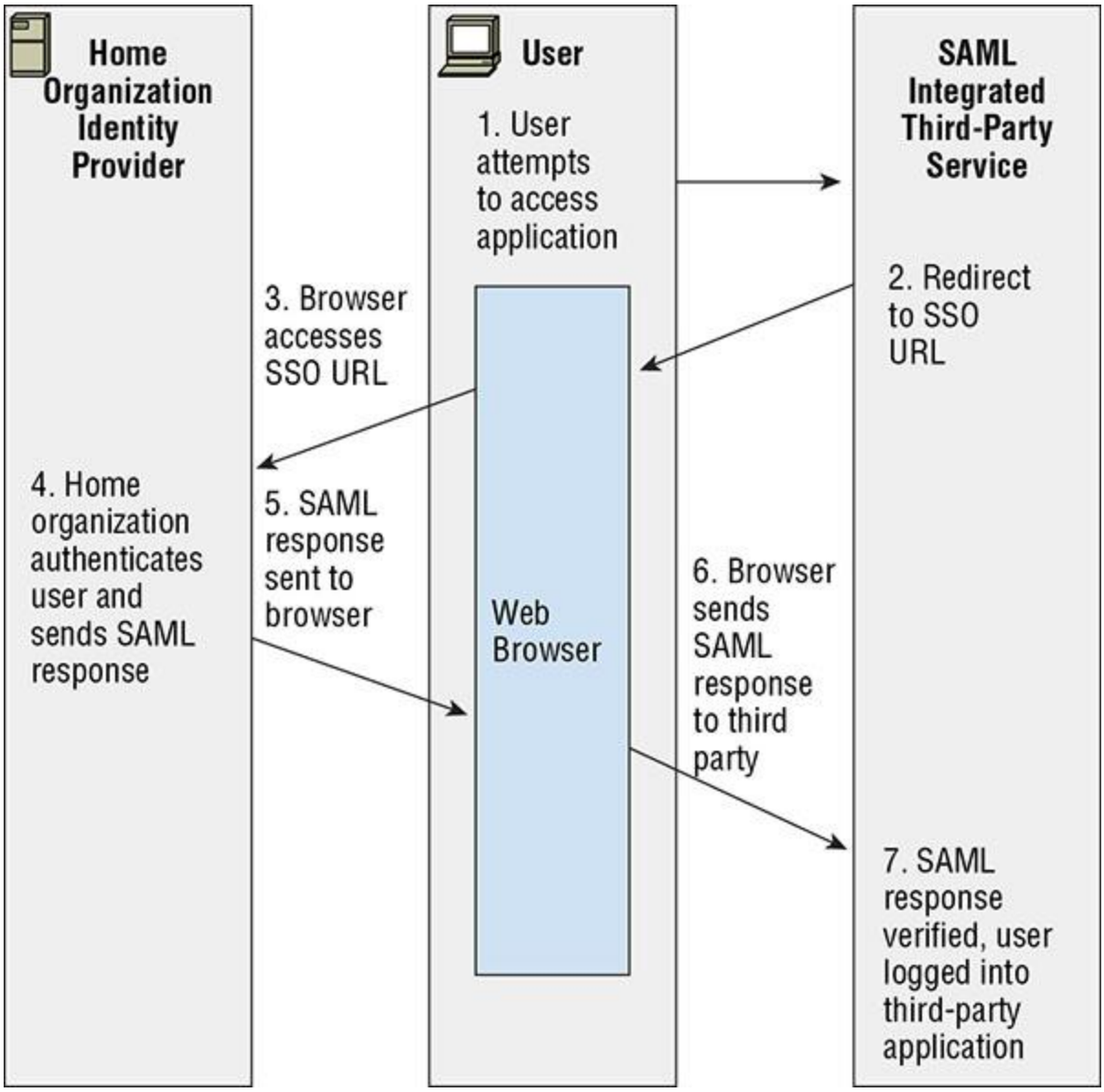
Highly Sensitive	Red	Blue	Green
Confidential	Purple	Orange	Yellow
Internal Use	Black	Gray	White
Public	Clear	Clear	Clear

    0. RBAC
    1. DAC
    2. MAC
    3. TBAC
35. Which of the following is not a valid LDAP DN (distinguished name)?
    0. cn=ben+ou=sales
    1. ou=example
    2. cn=ben,ou=example;
    3. ou=example,dc=example,dc=com+dc=org
36. When a subject claims an identity, what process is occurring?
    0. Login
    1. Identification
    2. Authorization
    3. Token presentation
37. Dogs, guards, and fences are all common examples of what type of control?
    0. Detective
    1. Recovery
    2. Administrative
    3. 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?
    0. Change maximum age from 1 year to 180 days.
    1. Increase the minimum password length from 8 characters to 16 characters.
    2. Increase the password complexity so that at least three character classes (such as uppercase, lowercase, numbers, and symbols) are required.
    3. Retain a password history of at least four passwords to prevent reuse.
39. What is the stored sample of a biometric factor called?
    0. A reference template

1. A token store
2. A biometric password
3. An enrollment artifact

40. When might an organization using biometrics choose to allow a higher FRR instead of a higher FAR?
    0. When security is more important than usability
    1. When false rejection is not a concern due to data quality
    2. When the CER of the system is not known
    3. When the CER of the system is very high
41. Susan is working to improve the strength of her organization's passwords by changing the password policy. The password system that she is using allows uppercase and lowercase letters as well as numbers but no other characters. How much additional complexity does adding a single character to the minimum length of passwords for her organization create?
    0. 26 times more complex
    1. 62 times more complex
    2. 36 times more complex
    3. 2^62 times more complex
42. Which pair of the following factors is key for user acceptance of biometric identification systems?
    0. The FAR
    1. The throughput rate and the time required to enroll
    2. The CER and the ERR
    3. How often users must reenroll and the reference profile requirements

Alex is in charge of SAML integration with a major third-party partner that provides a variety of business productivity services for his organization. Use the following diagram and your knowledge of SAML integrations and security architecture design to answer questions 43–45.



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?
    0. Use SAML's secure mode to provide secure authentication.
    1. Implement TLS using a strong cipher suite, which will protect against both types of attacks.
    2. Implement TLS using a strong cipher suite and use digital signatures.
    3. Implement TLS using a strong cipher suite and message hashing.
44. If Alex's organization is one that is primarily made up of offsite, traveling users, what availability risk does integration of critical business applications to onsite authentication create, and how could he solve it?
    0. Third-party integration may not be trustworthy; use SSL and digital signatures.

