SY0-401

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/

Security Plus 401

Exam A

QUESTION 1
When Ann an employee returns to work and logs into her workstation she notices that, several desktop configuration settings have changed. Upon a review of the CCTV logs, it is determined that someone logged into Ann's workstation. Which of the following could have prevented this from happening?

A. Password complexity policy
B. User access reviews
C. Shared account prohibition policy
D. User assigned permissions policy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A security administrator discovered that all communication over the company's encrypted wireless network is being captured by savvy employees with a wireless sniffing tool and is then being decrypted in an attempt to steal other employee's credentials. Which of the following technology is MOST likely in use on the company's wireless?

A. WPA with TKIP
B. VPN over open wireless
C. WEP128-PSK
D. WPA2-Enterprise

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
The chief Risk officer is concerned about the new employee BYOD device policy and has requested the security department implement mobile security controls to protect corporate data in the event that a device is lost or stolen. The level of protection must not be compromised even if the communication SIM is removed from the device. Which of the following BEST meets the requirements? (Select TWO)

A. Asset tracking
B. Screen-locks
C. GEO-Tracking
D. Patch management
E. Device encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
An administrator is building a development environment and requests that three virtual servers are cloned and placed in a new virtual network isolated from the production network. Which of the following describes the environment the administer is building?

A. Cloud
B. Trusted
C. Sandbox
D. Snapshot

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
An administrator needs to connect a router in one building to a router in another using Ethernet. Each router is connected to a managed switch and the switches are connected to each other via a fiber line. Which of the following should be configured to prevent unauthorized devices from connecting to the network?

A. Configure each port on the switches to use the same VLAN other than the default one
B. Enable VTP on both switches and set to the same domain
C. Configure only one if the routers to run DHCP services
D. Implement port security on the switches

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Joe, an employee is taking a taxi through a busy city and starts to receive unsolicited files sent to his Smartphone. Which of the following is this an example of?

A. Vishing
B. Bluejacking
C. War Driving
D. SPIM
E. Bluesnarfing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
The datacenter design team is implementing a system, which requires all servers installed in racks to face in a predetermined direction. AN infrared camera will be used to verify that servers are properly racked. Which of the following datacenter elements is being designed?

A. Hot and cold aisles
B. Humidity control
C. HVAC system
D. EMI shielding

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Computer evidence at a crime is preserved by making an exact copy of the hard disk. Which of the following does this illustrate?

A. Taking screenshots
B. System image capture
C. Chain of custody
D. Order of volatility

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following concepts is used by digital signatures to ensure integrity of the data?

A. Non-repudiation
B. Hashing
C. Transport encryption
D. Key escrow

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

An employee recently lost a USB drive containing confidential customer data. Which of the following controls could be utilized to minimize the risk involved with the use of USB drives?

A. DLP
B. Asset tracking
C. HSM
D. Access control

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A company uses PGP to ensure that sensitive email is protected. Which of the following types of cryptography is being used here for the key exchange?

A. Symmetric
B. Session-based
C. Hashing
D. Asymmetric

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
An IT security manager is asked to provide the total risk to the business. Which of the following calculations would he security manager choose to determine total risk?

A. (Threats X vulnerability X asset value) x controls gap
B. (Threats X vulnerability X profit) x asset value
C. Threats X vulnerability X control gap
D. Threats X vulnerability X asset value

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Joe a company's new security specialist is assigned a role to conduct monthly vulnerability scans across the network. He notices that the scanner is returning a large amount of false positives or failed audits. Which of the following should Joe recommend to remediate these issues?

A. Ensure the vulnerability scanner is located in a segmented VLAN that has access to the company's servers
B. Ensure the vulnerability scanner is configure to authenticate with a privileged account
C. Ensure the vulnerability scanner is attempting to exploit the weaknesses it discovers
D. Ensure the vulnerability scanner is conducting antivirus scanning

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A user reports being unable to access a file on a network share. The security administrator determines that the file is marked as confidential and that the user does not have the appropriate access level for that file. Which of the following is being implemented?

A. Mandatory access control
B. Discretionary access control
C. Rule based access control
D. Role based access control

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A large corporation has data centers geographically distributed across multiple continents. The company needs to securely transfer large amounts of data between the data center. The data transfer can be accomplished physically or electronically, but must prevent eavesdropping while the data is on transit. Which of the following represents the BEST cryptographic solution?

A. Driving a van full of Micro SD cards from data center to data center to transfer data
B. Exchanging VPN keys between each data center vs an SSL connection and transferring the data in the VPN
C. Using a courier to deliver symmetric VPN keys to each data center and transferring data in the VPN
D. Using PKI to encrypt each file and transferring them via an Internet based FTP or cloud server

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
An administrator has two servers and wants them to communicate with each other using a secure algorithm. Which of the following choose to provide both CRC integrity checks and RCA encryption?

A. NTLM
B. RSA
C. CHAP
D. ECDHE

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A small company has recently purchased cell phones for managers to use while working outside if the office. The company does not currently have a budget for mobile device management and is primarily concerned with deterring leaks if sensitive information obtained by unauthorized access to unattended phones. Which of the following would provide the solution BEST meets the company's requirements?

A. Screen-lock

B. Disable removable storage
C. Full device encryption
D. Remote wiping

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
The administrator receives a call from an employee named Joe. Joe says the Internet is down and he is receiving a blank page when typing to connect to a popular sports website. The administrator asks Joe to try visiting a popular search engine site, which Joe reports as successful. Joe then says that he can get to the sports site on this phone. Which of the following might the administrator need to configure?

A. The access rules on the IDS
B. The pop up blocker in the employee's browser
C. The sensitivity level of the spam filter
D. The default block page on the URL filter

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
After reviewing the firewall logs of her organization's wireless Aps, Ann discovers an unusually high amount of failed authentication attempts in a particular segment of the building. She remembers that a new business moved into the office space across the street. Which of the following would be the BEST option to begin addressing the issue?

A. Reduce the power level of the AP on the network segment
B. Implement MAC filtering on the AP of the affected segment
C. Perform a site survey to see what has changed on the segment
D. Change the WPA2 encryption key of the AP in the affected segment

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A security administrator looking through IDS logs notices the following entry: (where email=joe@joe.com and passwd= ` or 1==1') Which of the following attacks had the administrator discovered?

A. SQL injection
B. XML injection
C. Cross-site script
D. Header manipulation

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A security administrator must implement a wireless security system, which will require users to enter a 30 character ASCII password on their clients. Additionally the system must support 3DS wireless encryption. Which of the following should be implemented?

A. WPA2-CCMP with 802.1X
B. WPA2-PSK
C. WPA2-CCMP
D. WPA2-Enterprise

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

Ann a technician received a spear-phishing email asking her to update her personal information by clicking the link within the body of the email. Which of the following type of training would prevent Ann and other employees from becoming victims to such attacks?

A. User Awareness
B. Acceptable Use Policy
C. Personal Identifiable Information
D. Information Sharing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
A company wants to ensure that all aspects if data are protected when sending to other sites within the enterprise. Which of the following would ensure some type of encryption is performed while data is in transit?

A. SSH
B. SHA1
C. TPM
D. MD5

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A database administrator would like to start encrypting database exports stored on the SAN, but the storage administrator warms that this may drastically increase the amount of disk space used by the exports. Which of the following explains the reason for the increase in disk space usage?

A. Deduplication is not compatible with encryption
B. The exports are being stored on smaller SAS drives
C. Encrypted files are much larger than unencrypted files
D. The SAN already uses encryption at rest

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

The Chief Information Officer (CIO) receives an anonymous threatening message that says "beware of the 1st of the year". The CIO suspects the message may be from a former disgruntled employee planning an attack. Which of the following should the CIO be concerned with?

A. Smurf Attack
B. Trojan
C. Logic bomb
D. Virus

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26

Joe Has read and write access to his own home directory. Joe and Ann are collaborating on a project, and Joe would like to give Ann write access to one particular file in this home directory. Which of the following types of access control would this reflect?

A. Role-based access control
B. Rule-based access control
C. Mandatory access control

D. Discretionary access control

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following attacks could be used to initiate a subsequent man-in-the-middle attack?

A. ARP poisoning
B. DoS
C. Replay
D. Brute force

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following can only be mitigated through the use of technical controls rather that user security training?

A. Shoulder surfing
B. Zero-day
C. Vishing
D. Trojans

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Ann an employee is visiting Joe, an employee in the Human Resources Department. While talking to Joe, Ann notices a spreadsheet open on Joe's computer that lists the salaries of all employees in her department. Which of the following forms of social engineering would BEST describe this situation?

A. Impersonation
B. Dumpster diving
C. Tailgating
D. Shoulder surfing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
The Chief Technology Officer (CTO) wants to improve security surrounding storage of customer passwords. The company currently stores passwords as SHA hashes. Which of the following can the CTO implement requiring the LEAST change to existing systems?

A. Smart cards
B. TOTP
C. Key stretching
D. Asymmetric keys

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following protocols provides for mutual authentication of the client and server?

A. Two-factor authentication
B. Radius
C. Secure LDAP
D. Biometrics

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following types of risk reducing policies also has the added indirect benefit of cross training employees when implemented?

A. Least privilege
B. Job rotation
C. Mandatory vacations
D. Separation of duties

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A software developer utilizes cryptographic functions to generate codes that verify message integrity. Due to the nature if the data that is being sent back and forth from the client application to the server, the developer would like to change the cryptographic function to one that verities both authentication and message integrity. Which of the following algorithms should the software developer utilize?

A. HMAC
B. SHA
C. Two Fish
D. RIPEMD

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
An administrator would like to review the effectiveness of existing security in the enterprise. Which of the following would be the BEST place to start?

A. Review past security incidents and their resolution
B. Rewrite the existing security policy
C. Implement an intrusion prevention system
D. Install honeypot systems

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
A new virtual server was created for the marketing department. The server was installed on an existing host machine. Users in the marketing department report that they are unable to connect to the server. Technicians verify that the server has an IP address in the same VLAN as the marketing department users. Which of the following is the MOST likely reason the users are unable to connect to the server?

A. The new virtual server's MAC address was not added to the ACL on the switch
B. The new virtual server's MAC address triggered a port security violation on the switch
C. The new virtual server's MAC address triggered an implicit deny in the switch
D. The new virtual server's MAC address was not added to the firewall rules on the switch

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Users have been reporting that their wireless access point is not functioning. They state that it allows slow connections to the internet, but does not provide access to the internal network. The user provides the SSID and the technician logs into the company's access point and finds no issues. Which of the following should the technician do?

A. Change the access point from WPA2 to WEP to determine if the encryption is too strong

B. Clear all access logs from the AP to provide an up-to-date access list of connected users
C. Check the MAC address of the AP to which the users are connecting to determine if it is an imposter
D. Reconfigure the access point so that it is blocking all inbound and outbound traffic as a troubleshooting gap

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A new security analyst is given the task of determining whether any of the company's server are vulnerable to a recently discovered attack on an old version of SHH. Which of the following is the quickest FIRST step toward determining the version of SSH running on these servers?

A. Passive scanning
B. Banner grabbing
C. Protocol analysis
D. Penetration testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A network inventory discovery application requires non-privileged access to all hosts on a network for inventory of installed applications. A service account is created to be by the network inventory discovery application for accessing all hosts. Which of the following is the MOST efficient method for granting the account non-privileged access to the hosts?

A. Implement Group Policy to add the account to the users group on the hosts
B. Add the account to the Domain Administrator group
C. Add the account to the Users group on the hosts
D. Implement Group Policy to add the account to the Power Users group on the hosts.

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 39
When designing a corporate NAC solution, which of the following is the MOST relevant integration issue?

A. Infrastructure time sync
B. End user mobility
C. 802.1X supplicant compatibility
D. Network Latency
E. Network Zoning

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following access methods uses radio frequency waves for authentication?

A. Video surveillance
B. Mantraps
C. Proximity readers
D. Biometrics

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following authentication methods can use the SCTP and TLS protocols for reliable packet transmissions?

A. TACACS+
B. SAML
C. Diameter
D. Kerberos

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following authentication protocols makes use of UDP for its services?

A. RADIUS
B. TACACS+
C. LDAP
D. XTACACS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is considered a risk management BEST practice of succession planning?

A. Reducing risk of critical information being known to an individual person who may leave the organization
B. Implementing company-wide disaster recovery and business continuity plans
C. Providing career advancement opportunities to junior staff which reduces the possibility of insider threats
D. Considering departmental risk management practices in place of company-wide practices

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following is the BEST technology for the sender to use in order to secure the in-band exchange of a shared key?

A. Steganography
B. Hashing algorithm
C. Asymmetric cryptography
D. Steam cipher

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following design components is used to isolate network devices such as web servers?

A. VLAN
B. VPN
C. NAT
D. DMZ

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following is MOST critical in protecting control systems that cannot be regularly patched?

A. Asset inventory
B. Full disk encryption

C. Vulnerability scanning
D. Network segmentation

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Identifying residual is MOST important to which of the following concepts?

A. Risk deterrence
B. Risk acceptance
C. Risk mitigation
D. Risk avoidance

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is replayed during wireless authentication to exploit a weak key infrastructure?

A. Preshared keys
B. Ticket exchange
C. Initialization vectors
D. Certificate exchange

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following steps of incident response does a team analyze the incident and determine steps to prevent a future occurrence?

A. Mitigation
B. Identification
C. Preparation
D. Lessons learned

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A technician wants to secure communication to the corporate web portal, which is currently using HTTP. Which of the following is the FIRST step the technician should take?

A. Send the server's public key to the CA
B. Install the CA certificate on the server
C. Import the certificate revocation list into the server
D. Generate a certificate request from the server

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
An organization has a need for security control that identifies when an organizational system has been unplugged and a rouge system has been plugged in. The security control must also provide the ability to supply automated notifications. Which of the following would allow the organization to BEST meet this business requirement?

A. MAC filtering
B. ACL

C. SNMP
D. Port security

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Internet banking customers currently use an account number and password to access their online accounts. The bank wants to improve security on high value transfers by implementing a system which call users back on a mobile phone to authenticate the transaction with voice verification. Which of the following authentication factors are being used by the bank?

A. Something you know, something you do, and something you have
B. Something you do, somewhere you are, and something you have
C. Something you are, something you do and something you know
D. Something you have, something you are, and something you know

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
A security administrator has concerns that employees are installing unapproved applications on their company provide smartphones. Which of the following would BEST mitigate this?

A. Implement remote wiping user acceptance policies
B. Disable removable storage capabilities
C. Implement an application whitelist
D. Disable the built-in web browsers

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
The security manager must store a copy of a sensitive document and needs to verify at a later point that the document has not been altered. Which of the following will accomplish the security managers objective?

A. RSA
B. AES
C. MD5
D. SHA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A security Operations Center was scanning a subnet for infections and found a contaminated machine. One of the administrators disabled the switch port that the machine was connected to, and informed a local technician of the infection. Which of the following steps did the administrator perform?

A. Escalation
B. Identification
C. Notification
D. Quarantine
E. Preparation

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A security administrator wants to block unauthorized access to a web server using a locally installed software program. Which of the following should the

administrator deploy?

A. NIDS
B. HIPS
C. NIPS
D. HIDS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
A network administrator has identified port 21 being open and the lack of an IDS as a potential risk to the company. Due to budget constraints, FTP is the only option that the company can is to transfer data and network equipment cannot be purchased. Which of the following is this known as?

A. Risk transference
B. Risk deterrence
C. Risk acceptance
D. Risk avoidance

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58

A security administrator is investigating a recent server breach. The breach occurred as a result of a zero-day attack against a user program running on the server. Which of the following logs should the administrator search for information regarding the breach?

A. Application log
B. Setup log
C. Authentication log
D. System log

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A user attempts to install a new and relatively unknown software recommended by a colleague. The user is unable to install the program, despite having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?

A. Application black listing
B. Network Intrusion Prevention System
C. Group policy
D. Application white listing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A system administrator is configuring shared secrets on servers and clients. Which of the following authentication services is being deployed by the administrator? (Select TWO)

A. Kerberos
B. RADIUS
C. TACACS+
D. LDAP

E. Secure LDAP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
The finance department just procured a software application that needs to communicate back to the vendor server via SSL. Which of the following default ports on the firewall must the security engineer open to accomplish this task?

A. 80
B. 130
C. 443
D. 3389

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
After an audit, it was discovered that an account was not disabled in a timely manner after an employee has departed from the organization. Which of the following did the organization fail to properly implement?

A. Routine account audits
B. Account management processes
C. Change management processes
D. User rights and permission reviews

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
The Chief Security Officer (CSO) for a datacenter in a hostile environment is concerned about protecting the facility from car bomb attacks. Which of the following BEST would protect the building from this threat? (Select TWO)

A. Dogs
B. Fencing
C. CCTV
D. Guards
E. Bollards
F. Lighting

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Users can authenticate to a company's web applications using their credentials form a popular social media site. Which of the following poses the greatest risk with this integration?

A. Malicious users can exploit local corporate credentials with their social media credentials
B. Changes to passwords on the social media site can be delayed from replicating to the company
C. Data loss from the corporate servers can create legal liabilities with the social media site
D. Password breaches to the social media affect the company application as well

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A corporation has experienced several media leaks of proprietary data on various web forums. The posts were made during business hours and it is believed that the culprit is posting during work hours from a corporate machine. The Chief Information Officer (CIO) wants to scan internet traffic and keep records for later use in

legal proceedings once the culprit is found. Which of the following provides the BEST solution?

A. Protocol analyzer
B. NIPS
C. Proxy server
D. HIDS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
The security administrator runs an rpm verify command which records the MD5 sum, permissions, and timestamp of each file on the system. The administrator saves this information to a separate server. Which of the following describes the procedure the administrator has performed?

A. Host software base-lining
B. File snapshot collection
C. TPM
D. ROMDB verification

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Users are trying to communicate with a network but are unable to do so. A network administrator sees connection attempts on port 20 from outside IP addresses that are being blocked. How can the administrator resolve this?

A. Enable stateful FTP on the firewall
B. Enable inbound SSH connections
C. Enable NETBIOS connections in the firewall
D. Enable HTTPS on port 20

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
In order to enter a high-security datacenter, users are required to speak the password into a voice recognition system. Ann a member if the sales department over hears the password and upon speaks it into the system The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?

A. An authentication factor
B. Discretionary access
C. Time of day restrictions
D. Least privilege restrictions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Given the following list of corporate access points, which of the following attacks is MOST likely underway if the company wireless network uses the same wireless hardware throughout?

MAC SID
00:01:AB:FA:CD:34 Corporate AP
00:01:AB:FA:CD:35 Corporate AP
00:01:AB:FA:CD:36 Corporate AP
00:01:AB:FA:CD:37 Corporate AP
00:01:AB:FA:CD:34 Corporate AP

A. Packet sniffing
B. Evil Twin
C. WPS attack
D. Rogue access point

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A system administrator has noticed network performance issues and wants to gather performance data from the gateway router. Which of the following can be used to perform this action?

A. SMTP
B. iSCSI
C. SNMP
D. IPSec

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following technologies was developed to allow companies to use less-expensive storage while still maintaining the speed and redundancy required in a business environment?

A. RAID
B. Tape Backup
C. Load Balancing
D. Clustering

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
An employee needs to connect to a server using a secure protocol on the default port. Which of the following ports should be used?

A. 21
B. 22
C. 80
D. 110

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following is replayed during wireless authentication to exploit a weal key infrastructure?

A. Preshared keys
B. Ticket exchange
C. Initialization vectors
D. Certificate exchange

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A new security policy being implemented requires all email within the organization be digitally signed by the author using PGP. Which of the following would needs to be created for each user?

A. A certificate authority
B. A key escrow
C. A trusted key
D. A public and private key

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following authentication provides users XML for authorization and authentication?

A. Kerberos
B. LDAP
C. RADIUS
D. SAML

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A company wants to prevent end users from plugging unapproved smartphones into PCs and transferring data. Which of the following would be the BEST control to implement?

A. MDM
B. IDS
C. DLP
D. HIPS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77

The ore-sales engineering team needs to quickly provide accurate and up-to-date information to potential clients. This information includes design specifications and engineering data that is developed and stored using numerous applications across the enterprise. Which of the following authentication technique is MOST appropriate?

A. Common access cards
B. TOTP
C. Single sign-on
D. HOTP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
After a security incident involving a physical asset, which of the following should be done at the beginning?

A. Record every person who was in possession of assets, continuing post-incident
B. Create working images of data in the following order , hard drive then RAM
C. Back up storage devices so work can be performed on the devices immediately
D. Write a report detailing the incident and mitigation suggestions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
A network engineer is configuring a VPN tunnel connecting a company's network to a business partner. Which of the following protocols should be used for key exchange?

A. SHA-1
B. RC4
C. Blowfish
D. Diffie-Hellman

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following types of cloud computing would be MOST appropriate if an organization required complete control of the environment?

A. Hybrid Cloud
B. Private cloud
C. Community cloud
D. Community cloud
E. Public cloud

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
The database server used by the payroll system crashed at 3 PM and payroll is due at 5 PM. Which of the following metrics is MOST important is this instance?

A. ARO
B. SLE
C. MTTR
D. MTBF

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following is an attack designed to activate based on time?

A. Logic Bomb
B. Backdoor
C. Trojan
D. Rootkit

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A network security engineer notices unusual traffic on the network from a single IP attempting to access systems on port 23. Port 23 is not used anywhere on the network. Which of the following should the engineer do to harden the network from this type of intrusion in the future?

A. Disable unnecessary services on servers
B. Disable unused accounts on servers and network devices
C. Implement password requirements on servers and network devices
D. Enable auditing on event logs

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following documents outlines the responsibility of both participants in an agreement between two organizations?

A. RFC
B. MOU
C. RFQ
D. SLA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Users in the HR department were recently informed that they need to implement a user training and awareness program which is tailored to their department.
Which of the following types of training would be the MOST appropriate for this department?

A. Handing PII
B. Risk mitigation
C. Input validation
D. Hashing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following incident response plan steps would MOST likely engaging business professionals with the security team to discuss changes to existing procedures?

A. Recovery
B. Incident identification
C. Isolation / quarantine
D. Lessons learned
E. Reporting

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
A company is starting to allow employees to use their own personal without centralized management. Employees must contract IT to have their devices configured to use corporate email; access is also available to the corporate cloud-based services. Which of the following is the BEST policy to implement under these circumstances?

A. Acceptable use policy
B. Security policy
C. Group policy
D. Business Agreement policy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following BEST explains Platform as a Service?

