D - 2N

1. A Chief Executive Officer (CEO) is steering company towards cloud computing. The CEO is requesting a federated sign-on method to have users sign into the sales application. Which of the following methods will be effective for this purpose?
[✓ A. SAML]
B. RADIUS
C. Kerberos
D. LDAP

2. An administrator is configuring a new Linux web server where each user account is confined to a cheroot jail. Which of the following describes this type of control?
A. SysV
[✓ B. Sandbox]
C. Zone
D. Segmentation

3. Recently clients are stating they can no longer access a secure banking site's webpage. In reviewing the clients' web browser settings, the certificate chain is showing the following:

Certificate Chain:
X Digi Cert
Digi Cert High assurance C3
* banksite.com

Certificate Store:
Digi Cert Others Certificate Store
Digi Cert High assurance C3 Others Certificate Store

Based on the information provided, which of the following is the problem when connecting to the website?
A. The certificate signature request was invalid
B. Key escrow is failing for the certificate authority
[✓ C. The certificate authority has revoked the certificate]
D. The clients do not trust the certificate authority

4. A company often processes sensitive data for the government. The company also processes a large amount of commercial work and as such is often providing tours to potential customers that take them into various workspaces. Which of the following security methods can provide protection against tour participants viewing sensitive information at minimal cost?
A. Strong passwords
B. Screen protectors
[✓ C. Clean-desk policy]
D. Mantraps

5. Joe is a helpdesk specialist. During a routine audit, a company discovered that his credentials were used while he was on vacation. The investigation further confirmed that Joe still has his badge and it was last used to exit the facility. Which of the following access control methods is MOST appropriate for preventing such occurrences in the future?
[✓ A. Access control where the credentials cannot be used except when the associated badge is in the facility]
B. Access control where system administrators may limit which users can access their systems
C. Access control where employee's access permissions is based on the job title
D. Access control system where badges are only issued to cleared personnel

6. A security architect is designing an enterprise solution for the sales force of a corporation which handles sensitive customer data. The solution must allow users to work from remote offices and support traveling users. Which of the following is the MOST appropriate control for the architect to focus onto ensure confidentiality of data stored on laptops?
[✓ A. Full-disk encryption]
B. Digital sign
C. Federated identity management
D. Cable locks

7. A security administrator needs a method to ensure that only employees can get onto the internal network when plugging into a network switch. Which of the following BEST

meets that requirement?
[✓ A.] NAC
B. UTM
C. DMZ
D. VPN

8. Having adequate lighting on the outside of a building is an example of which of the following security controls?
[✓ A.] Deterrent
B. Compensating
C. Detective
D. Preventative

9. During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions. Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?
A. Time-of-day restrictions
[✓ B.] User access reviews
C. Group-based privileges
D. Change management policies

10. An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data. In which of the following documents would this concern MOST likely be addressed?
[✓ A.] Service level agreement
[✓ B.] Interconnection security agreement
C. Non-disclosure agreement
D. Business process analysis

11. A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources. Which of the following should be implemented?
A. Mandatory access control
[✓ B.] Discretionary access control
C. Role based access control
D. Rule-based access control

12. Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?
A. Spear phishing
[✓ B.] Main-in-the-middle
C. URL hijacking
D. Transitive access

13. A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Choose two.)
[✓ A.] SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
[✓ F.] FTPS

14. A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected. Which of the following MUST the technician implement?
[✓ A.] Dual factor authentication
B. Transitive authentication
C. Single factor authentication
D. Biometric authentication

15. After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that

the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

[✓ A.] The company implements a captive portal
B. The thermostat is using the inencryption algorithm
C. the WPA2 shared likely is incorrect
D. The company's DHCP server scope is full

16. A switch is set up to allow only 2 simultaneous MAC addresses per switch port. An administrator is reviewing a log and determines that a switch ort has been deactivated in a conference room after it detected 3 or more MAC addresses on the same port. Which of the following reasons could have caused this port to be disabled?

A. A pc had a NIC replaced and reconnected to the switch
B. An ip telephone has been plugged in
C. A rouge access point was plugged in
[✓ D.] An arp attack was launched from a pc on this port

17. Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

A. armored virus
B. logic bomb
[✓ C.] polymorphic virus
D. Trojan

18. A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

A. RSA
[✓ B.] TwoFish
C. Diffie-Helman
D. NTLMv2
E. RIPEMD

19. Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

A. MOU
B. ISA
C. BPA
[✓ D.] SLA

20. Which of the following are MOST susceptible to birthday attacks?

[✓ A.] Hashed passwords
B. Digital certificates
C. Encryption passwords
D. One time passwords

21. Joe, a computer forensic technician, responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive. Which of the following procedures did Joe follow?