1. If the home organization is offline, traveling users won't be able to access third-party applications; implement a hybrid cloud/local authentication system.
2. Local users may not be properly redirected to the third-party services; implement a local gateway.
3. 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?
    0. An awareness campaign about trusted third parties
    1. TLS
    2. Handling redirects at the local site
    3. 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?
    0. MAC, because it provides greater scalability and flexibility because you can simply add more labels as needed
    1. DAC, because allowing individual administrators to make choices about the objects they control provides scalability and flexibility
    2. MAC, because compartmentalization is well suited to flexibility and adding compartments will allow it to scale well
    3. 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?
    0. Log review
    1. Manual review of permissions
    2. Signature-based detection
    3. Review the audit trail
48. Lauren 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?
    0. SAML
    1. SOAP
    2. SPML
    3. 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?
    0. A brute-force attack
    1. A pass-the-hash attack
    2. A rainbow table attack
    3. 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?
    0. PKI
    1. Federation
    2. Single sign-on
    3. Provisioning
51. Lauren 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?
    0. Privilege creep
    1. Rights collision
    2. Least privilege
    3. 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?
    0. Identity proofing
    1. Registration
    2. Directory management
    3. Session management
53. Jim configures his LDAP client to connect to an LDAP directory server. According to the configuration guide, his client should connect to the server on port 636. What does this indicate to Jim about the configuration of the LDAP server?
    0. It requires connections over SSL/TLS.
    1. It supports only unencrypted connections.
    2. It provides global catalog services.
    3. It does not provide global catalog services.
54. The X.500 standards cover what type of important identity systems?
    0. Kerberos
    1. Provisioning services
    2. Biometric authentication systems
    3. Directory services
55. Microsoft's Active Directory Domain Services is based on which of the following technologies?
    0. RADIUS
    1. LDAP
    2. SSO
    3. PKI
56. Lauren 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?
    0. Require users to create unique questions that only they will know.
    1. Require new users to bring their driver's license or passport in person to the bank.
    2. Use information that both the bank and the user have such as questions pulled from their credit report.
    3. Call the user on their registered phone number to verify that they are who they claim to be.
57. By default, in what format does OpenLDAP store the value of the userPassword attribute?

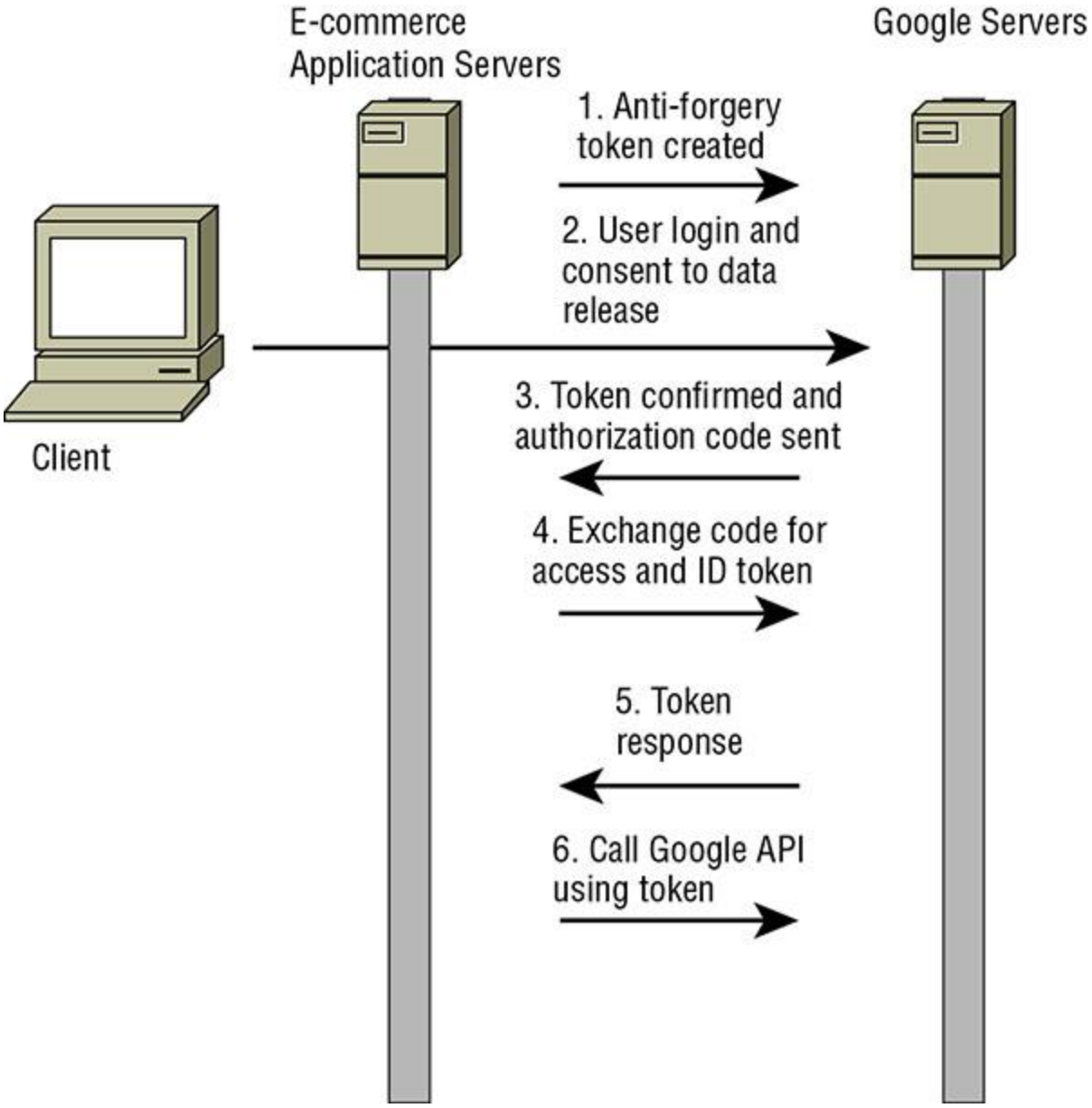
0. In the clear
1. Salted and hashed
2. MD5 hashed
3. Encrypted using AES256 encryption

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?
    0. A registration error
    1. A Type 1 error
    2. A Type 2 error
    3. A time of use, method of use error
59. What type of access control is typically used by firewalls?
    0. Discretionary access controls
    1. Rule-based access controls
    2. Task-based access control
    3. Mandatory access controls
60. When you input a user ID and password, you are performing what important identity and access management activity?
    0. Authorization
    1. Validation
    2. Authentication
    3. 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?
    0. Add a reader that requires a PIN for passcard users.
    1. Add a camera system to the facility to observe who is accessing servers.
    2. Add a biometric factor.
    3. Replace the magnetic stripe keycards with smartcards.
62. Which of the following is a ticket-based authentication protocol designed to provide secure communication?
    0. RADIUS
    1. OAuth
    2. SAML
    3. Kerberos
63. What type of access control is composed of policies and procedures that support regulations, requirements, and the organization's own policies?
    0. Corrective
    1. Logical
    2. Compensating
    3. Administrative

64. In a Kerberos environment, when a user needs to access a network resource, what is sent to the TGS?
    0. A TGT
    1. An AS
    2. The SS
    3. A session key
65. Which objects and subjects have a label in a MAC model?
    0. Objects and subjects that are classified as Confidential, Secret, or Top Secret have a label.
    1. All objects have a label, and all subjects have a compartment.
    2. All objects and subjects have a label.
    3. All subjects have a label and all objects have a compartment.