A. An external entity that provides a physical or virtual instance of an installed operating system
B. A third party vendor supplying support services to maintain physical platforms and servers
C. An external group providing operating systems installed on virtual servers with web applications
D. An internal group providing physical server instances without installed operating systems or support

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
One of the senior managers at a company called the help desk to report to report a problem. The manager could no longer access data on a laptop equipped with FDE. The manager requested that the FDE be removed and the laptop restored from a backup. The help desk informed the manager that the recommended solution was to decrypt the hard drive prior to reinstallation and recovery. The senior manager did not have a copy of the private key associated with the FDE on the laptop. Which of the following tools or techniques did the help desk use to avoid losing the data on the laptop?

A. Public key
B. Recovery agent
C. Registration details
D. Trust Model

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
An employee in the accounting department recently received a phishing email that instructed them to click a link in the email to view an important message from the IRS which threatened penalties if a response was not received by the end of the business day. The employee clicked on the link and the machine was infected with malware. Which of the following principles BEST describes why this social engineering ploy was successful?

A. Scarcity
B. Familiarity
C. Social proof
D. Urgency

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A security technician received notification of a remotely exploitable vulnerability affecting all multifunction printers firmware installed throughout the organization. The vulnerability allows a malicious user to review all the documents processed by the affected printers. Which of the following compensating controls can the security technician to mitigate the security risk of a sensitive document leak?

A. Create a separate printer network
B. Perform penetration testing to rule out false positives
C. Install patches on the print server
D. Run a full vulnerability scan of all the printers

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A systems administrator has made several unauthorized changes to the server cluster that resulted in a major outage. This event has been brought to the attention of the Chief Information Office (CIO) and he has requested immediately implement a risk mitigation strategy to prevent this type of event from reoccurring. Which of the following would be the BEST risk mitigation strategy to implement in order to meet this request?

A. Asset Management
B. Change Management
C. Configuration Management
D. Incident Management

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
AN incident occurred when an outside attacker was able to gain access to network resources. During the incident response, investigation security logs indicated multiple failed login attempts for a network administrator. Which of the following controls, if in place could have BEST prevented this successful attack?

A. Password history
B. Password complexity
C. Account lockout
D. Account expiration

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Joe needs to track employees who log into a confidential database and edit files. In the past, critical files have been edited, and no one admits to making the edits. Which of the following does Joe need to implement in order to enforce accountability?

A. Non-repudiation
B. Fault tolerance
C. Hashing
D. Redundancy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A new mobile banking application is being developed and uses SSL / TLS certificates but penetration tests show that it is still vulnerable to man-in-the-middle attacks, such as DNS hijacking. Which of the following would mitigate this attack?

A. Certificate revocation
B. Key escrow
C. Public key infrastructure
D. Certificate pinning

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
One month after a software developer was terminated the helpdesk started receiving calls that several employees computers were being infected with malware. Upon further research, it was determined that these employees had downloaded a shopping toolbar. It was this toolbar that downloaded and installed the errant code. Which of the following attacks has taken place?

A. Logic bomb

B. Cross-site scripting
C. SQL injection
D. Malicious add-on

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following would an attacker use to penetrate and capture additional traffic prior to performing an IV attack?

A. DNS poisoning
B. DDoS
C. Replay attack
D. Dictionary attacks

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
An administrator has concerns regarding the company's server rooms Proximity badge readers were installed, but it is discovered this is not preventing unapproved personnel from tailgating into these area. Which of the following would BEST address this concern?

A. Replace proximity readers with turn0based key locks
B. Install man-traps at each restricted area entrance
C. Configure alarms to alert security when the areas are accessed
D. Install monitoring cameras at each entrance

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following would be a reason for developers to utilize an AES cipher in CCM mode (Counter with Chain Block Message Authentication Code)?

A. It enables the ability to reverse the encryption with a separate key
B. It allows for one time pad inclusions with the passphrase
C. Counter mode alternates between synchronous and asynchronous encryption
D. It allows a block cipher to function as a steam cipher

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
one of the findings of risk assessment is that many of the servers on the data center subnet contain data that is in scope for PCI compliance, Everyone in the company has access to these servers, regardless of their job function. Which of the following should the administrator do?

A. Segment the network
B. Use 802.1X
C. Deploy a proxy sever
D. Configure ACLs
E. Write an acceptable use policy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Various employees have lost valuable customer data due to hard drives failing in company provided laptops. It has been discovered that the hard drives used in one model of laptops provided by the company has been recalled by the manufactory, The help desk is only able to replace the hard drives after they fail because there is no centralized records of the model of laptop given to each specific user. Which of the following could have prevented this situation from occurring?

A. Data backups
B. Asset tracking
C. Support ownership
D. BYOD policies

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Attempting to inject 50 alphanumeric key strokes including spaces into an application input field that only expects four alpha characters in considered which of the following attacks?

A. XML injection
B. Buffer overflow
C. LDAP Injection
D. SQL injection

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
An organization is required to log all user internet activity. Which of the following would accomplish this requirement?

A. Configure an access list on the default gateway router. Configure the default gateway router to log all web traffic to a syslog server
B. Configure a firewall on the internal network. On the client IP address configuration, use the IP address of the firewall as the default gateway, configure the firewall to log all traffic to a syslog server
C. Configure a proxy server on the internal network and configure the proxy server to log all web traffic to a syslog server
D. Configure an access list on the core switch, configure the core switch to log all web traffic to a syslog server

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
An agent wants to create fast and efficient cryptographic keys to use with Diffie-Hellman without using prime numbers to generate the keys. Which of the following should be used?

A. Elliptic curve cryptography
B. Quantum cryptography
C. Public key cryptography
D. Symmetric cryptography

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Joe an application developer is building an external facing marketing site. There is an area on the page where clients may submit their feedback to articles that are posted. Joe filters client-side JAVA input. Which of the following is Joe attempting to prevent?

A. SQL injections
B. Watering holes
C. Cross site scripting
D. Pharming

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106

A video surveillance audit recently uncovered that an employee plugged in a personal laptop and used the corporate network to browse inappropriate and potentially malicious websites after office hours. Which of the following could BEST prevent a situation like this form occurring again?

A. Intrusion detection
B. Content filtering
C. Port security
D. Vulnerability scanning

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A server administrator notes that a fully patched application often stops running due to a memory error. When reviewing the debugging logs they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describes?

A. Malicious add-on
B. SQL injection
C. Cross site scripting
D. Zero-day

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A resent OS patch caused an extended outage. It took the IT department several hours to uncover the cause of the issue due to the system owner who installed the patch being out of the office. Which of the following could help reduce the likelihood of this situation occurring in the future?

A. Separation of duties
B. Change management procedures
C. Incident management procedures
D. User rights audits and reviews

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
The Chief Information Security Officer (CISO) is concerned that users could bring their personal laptops to work and plug them directly into the network port under their desk. Which of the following should be configured on the network switch to prevent this from happening?

A. Access control lists
B. Loop protection
C. Firewall rule
D. Port security

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Ann a network administrator has been tasked with strengthening the authentication of users logging into systems in area containing sensitive information. Users log in with usernames and passwords, following by a retinal scan. Which of the following could she implement to add an additional factor of authorization?

A. Requiring PII usage
B. Fingerprint scanner
C. Magnetic swipe cards

D. Complex passphrases

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
In an environment where availability is critical such as Industrial control and SCADA networks, which of the following technologies in the MOST critical layer of defense for such systems?

A. Log consolidation
B. Intrusion Prevention system
C. Automated patch deployment
D. Antivirus software

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A security manager installed a standalone fingerprint reader at the data center. All employees that need to access the data center have been enrolled to the reader and local reader database is always kept updates. When an employee who has been enrolled uses the fingerprint reader the door to the data center opens. Which of the following does this demonstrate? (Select THREE)

A. Two-factor authentication
B. Single sign-on
C. Something you have
D. Identification
E. Authentication
F. Authorization

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 113
A network technician is configuring clients for VLAN access. The network address for the sales department is 192.168.0.64 with a broadcast address of 192.168.0.71 Which of the following IP address/subnet mask combinations could be used to correctly configure a client machine in the sales department?

A. 192.168.0.64/29
B. 192.168.0.66/27
C. 192.168.0.67/29
D. 192.168.0.70/28

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
The help desk is experiencing a higher than normal amount of calls from users reporting slow response from the application server. After analyzing the data from a packet capturing tool, the head of the network engineering department determines that the issue is due, in part from the increase of personnel recently hired to perform application development. Which of the following would BEST assist in correcting this issue?

A. Load balancer
B. Spam filter
C. VPN Concentrator
D. NIDS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Two organizations want to share sensitive data with one another from their IT systems to support a mutual customer base. Both organizations currently have secure

network and security policies and procedures. Which of the following should be the PRIMARY security considerations by the security managers at each organization prior to sharing information? (Select THREE)

A. Physical security controls
B. Device encryption
C. Outboarding/Offboarding
D. Use of digital signatures
E. SLA/ISA
F. Data ownership
G. Use of smartcards or common access cards
H. Patch management

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw. Which of the following attacks has MOST likely occurred?

A. Cookie stealing
B. Zero-day
C. Directory Traversal
D. XML injection

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
A company's password and authentication policies prohibit the use of shared passwords and transitive trust. Which of the following if implemented would violate company policy? (Select TWO)

A. Discretionary access control
B. Federation
C. Single sign-on
D. TOTP
E. Two-factor authentication

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following types of attacks is based on coordinating small slices of a task across multiple systems?

A. DDos
B. Spam
C. Spoofing
D. Dos

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Which of the following authentication provides users XML for authorization and authentication?

A. Kerberos
B. LDAP
C. RADIUS
D. SAML

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
A system security analyst wants to capture data flowing in and out of the enterprise. Which of the following would MOST likely help in achieving this goal?

A. Taking screenshots
B. Analyzing Big Data metadata
C. Analyzing network traffic and logs
D. Capturing system image

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
The security manager reports that the process of revoking certificates authority is too slow and should be automated. Which of the following should be used to automate this process?

A. CRL
B. GPG
C. OCSP
D. Key escrow

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A user attempts to install a new and relatively unknown software program recommended by a colleague. The user is unable to install the program, dispute having

successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?

A. Application black listing
B. Network Intrusion Prevention System
C. Group Policy
D. Application White Listing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
A company needs to provide web-based access to shared data sets to mobile users, while maintaining a standardized set of security controls. Which of the following technologies is the MOST appropriate storage?

A. Encrypted external hard drives
B. Cloud storage
C. Encrypted mobile devices
D. Storage Area Network

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
An employee's mobile device associates with the company's guest WiFi SSID, but then is unable to retrieve email. The email settings appear to be correct. Which of the following is the MOST likely cause?

A. The employee has set the network type to WPA instead of WPA2
B. The network uses a captive portal and requires a web authentication
C. The administrator has blocked the use of the personal hot spot feature
D. The mobile device has been placed in airplane mode

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A malicious individual used an unattended customer service kiosk in a busy store to change the prices of several products. The alteration was not noticed until several days later and resulted in the loss of several thousand dollars for the store. Which of the following would BEST prevent this from occurring again?

A. Password expiration
B. Screen locks
C. Inventory control
D. Asset tracking

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
In order to enter a high-security data center, users are required to speak the correct password into a voice recognition system, Ann a member of the sales department, overhears the password and later speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?

A. An authentication factor
B. Discretionary Access
C. Time of Day Restrictions
D. Least Privilege Restrictions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
A company requires that all users enroll in the corporate PKI structure and digitally sign all emails. Which of the following are primary reasons to sign emails with digital certificates? (Select TWO)

A. To establish non-repudiation
B. To ensure integrity
C. To prevent SPAM
D. To establish data loss prevention
E. To protect confidentiality
F. To establish transport encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
The help desk is experiencing a higher than normal amount of calls from users reporting slow response from the application server. After analyzing the data from a packet capturing tool, the head of the network engineering department determines that the issue is due in part from the increase of personnel recently hired to perform application development. Which of the following would BEST assist in correcting this issue?

A. Load Balancer
B. Spam Filter
C. VPN Concentrator
D. NIDS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
The security manager must store a copy of a sensitive document and needs to verify at a later point in time that the document has not been altered. Which of the following with accomplish the security manager's objective?

A. RSA
B. AES
C. MD5
D. SHA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
The Chief Information Officer (CIO) has asked a security analyst to determine the estimated costs associated with each potential breach of their database that contains customer information. Which of the following is the risk calculation that the CIO is asking for?

A. Impact
B. SLE
C. ARO
D. ALE

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
A security assurance officer is preparing a plan to measure the technical state of a customer's enterprise. The testers employed to perform the audit will be given access to the customer facility and network. The testers will not be given access to the details of custom developed software used by the customer. However the testers with have access to the source code for several open source applications and pieces of networking equipment used at the facility, but these items will not be within the scope of the audit. Which of the following BEST describes the appropriate method of testing or technique to use in this scenario? (Select TWO)

A. Social engineering
B. All source
C. Black box
D. Memory dumping

E. Penetration

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following authentication services combines authentication and authorization in a use profile and use UDP?

A. LDAP
B. Kerberos
C. TACACS+
D. RADIUS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
A security administrator is designing an access control system, with an unlimited budget, to allow authenticated users access to network resources. Given that a multifactor authentication solution is more secure, which of the following is the BEST combination of factors?

A. Retina scanner, thumbprint scanner, and password
B. Username and password combo, voice recognition scanner, and retina scanner
C. Password, retina scanner, and proximity reader
D. One-time password pad, palm-print scanner, and proximity photo badges

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
A network administrator is responsible for securing applications against external attacks. Every month, the underlying operating system is updated. There is no process in place for other software updates. Which of the following processes could MOST effectively mitigate these risks?

A. Application hardening
B. Application change management
C. Application patch management
D. Application firewall review

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Which of the following technologies was developed to allow companies to use less-expensive storage while still maintaining the speed and redundancy required in a business environment?

A. RAID
B. Tape Backup
C. Load balancing
D. Clustering

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
The access control list (ACL) for a file on a server is as follows:

User: rwx
User: Ann: r- -
User: Joe: r- -
Group: rwx

Group: sales: r-x
Other: r-x
Joe and Ann are members of the Human Resources group. Will Ann and Joe be able to run the file?

A. No since Ann and Joe are members of the Sales group owner of the file
B. Yes since the regular permissions override the ACL for the file
C. No since the ACL overrides the regular permissions for the file
D. Yes since the regular permissions and the ACL combine to create the effective permissions on the file

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Using a protocol analyzer, a security consultant was able to capture employees credentials. Which of the following should the consultant recommend to the company, in order to mitigate the risk of employees credentials being captured in the same manner in the future?

A. Wiping of remnant data
B. Hashing and encryption of data in-use
C. Encryption of data in-transit
D. Hashing of data at-rest

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A Company has recently identified critical systems that support business operations. Which of the following will once defined, be the requirement for restoration of these systems within a certain period of time?

A. Mean Time Between Failure
B. Mean Time to Restore
C. Recovery Point Objective

D. Recovery Time Objective

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
The software developer is responsible for writing the code and promoting from the development network to the quality network. The network administrator is responsible for promoting code to the application servers. Which of the following practices are they following to ensure application integrity?

A. Job rotation
B. Implicit deny
C. Least privilege
D. Separation of duties

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Ann is traveling for business and is attempting to use the hotel's wireless network to check for new messages. She selects the hotel's wireless SSID from a list of networks and successfully connects. After opening her email client and waiting a few minutes, the connection times out. Which of the following should Ann do to retrieve her email messages?

A. Change the authentication method for her laptop's wireless card from WEP to WPA2
B. Open a web browser and authenticate using the captive portal for the hotel's wireless network
C. Contact the front desk and have the MAC address of her laptop added to the MAC filter on the hotel's wireless network
D. Change the incoming email protocol from IMAP to POP3

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Which of the following password attacks involves attempting all kinds of keystroke combinations on the keyboard with the intention to gain administrative access?

A. Dictionary
B. Hybrid
C. Watering hole
D. Brute Force

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Ann a security administrator is strengthening the security controls of the company's campus. Her goal is to prevent people from accessing open locations that are not supervised, such as around the receiving dock. She is also concerned that employees are using these entry points as a way of bypassing the security guard at the main entrance. Which of the following should Ann recommend that would BEST address her concerns?

A. Increase the lighting surrounding every building on campus
B. Build fences around campus with gate entrances
C. Install cameras to monitor the unsupervised areas
D. Construct bollards to prevent vehicle entry in non-supervised areas

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
While an Internet cafй a malicious user is causing all surrounding wireless connected devices to have intermittent and unstable connections to the access point. Which of the following is MOST likely being used?

A. Evil Twin
B. Interference
C. Packet sniffer
D. Rogue AP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
A password audit has revealed that a significant percentage if end-users has passwords that are easily cracked. Which of the following is the BEST technical control that could be implemented to reduce the amount of easily " crackable" passwords in use?

A. Credential management
B. Password history
C. Password complexity
D. Security awareness training

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
While working on a new project a security administrator wants to verify the integrity of the data in the organizations archive library. Which of the following is the MOST secure combination to implement to meet this goal? (Select TWO)

A. Hash with SHA
B. Encrypt with Diffie-Hellman
C. Hash with MD5
D. Hash with RIPEMD
E. Encrypt with AES

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
A company has been attacked and their website has been altered to display false information. The security administrator disables the web server service before restoring the website from backup. An audit was performed on the server and no other data was altered. Which of the following should be performed after the server has been restored?

A. Monitor all logs for the attacker's IP
B. Block port 443 on the web server
C. Install and configure SSL to be used on the web server
D. Configure the web server to be in VLAN 0 across the network

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
A security administrator suspects that an employee in the IT department is utilizing a reverse proxy to bypass the company's content filter and browse unapproved and non-work related sites while at work. Which of the following tools could BEST be used to determine how the employee is connecting to the reverse proxy?

A. Port scanner
B. Vulnerability scanner
C. Honeypot
D. Protocol analyzer

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
Joe a company's network engineer is concerned that protocols operating at the application layer of the OSI model are vulnerable to exploitation on the network. Which of the following protocols should he secure?

A. SNMP
B. SSL
C. ICMP
D. NetBIOS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Which of the following attacks could be used to initiate a subsequent man-in-the-middle attack?

A. ARP poisoning
B. DoS
C. Replay
D. Brute force

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
Ann a security technician receives a report from a user that is unable to access an offsite SSN server. Ann checks the firewall and see the following rules:

Allow TCP 80
Allow TCP 443
Deny TCP 23
Deny TCP 20
Deny TCP 21

Which of the following is preventing the users from accessing the SSH server?

A. Deny TCP 20
B. Deny TCP 21
C. Deny TCP 23
D. Implicit deny

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
An administrator uses a server with a trusted OS and is configuring an application to go into production tomorrow, In order to make a new application work properly, the administrator creates a new policy that labels the application and assigns it a security context within the trusted OS. Which of the following control methods is the administrator using by configuring this policy?

A. Time based access control
B. Mandatory access control
C. Role based access control
D. Rule based access control

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A security administrator has been tasked with assisting in the forensic investigation of an incident relating to employee misconduct. The employee's supervisor believes evidence of this ,misconduct can be found on the employee's assigned workstation. Which of the following choices BEST describes what should be done? (Select TWO)

A. Record time as offset as required and conduct a timeline analysis
B. Update antivirus definitions and conduct a full scan for infected files
C. Analyze network traffic, system, and file logs

D. Create an additional local admin account on that workstation to conduct work from

E. Delete other user profiles on the system to help narrow down the search space

F. Patch the system before reconnecting it to the network

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153

Joe a web developer wants to make sure his application is not susceptible to cross-site request forgery attacks. Which of the following is one way to prevent this type of attack?

A. The application should always check the HTTP referrer header

B. The application should always check the HTTP Request header

C. The application should always check the HTTP Host header

D. The application should always use SSL encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154

A security technician has been tasked with opening ports on a firewall to allow users to browse the internet. Which of the following ports should be opened on the firewall? (Select Three)

A. 22

B. 53

C. 80

D. 110

E. 443

F. 445

G. 8080

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
A rogue programmer included a piece of code in an application to cause the program to halt at 2:00 PM on Monday afternoon when the application is most utilized. This is Which of the following types of malware?

A. Trojan
B. Virus
C. Logic Bomb
D. Botnets

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
After connecting to the corporate network a user types the URL if a popular social media website in the browser but reports being redirected to a login page with the corporate logo. Which of the following is this an example of?

A. LEAP
B. MAC filtering
C. WPA2-Enterprise
D. Captive portal

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
The Quality Assurance team is testing a third party application. They are primarily testing for defects and have some understanding of how the application works. Which of the following is the team performing?

A. Grey box testing
B. White box testing
C. Penetration testing
D. Black box testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
A user Ann has her assigned token but she forgotten her password. Which of the following appropriately categorizes the authentication factor that will fail in this scenario?

A. Something you do
B. Something you know
C. Something you are
D. Something you have

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
An employee from the fire Marshall's office arrives to inspect the data center, The operator allows him to bypass the multi-factor authentication to enter the data center. Which of the following types of attacks may be underway?

A. Impersonation
B. Hoax

C. Tailgating
D. Spoofing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
A company recently received accreditation for a secure network, In the accreditation letter, the auditor specifies that the company must keep its security plan current with changes in the network and evolve the systems to adapt to new threats. Which of the following security controls will BEST achieve this goal?

A. Change management
B. Group Policy
C. Continuous monitoring
D. Credential management

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A cyber security administrator receives a list of IPs that have been reported as attempting to access the network. To identify any possible successful attempts across the enterprise, which of the following should be implemented?

A. Monitor authentication logs
B. Disable unnecessary accounts
C. Time of day restrictions
D. Separation of duties

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
Which of the following exploits either a host file on a target machine or vulnerabilities on a DNS server in order to carry out URL redirection?

A. Pharming
B. Spoofing
C. Vishing
D. Phishing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Ann a new small business owner decides to implement WiFi access for her customers. There are several other businesses nearby who also have WiFi hot spots. Ann is concerned about security of the wireless network and wants to ensure that only her customers have access. Which of the following choices BEST meets her intent of security and access?

A. Enable port security
B. Enable WPA
C. Disable SSID broadcasting
D. Enable WEP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
A security engineer is tasked with encrypting corporate email. Which of the following technologies provide the MOST complete protection? (Select TWO)

A. PGP/GPG
B. S/MIME
C. IPSEC
D. Secure POP3
E. IMAP
F. HMAC

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
Which of the following is the GREATEST security concern of allowing employees to bring in their personally owned tablets and connecting to the corporate network?

A. Tablet network connections are stored and accessible from the corporate network
B. The company's attack surface increases with the non-corporate devices
C. Personally purchased media may be available on the network for others to stream
D. Encrypted tablets are harder to access to determine if they are infected

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
Searching for systems infected with malware is considered to be which of the following phases of incident response?