[✓ A.] Order of volatility
B. Chain of custody
C. Recovery procedure
D. Incident isolation

22. A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non- repudiation. Which of the following implements all these requirements?

A. Bcrypt
B. Blowfish
[✓ C.] PGP
D. SHA

323. Given the log output:

```
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: msmith]
[Source: 10.0.12.45]
```

[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015

Which of the following should the network administrator do to protect data security?
A. Configure port security for logons
[✓ B.] Disable telnet and enable SSH
C. Configure an AAA server
D. Disable password and enable RSA authentication

24. The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?
A. Certificate revocation list
[✓ B.] Intermediate authority
C. Recovery agent
D. Root of trust

25. The Chief Executive Officer (CEO) of a major defense contracting company a traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?
A. Remote wipe
[✓ B.] Full device encryption
C. BIOS password
D. GPS tracking

26. In an effort to reduce data storage requirements, a company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems. Which of the following algorithms is BEST suited for this purpose?
A. MD5
[✓ B.] SHA
C. RIPEMD
D. AES

27. A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files. Which of the following should the organization implement in order to be compliant with the new policy?
[✓ A.] Replace FTP with SFTP and replace HTTP with TLS
B. Replace FTP with FTPS and replaces HTTP with TFTP
C. Replace FTP with SFTP and replace HTTP with Telnet
D. Replace FTP with FTPS and replaces HTTP with IPSec

28. A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes. Which of the following risk management strategies BEST describes management's response?
A. Deterrence
B. Mitigation
[✓ C.] Avoidance
D. Acceptance

29. Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?
[✓ A.] Account lockout
B. Group Based Privileges
C. Least privilege
D. Password complexity

30. Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys. Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?
A. Key escrow
[✓ B.] Digital signatures

[✓ C. PKI]
D. Hashing

31. An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient. Which of the following capabilities would be MOST appropriate to consider implementing is response to the new requirement?
A. Transitive trust
B. Symmetric encryption
C. Two-factor authentication
[✓ D. Digital signatures]
E. One-time passwords

32. Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data. Which of the following controls can be implemented to mitigate this type of inside threat?
A. Digital signatures
[✓ B. File integrity monitoring]
C. Access controls
D. Change management
E. Stateful inspection firewall

33. The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?
A. Collision resistance
B. Rainbow table
[✓ C. Key stretching]
D. Brute force attack

34. Which of the following is commonly used for federated identity management across multiple organizations?
[✓ A. SAML]
B. Active Directory
C. Kerberos
D. LDAP

35. A security administrator has been asked to implement a VPN that will support remote access over IPSEC. Which of the following is an encryption algorithm that would meet this requirement?
A. MD5
[✓ B. AES]
C. UDP
D. PKI

36. A security administrator is evaluating three different services: radius, diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?
A. It provides authentication services
[✓ B. It uses tickets to identify authenticated users]
C. It provides single sign-on capability
D. It uses XML for cross-platform interoperability

37. Which of the following can affect electrostatic discharge in a network operations center?
A. Fire suppression
B. Environmental monitoring
C. Proximity card access
[✓ D. Humidity controls]

38. A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?
[✓ A. Header manipulation]
B. Cookie hijacking
C. Cross-site scripting
D. Xml injection

39. A company would like to prevent the use of a known set of applications from being used on company computers. Which of the following should the security administrator

implement?

A. Whitelisting

B. Anti-malware

C. Application hardening

[✓ D] Blacklisting

E. Disable removable media

40. A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company. Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

A. Asset control

B. Device access control

C. Storage lock out

D. Storage segmentation

41. A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and law performing edge switch on the network has been elected to be the root bridge. Which of the following explains this scenario?

A. The switch also serves as the DHCP server

[✓ B] The switch has the lowest MAC address

C. The switch has spanning tree loop protection enabled

D. The switch has the fastest uplink port

42. An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead. Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

A. Rule-based access control

B. Role-based access control

C. Mandatory access control

[✓ D.] Discretionary access control

43. While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Choose two.)

[✓ A.] Minimum complexity

B. Maximum age limit

C. Maximum length

[✓ D] Minimum length

E. Minimum age limit

F. Minimum re-use limit

44. A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

A. Deploy antivirus software and configure it to detect and remove pirated software

B. Configure the firewall to prevent the downloading of executable files

[✓ C] Create an application whitelist and use OS controls to enforce it

D. Prevent users from running as administrator so they cannot install software.

45. A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility. Which of the following configuration commands should be implemented to enforce this requirement?