    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.

    Use this information and the following diagram of an example authentication flow to answer questions 66–68.



66. When the e-commerce application creates an account for a Google user, where should that user's password be stored?
    0. The password is stored in the e-commerce application's database.
    1. The password is stored in memory on the e-commerce application's server.
    2. The password is stored in Google's account management system.
    3. The password is never stored; instead, a salted hash is stored in Google's account management system.
67. Which system or systems is/are responsible for user authentication for Google users?
    0. The e-commerce application.
    1. Both the e-commerce application and Google servers.
    2. Google servers.
    3. The diagram does not provide enough information to determine this.

68. What type of attack is the creation and exchange of state tokens intended to prevent?
    0. XSS
    1. CSRF
    2. SQL injection
    3. XACML
69. Questions like “What is your pet’s name?” are examples of what type of identity proofing?
    0. Knowledge-based authentication
    1. Dynamic knowledge-based authentication
    2. Out-of-band identity proofing
    3. A Type 3 authentication factor
70. Lauren builds 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 Lauren using?
    0. A capability table
    1. An access control list
    2. An access control matrix
    3. A subject/object rights management system
71. During a review of support incidents, 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?
    0. Two-factor authentication
    1. Biometric authentication
    2. Self-service password reset
    3. Passphrases
72. 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?
    0. Use the built-in encryption in RADIUS.
    1. Implement RADIUS over its native UDP using TLS for protection.
    2. Implement RADIUS over TCP using TLS for protection.
    3. Use an AES256 pre-shared cipher between devices.
73. 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?
    0. Kerberos
    1. OAuth
    2. OpenID
    3. LDAP
74. 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?
    0. Use session IDs for all access and verify system IP addresses of all workstations.

1. Set session time-outs for applications and use password-protected screensavers with inactivity time-outs on workstations.
2. Use session IDs for all applications, and use password protected screensavers with inactivity time-outs on workstations.
3. Set session time-outs for applications and verify system IP addresses of all workstations.

75. Match each of the numbered security controls listed with exactly one of the lettered categories shown. Choose the category that best describes each control. You may use each control category once, more than once, or not at all.

    Controls

    0. Password
    1. Account reviews
    2. Badge readers
    3. MFA
    4. IDP

    Categories

    5. Administrative
    6. Technical
    7. Physical

76. The financial services company that Susan works for provides a web portal for its users. When users need to verify their identity, the company uses information from third-party sources to ask questions based on their past credit reports, such as "Which of the following streets did you live on in 2007?" What process is Susan's organization using?
    0. Identity proofing
    1. Password verification
    2. Authenticating with Type 2 authentication factor
    3. Out-of-band identity proofing
77. The United States (U.S.) government CAC is an example of what form of Type 2 authentication factor?
    0. A token
    1. A biometric identifier
    2. A smart card
    3. A PIV
78. What authentication technology can be paired with OAuth to perform identity verification and obtain user profile information using a RESTful API?
    0. SAML
    1. Shibboleth
    2. OpenID Connect
    3. Higgins
79. Jim has Secret clearance and is accessing files that use a mandatory access control scheme to apply the Top Secret, Secret, Confidential, and Unclassified label scheme.

What classification levels of data can he access, provided that he has a valid need-to-know?

0. Top Secret and Secret
1. Secret, Confidential, and Unclassified
2. Secret data only
3. Secret and Unclassified

80. 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?
    0. Constrained interface
    1. Context-dependent control
    2. Content-dependent control
    3. Least privilege
81. 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

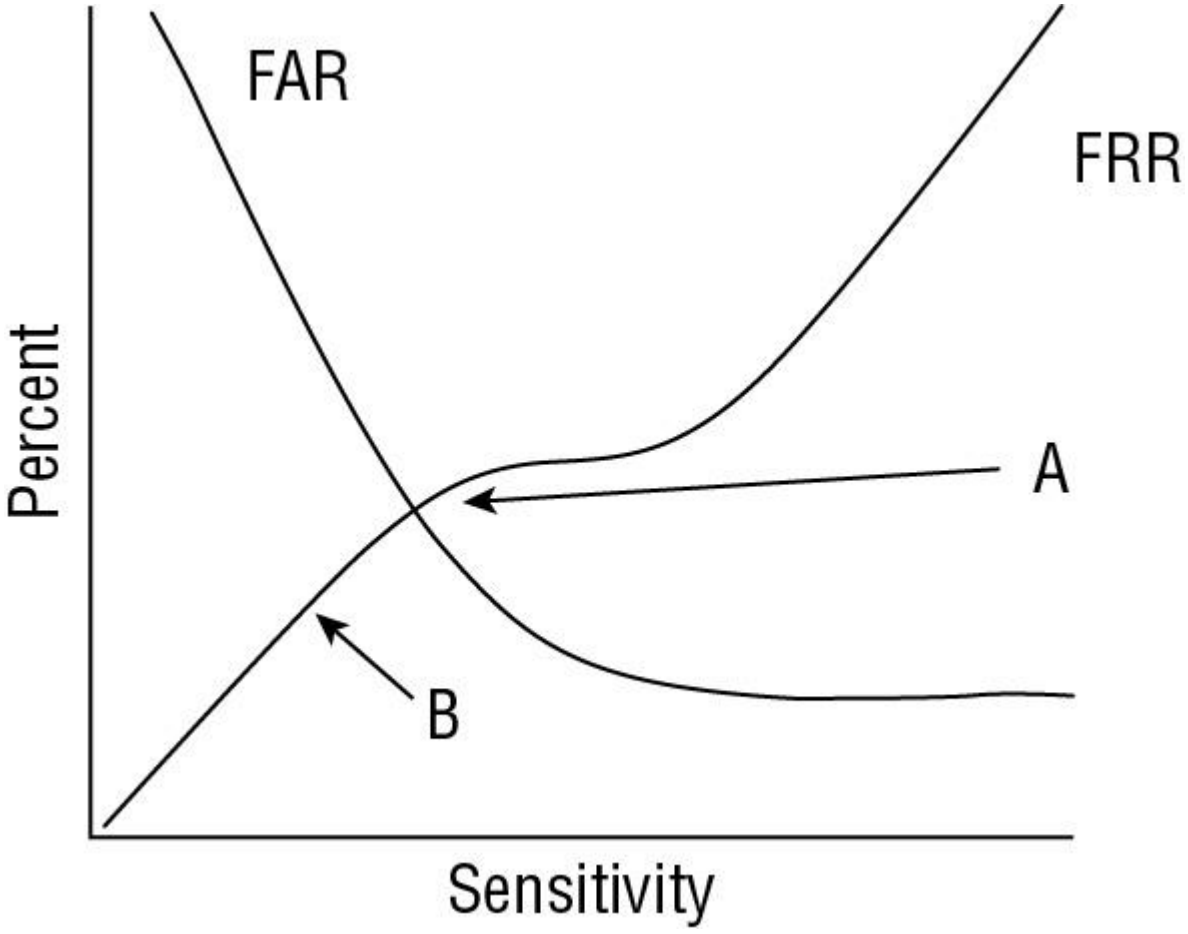
    0. Password
    1. ID card
    2. Retinal scan
    3. Smartphone token
    4. Fingerprint analysis