A. Containment
B. Preparation
C. Mitigation
D. Identification

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A technician has deployed a new VPN concentrator, The device needs to authenticate users based on a backend directory service, Which of the following services could be run on the VPN concentrator to perform this authentication?

A. Kerberos
B. RADIUS
C. GRE
D. IPSec

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
A webpage displays a potentially offensive advertisement on a computer. A customer walking by notices the displayed advertisement and files complaint. Which of the following can BEST reduce the likelihood of this incident occurring again?

A. Clean-desk policies
B. Screen-locks
C. Pop-up blocker
D. Antispyware software

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
Which of the following is an attack designed to activate based on date?

A. Logic bomb
B. Backdoor
C. Trojan
D. Rootkit

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
A malicious user has collected the following list of information:

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
168.1.5 OpenSSH-Server_5.8

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
168.1.7 OpenSSH-Server_5.7

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
168.1.9 OpenSSH-Server_5.7
Which of the following techniques is MOST likely to gather this type of data?

A. Banner grabbing
B. Port scan
C. Host scan
D. Ping scan

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 174
A company wants to prevent unauthorized access to its secure data center. Which of the following security controls would be MOST appropriate?

A. Alarm to local police
B. Camera
C. Security guard
D. Motion detector

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
Company policy requires employees to change their passwords every 60 days. The security manager has verified all systems are configured to expire passwords after 60 days. Despite the policy and technical configuration, weekly password audits suggest that some employees have had the same weak passwords in place longer than 60 days. Which of the following password parameters is MOST likely misconfigured?

A. Minimum lifetime
B. Complexity
C. Length
D. Maximum lifetime

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
The Chief Technical Officer (CTO) has been informed of a potential fraud committed by a database administrator performing several other job functions within the company. Which of the following is the BEST method to prevent such activities in the future?

A. Job rotation
B. Separation of duties
C. Mandatory Vacations
D. Least Privilege

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
An administrator would like to utilize encryption that has comparable speed and strength to the AES cipher without using AES itself. The cipher should be able to operate in the same modes as AES and utilize the same minimum bit strength. Which of the following algorithms should the administrator select?

A. RC4
B. Rijndael
C. SHA
D. TwoFish
E. 3DES

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A security analyst has a sample of malicious software and needs to know what the sample does. The analyst runs the sample in a carefully-controlled and monitored virtual machine to observe the software's behavior. The approach of malware analysis can BEST be described as:

A. Static testing
B. Security control testing
C. White box testing
D. Sandboxing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Which of the following has a storage root key?

A. HSM
B. EFS
C. TPM
D. TKIP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
A user was reissued a smart card after the previous smart card had expired. The user is able to log into the domain but is now unable to send digitally signed or encrypted email. Which of the following would the user need to perform?

A. Remove all previous smart card certificates from the local certificate store.
B. Publish the new certificates to the global address list.
C. Make the certificates available to the operating system.
D. Recover the previous smart card certificates.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
When creating a public / private key pair, for which of the following ciphers would a user need to specify the key strength?

A. SHA
B. AES
C. DES
D. RSA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Deploying a wildcard certificate is one strategy to:

A. Secure the certificate's private key.
B. Increase the certificate's encryption key length.
C. Extend the renewal date of the certificate.
D. Reduce the certificate management burden.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
A company has several conference rooms with wired network jacks that are used by both employees and guests. Employees need access to internal resources and guests only need access to the Internet. Which of the following combinations is BEST to meet the requirements?

A. NAT and DMZ
B. VPN and IPSec
C. Switches and a firewall
D. 802.1x and VLANs

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Which of the following network design elements allows for many internal devices to share one public IP address?

A. DNAT
B. PAT
C. DNS
D. DMZ

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
A software company has completed a security assessment. The assessment states that the company should implement fencing and lighting around the property. Additionally, the assessment states that production releases of their software should be digitally signed. Given the recommendations, the company was deficient in which of the following core security areas? (Select TWO).

A. Fault tolerance
B. Encryption
C. Availability
D. Integrity
E. Safety
F. Confidentiality

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
A computer is suspected of being compromised by malware. The security analyst examines the computer and finds that a service called Telnet is running and connecting to an external website over port 443. This Telnet service was found by comparing the system's services to the list of standard services on the company's system image. This review process depends on:

A. MAC filtering.
B. System hardening.
C. Rogue machine detection.
D. Baselining.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
A network technician is on the phone with the system administration team. Power to the server room was lost and servers need to be restarted. The DNS services must be the first to be restarted. Several machines are powered off. Assuming each server only provides one service, which of the following should be powered on FIRST to establish DNS services?

A. Bind server
B. Apache server
C. Exchange server
D. RADIUS server

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
A datacenter requires that staff be able to identify whether or not items have been removed from the facility. Which of the following controls will allow the organization to provide automated notification of item removal?

A. CCTV
B. Environmental monitoring
C. RFID
D. EMI shielding

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
A company needs to receive data that contains personally identifiable information. The company requires both the transmission and data at rest to be encrypted. Which of the following achieves this goal? (Select TWO).

A. SSH
B. TFTP
C. NTLM
D. TKIP
E. SMTP
F. PGP/GPG

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
Which of the following describes a type of malware which is difficult to reverse engineer in a virtual lab?

A. Armored virus
B. Polymorphic malware
C. Logic bomb
D. Rootkit

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
An auditing team has found that passwords do not meet best business practices. Which of the following will MOST increase the security of the passwords? (Select TWO).

A. Password Complexity
B. Password Expiration
C. Password Age
D. Password Length
E. Password History

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
A new network administrator is setting up a new file server for the company. Which of the following would be the BEST way to manage folder security?

A. Assign users manually and perform regular user access reviews
B. Allow read only access to all folders and require users to request permission
C. Assign data owners to each folder and allow them to add individual users to each folder
D. Create security groups for each folder and assign appropriate users to each group

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
A security administrator must implement a system to allow clients to securely negotiate encryption keys with the company's server over a public unencrypted communication channel. Which of the following implements the required secure key negotiation? (Select TWO).

A. PBKDF2
B. Symmetric encryption
C. Steganography
D. ECDHE
E. Diffie-Hellman

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
When Ann an employee returns to work and logs into her workstation she notices that, several desktop configuration settings have changed. Upon a review of the CCTV logs, it is determined that someone logged into Ann's workstation. Which of the following could have prevented this from happening?

A. Password complexity policy
B. User access reviews
C. Shared account prohibition policy
D. User assigned permissions policy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
An attacker used an undocumented and unknown application exploit to gain access to a file server. Which of the following BEST describes this type of attack?

A. Integer overflow
B. Cross-site scripting
C. Zero-day

D. Session hijacking
E. XML injection

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
A system administrator is configuring UNIX accounts to authenticate against an external server. The configuration file asks for the following information DC=ServerName and DC=COM. Which of the following authentication services is being used?

A. RADIUS
B. SAML
C. TACACS+
D. LDAP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
A computer supply company is located in a building with three wireless networks. The system security team implemented a quarterly security scan and saw the following.

SSID State Channel Level
Computer AreUs1 connected 1 70dbm
Computer AreUs2 connected 5 80dbm
Computer AreUs3 connected 3 75dbm
Computer AreUs4 connected 6 95dbm

Which of the following is this an example of?

A. Rogue access point
B. Near field communication

C. Jamming
D. Packet sniffing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
Ann, a security administrator, has concerns regarding her company's wireless network. The network is open and available for visiting prospective clients in the conference room, but she notices that many more devices are connecting to the network than should be. Which of the following would BEST alleviate Ann's concerns with minimum disturbance of current functionality for clients?

A. Enable MAC filtering on the wireless access point.
B. Configure WPA2 encryption on the wireless access point.
C. Lower the antenna's broadcasting power.
D. Disable SSID broadcasting.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
Maintenance workers find an active network switch hidden above a dropped-ceiling tile in the CEO's office with various connected cables from the office. Which of the following describes the type of attack that was occurring?

A. Spear phishing
B. Packet sniffing
C. Impersonation
D. MAC flooding

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200

After copying a sensitive document from his desktop to a flash drive, Joe, a user, realizes that the document is no longer encrypted. Which of the following can a security technician implement to ensure that documents stored on Joe's desktop remain encrypted when moved to external media or other network based storage?

A. Whole disk encryption

B. Removable disk encryption

C. Database record level encryption

D. File level encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201

The Quality Assurance team is testing a new third party developed application. The Quality team does not have any experience with the application. Which of the following is the team performing?

A. Grey box testing

B. Black box testing

C. Penetration testing

D. White box testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202

The security team would like to gather intelligence about the types of attacks being launched against the organization. Which of the following would provide them with the MOST information?

A. Implement a honeynet
B. Perform a penetration test
C. Examine firewall logs
D. Deploy an IDS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
An SSL session is taking place. After the handshake phase has been established and the cipher has been selected, which of the following are being used to secure data in transport? (Select TWO)

A. Symmetrical encryption
B. Ephemeral Key generation
C. Diffie-Hellman
D. AES
E. RSA
F. Asymmetrical encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
Company A and Company B both supply contractual services to a fast paced and growing auto parts manufacturer with a small local Area Network (LAN) at its local site. Company A performs in-house billing and invoices services for the local auto parts manufactacturer. Company B provides in-house parts and widgets services for the local auto parts manufacturers. Which of the following is the BEST method to mitigate security risk within the environment?

A. Virtual Private Network
B. Role-Based access
C. Network segmentation

D. Public Key Infrastructure

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
The Chief Executive Officer (CEO) Joe notices an increase in the wireless signal in this office and thanks the IT director for the increase in network speed, Upon investigation the IT department finds an access point hidden in the dropped ceiling outside of joe's office. Which of the following types of attack is MOST likely occurring?

A. Packet sniffing
B. Bluesnarfing
C. Man-in-the-middle
D. Evil twin

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
A security administrator is reviewing the company's data backup plan. The plan implements nightly offsite data replication to a third party company. Which of the following documents specifies how much data can be stored offsite, and how quickly the data can be retrieved by the company from the third party?

A. MTBF
B. SLA
C. RFQ
D. ALE

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
Which of the following authentication services uses a default TCP port of 88?

A. Kerberos
B. TACACS+
C. SAML
D. LDAP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
A technician has been tasked with installing and configuring a wireless access point for the engineering department. After the AP has been installed, there has been reports the employees from other departments has been connecting to it without approval. Which of the following would BEST address these concerns?

A. Change the SSID of the AP so that it reflects a different department, obscuring its ownership
B. Implement WPA2 encryption in addition to WEP to protect the data-in-transit
C. Configure the AP to allow only to devices with pre-approved hardware addresses
D. Lower the antenna's power so that it only covers the engineering department's offices

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
A company has implemented full disk encryption. Clients must authenticate with a username and password at a pre-boot level to unlock the disk and again a username and password at the network login. Which of the following are being used? (Select TWO)

A. Multifactor authentication

B. Single factor authentication
C. Something a user is
D. Something a user has
E. Single sign-on
F. Something a user knows

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
Anne an employee receives the following email:
From: Human Resources
To: Employee
Subject: Updated employee code of conduct
Please click on the following link: http//external.site.com/codeofconduct.exe to review the updated code of conduct at your earliest convenience.
After clicking the email link, her computer is compromised. Which of the following principles of social engineering was used to lure Anne into clicking the phishing link in the above email?

A. Authority
B. Familiarity
C. Intimidation
D. Urgency

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
During a review a company was cited for allowing requestors to approve and implement their own change request. Which of the following would resolve the issue? (Select TWO)

A. Separation duties

B. Mandatory access
C. Mandatory vacations
D. Audit logs
E. Job Rotation
F. Time of day restrictions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
A security administrator wishes to protect session leys should a private key become discovered. Which of the following should be enabled in IPSec to allow this?

A. Perfect forward secrecy
B. Key escrow
C. Digital signatures
D. CRL

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
The security administrator notices a user logging into a corporate Unix server remotely as root. Which of the following actions should the administrator take?

A. Create a firewall rule to block SSH
B. Delete the root account
C. Disable remote root logins
D. Ensure the root account has a strong password

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 214
A workstation is exhibiting symptoms of malware and the network security analyst has decided to remove the system from the network. This represents which of the following stages of the Incident Handling Response?

A. Plan of action
B. Mitigation
C. Lesson Learned
D. Recovery

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
Which of the following would provide the MOST objective results when performing penetration testing for an organization?

A. An individual from outside the organization would be more familiar with the system
B. AN inside support staff member would know more about how the system could be compromised
C. An outside company would be less likely to skew the results in favor if the organization
D. An outside support staff member would be more likely to report accurate results due to familiarity with the system

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 216

An administrator would like users to authenticate to the network using only UDP protocols. Which of the following would meet this goal?

A. RADIUS
B. TACACS+
C. Kerberos
D. 802.1x

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217

When employing PKI to send signed and encrypted data the individual sending the data must have:
(Select TWO)

A. The receiver's private key
B. The root certificate
C. The sender's private key
D. The sender's public key
E. The receiver's public key

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218

Joe a technician is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?

A. OS hardening
B. Application control
C. Virtualization
D. Sandboxing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
A custom PKI application downloads a certificate revocation list (CRL) once per day. Management requests the list be checked more frequently. Which of the following is the BEST solution?

A. Refresh the CA public key each time a user logs in
B. Download the CRK every 60 seconds
C. Implement the OCSP protocol
D. Prompt the user to trust a certificate each time it is used

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
A security technician wants to improve the strength of a weak key by making it more secure against brute force attacks. Which of the following would achieve this?

A. Blowfish
B. Key stretching
C. Key escrow
D. Recovery agent

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
Joe uses his badge to enter the server room, Ann follows Joe entering without using her badge. It is later discovered that Ann used a USB drive to remove confidential data from a server. Which of the following principles is potentially being violated? (Select TWO)

A. Clean desk policy
B. Least privilege
C. Tailgating
D. Zero-day exploits
E. Data handling

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222
Ann the IT director wants to ensure that as hoc changes are not making their way to the production applications. Which of the following risk mitigation strategies should she implement in her department?

A. Change management
B. Permission reviews
C. Incident management
D. Perform routine audits

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
Which of the following would allow users from outside of an organization to have access to internal resources?

A. NAC
B. VLANS
C. VPN
D. NAT

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
Which of the following is BEST described by a scenario where management chooses not to implement a security control for a given risk?

A. Mitigation
B. Avoidance
C. Acceptance
D. Transference

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
Which of the following ports is used for TELNET by default?

A. 22
B. 23
C. 21
D. 20

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
When confidentiality is the primary concern which of the following types of encryption should be chosen?

A. Digital Signature
B. Symmetric
C. Asymmetric
D. Hashing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
A Windows- based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner?

A. Kill all system processes
B. Enable the firewall
C. Boot from CD/USB
D. Disable the network connection

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228

Ann a member of the Sales Department has been issued a company-owned laptop for use when traveling to remote sites. Which of the following would be MOST appropriate when configuring security on her laptop?

A. Configure the laptop with a BIOS password
B. Configure a host-based firewall on the laptop
C. Configure the laptop as a virtual server
D. Configure a host based IDS on the laptop

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
A security technician has removed the sample configuration files from a database server. Which of the following application security controls has the technician attempted?

A. Application hardening
B. Application baselines
C. Application patch management
D. Application input validation

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
Data confidentiality must be enforces on a secure database. Which of the following controls meets this goal? (Select TWO)

A. MAC
B. Lock and key
C. Encryption
D. Non-repudiation

E. Hashing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site do not record any footage. Which of the following types of controls was being used?

A. Detective
B. Corrective
C. Deterrent
D. Preventive

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
A network security administrator is trying to determine how an attacker gained access to the corporate wireless network. The network is configured with SSID broadcast disabled. The senior network administrator explains that this configuration setting would only have determined an unsophisticated attacker because of which of the following?

A. The SSID can be obtained with a wireless packet analyzer
B. The required information can be brute forced over time
C. Disabling the SSID only hides the network from other WAPs
D. The network name could be obtained through a social engineering campaign

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
Joe a system administrator receives reports that users attempting to reach the corporate website are arriving at an unfamiliar website instead. An investigation by a forensic analyst found that the name server log has several corporate IP addresses that were changed using Joe's credentials. Which of the following is this attack called?

A. Xmas attack
B. DNS poisoning
C. Web server attack
D. Spoofing attack

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
Joe a technician initiated scans if the company's 10 routers and discovered that half if the routers were not changed from their default configuration prior installed on the network. Which of the following would address this?

A. Secure router configuration
B. Implementing 802.1x
C. Enabling loop protection
D. Configuring port security

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
An employee attempts to go to a well-known bank site using the company-standard web browser by correctly typing in the address of the site into the web browser. The employee is directed to a website that looks like the bank's site but is not the actual bank site. The employee's user name and password are subsequently stolen. This is an example of which of the following?

A. Watering hole attack
B. Cross-site scripting
C. DNS poisoning
D. Man-in-the-middle attack

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
A user authenticates to a local directory server, The user then opens a virtualization client to connect to a virtual server. Instead of supplying a username/password combination, the user simply checks a use directory credentials checkbox to a authenticate to the virtual server. Which of the following authentication types has been utilized?

A. Transitive trust
B. Common access card
C. Multifactor authentication
D. Single sign-on

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
The new Chief Information Officer (CIO) of company ABC, Joe has noticed that company XWY is always one step ahead with similar products. He tasked his Chief Security Officer to implement new security controls to ensure confidentiality of company ABC's proprietary data and complete accountability for all data transfers. Which of the following security controls did the Chief Security Officer implement to BEST meet these requirements? (Select Two)

A. Redundancy
B. Hashing
C. DRP
D. Digital Signatures

E. Encryptions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
A worker dressed in a fire suppression company's uniform asks to be let into the server room to perform the annual check in the fire extinguishers. The system administrator allows the worker into the room, only to discover hours later that the worker was actually a penetration tester. Which of the following reasons allowed the penetration tester to access the server room?

A. Testing the fire suppression system represented a critical urgency
B. The pen tester assumed the authority of a reputable company
C. The pen tester used an intimidation technique on the administrator
D. The administrator trusted that the server room would remain safe

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
A company uses port security based on an approved MAC list to secure its wired network and WPA2 to secure its wireless network. Which of the following prevents an attacker from learning authorized MAC addresses?

A. Port security prevents access to any traffic that might provide an attacker with authorized MAC addresses
B. Port security uses certificates to authenticate devices and is not part of a wireless protocol
C. Port security relies in a MAC address length that is too short to be cryptographically secure over wireless networks
D. Port security encrypts data on the network preventing an attacker form reading authorized MAC addresses

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240

A security technician is implementing PKI on a Network. The technician wishes to reduce the amount of bandwidth used when verifying the validity of a certificate. Which of the following should the technician implement?

A. CSR
B. Key escrow
C. OSCR
D. CRL

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241

The network security manager has been notified by customer service that employees have been sending unencrypted confidential information via email. Which of the following should the manager select to BEST detect and provide notification of these occurrences?

A. DLP
B. SSL
C. DEP
D. UTM

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242

While troubleshooting a new wireless 802.11 ac network an administrator discovers that several of the older systems cannot connect. Upon investigation the administrator discovers that the older devices only support 802.11 a and RC4. The administrator does not want to affect the performance of the newer

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
11 ac devices on the network. Which of the following should the administrator do to accommodate all devices and provide the MOST security?

A. Disable channel bonding to allow the legacy devices and configure WEP fallback
B. Configure the AP in protected mode to utilize WPA2 with CCMP
C. Create a second SSID on the AP which utilizes WPA and TKIP
D. Configure the AP to utilize the 5Gh band only and enable WEP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
A security administrator is troubleshooting an authentication issues using a network sniffer. The security administrator reviews a packet capture of the authentication process and notices that authentication is performed using extensible markup over SOAP. Which of the following authentication services is the security administrator troubleshooting?

A. SAML
B. XTACACS
C. Secure LDAP
D. RADIUS

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 245
Given a class C network a technician has been tasked with creating a separate subnet for each of the eight departments in the company. Which of the following network masks would allow for each department to have a unique network space and what is the maximum number of hosts each department could have?

A. Network 255.255.255.192, 62 hosts
B. Network 255.255.255.224, 30 hosts
C. Network 255.255.255.240, 16 hosts
D. Network 255.255.255.248, 32 hosts

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
A software security concern when dealing with hardware and devices that have embedded software or operating systems is:

A. Patching may not always be possible
B. Configuration support may not be available
C. These is no way to verify if a patch is authorized or not
D. The vendor may not have a method for installation of patches

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
A major medical corporation is investigating deploying a web based portal for patients to access their medical records. The medical corporation has a long history of maintaining IT security but is considering having a third party vendor create the web portal. Which of the following areas is MOST important for the Chief Information Security Officer to focus on when reviewing proposal from vendors interested in creating the web portal?

A. Contractor background check
B. Confidentiality and availability
C. Redundancy and privacy
D. Integrity and confidentiality

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
Which of the following authentication methods requires the user, service provider and an identity provider to take part in the authentication process?

A. RADIUS
B. SAML
C. Secure LDAP
D. Kerberos

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
Which of the following types of malware is designed to provide access to a system when normal authentication fails?

A. Rootkit
B. Botnet
C. Backdoor
D. Adware

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 250
Ann is concerned that the application her team is currently developing is vulnerable to unexpected user input that could lead to issues within the memory is affected in a detrimental manner leading to potential exploitation. Which of the following describes this application threat?

A. Replay attack
B. Zero-day exploit
C. Distributed denial of service
D. Buffer overflow

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
Which of the following can be used for both encryption and digital signatures??

A. 3DES
B. AES
C. RSA
D. MD5

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
A user tries to visit a web site with a revoked certificate. In the background a server from the certificate authority only sends the browser revocation information about the domain the user is visiting. Which of the following is being used by the certificate authority in this exchange?

A. CSR
B. Key escrow
C. OCSP
D. CRL

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
Joe wants to employ MD5 hashing on the company file server. Which of the following is Joe trying to achieve?

A. Availability
B. Confidentiality
C. Non repudiation
D. Integrity

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254
By hijacking unencrypted cookies an application allows an attacker to take over existing web sessions that do not use SSL or end to end encryption. Which of the following choices BEST mitigates the security risk of public web surfing? (Select TWO)

A. WPA2
B. WEP
C. Disabling SSID broadcasting
D. VPN
E. Proximity to WIFI access point

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255

The security administration team at a company has been tasked with implementing a data-at-rest solution for its company storage. Due to the large amount of storage the Chief Information Officer (CISO) decides that a 128-bit cipher is needed but the CISO also does not want to degrade system performance any more than necessary. Which of the following encryptions needs BOTH of these needs?