A. LDAP server 10.55.199.3

B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233

C. SYSLOG SERVER 172.16.23.50

[✓ D.] TACAS server 192.168.1.100

46. A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert. Which of the following methods has MOST likely been used?

A. Cryptography
B. Time of check/time of use
C. Man in the middle
D. Covert timing
[✓ E. Steganography]

47. An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to. This is because the encryption scheme in use adheres to:

[✓ A. Asymmetric encryption]
B. Out-of-band key exchange
C. Perfect forward secrecy
D. Secure key escrow

48. Many employees are receiving email messages similar to the one shown below:

From IT department
To employee
Subject email quota exceeded
Please click on the following link http:www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quota.

Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI. Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

A. BLOCK http://www..info/"
B. DROP http://"website.info/email.php?
C. Redirect http://www,. Info/email.php?quota=TOhttp://company.com/corporate_polict.html
[✓ D. DENY http://.info/email.php?quota=1Gb]

49. A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ: Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCP From ANY to 172.31.64.4
B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
[✓ D. Deny TCP from 192.168.1.10 to 172.31.67.4]

50. The IT department needs to prevent users from installing untested applications. Which of the following would provide the BEST solution?

A. Job rotation
[✓ B. Least privilege]
C. Account lockout
D. Antivirus

51. An attack that is using interference as its main attack to impede network traffic is which of the following?

~~A.~~ Introducing too much data to a targets memory allocation
B. Utilizing a previously unknown security flaw against the target
[✓ C. Using a similar wireless configuration of a nearby network]
D. Inundating a target system with SYN requests

52. An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

A. DES
B. Blowfish

C. DSA
[✓ D.] Diffie-Hellman
E. 3DES

53. Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remakes. Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?
A. Data Labeling and disposal
[✓ B.] Use of social networking
C. Use of P2P networking
D. Role-based training

54. During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?
A. Network mapping
[✓ B.] Vulnerability scan
C. Port Scan
D. Protocol analysis

55. When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?
A. RC4
B. MD5
C. HMAC
[✓ D.] SHA

56. The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?
A. In-transit
[✓ B.] In-use
C. Embedded
D. At-rest

57. Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?
A. TACACS+
B. RADIUS
C. Kerberos
[✓ D.] SAML

58. A network technician is trying to determine the source of an ongoing network based attack. Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?
A. Proxy
[✓ B.] Protocol analyzer
C. Switch
D. Firewall

59. The security administrator has noticed cars parking just outside of the building fence line. Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Choose two.)
A. Create a honeynet
B. Reduce beacon rate
C. Add false SSIDs
[✓ D.] Change antenna placement
[✓ E.] Adjust power level controls
F. Implement a warning banner

60. A security administrator suspects that data on a server has been exhilarated as a result of un- authorized remote access. Which of the following would assist the administrator in con-firming the suspicions? (Choose two.)
A. Networking access control
[✓ B.] DLP alerts
[✓ C.] Log analysis
D. File integrity monitoring
E. Host firewall rules

61. A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated. Which of the following options will pro-vide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

[✓ A.] Put the VoIP network into a different VLAN than the existing data network.
B. Upgrade the edge switches from 10/100/1000 to improve network speed
C. Physically separate the VoIP phones from the data network
D. Implement flood guards on the data network

62. A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the server using RDP on a port other than the typical registered port for the RDP protocol?

[✓ A.] TLS
B. MPLS
C. SCP
D. SSH

63. Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

A. LDAP
B. Kerberos
C. SAML
[✓ D.] TACACS+

64. Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate- based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication. Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

A. Use of OATH between the user and the service and attestation from the company domain
[✓ B.] Use of active directory federation between the company and the cloud-based service
C. Use of smartcards that store x.509 keys, signed by a global CA
D. Use of a third-party, SAML-based authentication service for attestation

65. Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it. Which of the following BEST describes what the company?

A. The system integration phase of the SDLC
[✓ B.] The system analysis phase of SSDSLC
C. The system design phase of the SDLC
D. The system development phase of the SDLC

66. A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided form the role-based authentication system in use by the company. The situation can be identified for future mitigation as which of the following?

A. Job rotation
[✓ B.] Log failure
C. Lack of training
D. Insider threat

67. A security administrator needs an external vendor to an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system. Which of the following methods should the security administrator select the best balances security and efficiency?