    Category

    5. Something you have
    6. Something you know
    7. Something you are
82. Which of the following is not an access control layer?
    0. Physical
    1. Policy
    2. Administrative
    3. Technical
83. Ben uses a software-based token that changes its code every minute. What type of token is he using?
    0. Asynchronous
    1. Smart card
    2. Synchronous
    3. Static
84. What type of token-based authentication system uses a challenge/response process in which the challenge has to be entered on the token?
    0. Asynchronous
    1. Smart card
    2. Synchronous

3. RFID

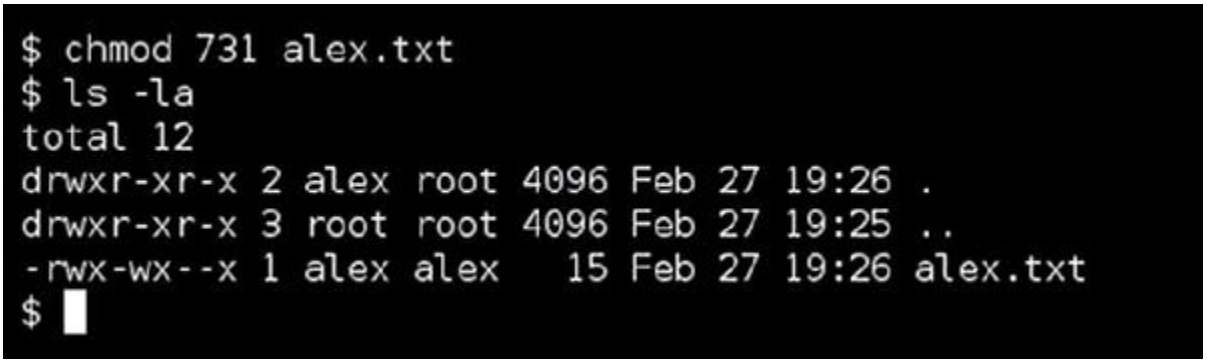
Ben's organization is adopting biometric authentication for its high-security building's access control system. Use the following chart to answer questions 85–87 about the organization's adoption of the technology.



85. Ben's company is considering configuring its systems to work at the level shown by point A on the diagram. To what level is it setting the sensitivity?
    0. The FRR crossover
    1. The FAR point
    2. The CER
    3. The CFR
86. At point B, what problem is likely to occur?
    0. False acceptance will be very high.
    1. False rejection will be very high.
    2. False rejection will be very low.
    3. False acceptance will be very low.
87. What should Ben do if the FAR and FRR shown in this diagram does not provide an acceptable performance level for his organization's needs?
    0. Adjust the sensitivity of the biometric devices.

1. Assess other biometric systems to compare them.
2. Move the CER.
3. Adjust the FRR settings in software.

88. What LDAP authentication mode can provide secure authentication?
    0. Anonymous
    1. SASL
    2. Simple
    3. S-LDAP
89. Which of the following Type 3 authenticators is appropriate to use by itself rather than in combination with other biometric factors?
    0. Voice pattern recognition
    1. Hand geometry
    2. Palm scans
    3. Heart/pulse patterns
90. What danger is created by allowing the OpenID relying party to control the connection to the OpenID provider?
    0. It may cause incorrect selection of the proper OpenID provider.
    1. It creates the possibility of a phishing attack by sending data to a fake OpenID provider.
    2. The relying party may be able to steal the client's username and password.
    3. The relying party may not send a signed assertion.
91. Jim is implementing a cloud identity solution for his organization. What type of technology is he putting in place?
    0. Identity as a service
    1. Employee ID as a service
    2. Cloud-based RADIUS
    3. OAuth
92. RAID-5 is an example of what type of control?
    0. Administrative
    1. Recovery
    2. Compensation
    3. Logical
93. 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?



    0. Role Based Access Control

1. Rule-based Access control
2. Mandatory Access Control (MAC)
3. Discretionary Access Control (DAC)

94. What open protocol was designed to replace RADIUS—including support for additional commands and protocols, replacing UDP traffic with TCP, and providing for extensible commands—but does not preserve backward compatibility with RADIUS?
    0. TACACS
    1. RADIUS-NG
    2. Kerberos
    3. Diameter
95. LDAP distinguished names (DNs) are made up of comma-separated components called relative distinguished names (RDNs) that have an attribute name and a value. DNs become less specific as they progress from left to right. Which of the following LDAP DNs best fits this rule?
    0. uid=ben,ou=sales,dc=example,dc=com
    1. uid=ben,dc=com,dc=example
    2. dc=com,dc=example,ou=sales,uid=ben
    3. ou=sales,dc=com,dc=example
96. 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?
    0. The Kerberos server is offline.
    1. There is a protocol mismatch.
    2. The client's TGTs have been marked as compromised and de-authorized.
    3. The Kerberos server and the local client's time clocks are not synchronized.
97. Kerberos, KryptoKnight, and SESAME are all examples of what type of system?
    0. SSO
    1. PKI
    2. CMS
    3. Directory
98. Which of the following access control categories would not include a door lock?
    0. Physical
    1. Directive
    2. Preventative
    3. Deterrent
99. What authentication protocol does Windows use by default for Active Directory systems?
    0. RADIUS
    1. Kerberos
    2. OAuth
    3. TACACS+
100. Alex configures his LDAP server to provide services on 636 and 3269. What type of LDAP services has he configured based on LDAP's default ports?
    0. Unsecure LDAP and unsecure global directory
    1. Unsecure LDAP and secure global directory