A. SHA1
B. DSA
C. AES
D. 3DES

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256

A company has a BYOD policy that includes tablets and smart phones. In the case of a legal investigation, which of the following poses the greatest security issues?

A. Recovering sensitive documents from a device if the owner is unable or unwilling to cooperate
B. Making a copy of all of the files on the device and hashing them after the owner has provided the PIN
C. Using GPS services to locate the device owner suspected in the investigation
D. Wiping the device from a remote location should it be identified as a risk in the investigation

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
After several thefts a Chief Executive Officer (CEO) wants to ensure unauthorized do not have to corporate grounds or its employees. The CEO just approved new budget line items for fences, lighting, locks and CCTVs. Which of the following is the primary focus?

A. Safety
B. Confidentiality
C. Availability
D. Integrity

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258
Which of the following steps in incident response procedures entails of the incident and identification of knowledge gained that can be applied to future handling of incidents?

A. Recovery procedures
B. Escalation and notification
C. Reporting
D. Lessons learned

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
Which of the following automated or semi-automated software testing techniques relies on inputting large amounts of random data to detect coding errors or application loopholes?

A. Fuzzing
B. Black box

C. Fault injection
D. SQL injection

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
A company's BYOD policy requires the installation of a company provide mobile agent on their on their personally owned devices which would allow auditing when an employee wants to connect a device to the corporate email system. Which of the following concerns will MOST affect the decision to use a personal device to receive company email?

A. Personal privacy
B. Email support
C. Data ownership
D. Service availability

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
A penetration tester is measuring a company's posture on social engineering. The penetration tester sends a phishing email claiming to be from IT asking employees to click a link to update their VPN software immediately. Which of the following reasons would explain why this attack could be successful?

A. Principle of Scarcity
B. Principle of Intimidation
C. Principle of Urgency
D. Principle of liking

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262

A new employee has joined the accounting department and is unable to access the accounting server. The employee can access other network resources and the Internet. Other accounting employees are able to access the accounting server without any issues. Which of the following is the MOST likely issue?

A. The server's IDS is blocking the new employee's connection

B. The workstation is unable to join the domain

C. The server's drive is not mapped on the new employee's workstation

D. The new account is not in the proper role-based profile

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263

A security specialist has been brought in to assess the organizational security policies. The specialist needs to start by reviewing the highest level policies. Which of the following is the overarching security policy for an organization?

A. Network Access Policy

B. Risk Management Policy

C. Remote Access Policy

D. Technical Implementation Guide

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264

Joe a sales employee is connecting to a wireless network and has entered the network information correctly. His computer remains connected to the network but he cannot access any resources on the network. Which of the following is the MOST likely cause of this issue?

A. The encryption is too strong
B. The network SSID is disabled
C. MAC filtering is enabled
D. The wireless antenna power is set too low

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
Which of the following is used to inform users of the repercussions of releasing proprietary information?

A. OLA
B. SLA
C. NDA
D. MOU

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
A review of administrative access has discovered that too many accounts have been granted administrative rights. Which of the following will alert the security team when elevated access is applied?

A. Establishing user access reviews
B. Establishing user based privileges
C. Establishing monitoring on accounts
D. Establishing group based privileges

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 267

When an authorized application is installed on a server, the application triggers an alert on the HIDS. This is known as a:

A. Vulnerability
B. False negative
C. False positive
D. Threat vector

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268

In which of the following scenarios would it be preferable to implement file level encryption instead of whole disk encryption?

A. A server environment where the primary security concern is integrity and not file recovery
B. A cloud storage environment where multiple customers use the same hardware but possess different encryption keys
C. A SQL environment where multiple customers access the same database
D. A large datacenter environment where each customer users dedicated hardware resources

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
For high availability which of the following would be MOST appropriate for fault tolerance?

A. RAID 0
B. Clustering
C. JBOD
D. Load Balancing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 270
When implementing a Public Key Infrastructure, which of the following should the sender use to digitally sign a document?

A. A CSR
B. A private key
C. A certificate authority
D. A public key

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
A military base wants to incorporate biometrics into its new security measures, but the head of security does not want them to be the sole method of authentication. For unmanned entry points, which of the following solutions would work BEST?

A. Use voice print and a bollard

B. Use a retina scanner and a thumbprint
C. Use CCTV and a PIN
D. Use a retina scan and a PIN code

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272
Ann a security administrator wants a limit access to the wireless network. Which of the following can be used to do this without using certificates?

A. Employ EPA-TLS
B. Employ PEAP on all laptops
C. Enable MAC filtering
D. Disable SSID broadcasting

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
A user has an Android smartphone that supports full device encryption. However when the user plus into a computer all of the files are immediately accessible. Which of the following should the user do to enforce full device confidentiality should the phone be lost or stolen?

A. Establish a PIN passphrase
B. Agree to remote wipe terms
C. Generate new media encryption keys
D. Download the encryption control app from the store

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274

The network manager has obtained a public IP address for use with a new system to be available via the internet. This system will be placed in the DMZ and will communicate with a database server on the LAN. Which of the following should be used to allow fir proper communication between internet users and the internal systems?

A. VLAN
B. DNS
C. NAT
D. HTTP
E. SSL

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275

After a new RADIUS server is added to the network, an employee is unable to connect to the company's WPA2-Enterprise WIFI network, which is configured to prompt for the employee's network username and password. The employee reports receiving an error message after a brief connection attempt, but is never prompted for credentials. Which of the following issues could be causing the problem?

A. The employee's account is locked out in the directory service
B. The new RADIUS server is overloading the wireless access point
C. The new RADIUS server's certificate is not trusted by the employee's PC
D. The employee's account is disabled in the RADIUS server's local database

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276

Ann the security administrator has been reviewing logs and has found several overnight sales personnel are accessing the finance department's network shares. Which of the following security controls should be implemented to BEST remediate this?

A. Mandatory access
B. Separation of duties
C. Time of day restrictions
D. Role based access

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
A fiber company has acquired permission to bury a fiber cable through a famer's land. Which of the following should be in the agreement with the farmer to protect the availability of the network?

A. No farm animals will graze near the burial site of the cable
B. No digging will occur near the burial site of the cable
C. No buildings or structures will be placed on top of the cable
D. No crops will be planted on top of the cable

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
The programmer confirms that there is potential for a buffer overflow on one of the data input fields in a corporate application. The security analyst classifies this as a (N).

A. Threat
B. Risk
C. Attack
D. Vulnerability

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
A security technician would like to use ciphers that generate ephemeral keys for secure communication. Which of the following algorithms support ephemeral modes? (Select TWO)

A. Diffie-Hellman
B. RC4
C. RIPEMO
D. NTLMv2
E. PAP
F. RSA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280
A security technician would like an application to use random salts to generate short lived encryption leys during the secure communication handshake process to increase communication security. Which of the following concepts would BEST meet this goal?

A. Ephemeral keys
B. Symmetric Encryption Keys
C. AES Encryption Keys
D. Key Escrow

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
A security administrator wishes to implement a method of generating encryption keys from user passwords to enhances account security. Which of the following would accomplish this task?

A. NTLMv2
B. Blowfish
C. Diffie-Hellman
D. PBKDF2

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282
Which of the following devices is used for the transparent security inspection of network traffic by redirecting user packets prior to sending the packets to the intended destination?

A. Proxies
B. Load balancers
C. Protocol analyzer
D. VPN concentrator

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
An administrator needs to allow both secure and regular web traffic into a network. Which of the following ports should be configured? (Select TWO)

A. 25

B. 53
C. 80
D. 110
E. 143
F. 443

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284
A recent audit had revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO)

A. Deploy a honeypot
B. Disable unnecessary services
C. Change default password
D. Implement an application firewall
E. Penetration testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
A local hospital with a large four-acre cam[us wants to implement a wireless network so that doctors can use tablets to access patients medical data. The hospital also wants to provide guest access to the internet for hospital patients and visitors in select areas. Which of the following areas should be addressed FIRST?

A. MAC filters
B. Site Survey
C. Power level controls
D. Antenna types

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 286
After making a bit-level copy of compromised server, the forensics analyst Joe wants to verify that he bid not accidentally make a change during his investigation. Which of the following should he perform?

A. Take a hash of the image and compare it to the one being investigated
B. Compare file sizes of all files prior to and after investigation
C. Make a third image and compare it to the second image being investigated
D. Compare the logs of the copy to the actual server

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287
Which of the following attacks is generally initiated from a botnet?

A. Cross site scripting attack
B. HTTP header injection
C. Distributed denial of service
D. A war driving attack

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288
A network security analyst has confirmed that the public facing web server has been compromised. Which of the following stages if the Incident Handling Response does this describe?

A. Analyzing
B. Recovering
C. Identification
D. Mitigation

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
Deploying compensating security controls is an example of:

A. Risk avoidance
B. Risk mitigation
C. Risk transference
D. Risk acceptance

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
A web startup wants to implement single sign-on where its customers can log on to the site by suing their personal and existing corporate email credentials regardless of which company they work for. Is this directly supported by SAML?

A. Mo not without extensive partnering and API integration with all required email providers
B. Yes SAML is a web based single sign-on implementation exactly fir this purpose
C. No a better approach would be to use required email providers LDAP or RADIUS repositories
D. Yes SAML can use oauth2 to provide this functionality out of the box

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 291
A security administrator is installing a single camera outside in order to detect unauthorized vehicles in the parking lot. Which of the following is the MOST important consideration when deploying a CCTV camera to meet the requirement?

A. Training
B. Expense
C. Resolution
D. Field of view

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 292
A system administrator wants to configure a setting that will make offline password cracking more challenging. Currently the password policy allows upper and lower case characters a minimum length of 5 and a lockout after 10 invalid attempts. Which of the following has the GREATEST impact on the time it takes to crack the passwords?

A. Increase the minimum password length to 8 while keeping the same character set
B. Implement an additional password history and reuse policy
C. Allow numbers and special characters in the password while keeping the minimum length at 5
D. Implement an account lockout policy after three unsuccessful logon attempts

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 293
Establishing a method to erase or clear memory is an example of securing which of the following?

A. Data in transit
B. Data at rest
C. Data in use
D. Data in motion

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294
Joe processes several requisitions during the day and during the night shift they are approved by Ann. This is an example of which of the following?

A. Separation of duties
B. Discretionary access
C. Mandatory access
D. Time of day restrictions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295
A security administrator would like to write an access rule to block the three IP addresses given below. Which of the following combinations should be used to include all of the given IP addresses?

A.
B.
C.

D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 296
168.12.255

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 297
168.12.227

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
168.12.229

A. 192.168.12.0/25
B. 192.168.12.128.28
C. 192.168.12.224/29
D. 192.168.12.225/30

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299
After installing a new Linux system the administrator runs a command that records the size, permissions, and MD5 sum of all the files on the system. Which of the following describes what the administrator is doing?

A. Identifying vulnerabilities
B. Design review
C. Host software baselining
D. Operating system hardening

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300
An intrusion has occurred in an internet facing system. The security administrator would like to gather forensic evidence while the system is still in operation. Which of the following procedures should the administrator perform FIRST on the system?

A. Make a drive image
B. Take hashes of system data
C. Collect information in RAM
D. Capture network traffic

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 301

Which of the following wireless standards is backwards compatible with 802.11g?

A. 802.11a
B. 802.11b
C. 802.11n
D. 802.1q

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 302

Which of the following ports will be used for logging into secure websites?

A. 80
B. 110
C. 142
D. 443

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 303

The below report indicates that the system is MOST likely infected by which of the following? Protocol LOCAL IP FOREIGN IP STATE
TCP 0.0.0:445 0.0.0.0:0 Listening
TCP 0.0.0.0:3390 0.0.0.0:0 Listening

A. Trojan
B. Worm
C. Logic bomb
D. Spyware

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 304
A security administrator is required to submit a detailed implementation plan and back out plan to get approval prior to updating the firewall and other security devices. Which of the following types of risk mitigation strategies is being followed?

A. Change management
B. Routine audit
C. Rights and permissions review
D. Configuration management

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305
Which of the following authentication services uses a default TCP of 389?

A. SAML
B. TACACS+
C. Kerberos
D. LDAP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 306
A software company sends their offsite backup tapes to a third party storage facility. TO meet confidentiality the tapes should be:

A. Labeled
B. Hashed
C. Encrypted
D. Duplicated

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

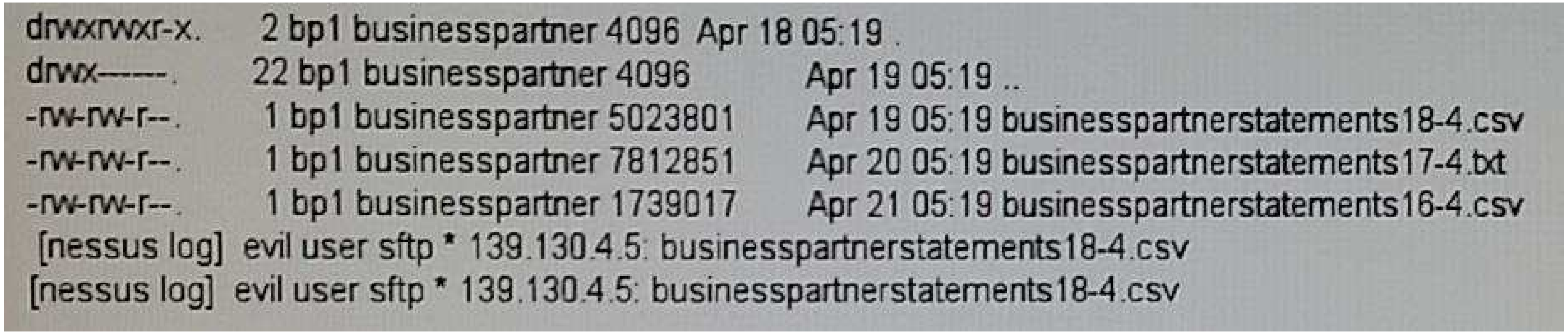
QUESTION 307
Ann a technician wants to implement a single protocol on a remote server which will enable her to encrypt and proxy all of her traffic though the remote server via SOCKS5. Which of the following should Ann enable to support both encryption and proxy services?

A. SSH
B. IPSEC
C. TLS
D. HTTPS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 308
Ann a system analyst discovered the following log. Which of the following or techniques does this indicate? {bp1@localmachine}$ Is-al
Total 12
Drwxrwxr-x



```
drwxrwxr-x.     2 bp1 businesspartner 4096  Apr 18 05:19 .
drwx------.    22 bp1 businesspartner 4096          Apr 19 05:19 ..
-rw-rw-r--.     1 bp1 businesspartner 5023801       Apr 19 05:19 businesspartnerstatements18-4.csv
-rw-rw-r--.     1 bp1 businesspartner 7812851       Apr 20 05:19 businesspartnerstatements17-4.txt
-rw-rw-r--.     1 bp1 businesspartner 1739017       Apr 21 05:19 businesspartnerstatements16-4.csv
 [nessus log]  evil user sftp * 139.130.4.5: businesspartnerstatements18-4.csv
[nessus log]  evil user sftp * 139.130.4.5: businesspartnerstatements18-4.csv
```

A. Protocol analyzer
B. Port scanner
C. Vulnerability
D. Banner grabbing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 309
A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors. The company decides that is wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client. Which of the following should the company implement?

A. Port security
B. WPA2
C. Mandatory Access Control
D. Network Intrusion Prevention

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 310
The helpdesk is receiving numerous reports that a newly installed biometric reader at the entrance of the data center has a high of false negatives. Which of the following is the consequence of this reported problem?

A. Unauthorized employees have access to sensitive systems
B. All employees will have access to sensitive systems
C. No employees will be able to access the datacenter
D. Authorized employees cannot access sensitive systems

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 311
A company administrator has a firewall with an outside interface connected to the internet and an inside interface connected to the corporate network. Which of the following should administrator configure to redirect traffic destined for the default HTTP port on the outside interface to an internal server listening on port 8080?

A. Create a dynamic PAT from port 80 the outside interface to the internal interface on port 8080
B. Create a dynamic NAT form port 8080 on the outside interface to the server IP address on port
C. Create a static PAT from port 80 on the outside interface to the internal interface on port 8080
D. Create a static PAP form port 8080 on the outside interface to the server IP address on port 80

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 312
A software developer places a copy of the source code for a sensitive internal application on a company laptop to work remotely. Which of the following policies is MOST likely being violated?

A. Clean desk
B. Data handling
C. Chain of custody
D. Social media

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 313
While testing a new host based firewall configuration a security administrator inadvertently blocks access to localhost which causes problems with applications running on the host. Which of the following addresses refer to localhost?

A. ::0
B. 127.0.0.0
C. 120.0.0.1
D. 127.0.0/8
E. 127::0.1

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 314
A user has reported inadvertently sending an encrypted email containing PII to an incorrect distribution group. Which of the following potential incident types is this?

A. Data sharing
B. Unauthorized viewing

C. Data breach
D. Unauthorized access

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 315
A company is exploring the option of letting employees use their personal laptops on the internal network. Which of the following would be the MOST common security concern in this scenario?

A. Credential management
B. Support ownership
C. Device access control
D. Antivirus management

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 316
A security engineer discovers that during certain times of day, the corporate wireless network is dropping enough packets to significantly degrade service. Which of the following should be the engineer's FIRST step in troubleshooting the issues?

A. Configure stronger encryption
B. Increase the power level
C. Change to a higher gain antenna
D. Perform a site survey

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317

A security administrator is reviewing the web logs and notices multiple attempts by users to access: http://www.comptia.org/idapsearch?user-*
Having identified the attack, which of the following will prevent this type of attack on the web server?

A. Input validation on the web server
B. Block port 389 on the firewall
C. Segregate the web server by a VLAN
D. Block port 3389 on the firewall

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 318

A breach at a credit card company resulted in customers credit card information being exposed . The company has conducted a full forensic investigation and identified the source of the breach. Which of the following should the company do NEXT?

A. Move to the incident identification phase
B. Implement the risk assessment plan
C. Implement damage and loss control procedures
D. Implement first responder processes

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 319

Joe a user upon arriving to work on Monday morning noticed several files were deleted from the system. There were no records of any scheduled network outages or upgrades to the system. Joe notifies the security department of the anomaly found and removes the system from the network. Which of the following is the NEXT action that Joe should perform?

A. Screenshots of systems
B. Call the local police
C. Perform a backup
D. Capture system image

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 320
The user of a news service accidently accesses another user's browsing history. From this the user can tell what competitors are reading, querying, and researching. The news service has failed to properly implement which of the following?

A. Application white listing
B. In-transit protection
C. Access controls
D. Full disk encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 321
A system requires administrators to be logged in as the "root" in order to make administrator changes. Which of the following controls BEST mitigates the risk associated with this scenario?

A. Require that all administrators keep a log book of times and justification for accessing root
B. Encrypt all users home directories using file-level encryption
C. Implement a more restrictive password rotation policy for the shared root account
D. Force administrator to log in with individual accounts and switch to root
E. Add the administrator to the local group

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 322
A defense contractor wants to use one of its classified systems to support programs from multiple intelligence agencies. Which of the following MUST be in place between the intelligence agencies to allow this?

A. A DRP
B. An SLA
C. A MOU
D. A BCP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 323
A penetration tester was able to obtain elevated privileges on a client workstation and multiple servers using the credentials of an employee. Which of the following controls would mitigate this issues? (Select TWO)

A. Separation of duties
B. Least privilege
C. Time of day restrictions
D. Account expiration
E. Discretionary access control
F. Password history

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 324
A security administrator must implement a system that will support and enforce the following file system access control model:
File name Security Label
Employee.doc Confidential
Salary.xls Confidential
Officephones.XLS Unclassified
PersonalPhones.XLS Restricted
Which of the following should the security administrator implement?

A. White and black listing
B. SCADA system
C. Trusted OS
D. Version system

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 325
Which of the following is considered the MOST effective practice when securing printers or scanners in an enterprise environment?

A. Routine vulnerability scanning of peripherals
B. Install in a hardened network segment
C. Turn off the power to the peripherals at night
D. Enable print sharing only from workstations

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 326
After a few users report problems with the wireless network, a system administrator notices that a new wireless access point has been powered up in the cafeteria.

The access point has the same SSID as the corporate network and is set to the same channel as nearby access points. However, the AP has not been connected to the Ethernet network. Which of the following is the MOST likely cause of the user's wireless problems?

A. AP channel bonding
B. An evil twin attack
C. Wireless interference
D. A rogue access point

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 327
A network technician at a company, Joe is working on a network device. He creates a rule to prevent users from connecting to a toy website during the holiday shopping season. This website is blacklisted and is known to have SQL injections and malware. Which of the following has been implemented?

A. Mandatory access
B. Network separation
C. Firewall rules
D. Implicit Deny

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 328
Company XYZ has suffered leaks of internally distributed confidential documents. Ann the network security analyst has been tasked to track down the culprit. She has decided to embed a four letter string of characters in documents containing proprietary information. Which of the following initial steps should Ann implement before sending documents?

A. Store one of the documents in a honey pot
B. Start antivirus scan on all the suspected computers
C. Add a signature to the NIDS containing the four letter string

D. Ask employees to report suspicious behaviors

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 329
Which of the following should a company deploy to prevent the execution of some types of malicious code?

A. Least privilege accounts
B. Host-based firewalls
C. Intrusion Detection systems
D. Application white listing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 330
An administrator in investigating a system that may potentially be compromised and sees the following log entries on the router.
*Jul 15 14:47:29.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) ->

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 331
10.1.5 (6667), 3 packets.
*Jul 15 14:47:38.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) ->

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 332
10.1.5 (6667), 6 packets.
*Jul 15 14:47:45.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) ->

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 333
10.1.5 (6667), 8 packets.
Which of the following BEST describes the compromised system?

A. It is running a rogue web server
B. It is being used in a man-in-the-middle attack

C. It is participating in a botnet
D. It is an ARP poisoning attack

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 334
A security administrator implements a web server that utilizes an algorithm that requires other hashing standards to provide data integrity. Which of the following algorithms would meet the requirement?

A. SHA
B. MD5
C. RIPEMD
D. HMAC

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335
Which of the following is the FIRST step in a forensics investigation when a breach of a client's workstation has been confirmed?

A. Transport the workstation to a secure facility
B. Analyze the contents of the hard drive
C. Restore any deleted files and / or folders
D. Make a bit-for-bit copy of the system

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 336
Company XYZ's laptops was recently stolen from a user which led to the exposure if confidential information. Which of the following should the security team implement on laptops to prevent future compromise?

A. Cipher locks
B. Strong passwords
C. Biometrics
D. Full Disk Encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 337
A wireless site survey has been performed at a company. One of the results of the report is that the wireless signal extends too far outside the building. Which of the following security issues could occur as a result of this finding?