A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
B. Have the external vendor come onsite and provide access to the PACS directly
[✓ C.] Set up VPN concentrator for the vendor and restrict access to the PACS using desktop

sharing
D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

68. A datacenter manager has been asked to prioritize critical system recovery priorities. Which of the following is the MOST critical for immediate recovery?
A. Communications software
[✓ B.] Operating system software
C. Weekly summary reports to management
D. Financial and production software

69. Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)
A. SQL injection
[✓ B.] Session hijacking
[✓ C.] Cross-site scripting
D. Locally shared objects
E. LDAP injection

70. When designing a web based client server application with single application server and database cluster backend, input validation should be performed:
A. On the client
B. Using database stored procedures
[✓ C.] On the application server
D. Using HTTPS

71. Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?
A. Egress traffic is more important than ingress traffic for malware prevention
[✓ B.] To rebalance the amount of outbound traffic and inbound traffic
C. Outbound traffic could be communicating to known botnet sources
D. To prevent DDoS attacks originating from external network

72. The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?
A. Password Reuse
B. Password complexity
C. Password History
[✓ D.] Password Minimum age

73. Which of the following would enhance the security of accessing data stored in the cloud? (Choose two.)
A. Block level encryption
[✓ B.] SAML authentication
C. Transport encryption
[✓ D.] Multifactor authentication
E. Predefined challenge questions
F. Hashing

74. A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host. Which of the following is preventing the remote user from being able to access the workstation?
[✓ A.] Network latency is causing remote desktop service request to time out
B. User1 has been locked out due to too many failed passwords
C. Lack of network time synchronization is causing authentication mismatches
D. The workstation has been compromised and is accessing known malware sites
E. The workstation host firewall is not allowing remote desktop connections

75. Ann has read and written access to an employee database, while Joe has only read access. Ann is leaving for a conference. Which of the following types of authorization could be utilized to trigger write access for Joe when Ann is absent?
A. Mandatory access control
B. Role-based access control
C. Discretionary access control
[✓ D.] Rule-based access control

76. Recently, the desktop support group has been performing a hardware refresh and has

replaced numerous computers. An auditor discovered that a number of the new computers did not have the company's antivirus software installed on them. Which of the following could be utilized to notify the network support group when computers without the antivirus software are added to the network?
A. Network port protection
[✓ B.] NAC
~~C.~~ NIDS
D. Mac Filtering

77. An administrator needs to protect against downgrade attacks due to various vulnerabilities in SSL/TLS. Which of the following actions should be performed? (Choose two.)
A. Set minimum protocol supported
B. Request a new certificate from the CA
[✓ C.] Configure cipher order
D. Disable flash cookie support
[✓ E.] Re-key the SSL certificate
F. Add the old certificate to the CRL

? 78. A developer needs to utilize AES encryption in an application but requires the speed of encryption and decryption to be as fast as possible. The data that will be secured is not sensitive so speed is valued over encryption complexity. Which of the following would BEST satisfy these requirements?
A. AES with output feedback
[✓ B] AES with cipher feedback
C. AES with cipher block chaining
D. AES with counter mode

79. During a code review a software developer discovers a security risk that may result in hundreds of hours of rework. The security team has classified these issues as low risk. Executive management has decided that the code will not be rewritten. This is an example of:
A. Risk avoidance
B. Risk transference
C. Risk mitigation
[✓ D.] Risk acceptance

80. A network was down for several hours due to a contractor entering the premises and plugging both ends of a network cable into adjacent network jacks. Which of the following would have prevented the network outage? (Choose Two)
[✓ A.] Port security
[✓ B.] Loop Protection
C. Implicit deny
D. Log analysis
E. Mac Filtering
F. Flood Guards

81. After disabling SSID broadcast, a network administrator still sees the wireless network listed in available networks on a client laptop. Which of the following attacks may be occurring?
[✓ A.] Evil Twin
B. ARP spoofing
C. Disassociation flooding
D. Rogue access point
E. TKIP compromise

82. A security manager is preparing the training portion of an incident plan. Which of the following job roles should receive training on forensics, chain of custody, and the order of volatility?
A. System owners
B. Data custodians
[✓ C.] First responders
D. Security guards

83. Virtualization that allows an operating system kernel to run multiple isolated instances of the guest is called:
A. Process segregation
B. Software defined network
[✓ C.] Containers

D. Emulation

84. Which of the following is a proprietary protocol commonly used for router authentication across an enterprise?
A. SAML
[✓ B.] TACACS
C. LDAP
D. RADIUS