2. Secure LDAP and secure global directory
3. Secure LDAP and unsecure global directory

Chapter 5: Identity and Access Management (Domain 5)

1. C. Capability tables list the privileges assigned to subjects and identify the objects that subjects can access. Access control lists are object-focused rather than subject-focused. Implicit deny is a principle that states that anything that is not explicitly allowed is denied, and a rights management matrix is not an access control model.
2. B. Since Jim's organization is using a cloud-based identity as a service solution, a third-party, on-premises identity service can provide the ability to integrate with the IDaaS solution, and the company's use of Active Directory is widely supported by third-party vendors. OAuth is used to log into third-party websites using existing credentials and would not meet the needs described. SAML is a markup language and would not meet the full set of AAA needs. Since the organization is using Active Directory, a custom in-house solution is unlikely to be as effective as a preexisting third-party solution and may take far more time and expense to implement.
3. C. Kerberos encrypts messages using secret keys, providing protection for authentication traffic. The KDC both is a single point of failure and can cause problems if compromised because keys are stored on the KDC that would allow attackers to impersonate any user. Like many authentication methods, Kerberos can be susceptible to password guessing.
4. C. Voice pattern recognition is "something you are," a biometric authentication factor, because it measures a physical characteristic of the individual authenticating.
5. B. Susan has used two distinct types of factors: the PIN and password are both Type 1 factors, and the retina scan is a Type 3 factor. Her username is not a factor.
6. B. Menus, shells, and database views are all commonly used for constrained interfaces. A keyboard is not typically a constrained interface, although physically constrained interfaces like those found on ATMs, card readers, and other devices are common.
7. C. Dictionary attacks use a dictionary or list of common passwords as well as variations of those words to attempt to log in as an authorized user. This attack shows a variety of passwords based on a similar base word, which is often a good indicator of a dictionary attack. A brute-force attack will typically show simple iteration of passwords, while a man-in-the-middle attack would not be visible in the authentication log. A rainbow table attack is used when attackers already have password hashes in their possession and would also not show up in logs.
8. During the Kerberos authentication process, the steps take place in the following order:

- E. User provides authentication credentials
- C. Client/TGS key generated
- B. TGT generated
- A. Client/server ticket generated
- D. User accesses service

9. B. Decentralized access control can result in less consistency because the individuals tasked with control may interpret policies and requirements differently and may perform their roles in different ways. Access outages, overly granular control, and training costs may occur, depending on specific implementations, but they are not commonly identified issues with decentralized access control.

10. B. A callback to a landline phone number is an example of a “somewhere you are” factor because of the fixed physical location of a wired phone. A callback to a mobile phone would be a “something you have” factor.
11. D. Kerberos uses realms, and the proper type of trust to set up for an Active Directory environment that needs to connect to a K5 domain is a realm trust. A shortcut trust is a transitive trust between parts of a domain tree or forest that shortens the trust path, a forest trust is a transitive trust between two forest root domains, and an external trust is a nontransitive trust between AD domains in separate forests.
12. B. TACACS+ is the only modern protocol on the list. It provides advantages of both TACACS and XTACACS as well as some benefits over RADIUS, including encryption of all authentication information. Super TACACS is not an actual protocol.
13. D. Kerberos, Active Directory Federation Services (ADFS), and Central Authentication Services (CAS) are all SSO implementations. RADIUS is not a single sign-on implementation, although some vendors use it behind the scenes to provide authentication for proprietary SSO.
14. C. Interface restrictions based on user privileges is an example of a constrained interface. Least privilege describes the idea of providing users with only the rights they need to accomplish their job, while need to know limits access based on whether a subject needs to know the information to accomplish an assigned task. Separation of duties focuses on preventing fraud or mistakes by splitting tasks between multiple subjects.
15. D. When the owner of a file makes the decisions about who has rights or access privileges to it, they are using discretionary access control. Role-based access controls would grant access based on a subject’s role, while rule-based controls would base the decision on a set of rules or requirements. Nondiscretionary access controls apply a fixed set of rules to an environment to manage access. Nondiscretionary access controls include rule-, role-, and lattice-based access controls.
16. D. Need to know is applied when subjects like Alex have access to only the data they need to accomplish their job. Separation of duties is used to limit fraud and abuse by having multiple employees perform parts of a task. Constrained interfaces restrict what a user can see or do and would be a reasonable answer if need to know did not describe his access more completely in this scenario. Context-dependent control relies on the activity being performed to apply controls, and this question does not specify a workflow or process.
17. D. The client in Kerberos logins uses AES to encrypt the username and password prior to sending it to the KDC.
18. C. The KDC uses the user’s password to generate a hash and then uses that hash to encrypt a symmetric key. It transmits both the encrypted symmetric key and an encrypted time-stamped TGT to the client.
19. B. The client needs to install the TGT for use until it expires and must also decrypt the symmetric key using a hash of the user’s password.
20. A. Retina scans can reveal additional information, including high blood pressure and pregnancy, causing privacy concerns. Newer retina scans don’t require a puff of air, and retina scanners are not the most expensive biometric factor. Their false positive rate can typically be adjusted in software, allowing administrators to adjust their acceptance rate as needed to balance usability and security.
21. C. Mandatory access control systems are based on a lattice-based model. Lattice-based models use a matrix of classification labels to compartmentalize data. Discretionary access models allow object owners to determine access to the objects they control, role-based access controls are often group based, and rule-based access controls like firewall ACLs apply rules to all subjects they apply to.

22. C. Dictionary, brute-force, and man-in-the-middle attacks are all types of attacks that are frequently aimed at access controls. Teardrop attacks are a type of denial of service attack.
23. A. Logging systems can provide accountability for identity systems by tracking the actions, changes, and other activities a user or account performs.
24. B. As an employee's role changes, they often experience privilege creep, which is the accumulation of old rights and roles. Account review is the process of reviewing accounts and ensuring that their rights match their owners' role and job requirements. Account revocation removes accounts, while re-provisioning might occur if an employee was terminated and returned or took a leave of absence and returned.
25. A. Biba uses a lattice to control access and is a form of the mandatory access control (MAC) model. It does not use rules, roles, or attributes, nor does it allow user discretion. Users can create content at their level or lower but cannot decide who gets access, levels are not roles, and attributes are not used to make decisions on access control.
26. C. RADIUS is an AAA protocol used to provide authentication and authorization; it's often used for modems, wireless networks, and network devices. It uses network access servers to send access requests to central RADIUS servers. Kerberos is a ticket-based authentication protocol; OAuth is an open standard for authentication allowing the use of credentials from one site on third-party sites; and EAP is the Extensible Authentication Protocol, an authentication framework often used for wireless networks.
27. A. Resource-based access controls match permissions to resources like a storage volume. Resource-based access controls are becoming increasingly common in cloud-based infrastructure as a service environments. The lack of roles, rules, or a classification system indicate that role-based, rule-based, and mandatory access controls are not in use here.
28. C. By default, RADIUS uses UDP and only encrypts passwords. RADIUS supports TCP and TLS, but this is not a default setting.
29. D. A key distribution center (KDC) provides authentication services, and ticket-granting tickets (TGTs) provide proof that a subject has authenticated and can request tickets to access objects. Authentication services (ASs) are part of the KDC. There is no TS in a Kerberos infrastructure.
30. D. Authorization provides a user with capabilities or rights. Roles and group management are both methods that could be used to match users with rights. Logins are used to validate a user.
31. C. Privilege creep occurs when users retain from roles they held previously rights they do not need to accomplish their current job. Unauthorized access occurs when an unauthorized user accesses files. *Excessive provisioning* is not a term used to describe permissions issues, and account review would help find issues like this.
32. B. Phishing is not an attack against an access control mechanism. While phishing can result in stolen credentials, the attack itself is not against the control system and is instead against the person being phished. Dictionary attacks and man-in-the-middle attacks both target access control systems.
33. B. Race conditions occur when two or more processes need to access the same resource in the right order. If an attacker can disrupt this order, they may be able to affect the normal operations of the system and gain unauthorized access or improper rights. Collisions occur when two different files produce the same result from a hashing operation, out-of-order execution is a CPU architecture feature that allows the use of otherwise unused cycles, and *determinism* is a philosophical term rather than something you should see on the CISSP exam!
34. C. Mandatory access controls use a lattice to describe how classification labels relate to each other. In this image, classification levels are set for each of the labels shown. A discretionary access control (DAC) system would show how the owner of the objects allows access. RBAC

could be either rule- or role-based access control and would use either system-wide rules or roles. Task-based access control (TBAC) would list tasks for users.

35. C. LDAP distinguished names are made up of zero or more comma-separated components known as relative distinguished names. cn=ben,ou=example; ends with a semicolon and is not a valid DN. It is possible to have additional values in the same RDN by using a plus sign between then.
36. B. The process of a subject claiming or professing an identity is known as identification. Authorization verifies the identity of a subject by checking a factor like a password. Logins typically include both identification and authorization, and token presentation is a type of authentication.
37. D. Dogs, guards, and fences are all examples of physical controls. While dogs and guards might detect a problem, fences cannot, so they are not all examples of detective controls. None of these controls would help repair or restore functionality after an issue, and thus they are not recovery controls, nor are they administrative controls that involve policy or procedures, although the guards might refer to them when performing their duties.
38. B. Password complexity is driven by length, and a longer password will be more effective against brute-force attacks than a shorter password. Each character of additional length increases the difficulty by the size of the potential character set (for example, a single lowercase character makes the passwords 26 times more difficult to crack). While each of the other settings is useful for a strong password policy, they won't have the same impact on brute-force attacks.
39. A. The stored sample of a biometric factor is called a reference profile or a reference template. None of the other answers is a common term used for biometric systems.
40. A. Organizations that have very strict security requirements that don't have a tolerance for false acceptance want to lower the false acceptance rate, or FAR, to be as near to zero as possible. That often means that the false rejection rate, or FRR, increases. Different biometric technologies or a better registration method can help improve biometric performance, but false rejections due to data quality are not typically a concern with modern biometric systems. In this case, knowing the crossover error rate, or CER, or having a very high CER doesn't help the decision.
41. B. The complexity of brute-forcing a password increases based on both the number of potential characters and the number of letters added. In this case, there are 26 lowercase letters, 26 uppercase letters, and 10 possible digits. That creates 62 possibilities. Since we added only a single letter of length, we get 62^1, or 62 possibilities, and thus, the new passwords would be 62 times harder to brute-force on average.
42. B. Biometric systems can face major usability challenges if the time to enroll is long (over a couple of minutes) and if the speed at which the biometric system is able to scan and accept or reject the user is too slow. FAR and FRR may be important in the design decisions made by administrators or designers, but they aren't typically visible to users. CER and ERR are the same and are the point where FAR and FRR meet. Reference profile requirements are a system requirement, not a user requirement.
43. C. TLS provides message confidentiality and integrity, which can prevent eavesdropping. When paired with digital signatures, which provide integrity and authentication, forged assertions can also be defeated. SAML does not have a security mode and relies on TLS and digital signatures to ensure security if needed. Message hashing without a signature would help prevent modification of the message but won't necessarily provide authentication.
44. B. Integration with cloud-based third parties that rely on local authentication can fail if the local organization's Internet connectivity or servers are offline. Adopting a hybrid cloud and local authentication system can ensure that Internet or server outages are handled, allowing

authentication to work regardless of where the user is or if their home organization is online. Using encrypted and signed communication does not address availability, redirects are a configuration issue with the third party, and a local gateway won't handle remote users. Also, host files don't help with availability issues with services other than DNS.

45. A. While many solutions are technical, if a trusted third party redirects to an unexpected authentication site, awareness is often the best defense. Using TLS would keep the transaction confidential but would not prevent the redirect. Handling redirects locally only works for locally hosted sites, and using a third-party service requires offsite redirects. An IPS might detect an attacker's redirect, but tracking the multitude of load-balanced servers most large providers use can be challenging, if not impossible. In addition, an IPS relies on visibility into the traffic, and SAML integrations should be encrypted for security, which would require a man-in-the-middle type of IPS to be configured.
46. B. Discretionary access control (DAC) can provide greater scalability by leveraging many administrators, and those administrators can add flexibility by making decisions about access to their objects without fitting into an inflexible mandatory access control system (MAC). MAC is more secure due to the strong set of controls it provides, but it does not scale as well as DAC and is relatively inflexible in comparison.
47. C. While signature-based detection is used to detect attacks, review of provisioning processes typically involves checking logs, reviewing the audit trail, or performing a manual review of permissions granted during the provisioning process.
48. C. Service Provisioning Markup Language, or SPML, is an XML-based language designed to allow platforms to generate and respond to provisioning requests. SAML is used to make authorization and authentication data, while XACML is used to describe access controls. SOAP, or Simple Object Access Protocol, is a messaging protocol and could be used for any XML messaging but is not a markup language itself.
49. C. Rainbow tables are databases of prehashed passwords paired with high-speed lookup functions. Since they can quickly compare known hashes against those in a file, using rainbow tables is the fastest way to quickly determine passwords from hashes. A brute-force attack may eventually succeed but will be very slow against most hashes. Pass-the-hash attacks rely on sniffed or otherwise acquired NTLM or LanMan hashes being sent to a system to avoid the need to know a user's password. Salts are data added to a hash to avoid the use of tools like rainbow tables. A salt added to a password means the hash won't match a rainbow table generated without the same salt.
50. B. Google's federation with other applications and organizations allows single sign-on as well as management of their electronic identity and its related attributes. While this is an example of SSO, it goes beyond simple single sign-on. Provisioning provides accounts and rights, and a public key infrastructure is used for certificate management.
51. D. When users have more rights than they need to accomplish their job, they have excessive privileges. This is a violation of the concept of least privilege. Unlike creeping privileges, this is a provisioning or rights management issue rather than a problem of retention of rights the user needed but no longer requires. *Rights collision* is a made-up term and thus is not an issue here.
52. B. Registration is the process of adding a user to an identity management system. This includes creating their unique identifier and adding any attribute information that is associated with their identity. Proofing occurs when the user provides information to prove who they are. Directories are managed to maintain lists of users, services, and other items. Session management tracks application and user sessions.

53. A. Port 636 is the default port for LDAP-S, which provides LDAP over SSL or TLS, thus indicating that the server supports encrypted connections. Since neither port 3268 nor 3269 is mentioned, we do not know if the server provides support for a global catalog.
54. D. The X.500 series of standards covers directory services. Kerberos is described in RFCs; biometric systems are covered by a variety of standards, including ISO standards; and provisioning standards include SCIM, SPML, and others.
55. B. Active Directory Domain Services is based on LDAP, the Lightweight Directory Access Protocol. Active Directory also uses Kerberos for authentication.
56. C. Identity proofing can be done by comparing user information that the organization already has, like account numbers or personal information. Requiring users to create unique questions can help with future support by providing a way for them to do password resets. Using a phone call only verifies that the individual who created the account has the phone that they registered and won't prove their identity. In-person verification would not fit the business needs of most websites.
57. A. By default, OpenLDAP stores the userPassword attribute in the clear. This means that ensuring that the password is provided to OpenLDAP in a secure format is the responsibility of the administrator or programmer who builds its provisioning system.
58. C. Type 2 errors occur in biometric systems when an invalid subject is incorrectly authenticated as a valid user. In this case, nobody except the actual customer should be validated when fingerprints are scanned. Type 1 errors occur when a valid subject is not authenticated; if the existing customer was rejected, it would be a Type 1 error. Registration is the process of adding users, but registration errors and time of use, method of use errors are not specific biometric authentication terms.
59. B. Firewalls use rule-based access control, or Rule-BAC, in their access control lists and apply rules created by administrators to all traffic that pass through them. DAC, or discretionary access control, allows owners to determine who can access objects they control, while task-based access control lists tasks for users. MAC, or mandatory access control, uses classifications to determine access.
60. C. When you input a username and password, you are authenticating yourself by providing a unique identifier and a verification that you are the person who should have that identifier (the password). Authorization is the process of determining what a user is allowed to do. Validation and login both describe elements of what is happening in the process; however, they aren't the most important identity and access management activity.
61. C. Kathleen should implement a biometric factor. The cards and keys are an example of a Type 2 factor, or "something you have." Using a smart card replaces this with another Type 2 factor, but the cards could still be loaned out or stolen. Adding a PIN suffers from the same problem: a PIN can be stolen. Adding cameras doesn't prevent access to the facility and thus doesn't solve the immediate problem (but it is a good idea!).
62. D. Kerberos is an authentication protocol that uses tickets and provides secure communications between the client, key distribution center (KDC), ticket-granting service (TGS), authentication server (AS), and endpoint services. RADIUS does not provide the same level of security by default, SAML is a markup language, and OAuth is designed to allow third-party websites to rely on credentials from other sites like Google or Microsoft.
63. D. Administrative access controls are procedures and the policies from which they derive. They are based on regulations, requirements, and the organization's own policies. Corrective access controls return an environment to its original status after an issue, while logical controls are technical access controls that rely on hardware or software to protect systems and data. Compensating controls are used in addition to or as an alternative to other controls.

64. A. When clients perform a client service authorization, they send a TGT and the ID of the requested service to the TGS, and the TGS responds with a client-to-server ticket and session key back to the client if the request is validated. An AS is an authentication server, and the SS is a service server, neither of which can be sent.
65. C. In a mandatory access control system, all subjects and objects have a label. Compartments may or may not be used, but there is not a specific requirement for either subjects or objects to be compartmentalized. The specific labels of Confidential, Secret, and Top Secret are not required by MAC.
66. D. Passwords are never stored for web applications in a well-designed environment. Instead, salted hashes are stored and compared to passwords after they are salted and hashed. If the hashes match, the user is authenticated.
67. C. When a third-party site integrates via OAuth 2.0, authentication is handled by the service provider's servers. In this case, Google is acting as the service provider for user authentication. Authentication for local users who create their own accounts would occur in the e-commerce application (or a related server), but that is not the question that is asked here.
68. B. The anti-forgery state token exchanged during OAuth sessions is intended to prevent cross-site request forgery. This makes sure that the unique session token with the authentication response from Google's OAuth service is available to verify that the user, not an attacker, is making a request. XSS attacks focus on scripting and would have script tags involved, SQL injection would have SQL code included, and XACML is the eXtensible Access Control Markup Language, not a type of attack.
69. A. Knowledge-based authentication relies on preset questions such as "What is your pet's name?" and the answers. It can be susceptible to attacks because of the availability of the answers on social media or other sites. Dynamic knowledge-based authentication relies on facts or data that the user already knows that can be used to create questions they can answer on an as-needed basis (for example, a previous address, or a school they attended).

    Out-of-band identity proofing relies on an alternate channel like a phone call or text message. Finally, Type 3 authentication factors are biometric, or "something you are," rather than knowledge based.

70. C. An access control matrix is a table that lists objects, subjects, and their privileges. Access control lists focus on objects and which subjects can access them. Capability tables list subjects and what objects they can access. Subject/object rights management systems are not based on an access control model.
71. C. Self-service password reset tools typically have a significant impact on the number of password reset contacts that a help desk has. Two-factor and biometric authentication both add additional complexity and may actually increase the number of contacts. Passphrases can be easier to remember than traditional complex passwords and may decrease calls, but they don't have the same impact that a self-service system does.
72. C. RADIUS supports TLS over TCP. RADIUS does not have a supported TLS mode over UDP. AES pre-shared symmetric ciphers are not a supported solution and would be very difficult to both implement and maintain in a large environment, and the built-in encryption in RADIUS only protects passwords.
73. B. OAuth provides the ability to access resources from another service and would meet Jim's needs. OpenID would allow him to use an account from another service with his application, and Kerberos and LDAP are used more frequently for in-house services.

74. B. Since physical access to the workstations is part of the problem, setting application time-outs and password-protected screensavers with relatively short inactivity time-outs can help prevent unauthorized access. Using session IDs for all applications and verifying system IP addresses would be helpful for online attacks against applications.
75. The security controls match with the categories as follows:
    1. Password: B. Technical.
    2. Account reviews: A. Administrative.
    3. Badge readers: C. Physical.
    4. MFA: B. Technical.
    5. IDP: B. Technical.

- Passwords, multifactor authentication (MFA) techniques, and intrusion prevention systems (IPS) are all examples of technical controls. Account reviews are an administrative control, while using badges to control access is a physical control.

76. A. Verifying information that an individual should know about themselves using third-party factual information (a Type 1 authentication factor) is sometimes known as dynamic knowledge-based authentication and is a type of identity proofing. Out-of-band identity proofing would use another means of contacting the user, like a text message or phone call, and password verification requires a password.
77. C. The US government's Common Access Card is a smart card. The US government also issues PIV cards, or personal identity verification cards.
78. C. OpenID Connect is a RESTful, JSON-based authentication protocol that, when paired with OAuth, can provide identity verification and basic profile information. SAML is the Security Assertion Markup Language, Shibboleth is a federated identity solution designed to allow web-based SSO, and Higgins is an open-source project designed to provide users with control over the release of their identity information.
79. C. In a mandatory access control system, classifications do not have to include rights to lower levels. This means that the only label we can be sure Jim has rights to is Secret. Despite that it is unclassified, Unclassified data remains a different label, and Jim may not be authorized to access it.
80. B. Time-based controls are an example of context-dependent controls. A constrained interface would limit what Susan was able to do in an application or system interface, while content-dependent control would limit her access to content based on her role or rights. Least privilege is used to ensure that subjects only receive the rights they need to perform their role.
81. The security controls match with the categories as follows:
    1. Password: B. Something you know.
    2. ID card: A. Something you have.
    3. Retinal scan: C. Something you are.
    4. Smartphone token: A. Something you have.
    5. Fingerprint analysis: C. Something you are.
82. B. Policy is a subset of the administrative layer of access controls. Administrative, technical, and physical access controls all play an important role in security.
83. C. Synchronous soft tokens, such as Google Authenticator, use a time-based algorithm that generates a constantly changing series of codes. Asynchronous tokens typically require a challenge to be entered on the token to allow it to calculate a response, which the server compares to the response it expects. Smartcards typically present a certificate but may have

other token capabilities built in. Static tokens are physical devices that can contain credentials and include smart cards and memory cards.

84. A. Asynchronous tokens use a challenge/response process in which the system sends a challenge and the user responds with a PIN and a calculated response to the challenge. The server performs the same calculations, and if both match, it authenticates the user. Synchronous tokens use a time-based calculation to generate codes. Smart cards are paired with readers and don't need to have challenges entered, and RFID devices are not used for challenge/response tokens.
85. C. The crossover error rate is the point where false acceptance rate and false rejection rate cross over and is a standard assessment used to compare the accuracy of biometric devices.
86. A. At point B, the false acceptance rate, or FAR, is quite high, while the false rejection rate, or FRR, is relatively low. This may be acceptable in some circumstances, but in organizations where a false acceptance can cause a major problem, it is likely that they should instead choose a point to the right of point A.
87. B. CER is a standard used to assess biometric devices. If the CER for this device does not fit the needs of the organization, Ben should assess other biometric systems to find one with a lower CER. Sensitivity is already accounted for in CER charts, and moving the CER isn't something Ben can do. FRR is not a setting in software, so Ben can't use that as an option either.
88. B. The Simple Authentication and Security Layer (SASL) for LDAP provides support for a range of authentication types, including secure methods. Anonymous authentication does not require or provide security, and simple authentication can be tunneled over SSL or TLS but does not provide security by itself. S-LDAP is not an LDAP protocol.
89. C. Palm scans compare the vein patterns in the palm to a database to authenticate a user. Vein patterns are unique, and this method is a better single-factor authentication method than voice pattern recognition, hand geometry, and pulse patterns, each of which can be more difficult to uniquely identify between individuals or can be fooled more easily.
90. B. Allowing the relying party to provide the redirect to the OpenID provider could allow a phishing attack by directing clients to a fake OpenID provider that can capture valid credentials. Since the OpenID provider URL is provided by the client, the relying party cannot select the wrong provider. The relying party never receives the user's password, which means that they can't steal it. Finally, the relying party receives the signed assertion but does not send one.
91. A. IDaaS, or identity as a service, provides an identity platform as a third-party service. This can provide benefits including integration with cloud services and removing overhead for maintenance of traditional on-premises identity systems, but it can also create risk due to third-party control of identity services and reliance on an offsite identity infrastructure.
92. B. Drives in a RAID-5 array are intended to handle failure of a drive. This is an example of a recovery control, which is used to return operations to normal function after a failure. Administrative controls are policies and procedures. Compensation controls help cover for issues with primary controls or improve them. Logical controls are software and hardware mechanisms used to protect resources and systems.
93. D. The Linux filesystem allows the owners of objects to determine the access rights that subjects have to them. This means that it is a discretionary access control. If the system enforced a role-based access control, Alex wouldn't set the controls; they would be set based on the roles assigned to each subject. A rule-based access control system would apply rules throughout the system, and a mandatory access control system uses classification labels.
94. D. Diameter was designed to provide enhanced, modern features to replace RADIUS. Diameter provides better reliability and a broad range of improved functionality. RADIUS-NG does not exist, Kerberos is not a direct competitor for RADIUS, and TACACS is not an open protocol.

95. A. In this example, uid=ben,ou=sales,dc=example,dc=com, the items proceed from most specific to least specific (broadest) from left to right, as required by a DN.
96. D. Kerberos relies on properly synchronized time on each end of a connection to function. If the local system time is more than five minutes out of sync, valid TGTs will be invalid and the system won't receive any new tickets.
97. A. Kerberos, KryptoKnight, and SESAME are all single sign-on, or SSO, systems. PKI systems are public key infrastructure systems, CMS systems are content management systems, and LDAP and other directory servers provide information about services, resources, and individuals.
98. B. Locks can be preventative access controls by stopping unwanted access, can deter potential intruders by making access difficult, and are physical access controls. They are not directive controls because they don't control the actions of subjects.
99. B. Windows uses Kerberos for authentication. RADIUS is typically used for wireless networks, modems, and network devices, while OAuth is primarily used for web applications. TACACS+ is used for network devices.
100. C. The default ports for SSL/TLS LDAP directory information and global catalog services are 636 and 3269, respectively. Unsecure LDAP uses 389, and unsecure global directory services use 3268.