A. Excessive wireless access coverage
B. Interference with nearby access points
C. Exhaustion of DHCP address pool
D. Unauthorized wireless access

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 338
Which of the following is a software vulnerability that can be avoided by using input validation?

A. Buffer overflow
B. Application fuzzing

C. Incorrect input
D. Error handling

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 339
A university has a building that holds the power generators for the entire campus. A risk assessment was completed for the university and the generator building was labeled as a high risk. Fencing and lighting was installed to reduce risk. Which of the following security goals would this meet?

A. Load balancing
B. Non-repudiation
C. Disaster recovery
D. Physical security

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 340
Log file analysis on a router reveals several unsuccessful telnet attempts to the virtual terminal (VTY) lines. Which of the following represents the BEST configuration used in order to prevent unauthorized remote access while maintaining secure availability for legitimate users?

A. Disable telnet access to the VTY lines, enable SHH access to the VTY lines with RSA encryption
B. Disable both telnet and SSH access to the VTY lines, requiring users to log in using HTTP
C. Disable telnet access to the VTY lines, enable SHH access to the VTY lines with PSK encryption
D. Disable telnet access to the VTY lines, enable SSL access to the VTY lines with RSA encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 341
Four weeks ago a network administrator applied a new IDS and allowed it to gather baseline data. As rumors of a layoff begins to spread the IDS alerted the network administrator that access to sensitive client files had risen for above normal. Which of the following kind of IDS is in use?

A. Protocol based
B. Heuristic based
C. Signature based
D. Anomaly based

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 342
A BYOD policy in which employees are able to access the wireless guest network in in effect in an organization. Some users however are using the Ethernet port in personal laptops to the wired network. Which of the following could an administrator use to ensure that unauthorized devices are not allowed to access the wired network?

A. VLAN access rules configured to reject packets originating from unauthorized devices
B. Router access lists configured to block the IP addresses of unauthorized devices
C. Firewall rules configured to block the MAC addresses of unauthorized devices
D. Port security configured shut down the port when unauthorized devices connect

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 343
During an office move a sever containing the employee information database will be shut down and transported to a new location. Which of the following would BEST ensure the availability of the employee database should happen to the server during the move?

A. The contents of the database should be encrypted; the encryption key should be stored off-site
B. A hash of the database should be taken and stored on an external drive prior to the move
C. The database should be placed on a drive that consists of a RAID array prior to the move
D. A backup of the database should be stored on an external hard drive prior to the move

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 344
Which of the following is primarily used to provide fault tolerance at the application level? (Select TWO)

A. Load balancing
B. RAID array
C. RAID 6
D. Server clustering
E. JBOD array

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 345
A security administrator would like the corporate webserver to select perfect forward secrecy ciphers first. Which of the following cipher suites should the administrator select to accomplish this goal?

A. DH-DSS-CAMELLA256-SHA
B. ECDHE-RSA-AES1280SHA
C. DH-RSA-AES128-SHA256
D. ADH-AES256-SHA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 346
An administrator is having difficulty configuring WPA2 Enterprise using EAP-PEAP-MSCHAPv2. The administrator has configured the wireless access points properly, and has configured policies on the RADIUS server and configured settings on the client computers. Which of the following is missing?

A. Client certificates are needed
B. A third party LEAP client must be installed
C. A RADIUS server certificate is needed
D. The use of CCMP rather than TKIP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 347
A business has recently adopted a policy allowing employees to use personal cell phones and tablets to access company email accounts while out of the office. Joe an employee was using a personal cell phone for email access and was recently terminated. It is suspected that Joe saved confidential client emails on his personal cell phone. Joe claims that the data on the phone is completely personal and refuse to allow the company access to inspect the cell phone. Which of the following is the MOST likely cause of this dispute?

A. Onboarding procedures
B. Fair use policy
C. Device ownership
D. User acceptance

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 348
Mobile tablets are used by employees on the sales floor to access customer data. Ann a customer recently reported that another customer was able to access her personal information on the tablet after the employee left the area. Which of the following would BEST prevent this issues from reoccurring?

A. Screen Locks
B. Full-device encryption
C. Application control
D. Asset tracking

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 349
Which of the following metrics is important for measuring the extent of data required during backup and recovery?

A. MOU
B. ARO
C. ALE
D. RPO

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 350
Which of the following can be used to ensure that sensitive records stored on a backend server can only be accessed by a front end server with the appropriate record key?

A. File encryption
B. Storage encryption
C. Database encryption
D. Full disk encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 351
An overseas Branch office within a company has many more technical and non-technical security incidents than other parts of the company. Which of the following management controls should be introduced to the branch office to improve their state of security?

A. Initial baseline configuration snapshots
B. Firewall, IPS and network segmentation
C. Event log analysis and incident response
D. Continuous security monitoring processes

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 352
Which of the following controls should critical application servers implement to protect themselves from other potentially compromised application services?

A. NIPS
B. Content filter
C. NIDS
D. Host-based firewalls

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 353
Which of the following would be used to allow a subset of traffic from a wireless network to an internal network?

A. Access control list
B. 802.1X
C. Port security
D. Load balancers

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 354
A company has identified a watering hole attack. Which of the following Best describes this type of attack?

A. Emails are being spoofed to look like they are internal emails
B. A cloud storage site is attempting to harvest user IDS and passwords
C. An online news site is hosting ads in iframes from another site
D. A local restaurant chains online menu is hosting malicious code

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 355

A security manager is discussing change in the security posture of the network, if a proposed application is approved for deployment. Which of the following is the MOST important the security manager must rely upon to help make this determination?

A. Ports used by new application
B. Protocols/services used by new application
C. Approved configuration items
D. Current baseline configuration

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 356
Joe the system administrator has noticed an increase in network activity from outside sources. He wishes to direct traffic to avoid possible penetration while heavily monitoring the traffic with little to no impact on the current server load. Which of the following would be BEST course of action?

A. Apply an additional firewall ruleset on the user PCs.
B. Configure several servers into a honeynet
C. Implement an IDS to protect against intrusion
D. Enable DNS logging to capture abnormal traffic

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 357
An assessment too reports that the company's web server may be susceptible to remote buffer overflow. The web server administrator insists that the finding is a false positive. Which of the following should the administrator do to verify if this is indeed a false positive?

A. Use a banner grabbing tool
B. Run a vulnerability scan
C. Enforce company policies
D. Perform a penetration test

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 358
A security administrator wants to implement a solution which will allow some applications to run under the user's home directory and only have access to files stored within the same user's folder, while other applications have access to shared folders. Which of the following should be implemented if the environment is concurrently shared by multiple users?

A. OS Virtualization
B. Trusted OS
C. Process sandboxing
D. File permission

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 359
The sales force in an organization frequently travel to remote sites and requires secure access to an internal server with an IP address of 192.168.0.220. Assuming services are using default ports, which of the following firewall rules would accomplish this objective? (Select Two)

A. Permit TCP 20 any 192.168.0.200
B. Permit TCP 21 any 192.168.0.200
C. Permit TCP 22 any 192.168.0.200
D. Permit TCP 110 any 192.168.0.200
E. Permit TCP 139 any 192.168.0.200
F. Permit TCP 3389 any 192.168.0.200

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 360
Ann a security administrator at a call center, has been experiencing problems with users intentionally installing unapproved and occasionally malicious software on their computers. Due to the nature of their jobs, Ann cannot change their permissions. Which of the following would BEST alleviate her concerns?

A. Deploy a HIDS suite on the users' computer to prevent application installation
B. Maintain the baseline posture at the highest OS patch level
C. Enable the pop-up blockers on the user's browsers to prevent malware
D. Create an approved application list and block anything not on it

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 361
Ann is the data owner of financial records for a company. She has requested that she have the ability to assign read and write privileges to her folders. The network administrator is tasked with setting up the initial access control system and handling Ann's administrator capabilities. Which of the following systems should be deployed?

A. Role-based
B. Mandatory
C. Discretionary
D. Rule-based

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 362
Which of the following will provide data encryption, key management and secure application launching?

A. TKIP
B. HSM
C. EFS
D. DLP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 363
It is MOST difficult to harden against which of the following?

A. XSS
B. Zero-day
C. Buffer overflow
D. DoS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
A business has set up a customer service Kiosk within a shopping mall. The location will be staffed by an employee using a laptop during the mall business hours, but there are still concerns regarding the physical safety of the equipment while not in use. Which of the following controls would BEST address this security concern?

A. Host-Based firewall
B. Cable locks
C. Locking cabinets
D. Surveillance video

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 365
A company has experienced problems with their ISP, which has failed to meet their informally agreed upon level of service. However the business has not negotiated any additional formal agreements beyond the standard customer terms. Which of the following is the BEST document that the company should prepare to negotiate with the ISP?

A. ISA
B. SLA
C. MOU
D. PBA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 366
A company would like to implement two-factor authentication for its vulnerability management database to require system administrators to use their token and random PIN codes. Which of the following authentication services accomplishes this objective?

A. SAML
B. TACACS+
C. Kerberos
D. RADIUS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 367
A company has a corporate infrastructure where end users manage their own certificate keys. Which of the following is considered the MOST secure way to handle

master keys associated with these certificates?

A. Key escrow with key recovery
B. Trusted first party
C. Personal Identity Verification
D. Trusted third party

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 368
A recent audit has revealed that several users have retained permissions to systems they should no longer have rights to after being promoted or changed job positions. Which of the following controls would BEST mitigate this issue?

A. Separation of duties
B. User account reviews
C. Group based privileges
D. Acceptable use policies

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369
Ann a new security specialist is attempting to access the internet using the company's open wireless network. The wireless network is not encrypted: however, once associated, ANN cannot access the internet or other company resources. In an attempt to troubleshoot, she scans the wireless network with NMAP, discovering the only other device on the wireless network is a firewall. Which of the following BEST describes the company's wireless network solution?

A. The company uses VPN to authenticate and encrypt wireless connections and traffic
B. The company's wireless access point is being spoofed
C. The company's wireless network is unprotected and should be configured with WPA2
D. The company is only using wireless for internet traffic so it does not need additional encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 370
Which of the following, if implemented, would improve security of remote users by reducing vulnerabilities associated with data-in-transit?

A. Full-disk encryption
B. A virtual private network
C. A thin-client approach
D. Remote wipe capability

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 371
A company wants to improve its overall security posture by deploying environmental controls in its datacenter. Which of the following is considered an environmental control that can be deployed to meet this goal?

A. Full-disk encryption
B. Proximity readers
C. Hard ward locks
D. Fire suppression

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 372
A programmer must write a piece of code to encrypt passwords and credit card information used by an online shopping cart. The passwords must be stored using one-way encryption, while credit card information must be stored using reversible encryption. Which of the following should be used to accomplish this task? (Select TWO)

A. SHA for passwords
B. 3DES for passwords
C. RC4 for passwords
D. AES for credit cards
E. MD5 for credit cards
F. HMAC for credit cards

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 373
A company needs to provide a secure backup mechanism for key storage in a PKI. Which of the following should the company implement?

A. Ephemeral keys
B. Steganography
C. Key escrow
D. Digital signatures

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 374
A security analyst must ensure that the company's web server will not negotiate weak ciphers with connecting web browsers. Which of the following supported list of ciphers MUST the security analyst disable? (Select THREE)

A. SHA

B. AES
C. RIPMED
D. NULL
E. DES
F. MD5
G. TWOFISH

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 375
A company's application is hosted at a data center. The data center providers security controls for the infrastructure. The data center provides a report identifying serval vulnerabilities regarding out of date OS patches. The company recommends the data center assumes the risk associated with the OS vulnerabilities. Which of the following concepts is being implemented?

A. Risk Transference
B. Risk Acceptance
C. Risk Avoidance
D. Risk Deterrence

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 376
Which of the following cryptographic methods is most secure for a wireless access point?

A. WPA with LEAP
B. TKIP
C. WEP with PSK
D. WPA2 with PSK

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 377
Which of the following cryptographic methods is most secure for a wireless access point?

A. WPA with LEAP
B. TKIP
C. WEP with PSK
D. WPA2 with PSK

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 378
Which of the following is considered an environmental control?

A. Video surveillance
B. Proper lighting
C. EMI shielding
D. Fencing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 379

A new web server has been provisioned at a third party hosting provider for processing credit card transactions. The security administrator runs the netstat command on the server and notices that ports 80, 443, and 3389 are in a listening state. No other ports are open. Which of the following services should be disabled to ensure secure communications?

A. HTTPS
B. HTTP
C. RDP
D. TELNET

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 380
An attacker Joe configures his service identifier to be the same as an access point advertised on a billboard. Joe then conducts a denial of service attack against the legitimate AP causing users to drop their connections and then reconnect to Joe's system with the same SSID. Which of the following Best describes this type of attack?

A. Bluejacking
B. WPS attack
C. Evil twin
D. War driving
E. Relay attack

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 381
A company used a partner company to develop critical components of an application. Several employees of the partner company have been arrested for cybercrime activities. Which of the following should be done to protect the interest of the company?

A. Perform a penetration test against the application

B. Conduct a source code review of the application
C. Perform a baseline review of the application
D. Scan the application with antivirus and anti-spyware products.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 382
Which of the following is a black box testing methodology?

A. Code, function, and statement coverage review
B. Architecture and design review
C. Application hardening
D. Penetration testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 383
An application developer has tested some of the known exploits within a new application. Which of the following should the administrator utilize to test for unidentified faults or memory leaks?

A. XSRF attacks
B. Fuzzing
C. Input Validations
D. SQL Injections

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 384
A technician wants to securely collect network device configurations and statistics through a scheduled and automated process. Which of the following should be implemented if configuration integrity is most important and a credential compromise should not allow interactive logons?

A. SNMPv3
B. TFTP
C. SSH
D. TLS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 385
A company wants to improve its overall security posture by deploying environmental controls in its datacenter. Which of the following is considered an environmental control that can be deployed to meet this goal?

A. Full-disk encryption
B. Proximity readers
C. Hardware locks
D. Fire suppression

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 386
Several employees clicked on a link in a malicious message that bypassed the spam filter and their PCs were infected with malware as a result. Which of the following BEST prevents this situation from occurring in the future?

A. Data loss prevention
B. Enforcing complex passwords
C. Security awareness training
D. Digital signatures

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 387
A security administrator wishes to prevent certain company devices from using specific access points, while still allowing them on others. All of the access points use the same SSID and wireless password. Which of the following would be MOST appropriate in this scenario?

A. Require clients to use 802.1x with EAPOL in order to restrict access
B. Implement a MAC filter on the desired access points
C. Upgrade the access points to WPA2 encryption
D. Use low range antennas on the access points that ne4ed to be restricted

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 388
A company has 5 users. Users 1, 2 and 3 need access to payroll and users 3, 4 and 5 need access to sales. Which of the following should be implemented to give the appropriate access while enforcing least privilege?

A. Assign individual permissions to users 1 and 2 for payroll. Assign individual permissions to users 4 and 5 for sales. Make user 3 an administrator.
B. Make all users administrators and then restrict users 1 and 2 from sales. Then restrict users 4 and 5 from payroll
C. Create two additional generic accounts, one for payroll and one for sales that users utilize
D. Create a sales group with users 3, 4 and 5. Create a payroll group with users 1, 2 and 3

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 389

A company is concerned that a compromised certificate may result in a man-in-the-middle attack against backend financial servers. In order to minimize the amount of time a compromised certificate would be accepted by other servers, the company decides to add another validation step to SSL/TLS connections. Which of the following technologies provides the FASTEST revocation capability?

A. Online Certificate Status Protocol (OCSP)
B. Public Key Cryptography (PKI)
C. Certificate Revocation Lists (CRL)
D. Intermediate Authority (CA)

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 390

A security administrator has deployed all laptops with Self encrypting Drives (SED) and enforces key encryption. Which of the following represents the greatest threat to maintaining data confidentiality with these devices?

A. Full data access can be obtained by connecting the drive or a SATA or USB adapter bypassing the SED hardware
B. A malicious employee can gain the SED encryption keys through software extraction allowing access to other laptops
C. If the laptop does not use a secure boot BIOS, the SED hardware is not enabled allowing full data access
D. Laptops that are placed in a sleep mode allow full data access when powered back on

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 391

Which of the following password attacks is MOST likely to crack the largest number of randomly generated passwords?

A. Hybrid
B. Birthday Attack
C. Dictionary
D. Rainbow tables

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 392
Which of the following controls would allow a company to reduce the exposure of sensitive systems from unmanaged devices on internal networks?

A. 802.1X
B. Data Encryption
C. Password strength
D. BGP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 393
An attacker Joe configures his service identifier to be as an access point advertised on a billboard. Joe then conducts a denial of service attack against the legitimate AP causing users to drop their connections and then reconnect to Joe's system with the same SSID. Which of the following BEST describes this of attack?

A. Bluejacking
B. WPS attack
C. Evil twin
D. War driving
E. Replay attack

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 394
Three of the primary security control types that can be implemented are.

A. supervisory, subordinate, and peer.
B. personal, procedural, and legal.
C. operational, technical, and management.
D. mandatory, discretionary, and permanent.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 395
Which of the following may be used with a BNC connector?

A. 10GBaseT
B. 1000BaseSX
C. 100BaseFX
D. 10Base2

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 396

a network technician has received comments from several users that cannot reach a particular website. Which of the following commands would provide the BEST information about the path taken across the network to this website?

A. Ping
B. Netstat
C. telnet
D. tracert

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 397
A technician is configuring a switch to support VOPIP phones. The technician wants to ensure the phones do not require external power packs. Which of the following would allow the phones to be powered using the network connection?

A. PoE+
B. PBX
C. PSTN
D. POTS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 398
A technician reports a suspicious individual is seen walking around the corporate campus. The individual is holding a smartphone and pointing a small antenna, in order to collect SSIDs. Which of the following attacks is occurring?

A. Rogue AP
B. Evil Twin
C. Man-in-the-middle
D. War driving

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 399
Users have reported receiving unsolicited emails in their inboxes, often times with malicious links embedded. Which of the following should be implemented in order to redirect these messages?

A. Proxy server
B. Spam filter
C. Network firewall
D. Application firewall.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 400
A company uses SSH to support internal users. They want to block external SSH connections from reaching internal machines. Which of the following should be blocked on the firewall?

A. 22
B. 23
C. 443
D. 8080

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 401
If an organization wants to implement a BYOD policy, which of the following administrative control policy considerations MUST be addressed? (select two)

A. Data archiving
B. Data ownership
C. Geo-tagging
D. Acceptable use
E. Remote wipe

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 402
A security technician wants to implement stringent security controls over web traffic by restricting the client source TCP ports allowed through the corporate firewall. Which of the following should the technician implement?

A. Deny port 80 and 443 but allow proxies
B. Only allow port 80 and 443
C. Only allow ports above 1024
D. Deny ports 80 and allow port 443

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 403
An administrator is configuring a network for all users in a single building. Which of the following design elements would be used to segment the network based on organizational groups (select two)

A. NAC
B. NAT

C. Subnetting
D. VLAN
E. DMZ
F. VPN

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 404
A datacenter has suffered repeated burglaries which led to equipment theft and arson. In the past, the thieves have demonstrated a determination to bypass any installed safeguards. After mantraps were installed to prevent tailgating, the thieves crashed through the wall of datacenter with a vehicle after normal business hours. Which of the following options could improve the safety and security of the datacenter further? (Select two)

A. Cipher locks
B. CCTV
C. Escape routes
D. K rated fencing
E. Fm200 fire suppression

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 405
which of the following can take advantage of man in the middle techniques to prevent data exfiltration?

A. DNS poisoning
B. URL hijacking
C. ARP spoofing
D. HTTPS inspection

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 406
An administrator must select an algorithm to encrypt data at rest. Which of the following could be used?

A. RIPEMD
B. Diffie-hellman
C. ECDSA
D. CHAP
E. Blowfish

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 407
RC4 is a strong encryption protocol that is general used with which of the following?

A. WPA2 CCMP
B. PEAP
C. WEP
D. EAP-TLS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 408

An outside security consultant produces a report of several vulnerabilities for a particular server. Upon further investigation, it is determine that the vulnerability reported does not apply to the platform the server is running on. Which of the following should the consultant do in order to produce more accurate results?

A. A black box test should be used to increase the validity of the scan
B. Perform a penetration test in addition to a vulnerability scan
C. Use banner grabbing to identify the target platform
D. Use baseline reporting to determine the actual configuration

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 409
a programmer has allocated a 32 bit variable to store the results of an operation between two user supplied 4 byte operands. To which of the following types of attack is this application susceptible?

A. XML injection
B. Command injection
C. Integer overflow
D. Header manipulation

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 410
A security administrator is reviewing logs and notices multiple attempts to access the HVAC controls by a workstation with an IP address from the open wireless network. Which of the following would be the best way to prevent this type of attack from occurring again?

A. Implement VLANs to separate the HVAC
B. Enable WPA2 security for the wireless network
C. Install a HIDS to protect the HVAC system
D. Enable Mac filtering for the wireless network

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 411
An application developer needs to allow employees to use their network credentials to access a new application being developed. Which of the following should be configured in the new application to enable this functionality?

A. LDAP
B. ACLs
C. SNMP
D. IPSec

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 412
During a routine audit it is discovered that someone has been using a state administrator account to log into a seldom used server. The person used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could BEST prevent this from occurring again?

A. Credential management
B. Group policy management

C. Acceptable use policies
D. Account expiration policies

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 413
A security engineer would like to analyze the effect of deploying a system without patching it to discover potential vulnerabilities. Which of the following practices would best allow for this testing while keeping the corporate network safe?

A. Perform grey box testing of the system to verify the vulnerabilities on the system
B. Utilize virtual machine snapshots to restore from compromises
C. Deploy the system in a sandbox environment on the virtual machine
D. Create network ACLs that restrict all incoming connections to the system

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 414
the internal audit group discovered that unauthorized users are making unapproved changes to various system configuration settings. This issue occurs when previously authorized users transfer from one department to another and maintain the same credentials. Which of the following controls can be implemented to prevent such unauthorized changes in the future?

A. Periodic access review
B. Group based privileges
C. Least privilege
D. Account lockout

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 415

in order to gain an understanding of the latest attack tools being used in the wild, an administrator puts a Unix server on the network with the root users password to set root. Which of the following best describes this technique?

A. Pharming
B. Honeypot
C. Gray box testing
D. phishing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 416

AN administrator, Ann, wants to ensure that only authorized devices are connected to a switch. She decides to control access based on MAC addresses. Which of the following should be configured?

A. Implicit deny
B. Private VLANS
C. Flood guard
D. Switch port security

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 417

an one time security audit revealed that employees do not have the appropriate access to system resources. The auditor is concerned with the fact that most of the accounts audited have unneeded elevated permission to sensitive resources. Which of the following was implemented to detect this issue?