85. While responding to an incident on a new Windows server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?
A. IPCONFIG
[✓ B.] Netstat
C. PSINFO
D. Net session

86. A system administrator must configure the company's authentication system to ensure that users will be unable to reuse the last ten passwords within a six months period. Which of the following settings must be configured? (Choose Two)
[✓ A.] Minimum password age
B. Password complexity
C. Password history
[✓ D.] Minimum password length
E. Multi-factor authentication
F. Do not store passwords with reversible encryption

87. An administrator requests a new VLAN be created to support the installation of a new SAN. Which of the following data transport?
[✓ A.] Fibre Channel
B. SAS
C. Sonet
D. ISCSI

88. Which of the following access control methodologies provides an individual with the most restrictive access rights to successfully perform their authorized duties?
A. Mandatory Access Control
B. Rule Based Access Control
[✓ C.] Least Privilege
D. Implicit Deny
E. Separation of Duties

89. An administrator wants to provide onboard hardware based cryptographic processing and secure key storage for full-disk encryption. Which of the following should the administrator use to fulfil the requirements?
A. AES
[✓ B.] TPM
C. FDE
D. PAM

90. When viewing IPS logs the administrator see systems all over the world scanning the network for servers with port 22 open. The administrator concludes that this traffic is a(N):
A. Risk
B. Vulnerability
C. Exploit
[✓ D.] Threat

91. Ann a user has been promoted from a sales position to sales manager. Which of the following risk mitigation strategies would be MOST appropriate when a user changes job roles?
A. Implement data loss prevention
B. Rest the user password
[✓ C.] User permissions review
D. Notify incident management

92. A system administrator is implementing a firewall ACL to block specific communication to and from a predefined list of IP addresses, while allowing all other communication. Which of the following rules is necessary to support this implementation?

A. Implicit allow as the last rule
B. Implicit allow as the first rule
C. Implicit deny as the first rule
[✓ D.] Implicit deny as the last rule

93. Joe a system architect wants to implement appropriate solutions to secure the company's distributed database. Which of the following concepts should be considered to help ensure data security? (Choose two.)
[✓ A.] Data at rest
B. Data in use
C. Replication
D. Wiping
[✓ E.] Retention
F. Cloud Storage

94. A forensics analyst is tasked identifying identical files on a hard drive. Due to the large number of files to be compared, the analyst must use an algorithm that is known to have the lowest collision rate. Which of the following should be selected?
A. MD5
B. RC4
[✓ C.] SHA-128
D. AES-256

95. A government agency wants to ensure that the systems they use have been deployed as security as possible. Which of the following technologies will enforce protections on these systems to prevent files and services from operating outside of a strict rule set?
A. Host-based Intrusion detection
[✓ B.] Host-based firewall
[✓ C.] Trusted OS
D. Antivirus

96. An organization receives an email that provides instruction on how to protect a system from being a target of new malware that is rapidly infecting systems. The incident response team investigates the notification and determines it to invalid and notifies users to disregard the email. Which of the following Best describes this occurrence?
A. Phishing
B. Scareware
C. SPAM
[✓ D.] Hoax

97. Joe an employee has reported to Ann a network technician an unusual device plugged into a USB port on a workstation in the call center. Ann unplugs the workstation and brings it to the IT department where an incident is opened. Which of the following should have been done first?
[✓ A.] Notify the incident response team lead
B. Document chain of custody
C. Take a copy of volatile memory
D. Make an image of the hard drive

98. A company is implementing a system to transfer direct deposit information to a financial institution. One of the requirements is that the financial institution must be certain that the deposit amounts within the file have not been changed. Which of the following should be used to meet the requirement?
A. Key escrow
B. Perfect forward secrecy
C. Transport encryption
[✓ D.] Digital signatures
E. File encryption

99. An organization uses a Kerberos-based LDAP service for network authentication. The service is also utilized for internal web applications. Finally access to terminal applications is achieved using the same authentication method by joining the legacy system to the Kerberos realm. This company is using Kerberos to achieve which of the following?
A. Trusted Operating System
B. Rule-based access control
[✓ C.] Single sign on
D. Mandatory access control

100. A recent audit has revealed that all employees in the bookkeeping department have access to confidential payroll information, while only two members of the bookkeeping department have job duties that require access to the confidential information. Which of the following can be implemented to reduce the risk of this information becoming compromised in this scenario? (Choose two.)

A. Rule-based access control

[✓ B.] Role-based access control

C. Data loss prevention

D. Separation of duties

[✓ E.] Group-based permissions