A. Continuous monitoring
B. Account review
C. Group based privileges
D. Credential management

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 418
a security analyst has a sample of malicious software and needs to know what the sample in a carefully controlled and monitored virtual machine to observe the software's behavior. After the software has run, the analyst returns the virtual machines OS to a pre-defined know good state using what feature of virtualization?

A. Host elasticity
B. Antivirus
C. sandbox
D. snapshots

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 419
Joe, the chief technical officer (CTO) is concerned that the servers and network devices may not be able to handle the growing needs of the company. He has asked his network engineer to being monitoring the performance of these devices and present statistics to management for capacity planning. Which of the following protocols should be used to this?

A. SNMP
B. SSH
C. TLS
D. ICMP

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 420
a security administrator is responsible for ensuring that there are no unauthorized devices utilizing the corporate network. During a routine scan, the security administrator discovers an unauthorized device belonging to a user in the marketing department. The user is using an android phone in order to browse websites. Which of the following device attributes was used to determine that the device was unauthorized?

A. An IMEI address
B. A phone number
C. A MAC address
D. An asset ID

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 421
a website is breached, exposing the usernames and MD5 password hashes of its entire user base. Many of these passwords are later cracked using rainbow tables. Which of the following actions could have helped prevent the use of rainbow tables on the password hashes?

A. use salting when computing MD5 hashes of the user passwords
B. Use SHA as a hashing algorithm instead of MD%
C. Require SSL for all user logins to secure the password hashes in transit
D. Prevent users from using a dictionary word in their password

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 422
Joe a network administrator is setting up a virtualization host that has additional storage requirements. Which of the following protocols should be used to connect the device to the company SAN? (Select Two)

A. Fibre channel
B. SCP
C. iSCSI
D. FDDI
E. SSL

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 423
A security administrator finds that an intermediate CA within the company was recently breached. The certificates held on this system were lost during the attack, and it is suspected that the attackers had full access to the system. Which of the following is the NEXT action to take in this scenario.

A. Use a recovery agent to restore the certificates used by the intermediate CA
B. Revoke the certificate for the intermediate CA
C. Recover the lost keys from the intermediate CA key escrow
D. Issue a new certificate for the root CA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 424
A recent online password audit has identified that stale accounts are at risk to brute force attacks. Which the following controls would best mitigate this risk?

A. Password length
B. Account disablement
C. Account lockouts

D. Password complexity

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 425
The security administrator generates a key pair and sends one key inside a rest file to a third party. The third party sends back a signed file. In this scenario, the file sent by the administrator is a:

A. CA
B. CRL
C. KEK
D. PKI
E. CSR

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 426
joe, a security technician, is configuring two new firewalls through the web on each. Each time joe connects, there is a warning message in the browser window about the certificate being untrusted. Which of the following will allow joe to configure a certificate for the firewall so that firewall administrators are able to connect both firewalls without experiencing the warning message?

A. Apply a permanent override to the certificate warning in the browser
B. Apply a wildcard certificate obtained from the company's certificate authority
C. Apply a self-signed certificate generated by each of the firewalls
D. Apply a single certificate obtained from a public certificate authority

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 427

a company has had their web application become unavailable several times in the past few months due to increased demand. Which of the following should the company perform to increase availability?

A. Implement a web application firewall to prevent DDoS attacks'

B. Configure the firewall to work with the IPS to rate limit customer requests

C. Implement a load balancer to distribute traffic based on back end server utilization

D. Configure the web server to detect race conditions and automatically restart the web services

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 428

a system administrator wants to prevent password compromises from offline password attacks. Which of the following controls should be configured to BEST accomplish this task? (Select TWO)

A. Password reuse

B. Password length

C. Password complexity

D. Password history

E. Account lockouts

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 429

a company recently experienced several security breaches that resulted in confidential data being infiltrated form the network. The forensic investigation revealed that the data breaches were caused by an insider accessing files that resided in shared folders who then encrypted the data and sent it to contacts via third party email. Management is concerned that other employees may also be sending confidential files outside of the company to the same organization. Management has requested that the IT department implement a solution that will allow them to; Track access and sue of files marked confidential, provide documentation that can be sued for investigations, prevent employees from sending confidential data via secure third party email, identify other employees that may be involved in these activities, which of the following would be the best choice to implement to meet the above requirements?

A. Web content filtering capable of inspe4cting and logging SSL traffic used by third party webmail providers
B. Full disk encryption on all computers with centralized event logging and monitoring enabled
C. Host based firewalls with real time monitoring and logging enabled
D. Agent-based DLP software with correlations and logging enabled

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 430
Which of the following BEST describes malware that tracks a user's web browsing habits and injects the attacker's advertisements into unrelated web pages? (Select TWO)

A. Logic bomb
B. Backdoor
C. Ransomware
D. Adware
E. Botnet
F. Spyware

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 431
The chief security officer (CSO) has issued a new policy to restrict generic or shared accounts on company systems. Which of the following sections of the policy requirements will have the most impact on generic and shared accounts?

A. Account lockout
B. Password length
C. Concurrent logins
D. Password expiration

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 432
joe an end user has received a virus detection warning. Which of the following is the first course of action that should be taken?

A. Recovery
B. Reporting
C. Remediation
D. Identification

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 433
a company has several public conference room areas with exposed network outlets. In the past, unauthorized visitors and vendors have used the outlets for internet access. The help desk manager does not want the outlets to be disabled due to the number of training sessions in the conference room and the amount of time it takes to get the ports either patched in or enabled. Which of the following is the best option for meeting this goal?

A. Flood guards
B. Port security
C. 802.1x
D. Loop protection
E. IPSec

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 434
an attacker unplugs the access point at a coffee shop. The attacker then runs software to make a laptop look like an access point and advertises the same network as the coffee shop normally does.
Which of the following describes this type of attack?

A. IV
B. Xmas
C. Packet sniffing
D. Evil twin
E. Rouge AP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 435
A network administrator argues that WPA2 encryption is not needed, as MAC filtering is enabled on the access point. Which of the following would show the administrator that wpa2 is also needed?

A. Deploy an evil twin with mac filtering
B. Flood access point with random mac addresses
C. Sniff and clone a mac address
D. DNS poison the access point

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 436
a security director has contracted an outside testing company to evaluate the security of a newly developed application. None of the parameters or internal workings of the application have been provided to the testing company prior to the start of testing. The testing company will be using:

A. Gray box testing
B. Active control testing
C. White box testing
D. Black box testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 437
while preparing for an audit a security analyst is reviewing the various controls in place to secure the operation of financial processes within the organization. Based on the pre assessment report, the department does not effectively maintain a strong financial transaction control environment due to conflicting responsibilities held by key personnel. If implemented, which of the following security concepts will most effectively address the finding?

A. Least privilege
B. Separation of duties
C. Time-based access control
D. Dual control

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 438
A chief privacy officer, joe, is concerned that employees are sending emails to addresses outside of the company that contain PII. He asks that the security technician to implement technology that will mitigate this risk. Which of the following would be the best option?

A. DLP
B. HIDS
C. Firewall
D. Web content filtering

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 439
the key management organization has implemented a key escrowing function. Which of the following technologies can provide protection for the PKI's escrowed keys?

A. CRL
B. OCSP
C. TPM
D. HSM

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 440
which of the following are unique to white box testing methodologies? (Select two)

A. Application program interface API testing
B. Bluesnarfing
C. External network penetration testing
D. Function, statement and code coverage
E. Input fuzzing

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 441
a technician installed two ground plane antennae on 802.11n bridges connecting two buildings 500 feet apart. After configuring both radios to work at 2.4ghz and implementing the correct configuration, connectivity tests between the two buildings are unsuccessful. Which of the following should the technician do to resolve the connectivity problem?

A. Substitute wireless bridges for wireless access points
B. Replace the 802.11n bridges with 802.11ac bridges
C. Configure both bridges to use 5GHz instead of 2.4GHz
D. Replace the current antennae with Yagi antennae

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 442
a company has had several security incidents in the past six months. It appears that the majority of the incidents occurred on systems with older software on development workstations. Which of the following should be implemented to help prevent similar incidents in the future?

A. Peer code review
B. Application whitelisting
C. Patch management
D. Host-based firewall

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 443
a router was shut down as a result of a DoS attack. Upon review of the router logs, it was determined that the attacker was able to connect to the router using a console cable to complete the attack. Which of the following should have been implemented on the router to prevent this attack? (select two)

A. IP ACLs should have been enabled on the console port on the router
B. Console access to the router should have been disabled
C. Passwords should have been enabled on the virtual terminal interfaces on the router
D. Virtual terminal access to the router should have been disabled
E. Physical access to the router should have been restricted

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 444
a systems administrator is configuring a new file server and has been instructed to configure writeable to by the department manager, and read only for the individual employee. Which of the following is the name for the access control methodology used?

A. Duty separation
B. Mandatory
C. Least privilege
D. Role-based

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 445
an administrator is implementing a security control that only permits the execution of allowed programs. Which of the following are cryptography concepts that should be used to identify the allowed programs? Select two

A. Digital signatures
B. Hashing

C. Asymmetric encryption
D. openID
E. key escrow

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 446
while responding to an incident on a Linux 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. Lsof
B. Tcpdump
C. Top
D. Ifconfig

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 447
a bank chief information security officer (CISO) is responsible for a mobile banking platform that operates natively on iOS and Andriod. Which of the following security controls helps protect the associated publicly accessible API endpoints?

A. Mobile device management
B. Jailbreak detection
C. Network segmentation
D. Application firewalls

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 448

a company is rolling out a new e-commerce website. The security analyst wants to reduce the risk of the new website being comprised by confirming that system patches are up to date, application hot fixes are current, and unneeded ports and services have been disabled. To do this, the security analyst will perform a :

A. Vulnerability assessment
B. White box test
C. Penetration test
D. Peer review

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 449

Joe, a security analyst, is attempting to determine if a new server meets the security requirements of his organization. As a step in this process, he attempts to identify a lack of security controls and to identify common misconfigurations on the server. Which of the following is joe attempting to complete?

A. Black hat testing
B. Vulnerability scanning
C. Black box testing
D. Penetration testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 450

a classroom utilizes workstations running virtualization software for a maximum of one virtual machine per working station. The network settings on the virtual machines are set to bridged. Which of the following describes how the switch in the classroom should be configured to allow for the virtual machines and host workstation to connect to network resources?

A. The maximum-mac settings of the ports should be set to zero
B. The maximum-mac settings of the ports should be set to one
C. The maximum-mac settings of the ports should be set to two
D. The maximum mac settings of the ports should be set to three

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 451
Which of the following attacks initiates a connection by sending specially crafted packets in which multiple TCP flags are set to 1?

A. Replay
B. Smurf
C. Xmas
D. Fraggle

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 452
a company transfers millions of files a day between their servers. A programmer for the company has created a program that indexes and verifies the integrity of each file as it is replicated between servers. The programmer would like to use the fastest algorithm to ensure integrity. Which of the following should the programmer use?

A. SHA1
B. RIPEMD
C. DSA
D. MD5

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 453
a system administrator is conducting baseline audit and determines that a web server is missing several critical updates. Which of the following actions should the administrator perform first to correct the issue?

A. Open a service ticket according to the patch management plan
B. Disconnect the network interface and use the administrative management console to perform the updates
C. Perform a backup of the server and install the require patches
D. Disable the services for the web server but leave the server alone pending patch updates

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 454
the it department has been tasked with reducing the risk of sensitive information being shared with unauthorized entities from computers it is saved on, without impeding the ability of the employees to access the internet. Implementing which of the following would be the best way to accomplish this objective?

A. Host-based firewalls
B. DLP
C. URL filtering
D. Pop-up blockers

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 455

a server crashes at 6 pm. Senior management has determined that data must be restored within two hours of a server crash. Additionally, a loss of more than one hour worth of data is detrimental to the company's financial well-being. Which of the following is the RTO?

A. 7pm
B. 8pm
C. 9pm
D. 10pm

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 456
To mitigate the risk of intrusion, an IT Manager is concerned with using secure versions of protocols and services whenever possible. In addition, the security technician is required to monitor the types of traffic being generated. Which of the following tools is the technician MOST likely to use?

A. Port scanner
B. Network analyzer
C. IPS
D. Audit Logs

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 457
An administrator is implementing a new management system for the machinery on the company's production line. One requirement is that the system only be accessible while within the production facility. Which of the following will be the MOST effective solution in limiting access based on this requirement?

A. Access control list
B. Firewall policy
C. Air Gap
D. MAC filter

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 458
A risk assessment team is concerned about hosting data with a cloud service provider (CSP) which of the following findings would justify this concern?

A. The cps utilizes encryption for data at rest and in motion
B. The CSP takes into account multinational privacy concerns
C. The financial review indicates the company is a startup
D. SLA state service tickets will be resolved in less than 15 minutes

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 459
A company wishes to prevent unauthorized employee access to the data center. Which of the following is the MOST secure way to meet this goal?

A. Use Motion detectors to signal security whenever anyone entered the center
B. Mount CCTV cameras inside the center to monitor people as they enter
C. Install mantraps at every entrance to the data center in conjunction with their badges
D. Place biometric readers at the entrances to verify employees identity

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 460

A company hosts a web server that requires entropy in encryption initialization and authentication. To meet this goal, the company would like to select a block cipher mode of operation that allows an arbitrary length IV and supports authenticated encryption. Which of the following would meet these objectives?

A. CFB
B. GCM
C. ECB
D. CBC

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 461
A chief information security officer (CISO) is providing a presentation to a group of network engineers. In the presentation, the CISO presents information regarding exploit kits. Which of the following might the CISO present?

A. Exploit kits are tools capable of taking advantage of multiple CVEs
B. Exploit kits are vulnerability scanners used by penetration testers
C. Exploit kits are WIFI scanning tools that can find new honeypots
D. Exploit kits are a new type of malware that allow attackers to control their computers

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 462
During a company-wide initiative to harden network security, it is discovered that end users who have laptops cannot be removed from the local administrator group. Which of the following could be used to help mitigate the risk of these machines becoming compromised?

A. Security log auditing
B. Firewalls
C. HIPS
D. IDS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 463
An administrator receives a security alert that appears to be from one of the company's vendors. The email contains information and instructions for patching a serious flaw that has not been publicly announced. Which of the following can an employee use to validate the authenticity if the email?

A. Hashing algorithm
B. Ephemeral Key
C. SSL certificate chain
D. Private key
E. Digital signature

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 464
A project team is developing requirements of the new version of a web application used by internal and external users. The application already features username and password requirements for login, but the organization is required to implement multifactor authentication to meet regulatory requirements. Which of the following would added requirements will satisfy the regulatory requirement? (Select THREE)

A. Digital certificate
B. Personalized URL
C. Identity verification questions
D. Keystroke dynamics
E. Tokenized mobile device
F. Time-of-day restrictions
G. Increased password complexity
H. Rule-based access control

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 465
A bank is planning to implement a third factor to protect customer ATM transactions. Which of the following could the bank implement?

A. SMS
B. Fingerprint
C. Chip and Pin
D. OTP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 466
Which of the following internal security controls is aimed at preventing two system administrators from completing the same tasks?

A. Least privilege
B. Separation of Duties
C. Mandatory Vacation
D. Security Policy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 467

An administrator performs a risk calculation to determine if additional availability controls need to be in place. The administrator estimates that a server fails and needs to be replaced once every 2 years at a cost of $8,000. Which of the following represents the factors that the administrator would use to facilitate this calculation?

A. ARO= 0.5; SLE= $4,000; ALE= $2,000
B. ARO=0.5; SLE=$8,000; ALE=$4,000
C. ARO=0.5; SLE= $4,000; ALE=$8,000
D. ARO=2; SLE= $4,000; ALE=$8,000
E. ARO=2; SLE= $8,000; ALE= $16,000

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 468
A security administrator needs to implement a technology that creates a secure key exchange. Neither party involved in the key exchange will have pre-existing knowledge of one another. Which of the following technologies would allow for this?

A. Blowfish
B. NTLM
C. Diffie-Hellman
D. CHAP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 469
A technician has been assigned a service request to investigate a potential vulnerability in the organization's extranet platform. Once the technician performs initial investigative measures, it is determined that the potential vulnerability was a false-alarm. Which of the following actions should the technician take in regards to the findings?

A. Write up the findings and disable the vulnerability rule in future vulnerability scans

B. Refer the issue to the server administrator for resolution
C. Mark the finding as a false-negative and close the service request
D. Document the results and report the findings according to the incident response plan

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 470
A security administrator is using a software program to test the security of a wireless access point. After running the program for a few hours, the access point sends the wireless secret key back to the software program. Which of the following attacks is this an example of?

A. WPS
B. IV
C. Deauth
D. Replay

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 471
A user, Ann, has been issued a smart card and is having problems opening old encrypted email. Ann published her certificates to the local windows store and to the global address list. Which of the following would still need to be performed?

A. Setup the email security with her new certificates
B. Recover her old private certificate
C. Reinstall her previous public certificate
D. Verify the correct email address is associated with her certificate

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 472
which of the following is a best practice when setting up a client to use the LDAPS protocol with a server?

A. The client should follow LDAP referrals to other secure servers on the network
B. The client should trust the CA that signed the server's certificate
C. The client should present a self-signed certificate to the server
D. The client should have access to port 389 on the server

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 473
A network manager needs a cost-effective solution to allow for the restoration of information with a RPO of 24 hours. The disaster recovery plan also requires that backups occur within a restricted timeframe during the week and be take offsite weekly. Which of the following should the manager choose to BEST address these requirements?

A. Daily incremental backup to tape
B. Disk-to-disk hourly server snapshots
C. Replication of the environment at a hot site
D. Daily differential backup to tape
E. Daily full backup to tape

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 474
Given the following set of firewall rules:

From the inside to outside allow source any destination any port any From inside to dmz allow source any destination any port tcp-80 From inside to dmz allow source any destination any port tcp-443 Which of the following would prevent FTP traffic from reaching a server in the DMZ from the inside network?

A. Implicit deny
B. Policy routing
C. Port forwarding
D. Forwarding proxy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 475
During a routine configuration audit, a systems administrator determines that a former employee placed an executable on an application server. Once the system was isolated and diagnosed, it was determined that the executable was programmed to establish a connection to a malicious command and control server. Which of the following forms of malware is best described in the scenario?

A. Logic bomb
B. Rootkit
C. Back door
D. Ransomware

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 476
The chief information officer (CIO) of a major company intends to increase employee connectivity and productivity by issuing employees mobile devices with access to their enterprise email, calendar, and contacts. The solution the CIO intends to use requires a PKI that automates the enrollment of mobile device certificates. Which of the following, when implemented and configured securely, will meet the CIO's requirement?

A. OCSP
B. SCEP

C. SAML
D. OSI

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 477
An attacker impersonates a fire marshal and demands access to the datacenter under the threat of a fine. Which of the following reasons make this effective? (select two)

A. Consensus
B. Authority
C. Intimidation
D. Trust
E. Scarcity

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 478
In the course of troubleshooting wireless issues from users a technician discovers that users are connecting to their home SSIDs which the technician scans but detects none of these SSIDs. The technician eventually discovers a rouge access point that spoofs any SSID request. Which of the following allows wireless use while mitigating this type of attack?

A. Configure the device to verify access point MAC addresses
B. Disable automatic connection to known SSIDs
C. Only connect to trusted wireless networks
D. Enable MAC filtering on the wireless access point

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 479
Which of the following describes the implementation of PAT?

A. Translating the source and destination IPS, but not the source and destination ports
B. A one to one persistent mapping between on private IP and one Public IP
C. Changing the priority of a TCP stream based on the source address
D. Associating multiple public IP addresses with one private address

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 480
Which of the following forms of software testing can best be performed with no knowledge of how a system is internally structured or functions? (Select Two)

A. Boundary testing
B. White box
C. Fuzzing
D. Black box
E. Grey Box

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 481
A load balancer has the ability to remember which server a particular client is using and always directs that client to the same server. This feature is called:

A. Cookie tracking
B. URL filtering
C. Session affinity
D. Behavior monitoring

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 482
A company has recently begun to provide internal security awareness for employees. Which of the following would be used to demonstrate the effectiveness of the training?

A. Metrics
B. Business impact analysis
C. Certificate of completion
D. Policies

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 483
Users in an organization are experiencing when attempting to access certain websites. The users report that when they type in a legitimate URL, different boxes appear on the screen, making it difficult to access the legitimate sites. Which of the following would best mitigate this issue?

A. Pop-up blockers
B. URL filtering
C. Antivirus
D. Anti-spam

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 484

A company hires a penetration testing team to test its overall security posture. The organization has not disclosed any information to the penetration testing team and has allocated five days for testing. Which of the following types of testing will the penetration testing team have to conduct?

A. Static analysis

B. Gray Box

C. White box

D. Black box

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 485

A web administrator has just implemented a new web server to be placed in production. As part of the company's security plan, any new system must go through a security test before it is placed in production, The security team runs a port scan resulting in the following data:
21 tcp open FTP
23 tcp open Telnet
22 tcp open SSH
25 UDP open smtp
110 tcp open pop3
443 tcp open https
Which of the following is the BEST recommendation for the web administrator?

A. Implement an IPS

B. Disable unnecessary services

C. Disable unused accounts

D. Implement an IDS

E. Wrap TELNET in SSL

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 486
Which of the following best describes the reason for using hot and cold aisles?

A. To ensure air exhaust from one aisle doesn't blow into the air intake of the next aisle
B. To ensure the dewpoint stays low enough that water doesn't condensate on equipment
C. To decrease amount of power wiring that is run to each aisle
D. Too maintain proper humidity in the datacenter across all aisles

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 487
An organization has an internal PKI that utilizes client certificates on each workstation. When deploying a new wireless network, the security engineer has asked that the new network authenticate clients by utilizes the existing client certificates. Which of the following authentication mechanisms should be utilized to meet this goal?

A. EAP-FAST
B. LEAP
C. PEAP
D. EAP-TLS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 488

An attacker is attempting to insert malicious code into an installer file that is available on the internet. The attacker is able to gain control of the web server that houses both the installer and the web page which features information about the downloadable file. To implement the attack and delay detection, the attacker should modify both the installer file and the:

A. SSL certificate on the web server
B. The HMAC of the downloadable file available on the website
C. Digital signature on the downloadable file
D. MD5 hash of the file listed on the website

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 489
After receiving the hard drive from detectives, the forensic analyst for a court case used a log to capture corresponding events prior to sending the evidence to lawyers. Which of the following do these actions demonstrate?

A. Chain of custody
B. Order if volatility
C. Data analysis
D. Tracking man hours and expenses

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 490
A group of users from multiple departments are working together on a project and will maintain their digital output in a single location. Which of the following is the BEST method to ensure access is restricted to use by only these users?

A. Mandatory access control
B. Rule-based access
C. Group based privileges

D. User assigned privileges

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 491
Which of the following technologies when applied to android and iOS environments, can an organization use to add security restrictions and encryption to existing mobile applications? (Select Two)

A. Mobile device management
B. Containerization
C. Application whitelisting
D. Application wrapping
E. Mobile application store

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 492
A server administrator discovers the web farm is using weak ciphers and wants to ensure that only stronger ciphers are accepted. Which of the following ciphers should the administrator implement in the load balancer? (Select Two)

A. SHA-129
B. DES
C. MD5
D. RC4
E. CRC-32

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 493
An application developer has coded a new application with a module to examine all user entries for the graphical user interface. The module verifies that user entries match the allowed types for each field and that OS and database commands are rejected before entries are sent for further processing within the application. These are example of:

A. Input validation
B. SQL injection
C. Application whitelisting
D. Error handling

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 494
Ann, a security administrator is hardening the user password policies. She currently has the following in place.
Passwords expire every 60 days
Password length is at least eight characters
Passwords must contain at least one capital letter and one numeric character Passwords cannot be reused until the password has been changed eight times She learns that several employees are still using their original password after the 60-day forced change. Which of the following can she implement to BEST mitigate this?

A. Lower the password expiry time to every 30days instead of every 60 days
B. Require that the password contains at least one capital, one numeric, and one special character
C. Change the re-usage time from eight to 16 changes before a password can be repeated
D. Create a rule that users can only change their passwords once every two weeks

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 495
Which of the following BEST describes disk striping with parity?

A. RAID O
B. RAID 1
C. RAID 2
D. RAID 5

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 496
Which of the following will allow the live state of the virtual machine to be easily reverted after a failed upgrade?

A. Replication
B. Backups
C. Fault tolerance
D. Snapshots

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 497
An organization currently uses FTP for the transfer of large files, due to recent security enhancements, is now required to use a secure method of file transfer and is testing both SFTP and FTPS as alternatives. Which of the following ports should be opened on the firewall in order to test the wto alternatives? (Select Two)

A. TCP 22
B. TCP 25
C. TCP 69
D. UDP 161

E. TCP 990
F. TCP 3380

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 498
Which of the following types of malware, attempts to circumvent malware detection by trying to hide its true location on the infected system?

A. Armored virus
B. Ransomware
C. Trojan
D. Keylogger

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 499
An attacker went to a local bank and collected disposed paper for the purpose of collecting data that could be used to steal funds and information from the bank's customers. This is an example of:

A. Impersonation
B. Whaling
C. Dumpster diving
D. Hoaxes

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 500
An employee reports work was being completed on a company owned laptop using a public wireless hotspot. A pop-up screen appeared and the user closed the pop-up. Seconds later the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

A. Ransomware
B. Rootkit
C. Scareware
D. Spyware

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 501
A small IT security form has an internal network composed of laptops, servers, and printers. The printers. The network has both wired and wireless segments and supports VPN access from remote sites. To protect the network from internal and external threats, including social engineering attacks, the company decides to implement stringent security controls. Which of the following lists is the BEST combination of security controls to implement?

A. Disable SSID broadcast, require full disk encryption on servers, laptop, and personally owned electronic devices, enable MAC filtering on WAPs, require photographic ID to enter the building
B. Enable port security; divide the network into segments for servers, laptops, public and remote users; apply ACLs to all network equipment; enable MAC filtering on WAPs; and require two-factor authentication for network access
C. Divide the network into segments for servers, laptops, public and remote users; require the use of one time pads for network key exchange and access; enable MAC filtering ACLs on all servers
D. Enable SSID broadcast on a honeynet; install monitoring software on all corporate equipment' install CCTVs to deter social engineering; enable SE Linux in permissive mode.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 502
A security analyst is working on a project team responsible for the integration of an enterprise SSO solution. The SSO solution requires the use of an open standard for the exchange of authentication and authorization across numerous web based applications. Which of the following solutions is most appropriate for the analyst to recommend in this scenario.

A. SAML
B. XTACACS
C. RADIUS
D. TACACS+
E. Secure LDAP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 503
A thief has stolen mobile device and removed its battery to circumvent GPS location tracking. The device user a four digit PIN. Which of the following is a mobile device security control that ensures the confidentiality of company data?

A. Remote wiping
B. Mobile Access control
C. Full device encryption
D. Inventory control

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 504

A user has called the help desk to report an enterprise mobile device was stolen. The technician receiving the call accesses the MDM administration portal to identify the device's last known geographic location. The technician determines the device is still communicating with the MDM. After taking note of the last known location, the administrator continues to follow the rest of the checklist. Which of the following identifies a possible next step for the administrator?

A. Remotely encrypt the device
B. Identify the mobile carrier's IP address
C. Reset the device password
D. Issue a remote wipe command

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 505

A risk management team indicated an elevated level of risk due to the location of a corporate datacenter in a region with an unstable political climate. The chief information officer (CIO) accepts the recommendation to transition the workload to an alternate datacenter in a more stable region. Which of the following forms of risk mitigation has the CIO elected to pursue?

A. Deterrence
B. Transference
C. Avoidance
D. Acceptance
E. sharing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 506

During a recent audit, the auditors cited the company's current virtual machine infrastructure as a concern. The auditors cited the fact that servers containing sensitive customer information reside on the same physical host as numerous virtual machines that follow less stringent security guild lines. Which of the following would be the best choice to implement to address this audit concern while maintain the current infrastructure?

A. Migrate the individual virtual machines that do not contain sensitive data to separate physical machines
B. Implement full disk encryption on all servers that do not contain sensitive customer data
C. Move the virtual machines that contain the sensitive information to a separate host
D. Create new VLANs and segment the network according to the level of data sensitivity 524 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?
E. A pc had a NIC replaced and reconnected to the switch
F. An ip telephone has been plugged in
G. A rouge access point was plugged in
H. An arp attack was launched from a pc on this port

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 507
a network administrator was to implement a solution that will allow authorized traffic, deny unauthorized traffic and ensure that appropriate ports are being used for a number of TCP and UDP protocols. Which of the following network controls would meet these requirements?

A. Stateful firewall
B. Web security gateway
C. URL filter
D. proxy server
E. web application firewall

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 508
Client computers login at specified times to check and update antivirus definitions using a dedicated account configured by the administrator. One day the clients are unable to login with the account, but the server still responds to ping requests. The administrator has not made any changed.
Which of the following most likely happened?

A. Group policy is blocking the connection attempts
B. The administrator account has been disabled
C. The switch port for the server has died
D. The password on the account has expired

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 509
In performing an authorized penetration test of an organization's system security, a penetration tester collects information pertaining to the application versions that reside on a server. Which of the following is the best way to collect this type of information?

A. Protocol analyzer
B. Banner grabbing
C. Port scanning
D. Code review

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 510
a company is deploying an new video conferencing system to be used by the executive team for board meetings. The security engineer has been asked to choose the strongest available asymmetric cipher to be used for encryption of board papers, and chose the strongest available stream cipher to be configured for video streaming. Which of the following ciphers should be chosen? (Select two)

A. RSA
B. RC4
C. 3DES
D. HMAC
E. SJA-256

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 511
Joe has hired several new security administrators and have been explaining the4 design of the company's network. He has described the position and descriptions of the company's firewalls, IDS sensors, antivirus server, DMZs, and HIPS. Which of the following best describes the incorporation of these elements?

A. Load balancers
B. Defense in depth
C. Network segmentation
D. UTM security appliance

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 512
a security administrator is selecting an MDM solution for an organization, which has strict security requirements for the confidentiality of its data on end user devices. The organization decides to allow BYOD, but requires that users wishing to participate agree to the following specific device configurations; camera disablement, password enforcement, and application whitelisting. The organization must be able to support a device portfolio of differing mobile operating systems. Which of the following represents the MOST relevant technical security criteria for the MDM?

A. Breadth of support for device manufacturers' security configuration APIS
B. Ability to extend the enterprise password polices to the chosen MDM
C. Features to support the backup and recovery of the stored corporate data

D. Capability to require the users to accept an AUP prior to device onboarding

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 513
employees are reporting that they have been receiving a large number of emails advertising products and services. Links in the email direct the users browsers to the websites for the items being offered. No reports of increased virus activity have been observed. A security administrator suspects that the users are the targets of:

A. A watering hole attack
B. Spear phishing
C. A spoofing attack
D. A spam campaign

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 514
an employee finds a usb drive in the employee lunch room and plugs the drive into a shared workstation to determine who owns the drive. When the drive is inserted, a command prompt opens and a script begins to run. The employee notifies a technician who determines that data on a server have been compromised. This is an example of:

A. Device removal
B. Data disclosure
C. Incident identification
D. Mitigation steps

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 515

A chief information officer (CIO) is concerned about PII contained in the organization's various data warehouse platforms. Since not all of the PII transferred to the organization is required for proper operation of the data warehouse application, the CIO requests the in needed PII data be parsed and securely discarded. Which of the following controls would be MOST appropriate in this scenario?

A. Execution of PII data identification assessments
B. Implementation of data sanitization routines
C. Encryption of data-at-rest
D. Introduction of education programs and awareness training
E. Creation of policies and procedures

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 516

the security administrator receives a service ticket saying a host based firewall is interfering with the operation of a new application that is being tested in delevopment. The administrator asks for clarification on which ports need to be open. The software vendor replies that it could use up to 20 ports and many customers have disabled the host based firewall. After examining the system the administrator sees several ports that are open for database and application servers that only used locally. The vendor continues to recommend disabling the host based firewall. Which of the following is the best course of action for the administrator to take?

A. Allow ports used by the application through the network firewall
B. Allow ports used externally through the host firewall
C. Follow the vendor recommendations and disable the host firewall
D. Allow ports used locally through the host firewall

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 517
a corporate wireless guest network uses an open SSID with a captive portal to authenticate guest users. Guests can obtain their portal password at the service desk. A security consultant alerts the administrator that the captive portal is easily bypassed, as long as one other wireless guest user is on the network. Which of the following attacks did the security consultant use?

A. ARP poisoning
B. DNS cache poisoning
C. MAC spoofing
D. Rouge DHCP server

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 518
A company requires that all wireless communication be compliant with the Advanced encryption standard. The current wireless infrastructure implements WEP + TKIP. Which of the following wireless protocols should be implemented?

A. CCMP
B. 802.1x
C. 802.3
D. WPA2
E. AES

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 519
A security analyst, while doing a security scan using packet c capture security tools, noticed large volumes of data images of company products being exfiltrated to foreign IP addresses. Which of the following is the FIRST step in responding to scan results?

A. Incident identification
B. Implement mitigation
C. Chain of custody
D. Capture system image

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 520
An administrator deploys a WPA2 Enterprise wireless network with EAP-PEAP-MSCHAPv2. The deployment is successful and company laptops are able to connect automatically with no user intervention. A year later, the company begins to deploy phones with wireless capabilities. Users report that they are receiving a warning when they attempt to connect to the wireless network from their phones. Which of the following is the MOST likely cause of the warning message?

A. Mutual authentication on the phone is not compatible with the wireless network
B. The phones do not support WPA2 Enterprise wireless networks
C. User certificates were not deployed to the phones
D. The phones' built in web browser is not compatible with the wireless network
E. Self-signed certificates were used on the RADIUS servers

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 521
an attacker has gained access to the company's web server by using the administrator's credentials. The attacker then begins to work on compromising the sensitive data on other servers. Which off the following BEST describes this type of attack?

A. Privilege escalation
B. Client-side attack
C. Man-in-the-middle

D. Transitive access

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 522
A security technician is concerned there4 is not enough security staff available the web servers and database server located in the DMZ around the clock. Which of the following technologies, when deployed, would provide the BEST round the clock automated protection?

A. HIPS & SIEM
B. NIPS & HIDS
C. HIDS& SIEM
D. NIPS&HIPS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 523
which of the following best describes the objectives of succession planning?

A. To identify and document the successive order in which critical systems should be reinstated following a disaster situation
B. To ensure that a personnel management plan is in place to ensure continued operation of critical processes during an incident
C. To determine the appropriate order in which contract internal resources, third party suppliers and external customers during a disaster response
D. To document the order that systems should be reinstated at the primary site following a failover operation at a backup site.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 524
a system administrator wants to use open source software but is worried about the source code being comprised. As a part of the download and installation process, the administrator should verify the integrity of the software by:

A. Creating a digital signature of the file before installation
B. Using a secure protocol like HTTPS to download the file
C. Checking the has against an official mirror that contains the same file
D. Encryption any connections the software makes

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 525
The chief security officer (CSO) has reported a rise in data loss but no break-ins have occurred. By doing which of the following would the CSO MOST likely to reduce the number of incidents?

A. Implement protected distribution
B. Employ additional firewalls
C. Conduct security awareness training
D. Install perimeter barricades

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 526
In an effort to test the effectiveness of an organization's security awareness training, a penetrator tester crafted an email and sent it to all of the employees to see how many of them clicked on the enclosed links. Which of the following is being tested?

A. How many employees are susceptible to a SPAM attack
B. How many employees are susceptible to a cross-site scripting attack

C. How many employees are susceptible to a phishing attack
D. How many employees are susceptible to a vishing attack

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 527
An attacker impersonates a fire marshal and demands access to the datacenter under the threat of a fire. Which of the following reasons make this effective? (Select TWO)

A. Consensus
B. Authority
C. Intimidation
D. Trust
E. Scarcity

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 528
Devices on the SCADA network communicate exclusively at Layer 2. Which of the following should be used to prevent unauthorized systems using ARP-based attacks to compromise the SCADA network?

A. Application firewall
B. IPSec
C. Hardware encryption
D. VLANS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 529
When information is shared between two separate organizations, which of the following documents would describe the sensitivity as well as the type and flow of the information?

A. SLA
B. ISA
C. BPA
D. MOA

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 530
Joe noticed that there is a larger than normal account of network on the printer VLAN of his organization, causing users to have to wait a long time for a print job. Upon investigation Joe discovers that printers were ordered and added to the network without his knowledge. Which of the following will reduce the risk of this occurring again in the future?

A. Log analysis
B. Loop protection
C. Access control list
D. Rule-based management

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 531
Company XYZ has encountered an increased amount of buffer overflow attacks. The programmer has been tasked to identify the issues and report any findings. Which of the following is the first step of action recommended in this scenario?

A. Baseline reporting
B. Capability Maturity Model
C. Code Review
D. Quality Assurance and testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 532
Jo an employee reports to the security manager that several files in a research and development folder that only JOE has access to have been improperly modified. The modified data on the files in recent and the modified by account is Joe's. The permissions on the folder have not been changed, and there is no evidence of malware on the server hosting the folder or on Joe's workstation. Several failed login attempts to Joe's account were discovered in the security log of the LDAP server. Given this scenario, which of the following should the security manager implement to prevent this in the future?

A. Generic account prohibition
B. Account lockout
C. Password complexity
D. User access reviews

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 533
A user contacts the help desk after being unable to log in to a corporate website. The user can log into the site from another computer in the next office, but not from the PC. The user's PC was able to connect earlier in the day. The help desk has user restart the NTP service. Afterwards the user is able to log into the website. The MOST likely reason for the initial failure was that the website was configured to use which of the following authentication mechanisms?

A. Secure LDAP
B. RADIUS
C. NTLMv2

D. Kerberos

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 534
A company requires that all wireless communication be compliant with the Advanced Encryption Standard. The current wireless infrastructure implements WEP +TKIP. Which of the following wireless protocols should be implemented?

A. CCMP
B. 802.1X
C. 802.3
D. WPA2
E. AES

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 535
A security analyst has been investigating an incident involving the corporate website. Upon investigation, it has been determined that users visiting the corporate website would be automatically redirected to a ,malicious site. Further investigation on the corporate website has revealed that the home page on the corporate website has been altered to include an unauthorized item. Which of the following would explain why users are being redirected to the malicious site?

A. DNS poisoning
B. XSS
C. Iframe
D. Session hijacking

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 536
A news and weather toolbar was accidently installed into a web browser. The toolbar tracks users online activities and sends them to a central logging server. Which of the following attacks took place?

A. Man-in-the-browser
B. Flash cookies
C. Session hijacking
D. Remote code execution
E. Malicious add-on

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 537
A project manager is working with an architectural firm that focuses on physical security. The project manager would like to provide requirements that support the primary goal of safely. Based on the project manager's desires, which of the following controls would the BEST to incorporate into the facility design?

A. Biometrics
B. Escape routers
C. Reinforcements
D. Access controls

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 538
While performing surveillance activities an attacker determines that an organization is using

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 539
1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security controls?

A. MAC spoofing
B. Pharming
C. Xmas attack
D. ARP poisoning

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 540
An administrator wants to configure a switch port so that it separates voice and data traffic. Which of the following MUST be configured on the switch port to enforce separation of traffic?

A. DMZ
B. VLAN
C. Subnetting
D. NAC

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 541
A company must send sensitive data over a non-secure network via web services. The company suspects that competitors are actively trying to intercept all transmissions. Some of the information may be valuable to competitors, even years after it has been sent. Which of the following will help mitigate the risk in the scenario?

A. Digitally sign the data before transmission
B. Choose steam ciphers over block ciphers
C. Use algorithms that allow for PFS
D. Enable TLS instead of SSL
E. Use a third party for key escrow

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 542
When implementing a mobile security strategy for an organization which of the following is the MOST influential concern that contributes to that organization's ability to extend enterprise policies to mobile devices?

A. Support for mobile OS
B. Support of mobile apps
C. Availability of mobile browsers
D. Key management for mobile devices

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 543
A recent review of accounts on various systems has found that after employees passwords are required to change they are recycling the same password as before. Which of the following policies should be enforced to prevent this from happening? (Select TWO)

A. Reverse encryption
B. Minimum password age
C. Password complexity
D. Account lockouts
E. Password history
F. Password expiration

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 544
A system administrator runs a network inventory scan every Friday at 10:00 am to track the progress of a large organization's operating system upgrade of all laptops. The system administrator discovers that some laptops are now only being reported as IP addresses. Which of the following options is MOST likely the cause of this issue?

A. HIDS
B. Host-based firewalls rules
C. All the laptops are currently turned off
D. DNS outage

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 545
A security administrator working for a law enforcement organization is asked to secure a computer system at the scene of a crime for transport to the law enforcement forensic facility. In order to capture as mush evidence as possible, the computer system has been left running. The security administrator begins

information by image which of the following system components FIRST?

A. NVRAM
B. RAM
C. TPM
D. SSD

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

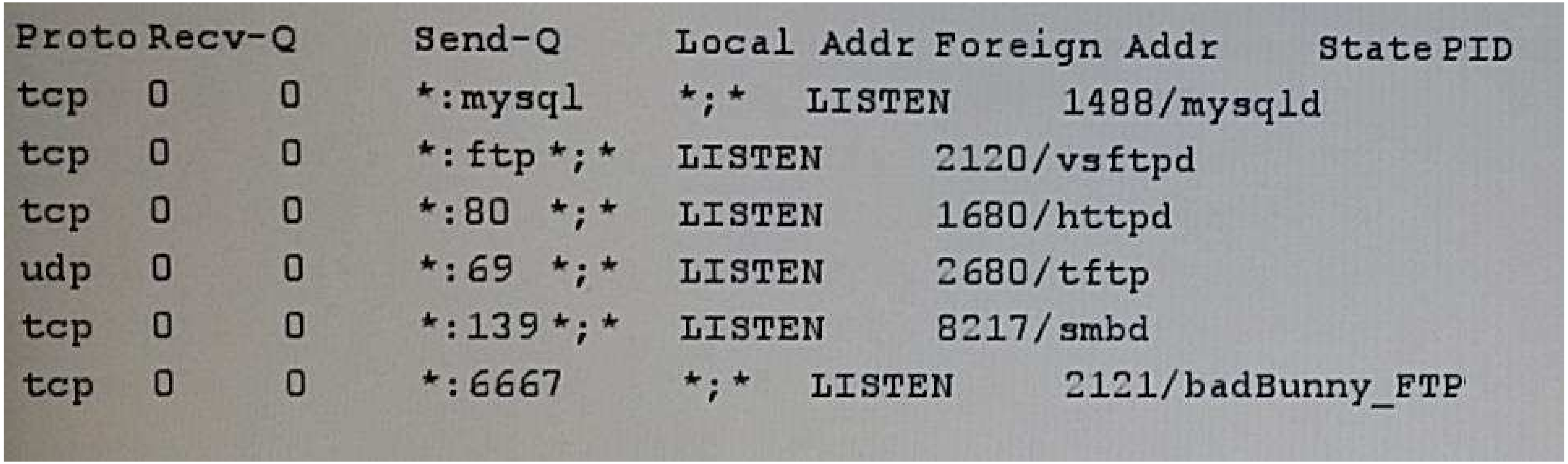
QUESTION 546
A new employee has been hired to perform system administration duties across a large enterprise comprised of multiple separate security domains. Each remote location implements a separate security domain. The new employee has successfully responded to and fixed computer issues for the main office. When the new employee tries to perform work on remote computers, the following messages appears. You need permission to perform this action. Which of the following can be implemented to provide system administrators with the ability to perform administrative tasks on remote computers using their uniquely assigned account?

A. Implement transitive trust across security domains
B. Enable the trusted OS feature across all enterprise computers
C. Install and configure the appropriate CA certificate on all domain controllers
D. Verify that system administrators are in the domain administrator group in the main office

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 547
An administrator is hardening systems and wants to disable unnecessary services. One Linux server hosts files used by a Windows web server on another machine. The Linux server is only used for secure file transfer, but requires a share for the Windows web server as well. The administrator see the following output from a netstat -1p command:



```
Proto Recv-Q      Send-Q      Local  Addr Foreign Addr     State PID
tcp    0      0      *:mysql     *;*   LISTEN      1488/mysqld
tcp    0      0      *: ftp *;*  LISTEN      2120/vsftpd
tcp    0      0      *:80  *;*   LISTEN      1680/httpd
udp    0      0      *:69  *;*   LISTEN      2680/tftp
tcp    0      0      *:139 *;*   LISTEN      8217/smbd
tcp    0      0      *:6667      *;*   LISTEN      2121/badBunny_FTP
```

Which of the following processes can the administrator kill without risking impact to the purpose and function of the Linux or Windows servers? (Select Three)

A. 1488
B. 1680
C. 2120
D. 2121
E. 2680
F. 8217

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 548
a project manager is evaluating proposals for a cloud commuting project. The project manager is particularly concerned about logical security controls in place at the service provider's facility. Which of the following sections of the proposal would be MOST important to review, given the project manager's concerns?

A. CCTV monitoring
B. Perimeter security lighting system
C. Biometric access system
D. Environmental system configuration

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 549
Which of the following is a way to implement a technical control to mitigate data loss in case of a mobile device theft?

A. Disk encryption
B. Encryption policy
C. Solid state drive
D. Mobile device policy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 550
A security administrator would like to ensure that some members of the building's maintenance staff are only allowed access to the facility during weekend hours. Access to the facility is controlled by badge swipe and a man trap. Which of the following options will BEST accomplish this goal?

A. CCTV
B. Security Guard
C. Time of day restrictions
D. Job rotation

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 551

A security manager received reports of several laptops containing confidential data stolen out of a lab environment. The lab is not a high security area and is secured with physical key locks. The security manager has no information to provide investigators related to who may have stolen the laptops. Which of the following should the security manager implement to improve legal and criminal investigations in the future?

A. Motion sensors
B. Mobile device management
C. CCTV
D. Cable locks
E. Full-disk encryption

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 552

A large bank has moved back office operations offshore to another country with lower wage costs in an attempt to improve profit and productivity. Which of the following would be a customer concern if the offshore staff had direct access to their data?

A. Service level agreements
B. Interoperability agreements
C. Privacy considerations
D. Data ownership

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 553
During a Linux security audit at a local college, it was noted that members of the dean's group were able to modify employee records in addition to modifying student records, resulting in an audit exception. The college security policy states that the dean's group should only have the ability to modify student records. Assuming that the correct user and group ownerships are in place, which of the following sets of permissions should have been assigned to the directories containing the employee records?

A. R-x---rwx

B. Rwxrwxrwx

C. Rwx----wx

D. Rwxrwxr--

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 554
An employee reports work was being completed on a company-owned laptop using a public wireless hotspot. A pop-up screen appeared, and the user closed the pop-up. Seconds later, the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

A. Ransomware

B. Rootkit

C. Scareware

D. Spyware

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 555
Which of the following can be mitigated with proper secure coding techniques?

A. Input validation

B. Error handling
C. Header manipulation
D. Cross-site scripting

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 556
Which of the following devices would be the most efficient way to filter external websites for staff on an internal network?

A. Protocol analyzer
B. Switch
C. Proxy
D. Router

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 557
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 558

An administrator needs to protect against downgrade attacks due to various vulnerabilities in SSL/TLS. Which of the following actions should be performed? (Select 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 559

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 560

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 this 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 561
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? (Select Two)

A. Port security
B. Loop Protection
C. Implicit deny
D. Log analysis
E. Mac Filtering
F. Flood Guards

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 562
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 563
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 564
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. Sandboxing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 565
Which of the following is a proprietary protocol commonly used for router authentication across an enterprise?

A. SAML
B. TACACS
C. LDAP
D. RADIUS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 566
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 567
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? (Select 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 568
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 569
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

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 570
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 571
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 572

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 573
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 574
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? (Select TWO)

A. Data at rest
B. Data in use
C. Replication
D. Wiping

E. Retention
F. Cloud Storage

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 575
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 576
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 577

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 578

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 bring 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 579

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 580
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 581
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? (Select TWO)

A. Rule-based access control
B. Role-based access control
C. Data loss prevention

D. Separation of duties
E. Group-based permissions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 582
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 583
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 584
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 585
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

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 586

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 587

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 588

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 589
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 590
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 591
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 592
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 593
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 594
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? (Select TWO)

A. SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
F FTPS

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 595
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 596
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 incorrect encryption algorithm
C. the WPA2 shared likely is incorrect
D. The company's DHCP server scope is full

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 597
A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site?
Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

A. Rule 1: deny from inside to outside source any destination any service smtp
B. Rule 2: deny from inside to outside source any destination any service ping
C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
D. Rule 4: deny from any to any source any destination any service any

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 598
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 599
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 600
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 601
Which of the following are MOST susceptible to birthday attacks?

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 602
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 603
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 604
Given the log output
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: msmith] [Source:

A.
B.

C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 605
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 606
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

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 607

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 608

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 be 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 609

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 610
A product manager a 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 611
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 612
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 613
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 614
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 615
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 616
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 617
Which of the following is commonly used for federated identity management across multiple organizations?

A. SAML
B. Active Directory
C. Kerberos
D. LDAP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 618
While performing surveillance activities, an attacker determines that an organization is using

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 619
1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

A. MAC spoofing
B. Pharming
C. Xmas attack
D. ARP poisoning

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 620
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 621
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 622
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 623
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 624
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

A.

B.

C.

D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 625
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

A.

B.

C.

D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 626
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 627
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 in response to the new requirement? a) Transitive trust
b) Symmetric encryption
c) Two-factor authentication
d) Digital signatures
e) One-time passwords

A.

B.

C.

D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 628
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 629
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? (Select two)

A. Minimum complexity
B. Maximum age limit
C. Maximum length
D. Minimum length
E. Minimum age limit
F. Minimum re-use limit

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 630
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.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 631
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 632
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 has 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 633

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.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 634

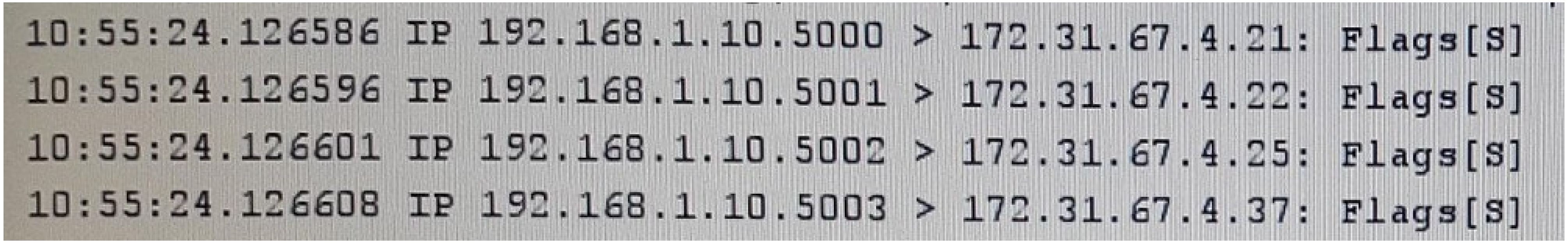
many employees are receiving email messages similar to the one shown below:
From IT department
To employee
Subject email quota exceeded
Pease click on the following link http:www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quota. Upon reviewing other 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 635
A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:



```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags[S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags[S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags[S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags[S]
```

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 TCO 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 636
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

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 637
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 638
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 639

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 640
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 641
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 642
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 643
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 644
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 645
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? (Select 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 646
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? (Select TWO)

A. Networking access control
B. DLP alerts

C. Log analysis
D. File integrity monitoring
E. Host firewall rules

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 647
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 648
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

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 649

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+

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 650

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 651

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 652
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 653
A security administrator needs an external vendor to correct 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 654
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 655
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 656
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 657
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 658
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

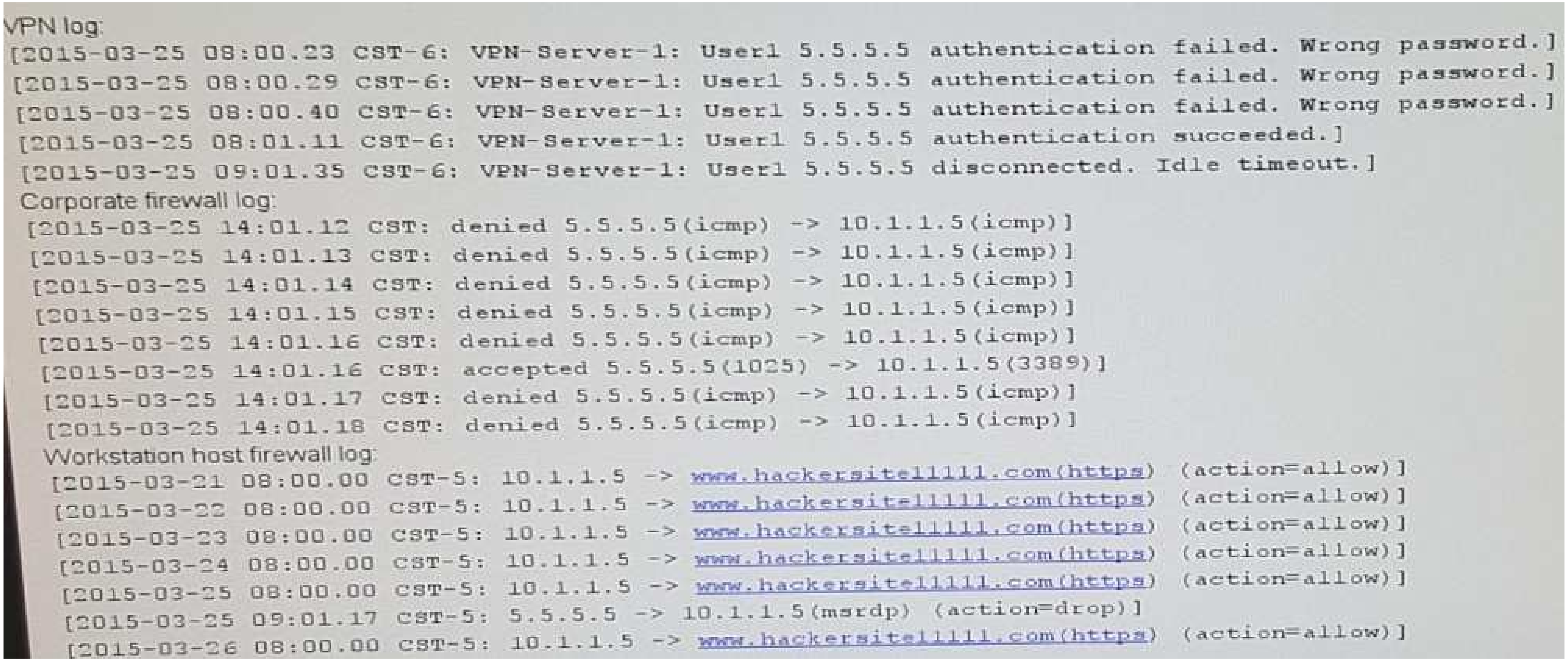
QUESTION 659
Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

A. Block level encryption
B. SAML authentication
C. Transport encryption
D. Multifactor authentication
E. Predefined challenge questions
F. Hashing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 660
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.



```
VPN log:
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
Corporate firewall log:
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
Workstation host firewall log:
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
```

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 661

During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem best be revisited?

A. Reporting

B. Preparation

C. Mitigation

D. Lessons learned

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 662

During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most l likely recommend during the audit out brief?

A. Discretionary access control for the firewall team

B. Separation of duties policy for the firewall team

C. Least privilege for the firewall team

D. Mandatory access control for the firewall team

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 663

Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

A. NAC
B. VLAN
C. DMZ
D. Subnet

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 664
An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server. Which of the following will most likely fix the uploading issue for the users?

A. Create an ACL to allow the FTP service write access to user directories
B. Set the Boolean selinux value to allow FTP home directory uploads
C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 665
An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity. Which of the following actions will help detect attacker attempts to further alter log files?

A. Enable verbose system logging
B. Change the permissions on the user's home directory
C. Implement remote syslog
D. Set the bash_history log file to "read only"

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 666
A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

A. Firmware version control
B. Manual software upgrades
C. Vulnerability scanning
D. Automatic updates
E. Network segmentation
F. Application firewalls

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 667
An administrator is configuring a network for all users in a single building. Which of the following design elements would be used to segment the network based on organizational groups? Select two

A. NAC
B. NAT
C. Subnetting
D. VLAN
E. DMZ
F. VPN

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 668

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

A. Time of day restrictions
B. Principle of least privilege
C. Role-based access control
D. Separation of duties

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 669

Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications. Which of the following best describes what she will do?

A. Enter random or invalid data into the application in an attempt to cause it to fault
B. Work with the developers to eliminate horizontal privilege escalation opportunities
C. Test the applications for the existence of built-in- back doors left by the developers
D. Hash the application to verify it won't cause a false positive on the HIPS.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 670

Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop. Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

A. full-disk encryption
B. Host-based firewall
C. Current antivirus definitions
D. Latest OS updates

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 671
An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times. Which of the following describes this type of attack?

A. Integer overflow attack
B. Smurf attack
C. Replay attack
D. Buffer overflow attack
E. Cross-site scripting attack

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 672
AN organization is moving its human resources system to a cloud services provider. The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which of the following options meets all of these requirements?

A. Two-factor authentication
B. Account and password synchronization
C. Smartcards with PINS
D. Federated authentication

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 673
The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations
B. Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 674
A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

A. Set up the scanning system's firewall to permit and log all outbound connections
B. Use a protocol analyzer to log all pertinent network traffic
C. Configure network flow data logging on all scanning system
D. Enable debug level logging on the scanning system and all scanning tools used.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 675
which of the following best describes the initial processing phase used in mobile device forensics?

A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 676
Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain \. Which of the following tools would aid her to decipher the network traffic?

A. Vulnerability Scanner
B. NMAP
C. NETSTAT
D. Packet Analyzer

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 677
AN administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

A. Find two identical messages with different hashes
B. Find two identical messages with the same hash
C. Find a common has between two specific messages

D. Find a common hash between a specific message and a random message

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 678

The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?

A. Upgrade the encryption to WPA or WPA2
B. Create a non-zero length SSID for the wireless router
C. Reroute wireless users to a honeypot
D. Disable responses to a broadcast probe request

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 679

Which of the following should be used to implement voice encryption?

A. SSLv3
B. VDSL
C. SRTP
D. VoIP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 680
During an application design, the development team specifics a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?

A. Application control
B. Data in-transit
C. Identification
D. Authentication

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 681
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

A. Time-of-day restrictions
B. Change management
C. Periodic auditing of user credentials
D. User rights and permission review

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 682
Joe a website administrator believes he owns the intellectual property for a company invention and has replacing images files on the company's public facing website in the DMZ, Joe is using steganography to hide stolen date. Which of the following controls can be implemented to mitigate this type of insider threat?

A. Digital signatures

B. File integrity monitoring
C. Access controls
D. Change management
E. Stateful inspection firewall

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 683
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

A. Performance and service delivery metrics
B. Backups are being performed and tested
C. Data ownership is being maintained and audited
D. Risk awareness is being adhered to and enforced

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 684
Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

A. Calculate the ALE
B. Calculate the ARO
C. Calculate the MTBF
D. Calculate the TCO

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 685
A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?

A. Signature based
B. Heuristic
C. Anomaly-based
D. Behavior-based

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 686
The chief Security Officer (CSO) has reported a rise in data loss but no break ins has occurred. By doing which of the following the CSO MOST likely to reduce the number of incidents?

A. Implement protected distribution
B. Empty additional firewalls
C. Conduct security awareness training
D. Install perimeter barricades

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 687
During a data breach cleanup it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

A. Reporting
B. Preparation
C. Mitigation
D. Lessons Learned

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 688
New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority. In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

A. Fail safe
B. Fault tolerance
C. Fail secure
D. Redundancy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 689
A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

A. It can protect multiple domains
B. It provides extended site validation
C. It does not require a trusted certificate authority
D. It protects unlimited subdomains

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 690
After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition. Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

A. Monitor VPN client access
B. Reduce failed login out settings
C. Develop and implement updated access control policies
D. Review and address invalid login attempts
E. Increase password complexity requirements
F. Assess and eliminate inactive accounts

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 691
A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle. Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

A. Architecture review
B. Risk assessment
C. Protocol analysis
D. Code review

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 692
A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts. Which of the following subnets would BEST meet the requirements?

A. 192.168.0.16 255.25.255.248
B. 192.168.0.16/28
C. 192.168.1.50 255.255.25.240
D. 192.168.2.32/27

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 693
A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network. Which of the following should be implemented in order to meet the security policy requirements?

A. Virtual desktop infrastructure (IDI)
B. WS-security and geo-fencing
C. A hardware security module (HSM)
D. RFID tagging system
E. MDM software
F. Security Requirements Traceability Matrix (SRTM)

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 694

The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers names and credit card numbers with the PIN. Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 695
A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network. Which of the following security measures did the technician MOST likely implement to cause this Scenario?

A. Deactivation of SSID broadcast
B. Reduction of WAP signal output power
C. Activation of 802.1X with RADIUS
D. Implementation of MAC filtering
E. Beacon interval was decreased

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 696
A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs., installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production. Which of the following would correct the deficiencies?

A. Mandatory access controls
B. Disable remote login
C. Host hardening
D. Disabling services

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 697
Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field. Which of the following has the application programmer failed to implement?

A. Revision control system
B. Client side exception handling
C. Server side validation
D. Server hardening

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 698
An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware the attacker is provided with access to the infected machine. Which of the following is being described?

A. Zero-day exploit
B. Remote code execution
C. Session hijacking
D. Command injection

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 699

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine. Which of the following can be implemented to reduce the likelihood of this attack going undetected?

A. Password complexity rules
B. Continuous monitoring
C. User access reviews
D. Account lockout policies

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 700

A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could:

A. Require the use of two different passwords held by two different individuals to open an account
B. Administer account creation on a role based access control approach
C. Require all new accounts to be handle by someone else other than a teller since they have different duties
D. Administer account creation on a rule based access control approach

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 701
A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day. Which of the following could the security administrator implement to reduce the risk associated with the finding?

A. Implement a clean desk policy
B. Security training to prevent shoulder surfing
C. Enable group policy based screensaver timeouts
D. Install privacy screens on monitors

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 702
Company policy requires the use if passphrases instead if passwords. Which of the following technical controls MUST be in place in order to promote the use of passphrases?

A. Reuse
B. Length
C. History
D. Complexity

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 703
During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again?

A. Credential management
B. Group policy management

C. Acceptable use policy
D. Account expiration policy

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 704
Which of the following should identify critical systems and components?

A. MOU
B. BPA
C. ITCP
D. BCP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 705
Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

A. Logic bomb
B. Trojan
C. Scareware
D. Ransomware

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 706
A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

A. SQL injection
B. Header manipulation
C. Cross-site scripting
D. Flash cookie exploitation

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 707
Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures. Which of the following should be implemented to correct this issue?

A. Decrease the room temperature
B. Increase humidity in the room
C. Utilize better hot/cold aisle configurations
D. Implement EMI shielding

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 708
A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality?

A. Format the device
B. Re-image the device
C. Perform virus scan in the device

D. Physically destroy the device

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 709
A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable. Which of the following MUST be implemented to support this requirement?

A. CSR
B. OCSP
C. CRL
D. SSH

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 710
A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used?

A. Gray box vulnerability testing
B. Passive scan
C. Credentialed scan
D. Bypassing security controls

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 711
The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets , and the internet via HTTP. The corporation does business have varying data retention and privacy laws. Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 712
While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy. Which of the following tool or technology would work BEST for obtaining more information on this traffic?

A. Firewall logs
B. IDS logs
C. Increased spam filtering
D. Protocol analyzer

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 713
A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

A. Enforce authentication for network devices
B. Configure the phones on one VLAN, and computers on another
C. Enable and configure port channels
D. Make users sign an Acceptable use Agreement

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 714
An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
B. Configure the smart phones so that the stored data can be destroyed from a centralized location
C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 715
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. Man-in-the-middle

C. URL hijacking
D. Transitive access

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 716
A user of the wireless network is unable to gain access to the network. The symptoms are:

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 717
) Unable to connect to both internal and Internet resources

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 718
) The wireless icon shows connectivity but has no network access The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate. Which of the following is the MOST likely cause of the connectivity issues?

A. The wireless signal is not strong enough
B. A remote DDoS attack against the RADIUS server is taking place
C. The user's laptop only supports WPA and WEP
D. The DHCP scope is full
E. The dynamic encryption key did not update while the user was offline

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 719
A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls. Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

A. Password complexity policies
B. Hardware tokens
C. Biometric systems
D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on
I. Lease privilege

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 720
A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal?

A. Device access control
B. Location based services
C. Application control
D. GEO-Tagging

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 721
A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off. Joe knows that he must collect the most volatile date first. Which of the following is the correct order in which Joe should collect the data?

A. CPU cache, paging/swap files, RAM, remote logging data
B. RAM, CPU cache. Remote logging data, paging/swap files
C. Paging/swap files, CPU cache, RAM, remote logging data
D. CPU cache, RAM, paging/swap files, remote logging data

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 722
An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot
B. Disable unnecessary services
C. Implement transport layer security
D. Increase application event logging

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 723
A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of the following should the security administrator do to rectify this issue?

A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
B. Recommend classifying each application into like security groups and segmenting the groups from one another
C. Recommend segmenting each application, as it is the most secure approach
D. Recommend that only applications with minimal security features should be segmented to protect them

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 724
A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report?

A. Architecture evaluation
B. Baseline reporting
C. Whitebox testing
D. Peer review

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 725
An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?

A. Tailgating
B. Shoulder surfing
C. Impersonation
D. Hoax

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 726
A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test. Which of the following has the administrator been tasked to perform?

A. Risk transference
B. Penetration test
C. Threat assessment
D. Vulnerability assessment

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 727
A security analyst is working on a project team responsible for the integration of an enterprise SSO solution. The SSO solution requires the use of an open standard for the exchange of authentication and authorization across numerous web-based applications. Which if the following solutions is MOST appropriate for the analyst to recommend in this scenario?

A. SAML
B. XTACACS
C. RADIUS
D. TACACS+
E. Secure LDAP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 728
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access
B. Spoofing
C. Man-in-the-middle
D. Replay

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 729

which of the following use the SSH protocol?

A. Stelnet
B. SCP
C. SNMP
D. FTPS
E. SSL
F. SFTP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 730
A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

A. Utilizing a single question for password recovery
B. Sending a PIN to a smartphone through text message
C. Utilizing CAPTCHA to avoid brute force attacks
D. Use a different e-mail address to recover password

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 731
A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?

A. Change management procedures
B. Job rotation policies

C. Incident response management

D. Least privilege access controls

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 732

A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

A. Install host-based firewalls on all computers that have an email client installed

B. Set the email program default to open messages in plain text

C. Install end-point protection on all computers that access web email

D. Create new email spam filters to delete all messages from that sender

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 733

A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage. Which of the following should be implemented?

A. Recovery agent

B. Ocsp

C. Crl

D. Key escrow

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 734

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?

A. GMAC
B. PCBC
C. CBC
D. GCM
E. CFB

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 735

The chief security officer (CS0) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the best solution for the network administrator to secure each internal website?

A. Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 736

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base. Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review
B. Component testing
C. Penetration testing
D. Vulnerability testing

Correct Answer:
Section: (none)
Explanation

Explanation/Reference: