Actualtests.SY0-401.820q

Number: SY0-401
Passing Score: 800
Time Limit: 120 min
File Version: 16.4

http://www.gratisexam.com/

A) I am so much inspired by the training and guidance provided to me by this VCE file for the preparation of exam and now I uploaded this outstanding file for you people.

B) It's still valid and there are a lot of fresh and updated questions. But if you know the answers of that dump you will succeed easily because the questions are similar.

C) It is considerable that this dump has made the whole process simple for taking exam.

D) This dump is valid, passed today with 92%, all questions from this dump.

E) Of the Total questions, only 10 came out in the exam. I recommend using the VCE, which contains most of the test questions.

Exam A

QUESTION 1
The security administrator needs to manage traffic on a layer 3 device to support FTP from a new remote site. Which of the following would need to be implemented?

A. Implicit deny
B. VLAN management
C. Port security
D. Access control lists

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

A. Hashing
B. Stream ciphers
C. Steganography
D. Block ciphers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following encrypts data a single bit at a time?

A. Stream cipher
B. Steganography
C. 3DES
D. Hashing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is used to verify data integrity?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 5
By default, which of the following uses TCP port 22? (Select THREE).

A. FTPS
B. STELNET
C. TLS
D. SCP
E. SSL
F. HTTPS
G. SSH
H. SFTP

Correct Answer: DGH
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Access mechanisms to data on encrypted USB hard drives must be implemented correctly otherwise:

A. user accounts may be inadvertently locked out.
B. data on the USB drive could be corrupted.
C. data on the hard drive will be vulnerable to log analysis.
D. the security controls on the USB drive can be bypassed.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8
A security administrator is segregating all web-facing server traffic from the internal network and restricting it to a single interface on a firewall. Which of the following BEST describes this new network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following was based on a previous X.500 specification and allows either unencrypted authentication or encrypted authentication through the use of TLS?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following has a storage root key?

A. HSM
B. EFS
C. TPM

D. TKIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A malicious person gained access to a datacenter by ripping the proximity badge reader off the wall near the datacenter entrance. This caused the electronic locks on the datacenter door to release because the:

A. badge reader was improperly installed.
B. system was designed to fail open for life-safety.
C. system was installed in a fail closed configuration.
D. system used magnetic locks and the locks became demagnetized.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
The concept of rendering data passing between two points over an IP based network impervious to all but the most sophisticated advanced persistent threats is BEST categorized as which of the following?

A. Stream ciphers
B. Transport encryption
C. Key escrow
D. Block ciphers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
On Monday, all company employees report being unable to connect to the corporate wireless network, which uses 802.1x with PEAP. A technician verifies that no configuration changes were made to the

wireless network and its supporting infrastructure, and that there are no outages. Which of the following is the MOST likely cause for this issue?

A. Too many incorrect authentication attempts have caused users to be temporarily disabled.
B. The DNS server is overwhelmed with connections and is unable to respond to queries.
C. The company IDS detected a wireless attack and disabled the wireless network.
D. The Remote Authentication Dial-In User Service server certificate has expired.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Which of the following would BEST deter an attacker trying to brute force 4-digit PIN numbers to access an account at a bank teller machine?

A. Account expiration settings
B. Complexity of PIN
C. Account lockout settings
D. PIN history requirements

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
An administrator discovers that many users have used their same passwords for years even though the network requires that the passwords be changed every six weeks. Which of the following, when used together, would BEST prevent users from reusing their existing password? (Select TWO).

A. Length of password
B. Password history
C. Minimum password age
D. Password expiration
E. Password complexity
F. Non-dictionary words

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A recent audit has discovered that at the time of password expiration clients are able to recycle the previous credentials for authentication. Which of the following controls should be used together to prevent this from occurring? (Select TWO).

A. Password age
B. Password hashing
C. Password complexity
D. Password history

E. Password length

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
In Kerberos, the Ticket Granting Ticket (TGT) is used for which of the following?

A. Identification
B. Authorization
C. Authentication
D. Multifactor authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites?

A. Spam filter
B. URL filter
C. Content inspection
D. Malware inspection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
When considering a vendor-specific vulnerability in critical industrial control systems which of the following techniques supports availability?

A. Deploying identical application firewalls at the border
B. Incorporating diversity into redundant design
C. Enforcing application white lists on the support workstations
D. Ensuring the systems' anti-virus definitions are up-to-date

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
During the information gathering stage of a deploying role-based access control model, which of the following information is MOST likely required?

A. Conditional rules under which certain systems may be accessed
B. Matrix of job titles with required access privileges
C. Clearance levels of all company personnel
D. Normal hours of business operation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Ann would like to forward some Personal Identifiable Information to her HR department by email, but she is worried about the confidentiality of the information. Which of the following will accomplish this task securely?

A. Digital Signatures
B. Hashing
C. Secret Key
D. Encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A company is trying to limit the risk associated with the use of unapproved USB devices to copy documents. Which of the following would be the BEST technology control to use in this scenario?

A. Content filtering
B. IDS
C. Audit logs
D. DLP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A company is trying to implement physical deterrent controls to improve the overall security posture of their data center. Which of the following BEST meets their goal?

A. Visitor logs
B. Firewall
C. Hardware locks
D. Environmental monitoring

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A company's employees were victims of a spear phishing campaign impersonating the CEO. The company would now like to implement a solution to improve the overall security posture by assuring their employees that email originated from the CEO. Which of the following controls could they implement to BEST meet this goal?

A. Spam filter
B. Digital signatures

C. Antivirus software
D. Digital certificates

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
A security technician is attempting to improve the overall security posture of an internal mail server. Which of the following actions would BEST accomplish this goal?

A. Monitoring event logs daily
B. Disabling unnecessary services
C. Deploying a content filter on the network
D. Deploy an IDS on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A bank has recently deployed mobile tablets to all loan officers for use at customer sites. Which of the following would BEST prevent the disclosure of customer data in the event that a tablet is lost or stolen?

A. Application control
B. Remote wiping
C. GPS
D. Screen-locks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is the primary security concern when deploying a mobile device on a network?

A. Strong authentication
B. Interoperability
C. Data security
D. Cloud storage technique

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following technical controls is BEST used to define which applications a user can install and run on a company issued mobile device?

A. Authentication
B. Blacklisting
C. Whitelisting
D. Acceptable use policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
After a company has standardized to a single operating system, not all servers are immune to a well-known OS vulnerability. Which of the following solutions would mitigate this issue?

A. Host based firewall
B. Initial baseline configurations
C. Discretionary access control
D. Patch management system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
A security administrator discovers an image file that has several plain text documents hidden in the file. Which of the following security goals is met by camouflaging data inside of other files?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A company determines a need for additional protection from rogue devices plugging into physical ports around the building.

Which of the following provides the highest degree of protection from unauthorized wired network access?

A. Intrusion Prevention Systems
B. MAC filtering
C. Flood guards
D. 802.1x

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A company is preparing to decommission an offline, non-networked root certificate server. Before sending the server's drives to be destroyed by a contracted company, the Chief Security Officer (CSO) wants to be certain that the data will not be accessed. Which of the following, if implemented, would BEST reassure the CSO? (Select TWO).

A. Disk hashing procedures
B. Full disk encryption
C. Data retention policies
D. Disk wiping procedures
E. Removable media encryption

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
During the analysis of a PCAP file, a security analyst noticed several communications with a remote server on port 53. Which of the following protocol types is observed in this traffic?

A. FTP
B. DNS
C. Email
D. NetBIOS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A compromised workstation utilized in a Distributed Denial of Service (DDOS) attack has been removed from the network and an image of the hard drive has been created. However, the system administrator stated that the system was left unattended for several hours before the image was created. In the event of a court case, which of the following is likely to be an issue with this incident?

A. Eye Witness
B. Data Analysis of the hard drive
C. Chain of custody
D. Expert Witness

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
During which of the following phases of the Incident Response process should a security administrator define and implement general defense against malware?

A. Lessons Learned
B. Preparation
C. Eradication
D. Identification

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Due to hardware limitation, a technician must implement a wireless encryption algorithm that uses the RC4 protocol. Which of the following is a wireless encryption solution that the technician should implement while ensuring the STRONGEST level of security?

A. WPA2-AES
B. 802.11ac
C. WPA-TKIP
D. WEP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Select TWO).

A. The CA's public key
B. Ann's public key
C. Joe's private key
D. Ann's private key
E. The CA's private key
F. Joe's public key

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify the validity's of Joe's certificate? (Select TWO).

A. The CA's public key
B. Joe's private key
C. Ann's public key
D. The CA's private key
E. Joe's public key
F. Ann's private key

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A technician wants to implement a dual factor authentication system that will enable the organization to authorize access to sensitive systems on a need-to-know basis. Which of the following should be implemented during the authorization stage?

A. Biometrics
B. Mandatory access control
C. Single sign-on
D. Role-based access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A security researcher wants to reverse engineer an executable file to determine if it is malicious. The file was found on an underused server and appears to contain a zero-day exploit. Which of the following can the researcher do to determine if the file is malicious in nature?

A. TCP/IP socket design review
B. Executable code review
C. OS Baseline comparison
D. Software architecture review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A recent spike in virus detections has been attributed to end-users visiting www.compnay.com. The business has an established relationship with an organization using the URL of www.company.com but not with the site that has been causing the infections. Which of the following would BEST describe this type of attack?

A. Typo squatting
B. Session hijacking
C. Cross-site scripting
D. Spear phishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A company has proprietary mission critical devices connected to their network which are configured remotely by both employees and approved customers. The administrator wants to monitor device security without changing their baseline configuration. Which of the following should be implemented to secure the devices without risking availability?

A. Host-based firewall
B. IDS
C. IPS
D. Honeypot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
An administrator has a network subnet dedicated to a group of users. Due to concerns regarding data and network security, the administrator desires to provide network access for this group only. Which of the following would BEST address this desire?

A. Install a proxy server between the users' computers and the switch to filter inbound network traffic.
B. Block commonly used ports and forward them to higher and unused port numbers.
C. Configure the switch to allow only traffic from computers based upon their physical address.
D. Install host-based intrusion detection software to monitor incoming DHCP Discover requests.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following is a security concern regarding users bringing personally-owned devices that they connect to the corporate network?

A. Cross-platform compatibility issues between personal devices and server-based applications
B. Lack of controls in place to ensure that the devices have the latest system patches and signature files
C. Non-corporate devices are more difficult to locate when a user is terminated
D. Non-purchased or leased equipment may cause failure during the audits of company-owned assets

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Due to issues with building keys being duplicated and distributed, a security administrator wishes to change to a different security control regarding a restricted area. The goal is to provide access based upon facial recognition. Which of the following will address this requirement?

A. Set up mantraps to avoid tailgating of approved users.
B. Place a guard at the entrance to approve access.
C. Install a fingerprint scanner at the entrance.
D. Implement proximity readers to scan users' badges.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A security administrator has concerns regarding employees saving data on company provided mobile devices. Which of the following would BEST address the administrator's concerns?

A. Install a mobile application that tracks read and write functions on the device.
B. Create a company policy prohibiting the use of mobile devices for personal use.
C. Enable GPS functionality to track the location of the mobile devices.
D. Configure the devices so that removable media use is disabled.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Identifying residual risk is MOST important to which of the following concepts?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
The information security technician wants to ensure security controls are deployed and functioning as intended to be able to maintain an appropriate security posture. Which of the following security techniques is MOST appropriate to do this?

A. Log audits
B. System hardening
C. Use IPS/IDS
D. Continuous security monitoring

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
A small company can only afford to buy an all-in-one wireless router/switch. The company has 3 wireless BYOD users and 2 web servers without wireless access. Which of the following should the company configure to protect the servers from the user devices? (Select TWO).

A. Deny incoming connections to the outside router interface.
B. Change the default HTTP port
C. Implement EAP-TLS to establish mutual authentication
D. Disable the physical switch ports
E. Create a server VLAN
F. Create an ACL to access the server

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Users can authenticate to a company's web applications using their credentials from 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 site affect the company application as well

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A security team has established a security awareness program. Which of the following would BEST prove the success of the program?

A. Policies
B. Procedures
C. Metrics
D. Standards

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to combine the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

A. Unified Threat Management
B. Virtual Private Network
C. Single sign on
D. Role-based management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following would allow the organization to divide a Class C IP address range into several ranges?

A. DMZ
B. Virtual LANs
C. NAT
D. Subnetting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
The security administrator is currently unaware of an incident that occurred a week ago. Which of the following will ensure the administrator is notified in a timely manner in the future?

A. User permissions reviews
B. Incident response team
C. Change management
D. Routine auditing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
An access point has been configured for AES encryption but a client is unable to connect to it. Which of the following should be configured on the client to fix this issue?

A. WEP
B. CCMP
C. TKIP
D. RC4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
The system administrator is tasked with changing the administrator password across all 2000 computers in the organization. Which of the following should the system administrator implement to accomplish this task?

A. A security group
B. A group policy
C. Key escrow
D. Certificate revocation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A network administrator wants to block both DNS requests and zone transfers coming from outside IP addresses. The company uses a firewall which implements an implicit allow and is currently configured with the following ACL applied to its external interfacE.
PERMIT TCP ANY ANY 80
PERMIT TCP ANY ANY 443

Which of the following rules would accomplish this task? (Select TWO).

A. Change the firewall default settings so that it implements an implicit deny
B. Apply the current ACL to all interfaces of the firewall
C. Remove the current ACL
D. Add the following ACL at the top of the current ACLDENY TCP ANY ANY 53
E. Add the following ACL at the bottom of the current ACLDENY ICMP ANY ANY 53
F. Add the following ACL at the bottom of the current ACLDENY IP ANY ANY 53

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
to the point answer.

QUESTION 64
Which of the following attacks would cause all mobile devices to lose their association with corporate access points while the attack is underway?

A. Wireless jamming
B. Evil twin

C. Rogue AP
D. Packet sniffing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
An administrator wants to ensure that the reclaimed space of a hard drive has been sanitized while the computer is in use. Which of the following can be implemented?

A. Cluster tip wiping
B. Individual file encryption
C. Full disk encryption
D. Storage retention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
A company is looking to improve their security posture by addressing risks uncovered by a recent penetration test. Which of the following risks is MOST likely to affect the business on a day-to-day basis?

A. Insufficient encryption methods
B. Large scale natural disasters
C. Corporate espionage
D. Lack of antivirus software

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
answer is fabulous.

QUESTION 67
Ann, an employee, is cleaning out her desk and disposes of paperwork containing confidential customer information in a recycle bin without shredding it first. This is MOST likely to increase the risk of loss from which of the following attacks?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68

A recently installed application update caused a vital application to crash during the middle of the workday. The application remained down until a previous version could be reinstalled on the server, and this resulted in a significant loss of data and revenue.

Which of the following could BEST prevent this issue from occurring again?

A. Application configuration baselines
B. Application hardening
C. Application access controls
D. Application patch management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern?

A. Change the encryption from TKIP-based to CCMP-based.
B. Set all nearby access points to operate on the same channel.
C. Configure the access point to use WEP instead of WPA2.
D. Enable all access points to broadcast their SSIDs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
answer is real.

QUESTION 70
The system administrator has deployed updated security controls for the network to limit risk of attack. The security manager is concerned that controls continue to function as intended to maintain appropriate security posture.

Which of the following risk mitigation strategies is MOST important to the security manager?

A. User permissions
B. Policy enforcement
C. Routine audits
D. Change management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A company is about to release a very large patch to its customers. An administrator is required to test patch installations several times prior to distributing them to customer PCs.

Which of the following should the administrator use to test the patching process quickly and often?

A. Create an incremental backup of an unpatched PC
B. Create an image of a patched PC and replicate it to servers
C. Create a full disk image to restore after each installation
D. Create a virtualized sandbox and utilize snapshots

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A vulnerability scan is reporting that patches are missing on a server. After a review, it is determined that the application requiring the patch does not exist on the operating system.

Which of the following describes this cause?

A. Application hardening
B. False positive
C. Baseline code review
D. False negative

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was

submitted by Company A?

A. Steganography
B. Hashing
C. Encryption
D. Digital Signatures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Ann, a sales manager, successfully connected her company-issued smartphone to the wireless network in her office without supplying a username/password combination. Upon disconnecting from the wireless network, she attempted to connect her personal tablet computer to the same wireless network and could not connect.

Which of the following is MOST likely the reason?

A. The company wireless is using a MAC filter.
B. The company wireless has SSID broadcast disabled.
C. The company wireless is using WEP.
D. The company wireless is using WPA2.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A security administrator is reviewing the company's continuity plan. The plan specifies an RTO of six hours and RPO of two days. Which of the following is the plan describing?

A. Systems should be restored within six hours and no later than two days after the incident.
B. Systems should be restored within two days and should remain operational for at least six hours.
C. Systems should be restored within six hours with a minimum of two days worth of data.
D. Systems should be restored within two days with a minimum of six hours worth of data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
The incident response team has received the following email messagE.

From: monitor@ext-company.com
To: security@company.com
Subject: Copyright infringement

A copyright infringement alert was triggered by IP address 13.10.66.5 at 09: 50: 01 GMT. After reviewing the following web logs for IP 13.10.66.5, the team is unable to correlate and identify the incident.

09: 45: 33 13.10.66.5 http: //remote.site.com/login.asp?user=john
09: 50: 22 13.10.66.5 http: //remote.site.com/logout.asp?user=anne
10: 50: 01 13.10.66.5 http: //remote.site.com/access.asp?file=movie.mov
11: 02: 45 13.10.65.5 http: //remote.site.com/download.asp?movie.mov=ok Which of the following is the MOST likely reason why the incident response team is unable to identify and correlate the incident?

A. The logs are corrupt and no longer forensically sound.
B. Traffic logs for the incident are unavailable.
C. Chain of custody was not properly maintained.
D. Incident time offsets were not accounted for.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
A server dedicated to the storage and processing of sensitive information was compromised with a rootkit and sensitive data was exfiltrated. Which of the following incident response procedures is best suited to restore the server?

A. Wipe the storage, reinstall the OS from original media and restore the data from the last known good backup.
B. Keep the data partition, restore the OS from the most current backup and run a full system antivirus scan.
C. Format the storage and reinstall both the OS and the data from the most current backup.
D. Erase the storage, reinstall the OS from most current backup and only restore the data that was not compromised.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
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: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Acme Corp has selectively outsourced proprietary business processes to ABC Services. Due to some technical issues, ABC services wants to send some of Acme Corp's debug data to a third party vendor for problem resolution. Which of the following MUST be considered prior to sending data to a third party?

A. The data should be encrypted prior to transport
B. This would not constitute unauthorized data sharing
C. This may violate data ownership and non-disclosure agreements
D. Acme Corp should send the data to ABC Services' vendor instead

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
An organization has introduced token-based authentication to system administrators due to risk of password compromise. The tokens have a set of numbers that automatically change every 30 seconds. Which of the following type of authentication mechanism is this?

A. TOTP
B. Smart card
C. CHAP
D. HOTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A security technician at a small business is worried about the Layer 2 switches in the network suffering from a DoS style attack caused by staff incorrectly cabling network connections between switches.

Which of the following will BEST mitigate the risk if implemented on the switches?

A. Spanning tree
B. Flood guards
C. Access control lists
D. Syn flood

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87

An administrator wants to establish a WiFi network using a high gain directional antenna with a narrow radiation pattern to connect two buildings separated by a very long distance. Which of the following antennas would be BEST for this situation?

A. Dipole
B. Yagi
C. Sector
D. Omni

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following is an XML based open standard used in the exchange of authentication and authorization information between different parties?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections?

A. 21/UDP
B. 21/TCP
C. 22/UDP
D. 22/TCP

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A user, Ann, is reporting to the company IT support group that her workstation screen is blank other than a window with a message requesting payment or else her hard drive will be formatted. Which of the following types of malware is on Ann's workstation?

A. Trojan
B. Spyware
C. Adware
D. Ransomware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following controls can be implemented together to prevent data loss in the event of theft of a mobile device storing sensitive information? (Select TWO).

A. Full device encryption
B. Screen locks
C. GPS
D. Asset tracking
E. Inventory control

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A way to assure data at-rest is secure even in the event of loss or theft is to use:

A. Full device encryption.
B. Special permissions on the file system.
C. Trusted Platform Module integration.
D. Access Control Lists.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A security audit identifies a number of large email messages being sent by a specific user from their company email account to another address external to the company. These messages were sent prior to a company data breach, which prompted the security audit. The user was one of a few people who had access to the leaked data. Review of the suspect's emails show they consist mostly of pictures of the user

at various locations during a recent vacation. No suspicious activities from other users who have access to the data were discovered.
Which of the following is occurring?

A. The user is encrypting the data in the outgoing messages.
B. The user is using steganography.
C. The user is spamming to obfuscate the activity.
D. The user is using hashing to embed data in the emails.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A security analyst is reviewing firewall logs while investigating a compromised web server. The following ports appear in the log:

22, 25, 445, 1433, 3128, 3389, 6667

Which of the following protocols was used to access the server remotely?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
An organization does not want the wireless network name to be easily discovered. Which of the following software features should be configured on the access points?

A. SSID broadcast
B. MAC filter
C. WPA2
D. Antenna placement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
A software developer wants to prevent stored passwords from being easily decrypted. When the password is stored by the application, additional text is added to each password before the password is hashed. This technique is known as:

A. Symmetric cryptography.
B. Private key cryptography.
C. Salting.
D. Rainbow tables.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
In 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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
A security technician has been asked to recommend an authentication mechanism that will allow users to authenticate using a password that will only be valid for a predefined time interval. Which of the following should the security technician recommend?

A. CHAP
B. TOTP
C. HOTP
D. PAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A security administrator must implement a wireless encryption system to secure mobile devices' communication. Some users have mobile devices which only support 56-bit encryption. Which of the following wireless encryption methods should be implemented?

A. RC4
B. AES
C. MD5
D. TKIP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which of the following is the GREATEST security risk of two or more companies working together under a Memorandum of Understanding?

A. Budgetary considerations may not have been written into the MOU, leaving an entity to absorb more cost than intended at signing.
B. MOUs have strict policies in place for services performed between the entities and the penalties for compromising a partner are high.
C. MOUs are generally loose agreements and therefore may not have strict guidelines in place to protect sensitive data between the two entities.
D. MOUs between two companies working together cannot be held to the same legal standards as SLAs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Joe, a user, reports to the system administrator that he is receiving an error stating his certificate has been revoked. Which of the following is the name of the database repository for these certificates?

A. CSR
B. OSCP
C. CA
D. CRL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Users are encouraged to click on a link in an email to obtain exclusive access to the newest version of a popular Smartphone. This is an example of.

A. Scarcity
B. Familiarity
C. Intimidation
D. Trust

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Which of the following types of attacks involves interception of authentication traffic in an attempt to gain unauthorized access to a wireless network?

A. Near field communication
B. IV attack
C. Evil twin
D. Replay attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following is a BEST practice when dealing with user accounts that will only need to be active for a limited time period?

A. When creating the account, set the account to not remember password history.
B. When creating the account, set an expiration date on the account.
C. When creating the account, set a password expiration date on the account.
D. When creating the account, set the account to have time of day restrictions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Which of the following types of authentication packages user credentials in a ticket?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which of the following is required to allow multiple servers to exist on one physical server?

A. Software as a Service (SaaS)
B. Platform as a Service (PaaS)
C. Virtualization
D. Infrastructure as a Service (IaaS)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Several employees submit the same phishing email to the administrator. The administrator finds that the links in the email are not being blocked by the company's security device. Which of the following might the administrator do in the short term to prevent the emails from being received?

A. Configure an ACL
B. Implement a URL filter
C. Add the domain to a block list
D. Enable TLS on the mail server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
LDAP and Kerberos are commonly used for which of the following?

A. To perform queries on a directory service
B. To store usernames and passwords for Federated Identity
C. To sign SSL wildcard certificates for subdomains
D. To utilize single sign-on capabilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
An administrator needs to renew a certificate for a web server. Which of the following should be submitted to a CA?

A. CSR
B. Recovery agent
C. Private key
D. CRL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
An administrator needs to submit a new CSR to a CA. Which of the following is a valid FIRST step?

A. Generate a new private key based on AES.
B. Generate a new public key based on RSA.
C. Generate a new public key based on AES.
D. Generate a new private key based on RSA.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 117
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 118
After recovering from a data breach in which customer data was lost, the legal team meets with the Chief Security Officer (CSO) to discuss ways to better protect the privacy of customer data.

Which of the following controls support this goal?

A. Contingency planning
B. Encryption and stronger access control
C. Hashing and non-repudiation
D. Redundancy and fault tolerance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
A security engineer, Joe, has been asked to create a secure connection between his mail server and the mail server of a business partner. Which of the following protocol would be MOST appropriate?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
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: D
Section: (none)
Explanation

Explanation/Reference:
answer is sophisticated.

QUESTION 121
A recent vulnerability scan found that Telnet is enabled on all network devices. Which of the following protocols should be used instead of Telnet?

A. SCP
B. SSH
C. SFTP
D. SSL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A network engineer is setting up a network for a company. There is a BYOD policy for the employees so that they can connect their laptops and mobile devices.

Which of the following technologies should be employed to separate the administrative network from the

network in which all of the employees' devices are connected?

A. VPN
B. VLAN
C. WPA2
D. MAC filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 123
A network administrator is asked to send a large file containing PII to a business associate.

Which of the following protocols is the BEST choice to use?

A. SSH
B. SFTP
C. SMTP
D. FTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124
When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability.

Which of the following is the type of vulnerability described?

A. Network based
B. IDS
C. Signature based
D. Host based

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
A malicious individual is attempting to write too much data to an application's memory. Which of the following describes this type of attack?

A. Zero-day
B. SQL injection
C. Buffer overflow
D. XSRF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Ann, a security administrator, wishes to replace their RADIUS authentication with a more secure protocol, which can utilize EAP. Which of the following would BEST fit her objective?

A. CHAP
B. SAML
C. Kerberos
D. Diameter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 128
A distributed denial of service attack can BEST be described as:

A. Invalid characters being entered into a field in a database application.
B. Users attempting to input random or invalid data into fields within a web browser application.
C. Multiple computers attacking a single target in an organized attempt to deplete its resources.
D. Multiple attackers attempting to gain elevated privileges on a target system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 129
Joe analyzed the following log and determined the security team should implement which of the following as

a mitigation method against further attempts?

Host 192.168.1.123
[00: 00: 01]Successful Login: 015 192.168.1.123 : local [00: 00: 03]Unsuccessful Login: 022 214.34.56.006 : RDP 192.168.1.124 [00: 00: 04]UnSuccessful Login: 010 214.34.56.006 : RDP 192.168.1.124 [00: 00: 07] UnSuccessful Login: 007 214.34.56.006 : RDP 192.168.1.124 [00: 00: 08]UnSuccessful Login: 003 214.34.56.006 : RDP 192.168.1.124

A. Reporting
B. IDS
C. Monitor system logs
D. Hardening

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 131
A systems administrator has implemented PKI on a classified government network. In the event that a disconnect occurs from the primary CA, which of the following should be accessible locally from every site to ensure users with bad certificates cannot gain access to the network?

A. A CRL
B. Make the RA available
C. A verification authority
D. A redundant CA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 132
While configuring a new access layer switch, the administrator, Joe, was advised that he needed to make sure that only devices authorized to access the network would be permitted to login and utilize resources. Which of the following should the administrator implement to ensure this happens?

A. Log Analysis
B. VLAN Management
C. Network separation
D. 802.1x

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
A vulnerability assessment indicates that a router can be accessed from default port 80 and default port 22. Which of the following should be executed on the router to prevent access via these ports? (Select TWO).

A. FTP service should be disabled
B. HTTPS service should be disabled
C. SSH service should be disabled
D. HTTP service should disabled
E. Telnet service should be disabled

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Results from a vulnerability analysis indicate that all enabled virtual terminals on a router can be accessed using the same password. The company's network device security policy mandates that at least one virtual terminal have a different password than the other virtual terminals. Which of the following sets of commands would meet this requirement?

A. line vty 0 6 P@s5W0Rd password line vty 7 Qwer++!Y password
B. line console 0 password password line vty 0 4 password P@s5W0Rd
C. line vty 0 3 password Qwer++!Y line vty 4 password P@s5W0Rd
D. line vty 0 3 password Qwer++!Y line console 0 password P@s5W0Rd

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 135
Joe, an employee, was escorted from the company premises due to suspicion of revealing trade secrets to a competitor. Joe had already been working for two hours before leaving the premises.

A security technician was asked to prepare a report of files that had changed since last night's integrity scan.

Which of the following could the technician use to prepare the report? (Select TWO).

A. PGP
B. MD5
C. ECC
D. AES
E. Blowfish
F. HMAC

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Ann has read and write access to an employee database, while Joe has only read access. Ann is leaving for a conference.

Which of the following types of authorization could be utilized to trigger write access for Joe when Ann is absent?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Human Resources suspects an employee is accessing the employee salary database. The administrator is asked to find out who it is. In order to complete this task, which of the following is a security control that should be in place?

A. Shared accounts should be prohibited.
B. Account lockout should be enabled
C. Privileges should be assigned to groups rather than individuals
D. Time of day restrictions should be in use

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 138
An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.

Which of the following should the administrator implement?

A. Snapshots

B. Sandboxing
C. Patch management
D. Intrusion detection system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
An auditor's report discovered several accounts with no activity for over 60 days. The accounts were later identified as contractors' accounts who would be returning in three months and would need to resume the activities. Which of the following would mitigate and secure the auditors finding?

A. Disable unnecessary contractor accounts and inform the auditor of the update.
B. Reset contractor accounts and inform the auditor of the update.
C. Inform the auditor that the accounts belong to the contractors.
D. Delete contractor accounts and inform the auditor of the update.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 140
Ann, the security administrator, wishes to implement multifactor security. Which of the following should be implemented in order to compliment password usage and smart cards?

A. Hard tokens
B. Fingerprint readers
C. Swipe badge readers
D. Passphrases

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Customers' credit card information was stolen from a popular video streaming company. A security consultant determined that the information was stolen, while in transit, from the gaming consoles of a particular vendor. Which of the following methods should the company consider to secure this data in the future?

A. Application firewalls
B. Manual updates
C. Firmware version control
D. Encrypted TCP wrappers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A new intern was assigned to the system engineering department, which consists of the system architect and system software developer's teams. These two teams have separate privileges. The intern requires privileges to view the system architectural drawings and comment on some software development projects. Which of the following methods should the system administrator implement?

A. Group based privileges
B. Generic account prohibition
C. User access review
D. Credential management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 143
One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

A. Mandatory access
B. Rule-based access control
C. Least privilege
D. Job rotation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 144
A small business needs to incorporate fault tolerance into their infrastructure to increase data availability. Which of the following options would be the BEST solution at a minimal cost?

A. Clustering
B. Mirrored server
C. RAID
D. Tape backup

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
A new application needs to be deployed on a virtual server. The virtual server hosts a SQL server that is used by several employees.

Which of the following is the BEST approach for implementation of the new application on the virtual server?

A. Take a snapshot of the virtual server after installing the new application and store the snapshot in a secure location.
B. Generate a baseline report detailing all installed applications on the virtualized server after installing the new application.
C. Take a snapshot of the virtual server before installing the new application and store the snapshot in a secure location.
D. Create an exact copy of the virtual server and store the copy on an external hard drive after installing the new application.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Ann wants to send a file to Joe using PKI. Which of the following should Ann use in order to sign the file?

A. Joe's public key
B. Joe's private key
C. Ann's public key
D. Ann's private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Which of the following protocols is used to validate whether trust is in place and accurate by returning responses of either "good", "unknown", or "revoked"?

A. CRL
B. PKI
C. OCSP
D. RA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
During a recent investigation, an auditor discovered that an engineer's compromised workstation was being used to connect to SCADA systems while the engineer was not logged in. The engineer is responsible for administering the SCADA systems and cannot be blocked from connecting to them. The SCADA systems cannot be modified without vendor approval which requires months of testing.

Which of the following is MOST likely to protect the SCADA systems from misuse?

A. Update anti-virus definitions on SCADA systems
B. Audit accounts on the SCADA systems
C. Install a firewall on the SCADA network
D. Deploy NIPS at the edge of the SCADA network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A security administrator must implement a network authentication solution which will ensure encryption of user credentials when users enter their username and password to authenticate to the network.

Which of the following should the administrator implement?

A. WPA2 over EAP-TTLS
B. WPA-PSK
C. WPA2 with WPS
D. WEP over EAP-PEAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 150
Several employees have been printing files that include personally identifiable information of customers. Auditors have raised concerns about the destruction of these hard copies after they are created, and management has decided the best way to address this concern is by preventing these files from being printed.

Which of the following would be the BEST control to implement?

A. File encryption
B. Printer hardening
C. Clean desk policies
D. Data loss prevention

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
The company's sales team plans to work late to provide the Chief Executive Officer (CEO) with a special report of sales before the quarter ends. After working for several hours, the team finds they cannot save or print the reports.

Which of the following controls is preventing them from completing their work?

A. Discretionary access control
B. Role-based access control
C. Time of Day access control
D. Mandatory access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A security engineer is asked by the company's development team to recommend the most secure method for password storage.

Which of the following provide the BEST protection against brute forcing stored passwords? (Select TWO).

A. PBKDF2
B. MD5
C. SHA2
D. Bcrypt
E. AES
F. CHAP

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 153
After entering the following information into a SOHO wireless router, a mobile device's user reports being unable to connect to the network:
PERMIT 0A: D1: FA. B1: 03: 37
DENY 01: 33: 7F: AB: 10: AB

Which of the following is preventing the device from connecting?

A. WPA2-PSK requires a supplicant on the mobile device.
B. Hardware address filtering is blocking the device.
C. TCP/IP Port filtering has been implemented on the SOHO router.
D. IP address filtering has disabled the device from connecting.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
The call center supervisor has reported that many employees have been playing preinstalled games on company computers and this is reducing productivity.

Which of the following would be MOST effective for preventing this behavior?

A. Acceptable use policies
B. Host-based firewalls
C. Content inspection
D. Application whitelisting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A company has decided to move large data sets to a cloud provider in order to limit the costs of new infrastructure. Some of the data is sensitive and the Chief Information Officer wants to make sure both parties have a clear understanding of the controls needed to protect the data.

Which of the following types of interoperability agreement is this?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
Which of the following solutions provides the most flexibility when testing new security controls prior to implementation?

A. Trusted OS
B. Host software baselining
C. OS hardening
D. Virtualization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following authentication services requires the use of a ticket-granting ticket (TGT) server in order to complete the authentication process?

A. TACACS+
B. Secure LDAP
C. RADIUS

D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which of the following BEST describes a protective countermeasure for SQL injection?

A. Eliminating cross-site scripting vulnerabilities
B. Installing an IDS to monitor network traffic
C. Validating user input in web applications
D. Placing a firewall between the Internet and database servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
Which of the following MOST interferes with network-based detection techniques?

A. Mime-encoding
B. SSL
C. FTP
D. Anonymous email accounts

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A certificate authority takes which of the following actions in PKI?

A. Signs and verifies all infrastructure messages
B. Issues and signs all private keys
C. Publishes key escrow lists to CRLs
D. Issues and signs all root certificates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks?

A. Malicious code on the local system
B. Shoulder surfing

C. Brute force certificate cracking
D. Distributed dictionary attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Separation of duties is often implemented between developers and administrators in order to separate which of the following?

A. More experienced employees from less experienced employees
B. Changes to program code and the ability to deploy to production
C. Upper level management users from standard development employees
D. The network access layer from the application access layer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 164
A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

A. The request needs to be sent to the incident management team.
B. The request needs to be approved through the incident management process.
C. The request needs to be approved through the change management process.
D. The request needs to be sent to the change management team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit.

They use the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?

A. Account lockout policy
B. Account password enforcement
C. Password complexity enabled
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A CRL is comprised of.

A. Malicious IP addresses.
B. Trusted CA's.
C. Untrusted private keys.
D. Public keys.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
Which of the following may significantly reduce data loss if multiple drives fail at the same time?

A. Virtualization
B. RAID
C. Load balancing
D. Server clustering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
Which of the following should be considered to mitigate data theft when using CAT5 wiring?

A. CCTV
B. Environmental monitoring
C. Multimode fiber
D. EMI shielding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

A. Management
B. Administrative
C. Technical
D. Operational

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

A. Connect the WAP to a different switch.
B. Create a voice VLAN.
C. Create a DMZ.
D. Set the switch ports to 802.1q mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

A. 10.4.4.125
B. 10.4.4.158
C. 10.4.4.165
D. 10.4.4.189

E. 10.4.4.199

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Which of the following algorithms has well documented collisions? (Select TWO).

A. AES
B. MD5
C. SHA
D. SHA-256
E. RSA

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
Which of the following is BEST used as a secure replacement for TELNET?

A. HTTPS
B. HMAC
C. GPG
D. SSH

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
Which of the following is an effective way to ensure the BEST temperature for all equipment within a datacenter?

A. Fire suppression
B. Raised floor implementation
C. EMI shielding
D. Hot or cool aisle containment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 178
Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?

A. SSLv2
B. SSHv1
C. RSA
D. TLS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

A. Incident management
B. Clean desk policy
C. Routine audits
D. Change management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
Which of the following is a difference between TFTP and FTP?

A. TFTP is slower than FTP.
B. TFTP is more secure than FTP.
C. TFTP utilizes TCP and FTP uses UDP.
D. TFTP utilizes UDP and FTP uses TCP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 181
Matt, an administrator, notices a flood fragmented packet and retransmits from an email server. After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was he MOST likely using to view this issue?

A. Spam filter
B. Protocol analyzer
C. Web application firewall
D. Load balancer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

A. Whaling
B. Impersonation
C. Privilege escalation
D. Spear phishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

A. Design reviews
B. Baseline reporting
C. Vulnerability scan
D. Code review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Which of the following is an example of a false positive?

A. Anti-virus identifies a benign application as malware.
B. A biometric iris scanner rejects an authorized user wearing a new contact lens.
C. A user account is locked out after the user mistypes the password too many times.
D. The IDS does not identify a buffer overflow.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 185
Data execution prevention is a feature in most operating systems intended to protect against which type of attack?

A. Cross-site scripting
B. Buffer overflow
C. Header manipulation
D. SQL injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 186
Use of group accounts should be minimized to ensure which of the following?

A. Password security
B. Regular auditing
C. Baseline management
D. Individual accountability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 187
Privilege creep among long-term employees can be mitigated by which of the following procedures?

A. User permission reviews
B. Mandatory vacations
C. Separation of duties
D. Job function rotation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 188
In which of the following scenarios is PKI LEAST hardened?

A. The CRL is posted to a publicly accessible location.
B. The recorded time offsets are developed with symmetric keys.
C. A malicious CA certificate is loaded on all the clients.
D. All public keys are accessed by an unauthorized user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 189
Configuring the mode, encryption methods, and security associations are part of which of the following?

A. IPSec
B. Full disk encryption
C. 802.1x
D. PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 190
Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

A. Code review
B. Penetration test
C. Protocol analyzer
D. Vulnerability scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 191
A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

A. Confidentiality
B. Availability
C. Succession planning
D. Integrity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 192
In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in QUESTION NO: from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

A. Take hashes

B. Begin the chain of custody paperwork
C. Take screen shots
D. Capture the system image
E. Decompile suspicious files

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 193
Which of the following is used to certify intermediate authorities in a large PKI deployment?

A. Root CA
B. Recovery agent
C. Root user
D. Key escrow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 194
Which of the following components MUST be trusted by all parties in PKI?

A. Key escrow
B. CA
C. Private key
D. Recovery key

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 195
Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

A. Steganography images
B. Internal memory
C. Master boot records
D. Removable memory cards
E. Public keys

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 196
Which of the following is the below pseudo-code an example of?

IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT

A. Buffer overflow prevention
B. Input validation
C. CSRF prevention
D. Cross-site scripting prevention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 197
A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 198
Which of the following can use RC4 for encryption? (Select TWO).

A. CHAP
B. SSL
C. WEP
D. AES
E. 3DES

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 199
Which of the following defines a business goal for system restoration and acceptable data loss?

A. MTTR
B. MTBF
C. RPO
D. Warm site

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 200
If Organization A trusts Organization B and Organization B trusts Organization C, then Organization A trusts Organization C. Which of the following PKI concepts is this describing?

A. Transitive trust
B. Public key trust
C. Certificate authority trust
D. Domain level trust

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 201
Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

A. Business continuity planning
B. Continuity of operations
C. Business impact analysis
D. Succession planning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 202
Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

A. Recovery agent
B. Certificate authority
C. Trust model
D. Key escrow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 203
Which of the following devices will help prevent a laptop from being removed from a certain location?

A. Device encryption
B. Cable locks
C. GPS tracking

D. Remote data wipes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 204
Which of the following is the MOST secure protocol to transfer files?

A. FTP
B. FTPS
C. SSH
D. TELNET

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 205
Suspicious traffic without a specific signature was detected. Under further investigation, it was determined that these were false indicators. Which of the following security devices needs to be configured to disable future false alarms?

A. Signature based IPS
B. Signature based IDS
C. Application based IPS
D. Anomaly based IDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 206
A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this?

A. Command shell restrictions
B. Restricted interface
C. Warning banners
D. Session output pipe to /dev/null

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 207
Which of the following protocols is used to authenticate the client and server's digital certificate?

A. PEAP
B. DNS
C. TLS
D. ICMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 208
Which of the following can be used to mitigate risk if a mobile device is lost?

A. Cable lock
B. Transport encryption
C. Voice encryption
D. Strong passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 209
Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

A. Record time offset
B. Clean desk policy
C. Cloud computing
D. Routine log review

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 210
Which of the following is an example of multifactor authentication?

A. Credit card and PIN
B. Username and password
C. Password and PIN
D. Fingerprint and retina scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 211
After Matt, a user, enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

`Please only use letters and numbers on these fields'

Which of the following is this an example of?

A. Proper error handling
B. Proper input validation
C. Improper input validation
D. Improper error handling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 212
Which of the following should the security administrator implement to limit web traffic based on country of origin? (Select THREE).

A. Spam filter
B. Load balancer
C. Antivirus
D. Proxies
E. Firewall
F. NIDS
G. URL filtering

Correct Answer: DEG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 213
Several bins are located throughout a building for secure disposal of sensitive information.
Which of the following does this prevent?

A. Dumpster diving
B. War driving
C. Tailgating
D. War chalking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 214
Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

A. Application design
B. Application security
C. Initial baseline configuration
D. Management of interfaces

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is outclass.

QUESTION 215
Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

A. Acceptable Use Policy
B. Physical security controls
C. Technical controls
D. Security awareness training

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 216
Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

A. HIDS
B. Firewall
C. NIPS
D. Spam filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 217
Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

A. War dialing
B. War chalking
C. War driving

D. Bluesnarfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 218
Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

A. Evil twin
B. DNS poisoning
C. Vishing
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 219
An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

A. CRL
B. Non-repudiation
C. Trust models
D. Recovery agents

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 220
Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 221
Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

A. Create a VLAN without a default gateway.
B. Remove the network from the routing table.
C. Create a virtual switch.
D. Commission a stand-alone switch.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 222
A security administrator implements access controls based on the security classification of the data and need-to-know information. Which of the following BEST describes this level of access control?

A. Implicit deny
B. Role-based Access Control
C. Mandatory Access Controls
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 223
A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 224
Which of the following could cause a browser to display the message below?

"The security certificate presented by this website was issued for a different website's address."

A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.

B. The website is using a wildcard certificate issued for the company's domain.
C. HTTPS://127.0.01 was used instead of HTTPS://localhost.
D. The website is using an expired self signed certificate.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 225
A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

A. Availability
B. Integrity
C. Confidentiality
D. Fire suppression

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 226
Which of the following pseudocodes can be used to handle program exceptions?

A. If program detects another instance of itself, then kill program instance.
B. If user enters invalid input, then restart program.
C. If program module crashes, then restart program module.
D. If user's input exceeds buffer length, then truncate the input.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 227
Which of the following technologies uses multiple devices to share work?

A. Switching
B. Load balancing
C. RAID
D. VPN concentrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 228
Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?

A. SFTP
B. HTTPS
C. TFTP
D. TLS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 229
Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 230
Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Select TWO).

A. Private hash
B. Recovery agent
C. Public key
D. Key escrow
E. CRL

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 231
Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

A. Incident management
B. Server clustering
C. Change management
D. Forensic analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 232
Which of the following can Pete, a security administrator, use to distribute the processing effort when generating hashes for a password cracking program?

A. RAID
B. Clustering
C. Redundancy
D. Virtualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 233
Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

A. Identify user habits
B. Disconnect system from network
C. Capture system image
D. Interview witnesses

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 234
Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point?

A. Placement of antenna
B. Disabling the SSID
C. Implementing WPA2
D. Enabling the MAC filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 235
Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

A. Implement WPA
B. Disable SSID
C. Adjust antenna placement
D. Implement WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 236
Which of the following is a management control?

A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 237
Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

A. Restoration and recovery strategies
B. Deterrent strategies
C. Containment strategies
D. Detection strategies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 238
In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using?

A. Three factor
B. Single factor
C. Two factor
D. Four factor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 239
Using proximity card readers instead of the traditional key punch doors would help to mitigate:

A. Impersonation
B. Tailgating

C. Dumpster diving
D. Shoulder surfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 240
Which of the following application attacks is used to gain access to SEH?

A. Cookie stealing
B. Buffer overflow
C. Directory traversal
D. XML injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 241
Which of the following is an authentication service that uses UDP as a transport medium?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 242
Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

A. Tethering
B. Screen lock PIN
C. Remote wipe
D. Email password
E. GPS tracking
F. Device encryption

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 243

Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 244
Which of the following should Pete, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from their company?

A. Privacy Policy
B. Least Privilege
C. Acceptable Use
D. Mandatory Vacations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 245
Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie?

A. Network based firewall
B. Anti-spam software
C. Host based firewall
D. Anti-spyware software

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
Which of the following protocols allows for secure transfer of files? (Select TWO).

A. ICMP
B. SNMP
C. SFTP
D. SCP
E. TFTP

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 247
Which of the following passwords is the LEAST complex?

A. MyTrain!45
B. Mytr@in!!
C. MyTr@in12
D. MyTr@in#8

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 248
During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR).

A. 21
B. 22
C. 23
D. 69
E. 3389
F. SSH
G. Terminal services
H. Rlogin
I. Rsync
J. Telnet

Correct Answer: BCFJ
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 249
Which of the following is an application security coding problem?

A. Error and exception handling
B. Patch management
C. Application hardening
D. Application fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 250
An IT security technician needs to establish host based security for company workstations. Which of the

following will BEST meet this requirement?

A. Implement IIS hardening by restricting service accounts.
B. Implement database hardening by applying vendor guidelines.
C. Implement perimeter firewall rules to restrict access.
D. Implement OS hardening by applying GPOs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 251
Which of the following is the MOST specific plan for various problems that can arise within a system?

A. Business Continuity Plan
B. Continuity of Operation Plan
C. Disaster Recovery Plan
D. IT Contingency Plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 252
Which of the following BEST describes the weakness in WEP encryption?

A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm.Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.
B. The WEP key is stored in plain text and split in portions across 224 packets of random data.Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
C. The WEP key has a weak MD4 hashing algorithm used.A simple rainbow table can be used to generate key possibilities due to MD4 collisions.
D. The WEP key is stored with a very small pool of random numbers to make the cipher text.As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 253
Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years.

Which of the following should Sara do to address the risk?

A. Accept the risk saving $10,000.
B. Ignore the risk saving $5,000.
C. Mitigate the risk saving $10,000.
D. Transfer the risk saving $5,000.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 254
Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 255
Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

A. Input validation
B. Network intrusion detection system
C. Anomaly-based HIDS
D. Peer review

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 256
Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

A. Sign in and sign out logs
B. Mantrap
C. Video surveillance
D. HVAC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 257
Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

A. Water base sprinkler system

B. Electrical
C. HVAC
D. Video surveillance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 258
Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

A. Hardware load balancing
B. RAID
C. A cold site
D. A host standby

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 259
Which of the following fire suppression systems is MOST likely used in a datacenter?

A. FM-200
B. Dry-pipe
C. Wet-pipe
D. Vacuum

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 260
A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 261

While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

A. Cross-site scripting
B. Buffer overflow
C. Header manipulation
D. Directory traversal

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 262
Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

A. Vulnerability assessment
B. Black box testing
C. White box testing
D. Penetration testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 263
A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 264
Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

A. Kerberos
B. Least privilege
C. TACACS+
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 265
Pete, the compliance manager, wants to meet regulations. Pete would like certain ports blocked only on all computers that do credit card transactions. Which of the following should Pete implement to BEST achieve this goal?

A. A host-based intrusion prevention system
B. A host-based firewall
C. Antivirus update system
D. A network-based intrusion detection system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 266
Pete, the system administrator, wants to restrict access to advertisements, games, and gambling web sites. Which of the following devices would BEST achieve this goal?

A. Firewall
B. Switch
C. URL content filter
D. Spam filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 267
Pete, the system administrator, wishes to monitor and limit users' access to external websites.
Which of the following would BEST address this?

A. Block all traffic on port 80.
B. Implement NIDS.
C. Use server load balancers.
D. Install a proxy server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 268
Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

A. PAT
B. NAP
C. DNAT
D. NAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 269
Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

A. Twofish
B. Diffie-Hellman
C. ECC
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 270
Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is $300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

A. $1,500
B. $3,750
C. $15,000
D. $75,000

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 271
Methods to test the responses of software and web applications to unusual or unexpected inputs is known as:

A. Brute force.
B. HTML encoding.
C. Web crawling.
D. Fuzzing.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 272
Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

A. TCP 23
B. UDP 69
C. TCP 22
D. TCP 21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is superb.

QUESTION 273
Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

A. Warm site
B. Load balancing
C. Clustering
D. RAID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 274
Which statement is TRUE about the operation of a packet sniffer?

A. It can only have one interface on a management network.
B. They are required for firewall operation and stateful inspection.
C. The Ethernet card must be placed in promiscuous mode.
D. It must be placed on a single virtual LAN interface.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 275
Which of the following firewall rules only denies DNS zone transfers?

A. deny udp any any port 53
B. deny ip any any
C. deny tcp any any port 53
D. deny all dns packets

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is genuine.

QUESTION 276
Which of the following BEST explains the use of an HSM within the company servers?

A. Thumb drives present a significant threat which is mitigated by HSM.
B. Software encryption can perform multiple functions required by HSM.
C. Data loss by removable media can be prevented with DLP.
D. Hardware encryption is faster than software encryption.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 277
Which of the following technologies can store multi-tenant data with different security requirements?

A. Data loss prevention
B. Trusted platform module
C. Hard drive encryption
D. Cloud computing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 278
Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

A. Matt should implement access control lists and turn on EFS.
B. Matt should implement DLP and encrypt the company database.
C. Matt should install Truecrypt and encrypt the company server.
D. Matt should install TPMs and encrypt the company database.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 279
Which of the following types of encryption will help in protecting files on a PED?

A. Mobile device encryption
B. Transport layer encryption
C. Encrypted hidden container

D. Database encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 280
Which of the following does full disk encryption prevent?

A. Client side attacks
B. Clear text access
C. Database theft
D. Network-based attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 281
Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
B. Tell the application development manager to code the application to adhere to the company's password policy.
C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 282
Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning?

A. A recent security breach in which passwords were cracked.
B. Implementation of configuration management processes.
C. Enforcement of password complexity requirements.
D. Implementation of account lockout procedures.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 283
Which of the following presents the STRONGEST access control?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 284
Which of the following encompasses application patch management?

A. Configuration management
B. Policy management
C. Cross-site request forgery
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 285
Sara, an application developer, implemented error and exception handling alongside input validation. Which of the following does this help prevent?

A. Buffer overflow
B. Pop-up blockers
C. Cross-site scripting
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 286
Which of the following is the LEAST volatile when performing incident response procedures?

A. Registers
B. RAID cache
C. RAM
D. Hard drive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 287
Pete, a developer, writes an application. Jane, the security analyst, knows some things about the overall application but does not have all the details. Jane needs to review the software before it is released to production. Which of the following reviews should Jane conduct?

A. Gray Box Testing
B. Black Box Testing
C. Business Impact Analysis
D. White Box Testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 288
The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST protect people from which of the following?

A. Rainbow tables attacks
B. Brute force attacks
C. Birthday attacks
D. Cognitive passwords attacks

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 289
Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number. Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent?

A. Collusion
B. Impersonation
C. Pharming
D. Transitive Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 290
Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

A. Interference

B. Man-in-the-middle
C. ARP poisoning
D. Rogue access point

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 291
Which of the following can be implemented with multiple bit strength?

A. AES
B. DES
C. SHA-1
D. MD5
E. MD4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 292
Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

A. No competition with the company's official social presence
B. Protection against malware introduced by banner ads
C. Increased user productivity based upon fewer distractions
D. Elimination of risks caused by unauthorized P2P file sharing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 293
Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option?

A. Use hardware already at an offsite location and configure it to be quickly utilized.
B. Move the servers and data to another part of the company's main campus from the server room.
C. Retain data back-ups on the main campus and establish redundant servers in a virtual environment.
D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 294
A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

A. Block cipher
B. Stream cipher
C. CRC
D. Hashing algorithm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 295
Which of the following is the BEST approach to perform risk mitigation of user access control rights?

A. Conduct surveys and rank the results.
B. Perform routine user permission reviews.
C. Implement periodic vulnerability scanning.
D. Disable user accounts that have not been used within the last two weeks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 296
Which of the following devices is BEST suited for servers that need to store private keys?

A. Hardware security module
B. Hardened network firewall
C. Solid state disk drive
D. Hardened host firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 297
All of the following are valid cryptographic hash functions EXCEPT:

A. RIPEMD.
B. RC4.
C. SHA-512.
D. MD4.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 298
In regards to secure coding practices, why is input validation important?

A. It mitigates buffer overflow attacks.
B. It makes the code more readable.
C. It provides an application configuration baseline.
D. It meets gray box testing standards.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 299
Which of the following would be used when a higher level of security is desired for encryption key storage?

A. TACACS+
B. L2TP
C. LDAP
D. TPM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 300
A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

A. Firewall
B. Application
C. IDS
D. Security

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 301
Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?

A. Registration
B. CA
C. CRL

D. Recovery agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 302
Employee badges are encoded with a private encryption key and specific personal information. The encoding is then used to provide access to the network. Which of the following describes this access control type?

A. Smartcard
B. Token
C. Discretionary access control
D. Mandatory access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 303
Which of the following devices would MOST likely have a DMZ interface?

A. Firewall
B. Switch
C. Load balancer
D. Proxy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 304
Which of the following application security testing techniques is implemented when an automated system generates random input data?

A. Fuzzing
B. XSRF
C. Hardening
D. Input validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 305
Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

A. Cognitive password
B. Password sniffing
C. Brute force
D. Social engineering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 306
A security administrator wants to check user password complexity. Which of the following is the BEST tool to use?

A. Password history
B. Password logging
C. Password cracker
D. Password hashing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 307
Certificates are used for: (Select TWO).

A. Client authentication.
B. WEP encryption.
C. Access control lists.
D. Code signing.
E. Password hashing.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 308
Which of the following is a hardware based encryption device?

A. EFS
B. TrueCrypt
C. TPM
D. SLE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

New Questions

QUESTION 309
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 310
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 311
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 312
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. Device encryption

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 313
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: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 314
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 315
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 316
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 317
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 318
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 319
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 320
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: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 321
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 322
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: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 323

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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 324
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: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 325
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 326
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 YRL filter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 327
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 328
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 329
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: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 330
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 331
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 332
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 333
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 334
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 335
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 336
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 337
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: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 338
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 339
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 340
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 341
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 honey pot systems

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 342
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 343
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 344
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 345
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 nonprivileged 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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 346
Which of the following file systems is from Microsoft and was included with their earliest operating systems?

A. NTFS
B. UFS
C. MTFS
D. FAT

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 347
The process of making certain that an entity (operating system, application, etc.) is as secure as it can be is known as:

A. Stabilizing
B. Reinforcing
C. Hardening
D. Toughening

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 348
What is the term for the process of luring someone in (usually done by an enforcement officer or a government agent)?

A. Enticement
B. Entrapment
C. Deceit
D. Sting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 349
Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

A. PAP, MSCHAPv2
B. CHAP, PAP
C. MSCHAPv2, NTLMv2
D. NTLM, NTLMv2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 350
Which of the following is an advantage of implementing individual file encryption on a hard drive which already deploys full disk encryption?

A. Reduces processing overhead required to access the encrypted files
B. Double encryption causes the individually encrypted files to partially lose their properties
C. Individually encrypted files will remain encrypted when copied to external media

D. File level access control only apply to individually encrypted files in a fully encrypted drive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 351
An IT director is looking to reduce the footprint of their company's server environment. They have decided to move several internally developed software applications to an alternate environment, supported by an external company. Which of the following BEST describes this arrangement?

A. Infrastructure as a Service
B. Storage as a Service
C. Platform as a Service
D. Software as a Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 352
A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 353
A security administrator wishes to change their wireless network so that IPSec is built into the protocol and NAT is no longer required for address range extension. Which of the following protocols should be used in this scenario?

A. WPA2
B. WPA
C. IPv6
D. IPv4

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 354
The network administrator is responsible for promoting code to applications on a DMZ web server. Which of the following processes is being followed to ensure application integrity?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 355
An IT auditor tests an application as an authenticated user. This is an example of which of the following types of testing?

A. Penetration
B. White box
C. Black box
D. Gray box

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 356
The manager has a need to secure physical documents every night, since the company began enforcing the clean desk policy. The BEST solution would include: (Select TWO).

A. Fire- or water-proof safe.
B. Department door locks.
C. Proximity card.
D. 24-hour security guard.
E. Locking cabinets and drawers.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 357
Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

A. Authentication server
B. Server certificate
C. Key length
D. EAP method

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 358
Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5
B. WEP
C. PEAP-MSCHAPv2
D. EAP-TLS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 359
Some customers have reported receiving an untrusted certificate warning when visiting the company's website. The administrator ensures that the certificate is not expired and that customers have trusted the original issuer of the certificate. Which of the following could be causing the problem?

A. The intermediate CA certificates were not installed on the server.
B. The certificate is not the correct type for a virtual server.
C. The encryption key used in the certificate is too short.
D. The client's browser is trying to negotiate SSL instead of TLS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 360
A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

A. DMZ
B. Cloud computing
C. VLAN
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 361
A company's business model was changed to provide more web presence and now its ERM software is no longer able to support the security needs of the company. The current data center will continue to provide network and security services. Which of the following network elements would be used to support the new

business model?

A. Software as a Service
B. DMZ
C. Remote access support
D. Infrastructure as a Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 362
Which of the following network devices is used to analyze traffic between various network interfaces?

A. Proxies
B. Firewalls
C. Content inspection
D. Sniffers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 363
Layer 7 devices used to prevent specific types of html tags are called:

A. Firewalls
B. Content filters
C. Routers
D. NIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 364
A network administrator needs to provide daily network usage reports on all layer 3 devices without compromising any data while gathering the information. Which of the following would be configured to provide these reports?

A. SNMP
B. SNMPv3
C. ICMP
D. SSH

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 365
A security administrator has been tasked to ensure access to all network equipment is controlled by a central server such as TACACS+. This type of implementation supports which of the following risk mitigation strategies?

A. User rights and permissions review
B. Change management
C. Data loss prevention
D. Implement procedures to prevent data theft

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 366
Company A sends a PGP encrypted file to company B. If company A used company B's public key to encrypt the file, which of the following should be used to decrypt data at company B?

A. Registration
B. Public key
C. CRLs
D. Private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 367
Which of the following types of authentication solutions use tickets to provide access to various resources from a central location?

A. Biometrics
B. PKI
C. ACLs
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 368
A corporation is looking to expand their data center but has run out of physical space in which to store hardware. Which of the following would offer the ability to expand while keeping their current data center operated by internal staff?

A. Virtualization
B. Subnetting
C. IaaS
D. SaaS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 369
After viewing wireless traffic, an attacker notices the following networks are being broadcasted by local access points:

Corpnet
Coffeeshop
FreePublicWifi

Using this information the attacker spoofs a response to make nearby laptops connect back to a malicious device. Which of the following has the attacker created?

A. Infrastructure as a Service
B. Load balancer
C. Evil twin
D. Virtualized network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 370
Which of the following concepts is enforced by certifying that email communications have been sent by who the message says it has been sent by?

A. Key escrow
B. Non-repudiation
C. Multifactor authentication
D. Hashing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 371
After a recent breach, the security administrator performs a wireless survey of the corporate network. The security administrator notices a problem with the following output:

MAC SSID ENCRYPTION POWER BEACONS
00:10:A1:36:12:CC MYCORP WPA2 CCMP 60 1202
00:10:A1:49:FC:37 MYCORP WPA2 CCMP 70 9102
FB:90:11:42:FA:99 MYCORP WPA2 CCMP 40 3031
00:10:A1:AA:BB:CC MYCORP WPA2 CCMP 55 2021
00:10:A1:FA:B1:07 MYCORP WPA2 CCMP 30 6044

Given that the corporate wireless network has been standardized, which of the following attacks is underway?

A. Evil twin
B. IV attack
C. Rogue AP
D. DDoS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 372
Input validation is an important security defense because it:

A. rejects bad or malformed data.
B. enables verbose error reporting.
C. protects mis-configured web servers.
D. prevents denial of service attacks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 373
In order to maintain oversight of a third party service provider, the company is going to implement a Governance, Risk, and Compliance (GRC) system. This system is promising to provide overall security posture coverage. Which of the following is the MOST important activity that should be considered?

A. Continuous security monitoring
B. Baseline configuration and host hardening
C. Service Level Agreement (SLA) monitoring
D. Security alerting and trending

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 374
A recent audit of a company's identity management system shows that 30% of active accounts belong to people no longer with the firm. Which of the following should be performed to help avoid this scenario? (Select TWO).

A. Automatically disable accounts that have not been utilized for at least 10 days.
B. Utilize automated provisioning and de-provisioning processes where possible.
C. Request that employees provide a list of systems that they have access to prior to leaving the firm.
D. Perform regular user account review / revalidation process.
E. Implement a process where new account creations require management approval.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 375
The Chief Information Officer (CIO) has mandated web based Customer Relationship Management (CRM) business functions be moved offshore to reduce cost, reduce IT overheads, and improve availability. The Chief Risk Officer (CRO) has agreed with the CIO's direction but has mandated that key authentication systems be run within the organization's network. Which of the following would BEST meet the CIO and CRO's requirements?

A. Software as a Service
B. Infrastructure as a Service
C. Platform as a Service
D. Hosted virtualization service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 376
Which of the following provides the BEST application availability and is easily expanded as demand grows?

A. Server virtualization
B. Load balancing
C. Active-Passive Cluster
D. RAID 6

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 377
An administrator connects VoIP phones to the same switch as the network PCs and printers. Which of the following would provide the BEST logical separation of these three device types while still allowing traffic between them via ACL?

A. Create three VLANs on the switch connected to a router
B. Define three subnets, configure each device to use their own dedicated IP address range, and then connect the network to a router
C. Install a firewall and connect it to the switch
D. Install a firewall and connect it to a dedicated switch for each device type

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 378
Which of the following wireless security measures can an attacker defeat by spoofing certain properties of their network interface card?

A. WEP

B. MAC filtering
C. Disabled SSID broadcast
D. TKIP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 379
Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

A. AES
B. 3DES
C. TwoFish
D. Blowfish

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 380
Which of the following BEST describes part of the PKI process?

A. User1 decrypts data with User2's private key
B. User1 hashes data with User2's public key
C. User1 hashes data with User2's private key
D. User1 encrypts data with User2's public key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 381
Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together?

A. Least privilege access
B. Separation of duties
C. Mandatory access control
D. Mandatory vacations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 382

A system administrator attempts to ping a hostname and the response is 2001:4860:0:2001::68. Which of the following replies has the administrator received?

A. The loopback address
B. The local MAC address
C. IPv4 address
D. IPv6 address

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 383
Which of the following allows a network administrator to implement an access control policy based on individual user characteristics and NOT on job function?

A. Attributes based
B. Implicit deny
C. Role based
D. Rule based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 384
Which of the following is a best practice when a mistake is made during a forensics examination?

A. The examiner should verify the tools before, during, and after an examination.
B. The examiner should attempt to hide the mistake during cross-examination.
C. The examiner should document the mistake and workaround the problem.
D. The examiner should disclose the mistake and assess another area of the disc.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 385
Which of the following allows lower level domains to access resources in a separate Public Key Infrastructure?

A. Trust Model
B. Recovery Agent
C. Public Key
D. Private Key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 386
Which of the following offers the LEAST secure encryption capabilities?

A. TwoFish
B. PAP
C. NTLM
D. CHAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 387
Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 388
Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter. The access records are used to identify which staff members accessed the data center in the event of equipment theft. Which of the following MUST be prevented in order for this policy to be effective?

A. Password reuse
B. Phishing
C. Social engineering
D. Tailgating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 389
Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

A. Hardware integrity
B. Data confidentiality
C. Availability of servers

D. Integrity of data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 390
When implementing fire suppression controls in a datacenter it is important to:

A. Select a fire suppression system which protects equipment but may harm technicians.
B. Ensure proper placement of sprinkler lines to avoid accidental leakage onto servers.
C. Integrate maintenance procedures to include regularly discharging the system.
D. Use a system with audible alarms to ensure technicians have 20 minutes to evacuate.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 391
Vendors typically ship software applications with security settings disabled by default to ensure a wide range of interoperability with other applications and devices. A security administrator should perform which of the following before deploying new software?

A. Application white listing
B. Network penetration testing
C. Application hardening
D. Input fuzzing testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 392
A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following should be recommended to isolate the VMs from one another?

A. Implement a virtual firewall
B. Install HIPS on each VM
C. Virtual switches with VLANs
D. Develop a patch management guide

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 393
Mandatory vacations are a security control which can be used to uncover which of the following?

A. Fraud committed by a system administrator
B. Poor password security among users
C. The need for additional security staff
D. Software vulnerabilities in vendor code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 394
Each server on a subnet is configured to only allow SSH access from the administrator's workstation. Which of the following BEST describes this implementation?

A. Host-based firewalls
B. Network firewalls
C. Network proxy
D. Host intrusion prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 395
During a security assessment, an administrator wishes to see which services are running on a remote server. Which of the following should the administrator use?

A. Port scanner
B. Network sniffer
C. Protocol analyzer
D. Process list

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 396
In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

A. Security control frameworks
B. Best practice
C. Access control methodologies
D. Compliance activity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 397
Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

A. Application patch management
B. Cross-site scripting prevention
C. Creating a security baseline
D. System hardening

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 398
A system administrator has noticed vulnerability on a high impact production server. A recent update was made available by the vendor that addresses the vulnerability but requires a reboot of the system afterwards. Which of the following steps should the system administrator implement to address the vulnerability?

A. Test the update in a lab environment, schedule downtime to install the patch, install the patch and reboot the server and monitor for any changes
B. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the patch, and monitor for any changes
C. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the update, reboot the server, and monitor for any changes
D. Backup the server, schedule downtime to install the patch, installs the patch and monitor for any changes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 399
Which of the following services are used to support authentication services for several local devices from a central location without the use of tokens?

A. TACACS+
B. Smartcards
C. Biometrics
D. Kerberos

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 400
A network administrator has recently updated their network devices to ensure redundancy is in place so that:

A. switches can redistribute routes across the network.
B. environmental monitoring can be performed.
C. single points of failure are removed.
D. hot and cold aisles are functioning.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 401
A network administrator recently updated various network devices to ensure redundancy throughout the network. If an interface on any of the Layer 3 devices were to go down, traffic will still pass through another interface and the production environment would be unaffected. This type of configuration represents which of the following concepts?

A. High availability
B. Load balancing
C. Backout contingency plan
D. Clustering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 402
A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?

A. User assigned privileges
B. Password disablement
C. Multiple account creation
D. Group based privileges

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 403
A network analyst received a number of reports that impersonation was taking place on the network. Session tokens were deployed to mitigate this issue and defend against which of the following attacks?

A. Replay
B. DDoS
C. Smurf
D. Ping of Death

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 404
Which of the following controls would prevent an employee from emailing unencrypted information to their personal email account over the corporate network?

A. DLP
B. CRL
C. TPM
D. HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 405
Which of the following is a measure of biometrics performance which rates the ability of a system to correctly authenticate an authorized user?

A. Failure to capture
B. Type II
C. Mean time to register
D. Template capacity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 406
A company with a US-based sales force has requested that the VPN system be configured to authenticate the sales team based on their username, password and a client side certificate. Additionally, the security administrator has restricted the VPN to only allow authentication from the US territory. How many authentication factors are in use by the VPN system?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 407
A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?

A. Transport encryption

B. IPsec
C. Non-repudiation
D. Public key infrastructure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 408
Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL?

PERMIT TCP ANY HOST 192.168.0.10 EQ 80
PERMIT TCP ANY HOST 192.168.0.10 EQ 443

A. It implements stateful packet filtering.
B. It implements bottom-up processing.
C. It failed closed.
D. It implements an implicit deny.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 409
Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

A. Social networking use training
B. Personally owned device policy training
C. Tailgating awareness policy training
D. Information classification training

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 410
A security administrator is concerned about the strength of user's passwords. The company does not want to implement a password complexity policy. Which of the following can the security Administrator implement to mitigate the risk of an online password attack against users with weak passwords?

A. Increase the password length requirements
B. Increase the password history
C. Shorten the password expiration period
D. Decrease the account lockout time

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 411
A company has purchased an application that integrates into their enterprise user directory for account authentication. Users are still prompted to type in their usernames and passwords. Which of the following types of authentication is being utilized here?

A. Separation of duties
B. Least privilege
C. Same sign-on
D. Single sign-on

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 412
Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

A. Scanning printing of documents.
B. Scanning of outbound IM (Instance Messaging).
C. Scanning copying of documents to USB.
D. Scanning of SharePoint document library.
E. Scanning of shared drives.
F. Scanning of HTTP user traffic.

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 413
A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

A. Backdoor
B. Spyware
C. Logic bomb
D. DDoS
E. Smurf

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 414
A security administrator plans on replacing a critical business application in five years. Recently, there was a security flaw discovered in the application that will cause the IT department to manually re- enable user accounts each month at a cost of $2,000. Patching the application today would cost $140,000 and take two

months to implement. Which of the following should the security administrator do in regards to the application?

A. Avoid the risk to the user base allowing them to re-enable their own accounts
B. Mitigate the risk by patching the application to increase security and saving money
C. Transfer the risk replacing the application now instead of in five years
D. Accept the risk and continue to enable the accounts each month saving money

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 415
The IT department has setup a share point site to be used on the intranet. Security has established the groups and permissions on the site. No one may modify the permissions and all requests for access are centrally managed by the security team. This is an example of which of the following control types?

A. Rule based access control
B. Mandatory access control
C. User assigned privilege
D. Discretionary access control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 416
Purchasing receives a phone call from a vendor asking for a payment over the phone. The phone number displayed on the caller ID matches the vendor's number. When the purchasing agent asks to call the vendor back, they are given a different phone number with a different area code.

Which of the following attack types is this?

A. Hoax
B. Impersonation
C. Spear phishing
D. Whaling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 417
Purchasing receives an automated phone call from a bank asking to input and verify credit card information. The phone number displayed on the caller ID matches the bank. Which of the following attack types is this?

A. Hoax
B. Phishing
C. Vishing
D. Whaling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 418
The IT department has setup a website with a series of questions to allow end users to reset their own accounts. Which of the following account management practices does this help?

A. Account Disablements
B. Password Expiration
C. Password Complexity
D. Password Recovery

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 419
An information bank has been established to store contacts, phone numbers and other records. A UNIX application needs to connect to the index server using port 389. Which of the following authentication services should be used on this port by default?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 420
An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this?

A. User rights reviews
B. Least privilege and job rotation
C. Change management
D. Change Control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 421
Which of the following is the default port for TFTP?

A. 20

B. 69
C. 21
D. 68

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 422
Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE).

A. Confidentiality
B. Availability
C. Integrity
D. Authorization
E. Authentication
F. Continuity

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 423
Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

A. Clustering
B. RAID
C. Backup Redundancy
D. Cold site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 424
Which of the following security concepts identifies input variables which are then used to perform boundary testing?

A. Application baseline
B. Application hardening
C. Secure coding
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 425
Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?

A. Session Key
B. Public Key
C. Private Key
D. Digital Signature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 426
Which of the following cryptographic related browser settings allows an organization to communicate securely?

A. SSL 3.0/TLS 1.0
B. 3DES
C. Trusted Sites
D. HMAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 427
Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

A. To ensure proper use of social media
B. To reduce organizational IT risk
C. To detail business impact analyses
D. To train staff on zero-days

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 428
A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

A. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP
B. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS
C. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS
D. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 429
A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews?

A. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.
B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.
C. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.
D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 430
A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of all servers to ensure that:

A. HDD hashes are accurate.
B. the NTP server works properly.
C. chain of custody is preserved.
D. time offset can be calculated.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 431
While rarely enforced, mandatory vacation policies are effective at uncovering:

A. Help desk technicians with oversight by multiple supervisors and detailed quality control systems.
B. Collusion between two employees who perform the same business function.
C. Acts of incompetence by a systems engineer designing complex architectures as a member of a team.
D. Acts of gross negligence on the part of system administrators with unfettered access to system and no oversight.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 432
A company hires outside security experts to evaluate the security status of the corporate network. All of the company's IT resources are outdated and prone to crashing. The company requests that all testing be performed in a way which minimizes the risk of system failures. Which of the following types of testing does the company want performed?

A. Penetration testing
B. WAF testing
C. Vulnerability scanning
D. White box testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 433
A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate this issue so that only security administrators can make changes to the firewall?

A. Mandatory vacations
B. Job rotation
C. Least privilege
D. Time of day restrictions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 434
A security administrator notices large amounts of traffic within the network heading out to an external website. The website seems to be a fake bank site with a phone number that when called, asks for sensitive information. After further investigation, the security administrator notices that a fake link was sent to several users. This is an example of which of the following attacks?

A. Vishing
B. Phishing
C. Whaling
D. SPAM
E. SPIM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 435
After a user performed a war driving attack, the network administrator noticed several similar markings where WiFi was available throughout the enterprise. Which of the following is the term used to describe these markings?

A. IV attack

B. War dialing
C. Rogue access points
D. War chalking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 436
The system administrator notices that their application is no longer able to keep up with the large amounts of traffic their server is receiving daily. Several packets are dropped and sometimes the server is taken offline. Which of the following would be a possible solution to look into to ensure their application remains secure and available?

A. Cloud computing
B. Full disk encryption
C. Data Loss Prevention
D. HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 437
After a recent internal audit, the security administrator was tasked to ensure that all credentials must be changed within 90 days, cannot be repeated, and cannot contain any dictionary words or patterns. All credentials will remain enabled regardless of the number of attempts made. Which of the following types of user account options were enforced? (Select TWO).

A. Recovery
B. User assigned privileges
C. Lockout
D. Disablement
E. Group based privileges
F. Password expiration
G. Password complexity

Correct Answer: FG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 438
A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop they notice several pictures of the employee's pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match.

Which of the following describes how the employee is leaking these secrets?

A. Social engineering
B. Steganography

C. Hashing
D. Digital signatures

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 439
During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

A. SSL 1.0
B. RC4
C. SSL 3.0
D. AES
E. DES
F. TLS 1.0

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 440
Review the following diagram depicting communication between PC1 and PC2 on each side of a router. Analyze the network traffic logs which show communication between the two computers as captured by the computer with IP 10.2.2.10.

DIAGRAM
PC1 PC2
[192.168.1.30]--------[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]----- ----[10.2.2.10] LOGS
10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN
10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK
10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK

Given the above information, which of the following can be inferred about the above environment?

A. 192.168.1.30 is a web server.
B. The web server listens on a non-standard port.
C. The router filters port 80 traffic.
D. The router implements NAT.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 441
The Chief Information Officer (CIO) wants to implement a redundant server location to which the production server images can be moved within 48 hours and services can be quickly restored, in case of a catastrophic failure of the primary datacenter's HVAC. Which of the following can be implemented?

A. Cold site

B. Load balancing
C. Warm site
D. Hot site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 442
The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection. Which of the following has happened on the workstation?

A. Zero-day attack
B. Known malware infection
C. Session hijacking
D. Cookie stealing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 443
Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device's removable media in the event that the device is lost or stolen?

A. Hashing
B. Screen locks
C. Device password
D. Encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 444
Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?

A. Subnetting
B. NAT
C. Quality of service
D. NAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 445
A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

A. ICMP
B. BGP
C. NetBIOS
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 446
A victim is logged onto a popular home router forum site in order to troubleshoot some router configuration issues. The router is a fairly standard configuration and has an IP address of 192.168.1.1. The victim is logged into their router administrative interface in one tab and clicks a forum link in another tab. Due to clicking the forum link, the home router reboots. Which of the following attacks MOST likely occurred?

A. Brute force password attack
B. Cross-site request forgery
C. Cross-site scripting
D. Fuzzing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 447
Which of the following assets is MOST likely considered for DLP?

A. Application server content
B. USB mass storage devices
C. Reverse proxy
D. Print server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 448
In order to securely communicate using PGP, the sender of an email must do which of the following when sending an email to a recipient for the first time?

A. Import the recipient's public key
B. Import the recipient's private key
C. Export the sender's private key
D. Export the sender's public key

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 449
A hacker has discovered a simple way to disrupt business for the day in a small company which relies on staff working remotely. In a matter of minutes the hacker was able to deny remotely working staff access to company systems with a script. Which of the following security controls is the hacker exploiting?

A. DoS
B. Account lockout
C. Password recovery
D. Password complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 450
A security specialist has been asked to evaluate a corporate network by performing a vulnerability assessment. Which of the following will MOST likely be performed?

A. Identify vulnerabilities, check applicability of vulnerabilities by passively testing security controls.
B. Verify vulnerabilities exist, bypass security controls and exploit the vulnerabilities.
C. Exploit security controls to determine vulnerabilities and mis-configurations.
D. Bypass security controls and identify applicability of vulnerabilities by passively testing security controls.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 451
A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network?

A. Spoof the MAC address of an observed wireless network client
B. Ping the access point to discover the SSID of the network
C. Perform a dictionary attack on the access point to enumerate the WEP key
D. Capture client to access point disassociation packets to replay on the local PC's loopback

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 452
After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

A. To allow load balancing for cloud support
B. To allow for business continuity if one provider goes out of business
C. To eliminate a single point of failure
D. To allow for a hot site in case of disaster
E. To improve intranet communication speeds

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 453
A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks. Which of the following is MOST likely the reason for the sub-interfaces?

A. The network uses the subnet of 255.255.255.128.
B. The switch has several VLANs configured on it.
C. The sub-interfaces are configured for VoIP traffic.
D. The sub-interfaces each implement quality of service.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 454
Which of the following should be enabled in a laptop's BIOS prior to full disk encryption?

A. USB
B. HSM
C. RAID
D. TPM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 455
Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login. Which is the following is MOST likely the issue?

A. The IP addresses of the clients have change
B. The client certificate passwords have expired on the server
C. The certificates have not been installed on the workstations
D. The certificates have been installed on the CA

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 456
Digital Signatures provide which of the following?

A. Confidentiality
B. Authorization
C. Integrity
D. Authentication
E. Availability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 457
A user ID and password together provide which of the following?

A. Authorization
B. Auditing
C. Authentication
D. Identification

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 458
RADIUS provides which of the following?

A. Authentication, Authorization, Availability
B. Authentication, Authorization, Auditing
C. Authentication, Accounting, Auditing
D. Authentication, Authorization, Accounting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 459
A recent intrusion has resulted in the need to perform incident response procedures. The incident response team has identified audit logs throughout the network and organizational systems which hold details of the security breach. Prior to this incident, a security consultant informed the company that they needed to implement an NTP server on the network. Which of the following is a problem that the incident response team will likely encounter during their assessment?

A. Chain of custody
B. Tracking man hours

C. Record time offset
D. Capture video traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 460
In order for network monitoring to work properly, you need a PC and a network card running in what mode?

A. Launch
B. Exposed
C. Promiscuous
D. Sweep

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 461
Which of the following utilities can be used in Linux to view a list of users' failed authentication attempts?

A. badlog
B. faillog
C. wronglog
D. killlog

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 462
A periodic update that corrects problems in one version of a product is called a

A. Hotfix
B. Overhaul
C. Service pack
D. Security update

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 463
A user has received an email from an external source which asks for details on the company's new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT?

A. Contact their manager and request guidance on how to best move forward
B. Contact the help desk and/or incident response team to determine next steps
C. Provide the requestor with the email information since it will be released soon anyway
D. Reply back to the requestor to gain their contact information and call them

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 464
Which of the following techniques enables a highly secured organization to assess security weaknesses in real time?

A. Access control lists
B. Continuous monitoring
C. Video surveillance
D. Baseline reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 465
Which of the following techniques can be used to prevent the disclosure of system information resulting from arbitrary inputs when implemented properly?

A. Fuzzing
B. Patch management
C. Error handling
D. Strong passwords

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 466
Encryption of data at rest is important for sensitive information because of which of the following?

A. Facilitates tier 2 support, by preventing users from changing the OS
B. Renders the recovery of data harder in the event of user password loss
C. Allows the remote removal of data following eDiscovery requests
D. Prevents data from being accessed following theft of physical equipment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 467
Which of the following is synonymous with a server's certificate?

A. Public key
B. CRL
C. Private key
D. Recovery agent

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 468
A network administrator noticed various chain messages have been received by the company. Which of the following security controls would need to be implemented to mitigate this issue?

A. Anti-spam
B. Antivirus
C. Host-based firewalls
D. Anti-spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 469
Which of the following types of application attacks would be used to specifically gain unauthorized information from databases that did not have any input validation implemented?

A. SQL injection
B. Session hijacking and XML injection
C. Cookies and attachments
D. Buffer overflow and XSS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 470
Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

A. HIPS on each virtual machine
B. NIPS on the network
C. NIDS on the network
D. HIDS on each virtual machine

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 471
A security administrator wants to get a real time look at what attackers are doing in the wild, hoping to lower the risk of zero-day attacks. Which of the following should be used to accomplish this goal?

A. Penetration testing
B. Honeynets
C. Vulnerability scanning
D. Baseline reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 472
Which of the following protocols is the security administrator observing in this packet capture?

12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 473
Which of the following is true about asymmetric encryption?

A. A message encrypted with the private key can be decrypted by the same key
B. A message encrypted with the public key can be decrypted with a shared key.
C. A message encrypted with a shared key, can be decrypted by the same key.
D. A message encrypted with the public key can be decrypted with the private key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 474
Which of the following is true about an email that was signed by User A and sent to User B?

A. User A signed with User B's private key and User B verified with their own public key.
B. User A signed with their own private key and User B verified with User A's public key.
C. User A signed with User B's public key and User B verified with their own private key.
D. User A signed with their own public key and User B verified with User A's private key.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 475
The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

A. HPM technology
B. Full disk encryption
C. DLP policy
D. TPM technology

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 476
Which of the following protocols encapsulates an IP packet with an additional IP header?

A. SFTP
B. IPSec
C. HTTPS
D. SSL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 477
A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone's boot loader and continues to target additional Windows PCs or phones. Which of the following malware categories BEST describes this program?

A. Zero-day
B. Trojan
C. Virus
D. Rootkit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 478
A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change

on the user's host:

Old `hosts' file:
127.0.0.1 localhost
New `hosts' file:
127.0.0.1 localhost
5.5.5.5 www.comptia.com

Which of the following attacks has taken place?

A. Spear phishing
B. Pharming
C. Phishing
D. Vishing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 479
An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place?

A. Shoulder surfing
B. Dumpster diving
C. Whaling attack
D. Vishing attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 480
A user commuting to work via public transport received an offensive image on their smart phone from another commuter. Which of the following attacks MOST likely took place?

A. War chalking
B. Bluejacking
C. War driving
D. Bluesnarfing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 481
An attacker attempted to compromise a web form by inserting the following input into the username field:
admin)(|(password=*))

Which of the following types of attacks was attempted?

A. SQL injection
B. Cross-site scripting
C. Command injection
D. LDAP injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

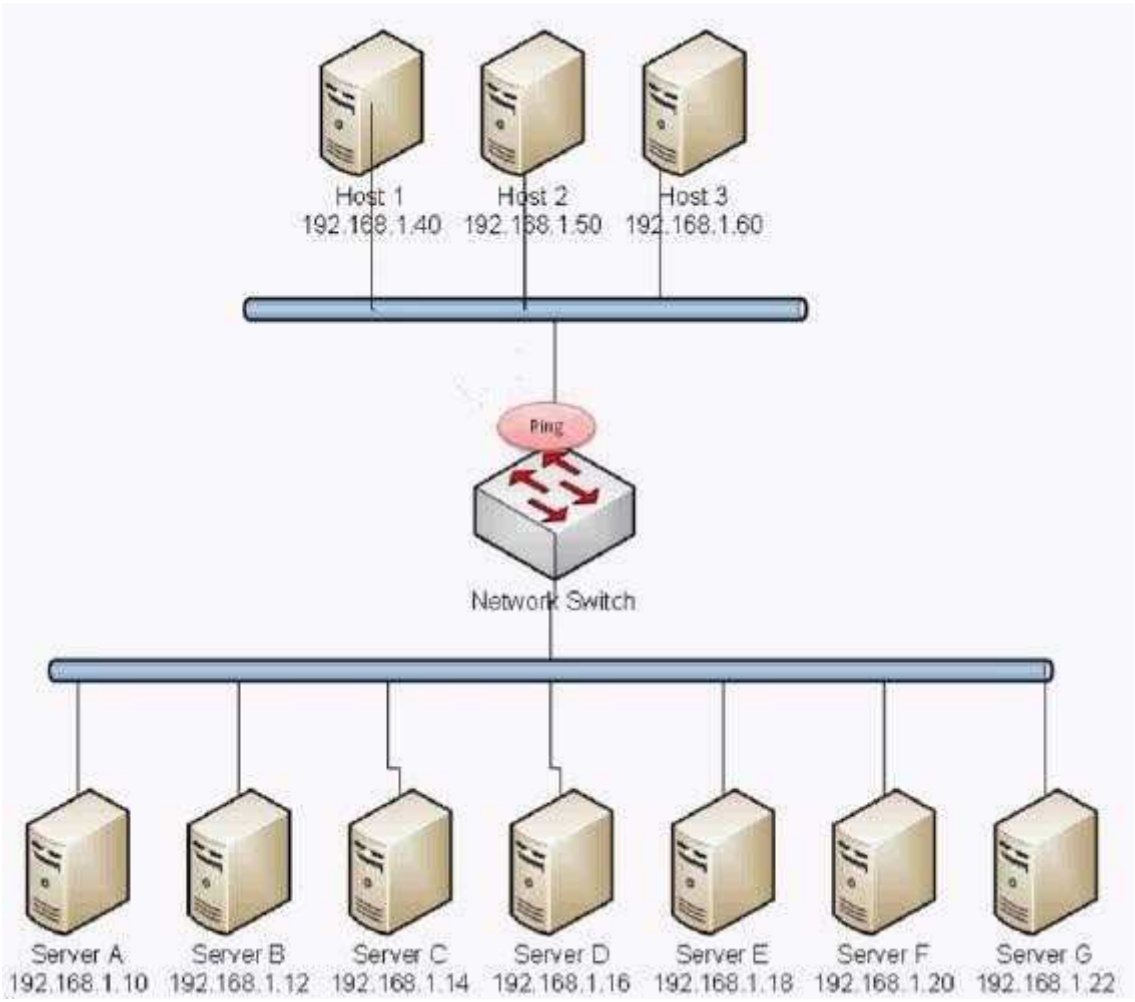
QUESTION 482
Which of the following is BEST carried out immediately after a security breach is discovered?

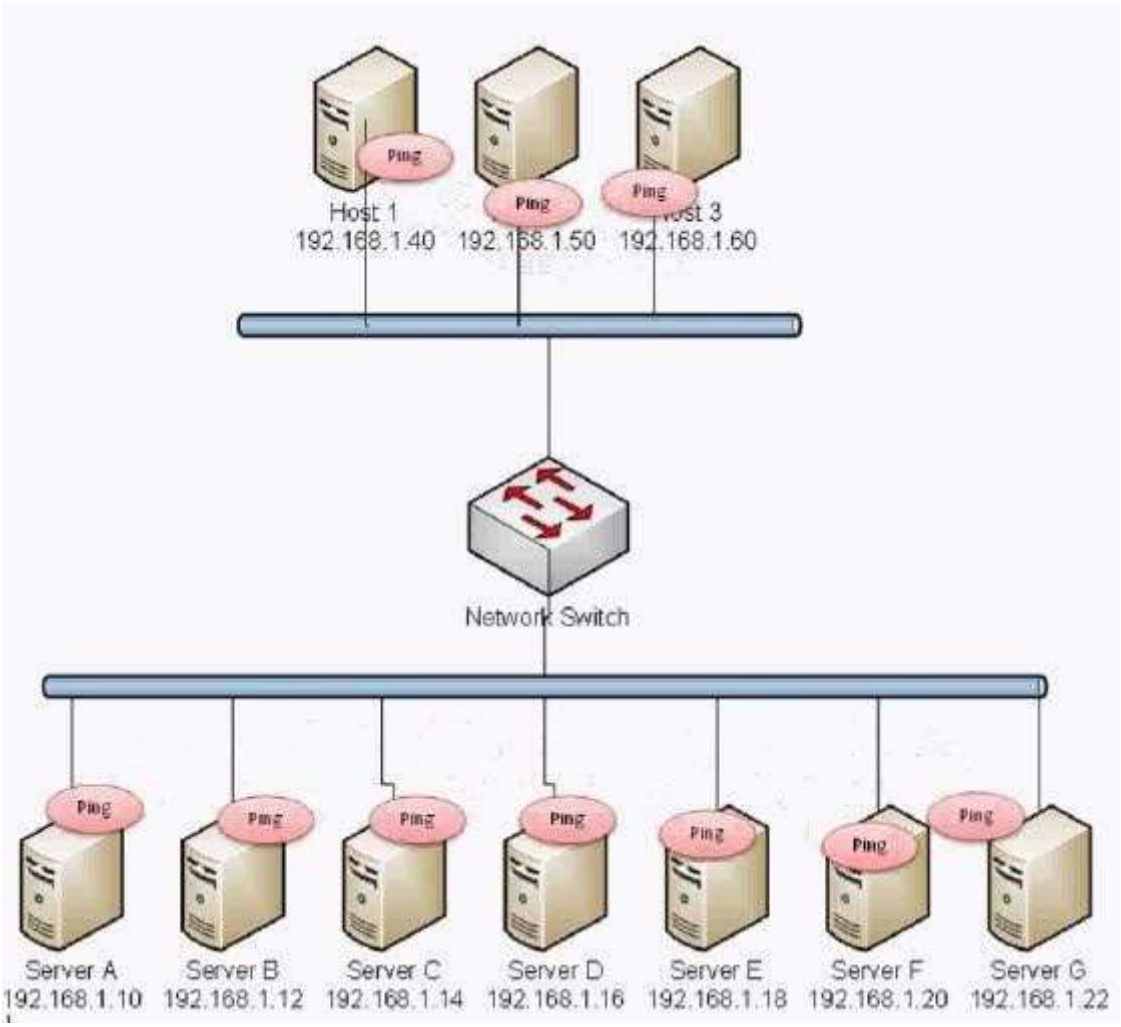
A. Risk transference
B. Access control revalidation
C. Change management
D. Incident management

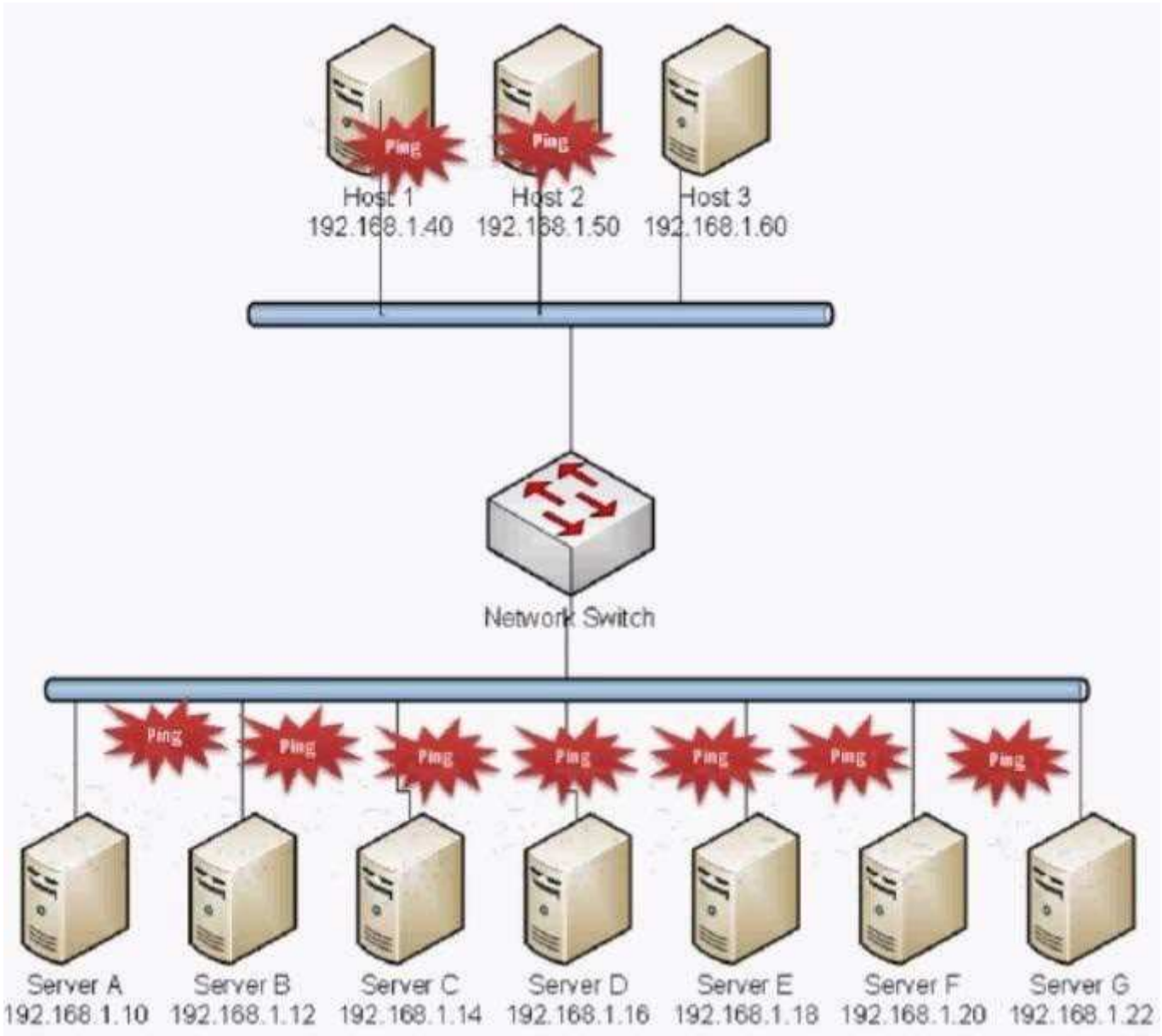
Correct Answer: D
Section: (none)
Explanation

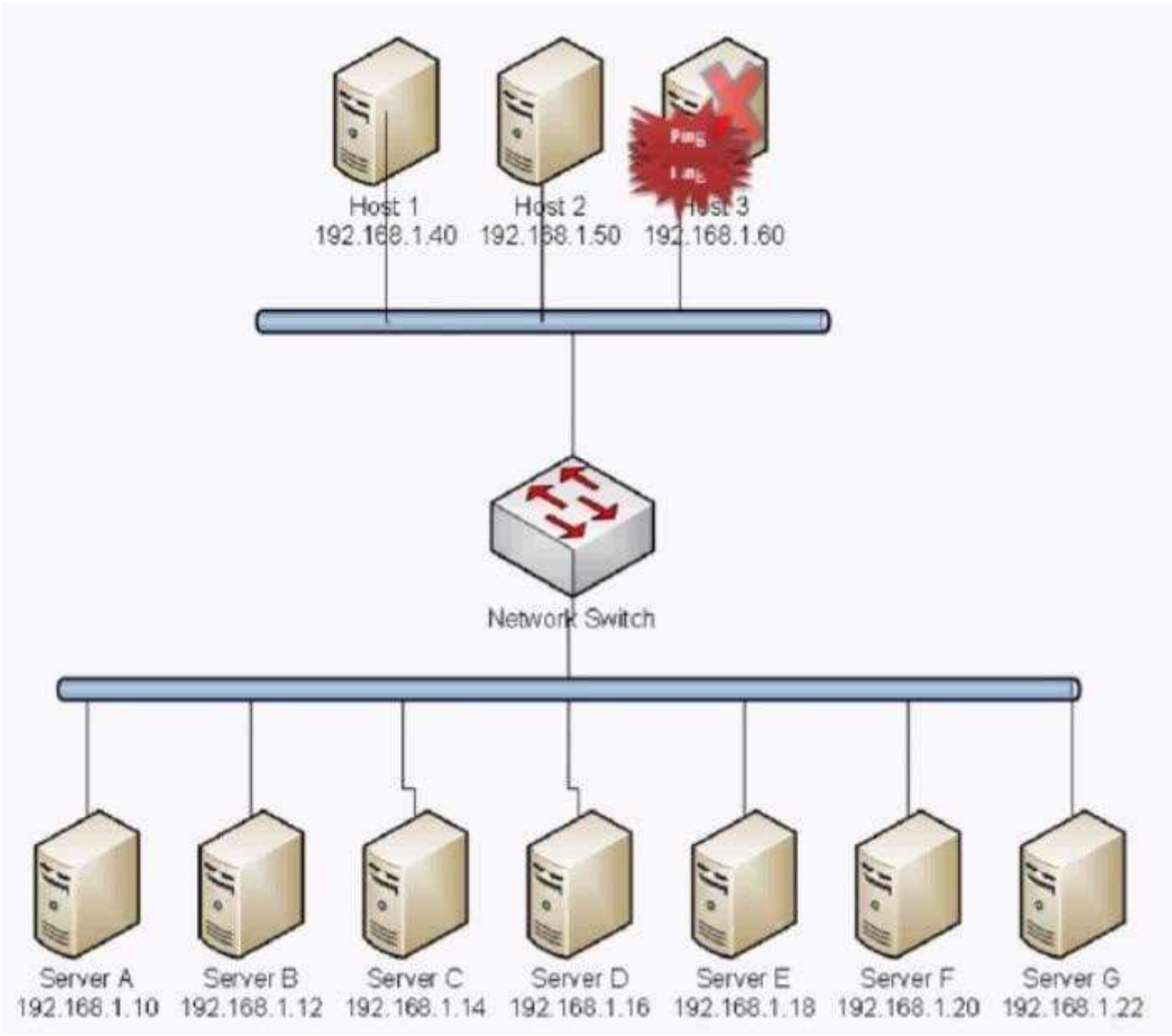
Explanation/Reference:
Explanation:

QUESTION 483
Which of the following BEST describes the type of attack that is occurring?


Host 1
192.168.1.40
Host 2
192.168.1.50
Host 3
192.168.1.60
Ping
Network Switch
Server A
192.168.1.10
Server B
192.168.1.12
Server C
192.168.1.14
Server D
192.168.1.16
Server E
192.168.1.18
Server F
192.168.1.20
Server G
192.168.1.22


Ping
Ping
Ping
Host 1
192.168.1.40
192.168.1.50
192.168.1.60
Network Switch
Ping
Ping
Ping
Ping
Ping
Ping
Ping
Server A
192.168.1.10
Server B
192.168.1.12
Server C
192.168.1.14
Server D
192.168.1.16
Server E
192.168.1.18
Server F
192.168.1.20
Server G
192.168.1.22


Ping
Ping
Host 1
192.168.1.40
Host 2
192.168.1.50
Host 3
192.168.1.60
Network Switch
Ping
Ping
Ping
Ping
Ping
Ping
Ping
Server A
192.168.1.10
Server B
192.168.1.12
Server C
192.168.1.14
Server D
192.168.1.16
Server E
192.168.1.18
Server F
192.168.1.20
Server G
192.168.1.22

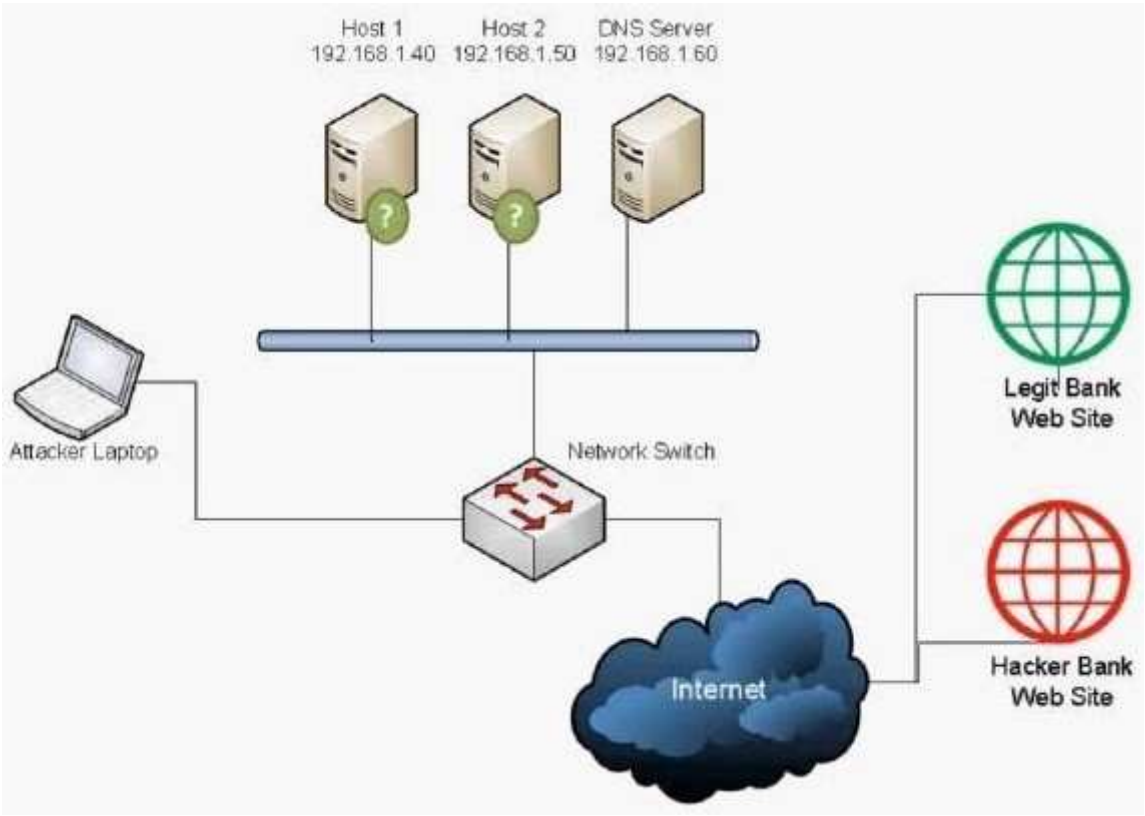


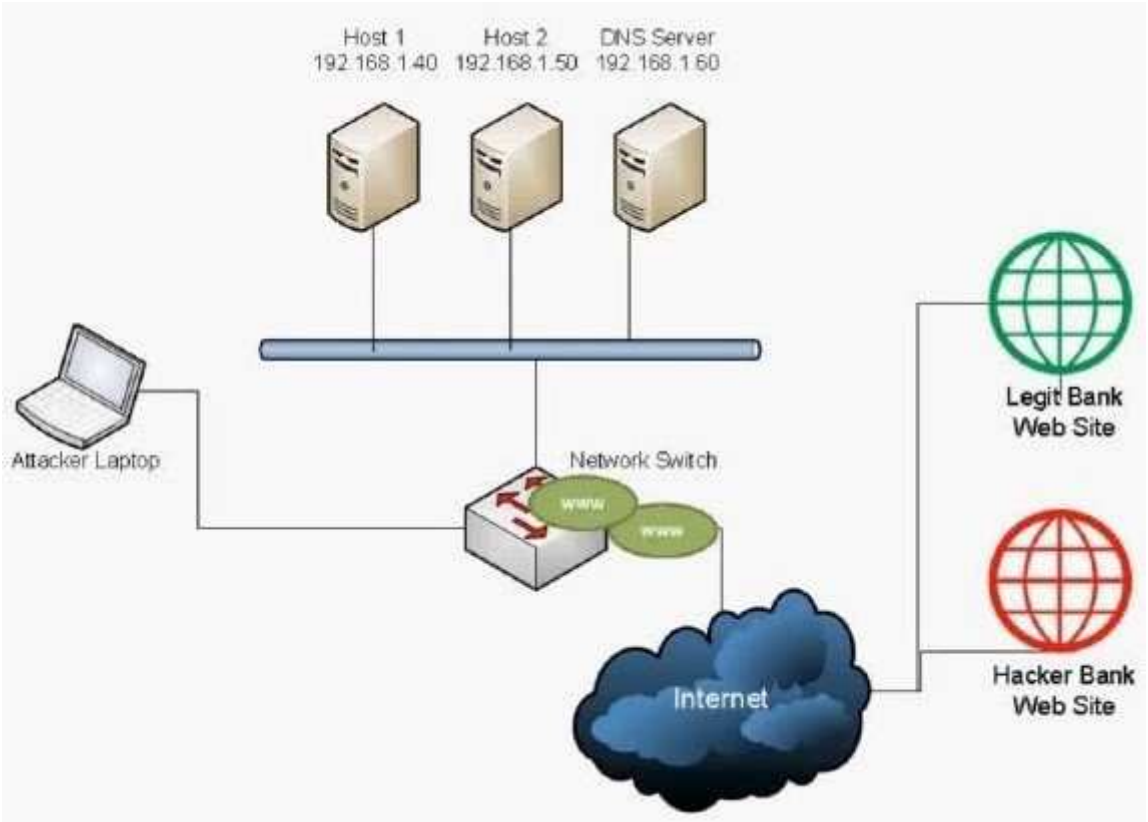
A. Smurf Attack
B. Man in the middle
C. Backdoor
D. Replay
E. Spear Phishing
F. Xmas Attack
G. Blue Jacking
H. Ping of Death

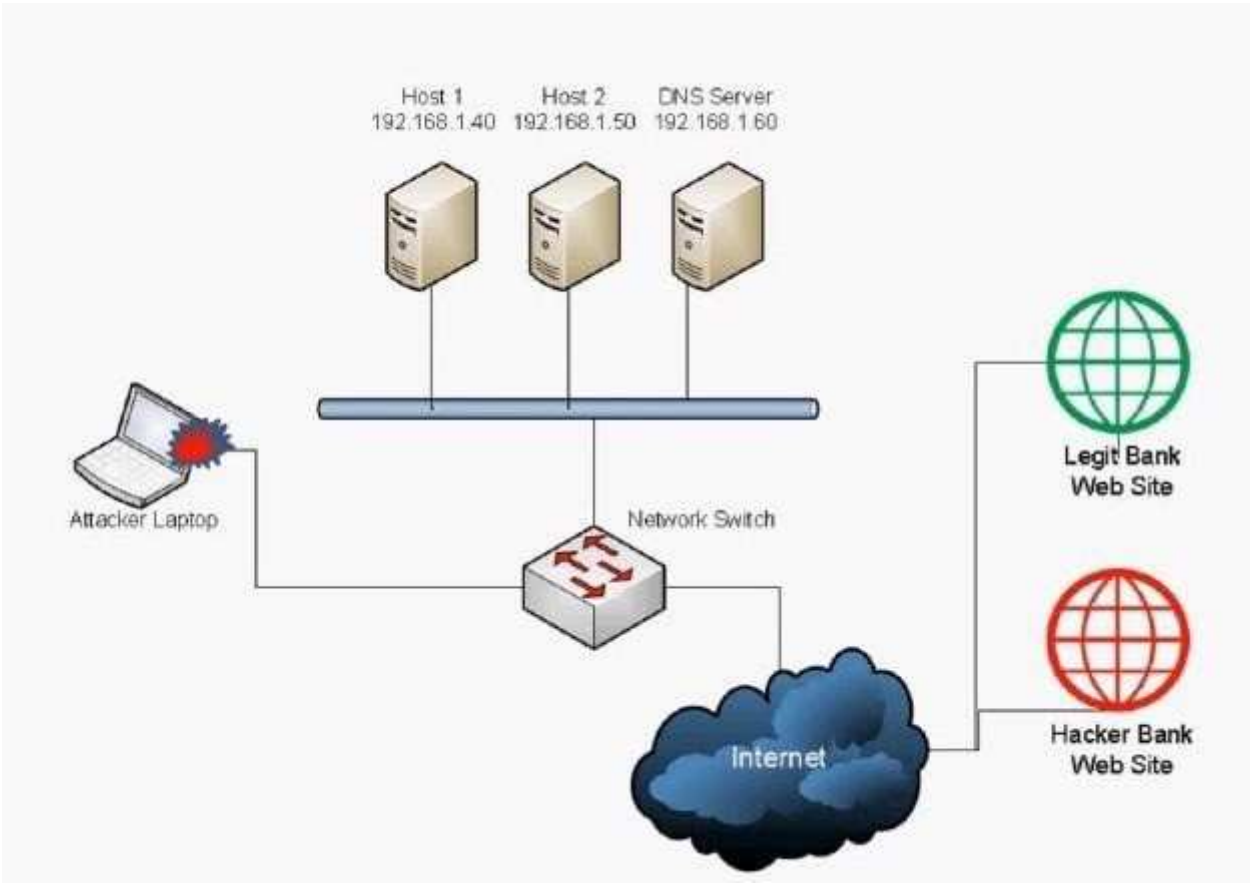
Correct Answer: A
Section: (none)
Explanation

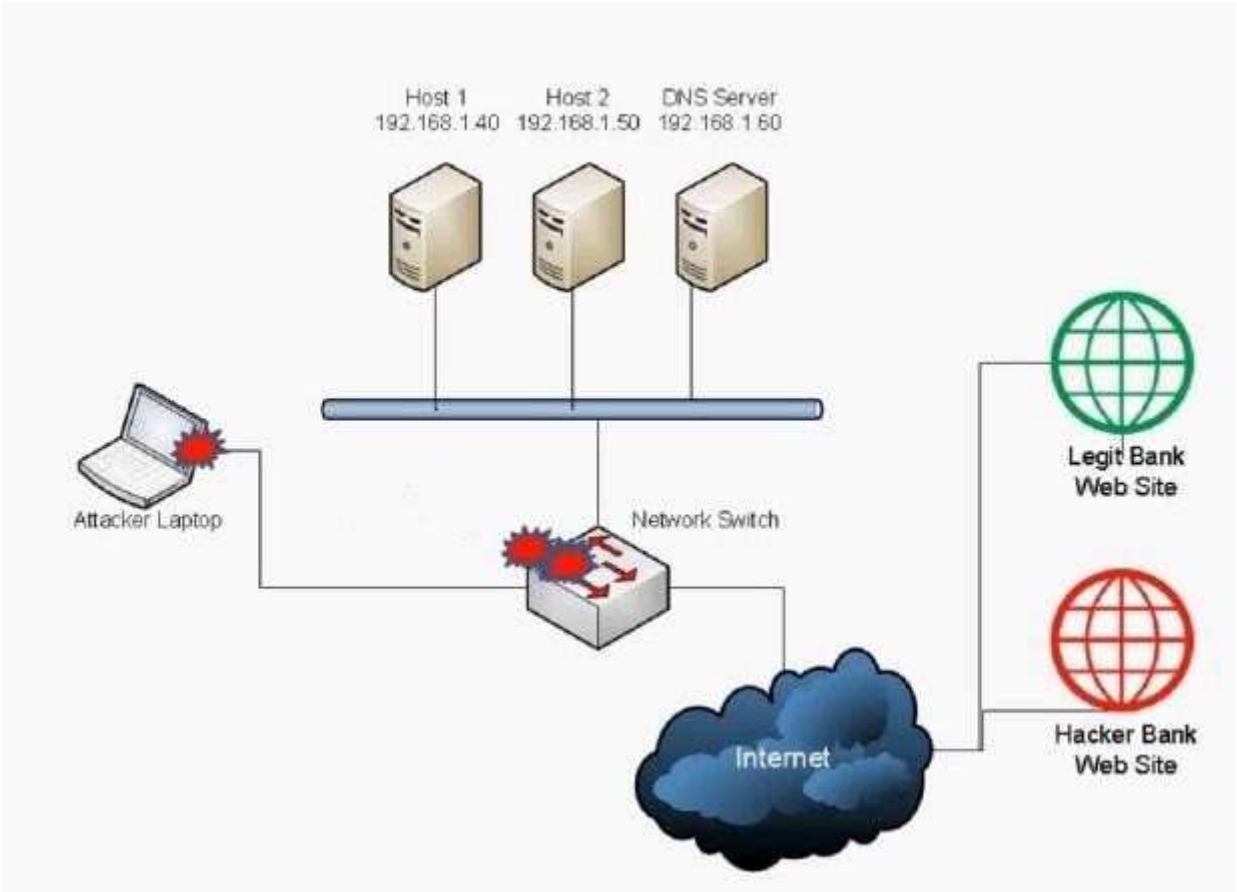
Explanation/Reference:
Explanation:

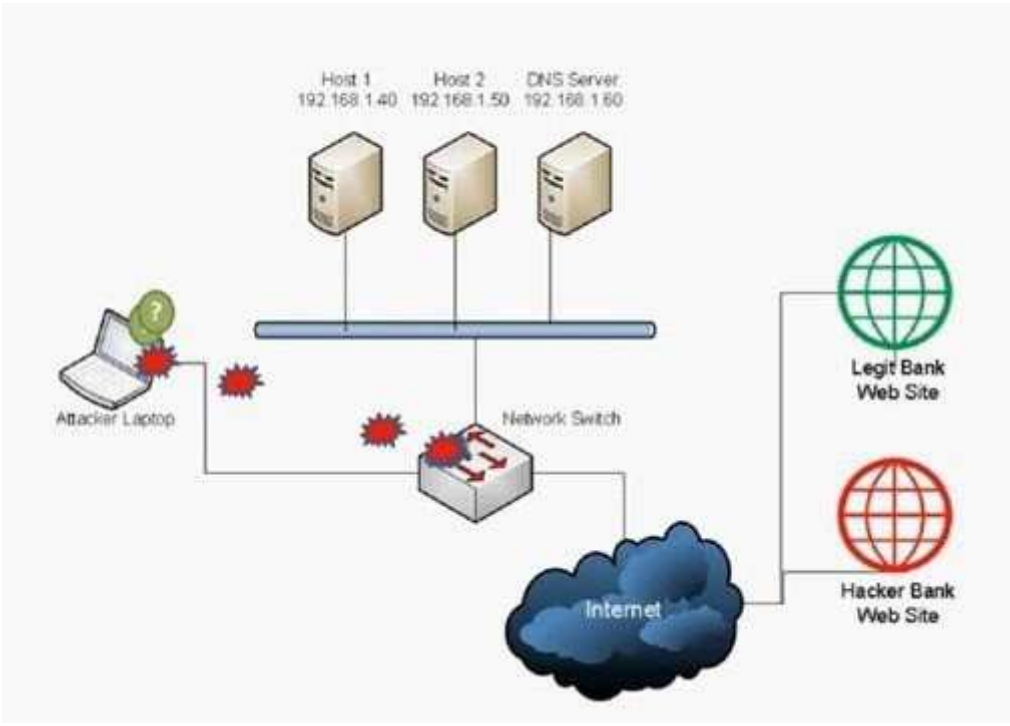
QUESTION 484
Which of the following BEST describes the type of attack that is occurring? (Select TWO).

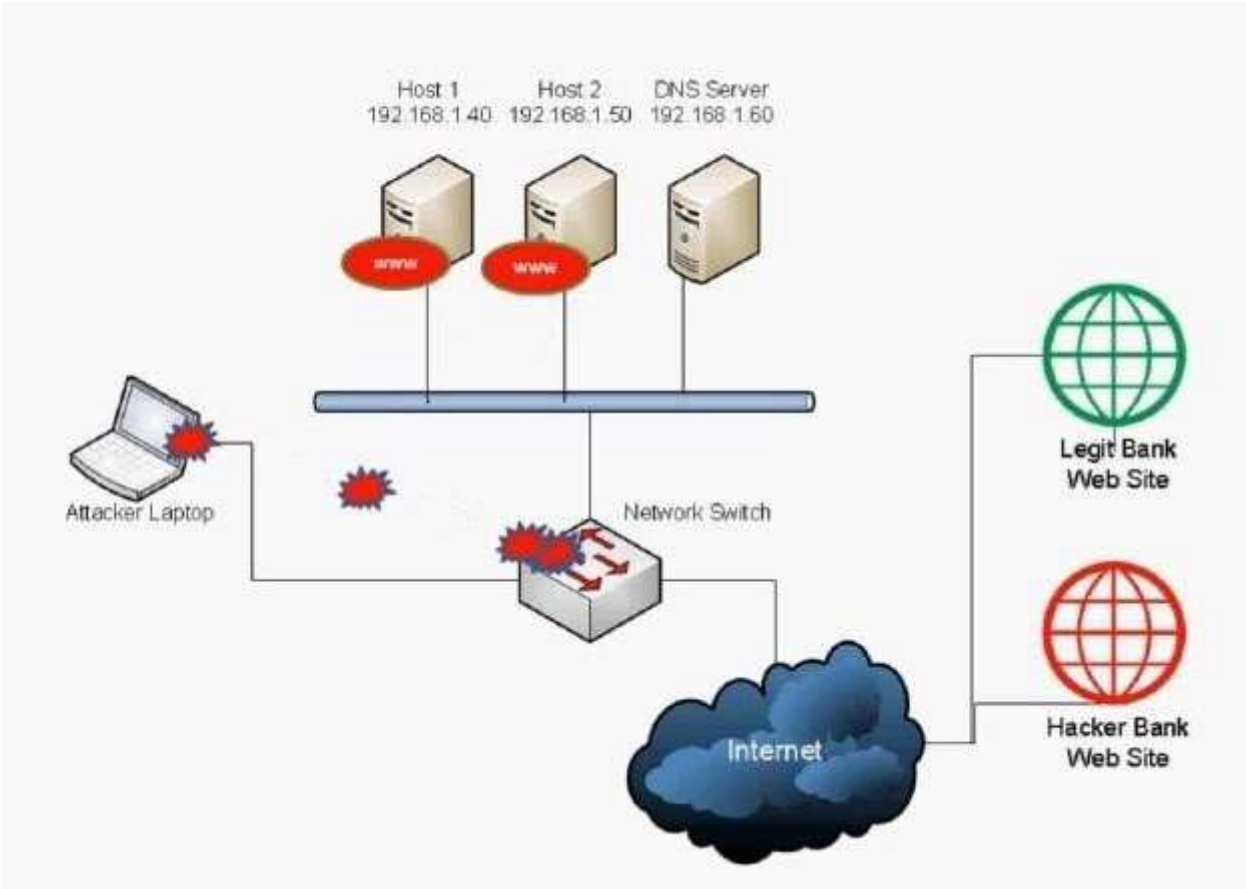

Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Attacker Laptop
Network Switch
Legit Bank
Web Site
Hacker Bank
Web Site
Internet

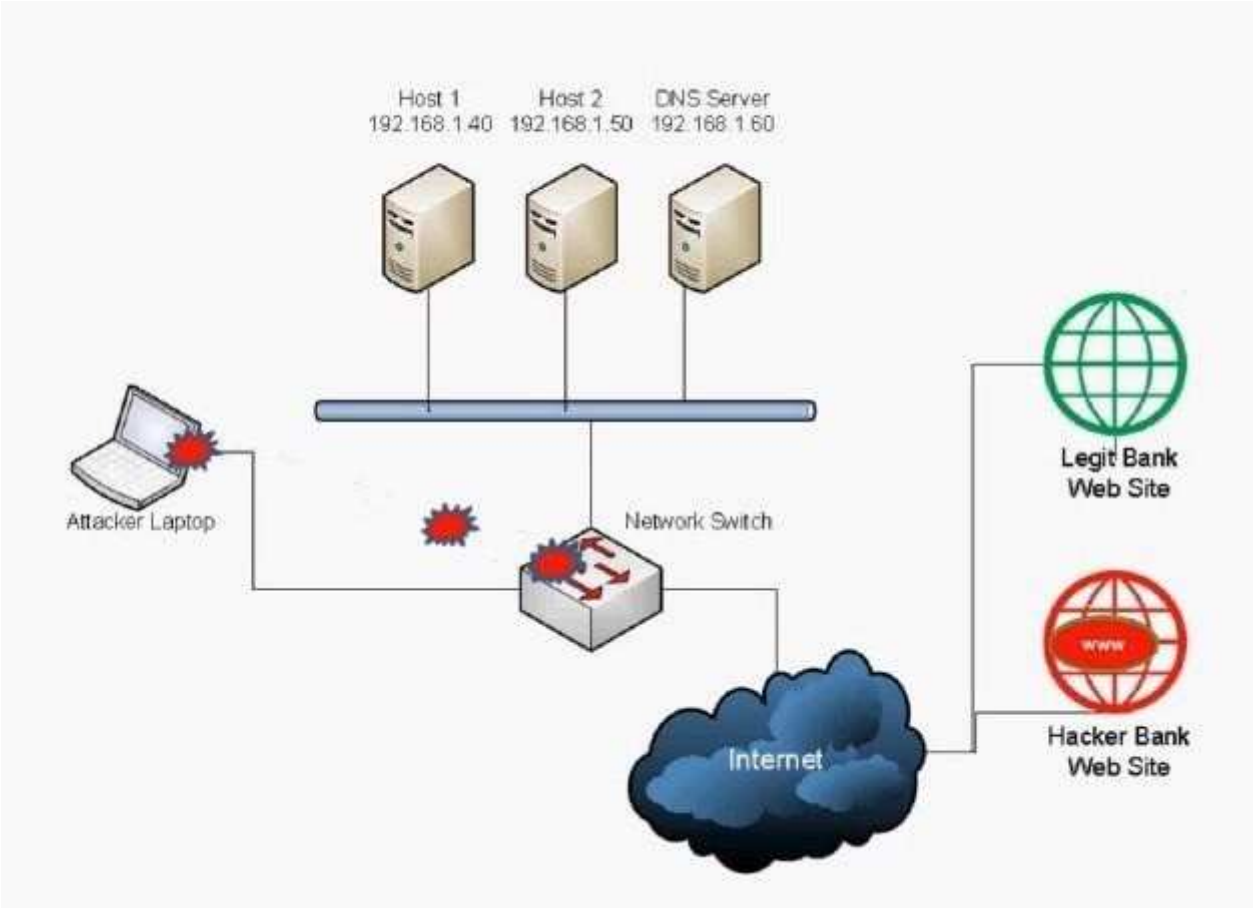

Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Attacker Laptop
Network Switch
Legit Bank
Web Site
Hacker Bank
Web Site
Internet


Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Attacker Laptop
Network Switch
Legit Bank
Web Site
Hacker Bank
Web Site
Internet


Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Attacker Laptop
Network Switch
Legit Bank
Web Site
Hacker Bank
Web Site
Internet


Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Attacker Laptop
Network Switch
Legit Bank
Web Site
Hacker Bank
Web Site
Internet


Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
www
www
Attacker Laptop
Network Switch
Legit Bank
Web Site
Hacker Bank
Web Site
Internet



A. DNS spoofing
B. Man-in-the-middle
C. Backdoor
D. Replay
E. ARP attack
F. Spear phishing
G. Xmas attack

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 485
Which of the following is a hardware-based security technology included in a computer?

A. Symmetric key
B. Asymmetric key
C. Whole disk encryption
D. Trusted platform module

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 486
Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

A. Internet content filter
B. Firewall
C. Proxy server
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 487
How often, at a MINIMUM, should Sara, an administrator, review the accesses and right of the users on her system?

A. Annually
B. Immediately after an employee is terminated
C. Every five years
D. Every time they patch the server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 488
An administrator is concerned that a company's web server has not been patched. Which of the following would be the BEST assessment for the administrator to perform?

A. Vulnerability scan
B. Risk assessment
C. Virus scan
D. Network sniffer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 489
An administrator notices that former temporary employees' accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

A. Implement a password expiration policy.
B. Implement an account expiration date for permanent employees.
C. Implement time of day restrictions for all temporary employees.
D. Run a last logon script to look for inactive accounts.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 490
A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

A. Logic bomb.
B. Backdoor.
C. Adware application.
D. Rootkit.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 491
Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 492
Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

A. RC4
B. 3DES
C. AES
D. MD5
E. PGP
F. Blowfish

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 493
Which of the following must be kept secret for a public key infrastructure to remain secure?

A. Certificate Authority

B. Certificate revocation list
C. Public key ring
D. Private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 494
Which of the following devices is BEST suited to protect an HTTP-based application that is susceptible to injection attacks?

A. Protocol filter
B. Load balancer
C. NIDS
D. Layer 7 firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 495
Which of the following is best practice to put at the end of an ACL?

A. Implicit deny
B. Time of day restrictions
C. Implicit allow
D. SNMP string

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 496
Which of the following security concepts can prevent a user from logging on from home during the weekends?

A. Time of day restrictions
B. Multifactor authentication
C. Implicit deny
D. Common access card

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 497
Which of the following would provide the STRONGEST encryption?

A. Random one-time pad
B. DES with a 56-bit key
C. AES with a 256-bit key
D. RSA with a 1024-bit key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 498
During a server audit, a security administrator does not notice abnormal activity. However, a network security analyst notices connections to unauthorized ports from outside the corporate network. Using specialized tools, the network security analyst also notices hidden processes running. Which of the following has MOST likely been installed on the server?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 499
A security administrator wants to ensure that the message the administrator sends out to their Chief Financial Officer (CFO) does not get changed in route. Which of the following is the administrator MOST concerned with?

A. Data confidentiality
B. High availability
C. Data integrity
D. Business continuity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 500
Which of the following can be performed when an element of the company policy cannot be enforced by technical means?

A. Develop a set of standards
B. Separation of duties
C. Develop a privacy policy
D. User training

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 501
Timestamps and sequence numbers act as countermeasures against which of the following types of attacks?

A. Smurf
B. DoS
C. Vishing
D. Replay

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 502
Which of the following would be used as a secure substitute for Telnet?

A. SSH
B. SFTP
C. SSL
D. HTTPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 503
Which of the following is described as an attack against an application using a malicious file?

A. Client side attack
B. Spam
C. Impersonation attack
D. Phishing attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 504
Which of the following assessment techniques would a security administrator implement to ensure that systems and software are developed properly?

A. Baseline reporting
B. Input validation
C. Determine attack surface
D. Design reviews

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 505
Which of the following would a security administrator implement in order to identify a problem between two applications that are not communicating properly?

A. Protocol analyzer
B. Baseline report
C. Risk assessment
D. Vulnerability scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 506
Which of the following would a security administrator implement in order to identify change from the standard configuration on a server?

A. Penetration test
B. Code review
C. Baseline review
D. Design review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 507
Which of the following tools would a security administrator use in order to identify all running services throughout an organization?

A. Architectural review
B. Penetration test
C. Port scanner
D. Design review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 508
Which of the following protocols provides transport security for virtual terminal emulation?

A. TLS

B. SSH
C. SCP
D. S/MIME

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 509
Based on information leaked to industry websites, business management is concerned that unauthorized employees are accessing critical project information for a major, well-known new product. To identify any such users, the security administrator could:

A. Set up a honeypot and place false project documentation on an unsecure share.
B. Block access to the project documentation using a firewall.
C. Increase antivirus coverage of the project servers.
D. Apply security updates and harden the OS on all project servers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 510
Which of the following is an indication of an ongoing current problem?

A. Alert
B. Trend
C. Alarm
D. Trap

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 511
Which of the following a programming interface that allows a remote computer to run programs on a local machine?

A. RPC
B. RSH
C. SSH
D. SSL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 512

Which of the following is the term for a fix for a known software problem?

A. Skiff
B. Patch
C. Slipstream
D. Upgrade

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 513
Connections using point-to-point protocol authenticate using which of the following? (Select TWO).

A. RIPEMD
B. PAP
C. CHAP
D. RC4
E. Kerberos

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 514
Which of the following will help prevent smurf attacks?

A. Allowing necessary UDP packets in and out of the network
B. Disabling directed broadcast on border routers
C. Disabling unused services on the gateway firewall
D. Flash the BIOS with the latest firmware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 515
An advantage of virtualizing servers, databases, and office applications is:

A. Centralized management.
B. Providing greater resources to users.
C. Stronger access control.
D. Decentralized management.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 516
A major security risk with co-mingling of hosts with different security requirements is:

A. Security policy violations.
B. Zombie attacks.
C. Password compromises.
D. Privilege creep.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 517
Which of the following attacks targets high level executives to gain company information?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 518
Which of the following can be used as an equipment theft deterrent?

A. Screen locks
B. GPS tracking
C. Cable locks
D. Whole disk encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 519
At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe?

A. Shoulder surfing
B. Tailgating
C. Whaling
D. Impersonation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 520
A company that has a mandatory vacation policy has implemented which of the following controls?

A. Risk control
B. Privacy control
C. Technical control
D. Physical control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 521
Which of the following is the MOST intrusive type of testing against a production system?

A. White box testing
B. War dialing
C. Vulnerability testing
D. Penetration testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 522
The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to correct this?

A. Disable the SSID broadcasting
B. Configure the access points so that MAC filtering is not used
C. Implement WEP encryption on the access points
D. Lower the power for office coverage only

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 523
Which of the following devices would be MOST useful to ensure availability when there are a large number of requests to a certain website?

A. Protocol analyzer
B. Load balancer
C. VPN concentrator
D. Web security gateway

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 524
Which of the following uses port 22 by default? (Select THREE).

A. SSH
B. SSL
C. TLS
D. SFTP
E. SCP
F. FTPS
G. SMTP
H. SNMP

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 525
Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of? (Select TWO).

A. Rootkit
B. Logic Bomb
C. Botnet
D. Backdoor
E. Spyware

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 526
The string:

` or 1=1-- -

Represents which of the following?

A. Bluejacking
B. Rogue access point
C. SQL Injection
D. Client-side attacks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 527
Joe, an administrator, installs a web server on the Internet that performs credit card transactions for customer payments. Joe also sets up a second web server that looks like the first web server. However, the second server contains fabricated files and folders made to look like payments were processed on this server but really were not. Which of the following is the second server?

A. DMZ
B. Honeynet
C. VLAN
D. Honeypot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 528
Which of the following can Joe, a security administrator, implement on his network to capture attack details that are occurring while also protecting his production network?

A. Security logs
B. Protocol analyzer
C. Audit logs
D. Honeypot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 529
Which of the following should Joe, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from his company?

A. Privacy Policy
B. Least Privilege
C. Acceptable Use
D. Mandatory Vacations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 530
Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

A. True negatives
B. True positives
C. False positives

D. False negatives

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is definite.

QUESTION 531
Joe, a security analyst, asks each employee of an organization to sign a statement saying that they understand how their activities may be monitored. Which of the following BEST describes this statement? (Select TWO).

A. Acceptable use policy
B. Risk acceptance policy
C. Privacy policy
D. Email policy
E. Security policy

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 532
A process in which the functionality of an application is tested without any knowledge of the internal mechanisms of the application is known as:

A. Black box testing
B. White box testing
C. Black hat testing
D. Gray box testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 533
Which of the following tools would allow Ann, the security administrator, to be able to BEST quantify all traffic on her network?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 534

Ann is starting a disaster recovery program. She has gathered specifics and team members for a meeting on site. Which of the following types of tests is this?

A. Structured walk through
B. Full Interruption test
C. Check list test
D. Table top exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 535
An internal auditing team would like to strengthen the password policy to support special characters. Which of the following types of password controls would achieve this goal?

A. Add reverse encryption
B. Password complexity
C. Increase password length
D. Allow single sign on

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 536
Ann, the software security engineer, works for a major software vendor. Which of the following practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release?

A. Product baseline report
B. Input validation
C. Patch regression testing
D. Code review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 537
Ann, a security analyst, is preparing for an upcoming security audit. To ensure that she identifies unapplied security controls and patches without attacking or compromising the system, Ann would use which of the following?

A. Vulnerability scanning
B. SQL injection
C. Penetration testing
D. Antivirus update

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 538
Ann, the security administrator, received a report from the security technician, that an unauthorized new user account was added to the server over two weeks ago. Which of the following could have mitigated this event?

A. Routine log audits
B. Job rotation
C. Risk likelihood assessment
D. Separation of duties

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 539
Which of the following ports should be opened on a firewall to allow for NetBIOS communication? (Select TWO).

A. 110
B. 137
C. 139
D. 143
E. 161
F. 443

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 540
Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?

A. Disable default SSID broadcasting.
B. Use WPA instead of WEP encryption.
C. Lower the access point's power settings.
D. Implement MAC filtering on the access point.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 541
After Ann, a user, logs into her banking websites she has access to her financial institution mortgage, credit card, and brokerage websites as well. Which of the following is being described?

A. Trusted OS
B. Mandatory access control
C. Separation of duties
D. Single sign-on

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 542
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 543
When an order was submitted via the corporate website, an administrator noted special characters (e.g., ";--" and "or 1=1 --") were input instead of the expected letters and numbers.

Which of the following is the MOST likely reason for the unusual results?

A. The user is attempting to highjack the web server session using an open-source browser.
B. The user has been compromised by a cross-site scripting attack (XSS) and is part of a botnet performing DDoS attacks.
C. The user is attempting to fuzz the web server by entering foreign language characters which are incompatible with the website.
D. The user is sending malicious SQL injection strings in order to extract sensitive company or customer data via the website.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 544
When a communications plan is developed for disaster recovery and business continuity plans, the MOST relevant items to include would be: (Select TWO).

A. Methods and templates to respond to press requests, institutional and regulatory reporting requirements.
B. Methods to exchange essential information to and from all response team members, employees, suppliers, and customers.
C. Developed recovery strategies, test plans, post-test evaluation and update processes.
D. Defined scenarios by type and scope of impact and dependencies, with quantification of loss potential.

E. Methods to review and report on system logs, incident response, and incident handling.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 545
Key elements of a business impact analysis should include which of the following tasks?

A. Develop recovery strategies, prioritize recovery, create test plans, post-test evaluation, and update processes.
B. Identify institutional and regulatory reporting requirements, develop response teams and communication trees, and develop press release templates.
C. Employ regular preventive measures such as patch management, change management, antivirus and vulnerability scans, and reports to management.
D. Identify critical assets systems and functions, identify dependencies, determine critical downtime limit, define scenarios by type and scope of impact, and quantify loss potential.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 546
End-user awareness training for handling sensitive personally identifiable information would include secure storage and transmission of customer:

A. Date of birth.
B. First and last name.
C. Phone number.
D. Employer name.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 547
Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

A. User rights reviews
B. Incident management
C. Risk based controls
D. Annual loss expectancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 548
The security officer is preparing a read-only USB stick with a document of important personal phone numbers, vendor contacts, an MD5 program, and other tools to provide to employees. At which of the following points in an incident should the officer instruct employees to use this information?

A. Business Impact Analysis
B. First Responder
C. Damage and Loss Control
D. Contingency Planning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 549
To ensure proper evidence collection, which of the following steps should be preformed FIRST?

A. Take hashes from the live system
B. Review logs
C. Capture the system image
D. Copy all compromised files

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 550
Joe, the security administrator, has determined that one of his web servers is under attack. Which of the following can help determine where the attack originated from?

A. Capture system image
B. Record time offset
C. Screenshots
D. Network sniffing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 551
Joe, the system administrator, is performing an overnight system refresh of hundreds of user computers. The refresh has a strict timeframe and must have zero downtime during business hours. Which of the following should Joe take into consideration?

A. A disk-based image of every computer as they are being replaced.
B. A plan that skips every other replaced computer to limit the area of affected users.
C. An offsite contingency server farm that can act as a warm site should any issues appear.
D. A back-out strategy planned out anticipating any unforeseen problems that may arise.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 552
A program displays:

ERROR: this program has caught an exception and will now terminate.

Which of the following is MOST likely accomplished by the program's behavior?

A. Operating system's integrity is maintained
B. Program's availability is maintained
C. Operating system's scalability is maintained
D. User's confidentiality is maintained

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 553
A security administrator wants to deploy a physical security control to limit an individual's access into a sensitive area. Which of the following should be implemented?

A. Guards
B. CCTV
C. Bollards
D. Spike strip

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 554
A network administrator uses an RFID card to enter the datacenter, a key to open the server rack, and a username and password to logon to a server. These are examples of which of the following?

A. Multifactor authentication
B. Single factor authentication
C. Separation of duties
D. Identification

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 555
Which of the following results in datacenters with failed humidity controls? (Select TWO).

A. Excessive EMI
B. Electrostatic charge
C. Improper ventilation
D. Condensation
E. Irregular temperature

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 556
An online store wants to protect user credentials and credit card information so that customers can store their credit card information and use their card for multiple separate transactions.

Which of the following database designs provides the BEST security for the online store?

A. Use encryption for the credential fields and hash the credit card field
B. Encrypt the username and hash the password
C. Hash the credential fields and use encryption for the credit card field
D. Hash both the credential fields and the credit card field

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 557
A security administrator is reviewing the below output from a password auditing tool:

P@ss.
@pW1.
S3cU4

Which of the following additional policies should be implemented based on the tool's output?

A. Password age
B. Password history
C. Password length
D. Password complexity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 558
Joe, a user, in a coffee shop is checking his email over a wireless network. An attacker records the temporary credentials being passed to Joe's browser. The attacker later uses the credentials to impersonate Joe and creates SPAM messages. Which of the following attacks allows for this impersonation?

A. XML injection
B. Directory traversal
C. Header manipulation
D. Session hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 559
A security architect wishes to implement a wireless network with connectivity to the company's internal network. Before they inform all employees that this network is being put in place, the architect wants to roll it out to a small test segment. Which of the following allows for greater secrecy about this network during this initial phase of implementation?

A. Disabling SSID broadcasting
B. Implementing WPA2 - TKIP
C. Implementing WPA2 - CCMP
D. Filtering test workstations by MAC address

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 560
Digital certificates can be used to ensure which of the following? (Select TWO).

A. Availability
B. Confidentiality
C. Verification
D. Authorization
E. Non-repudiation

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 561
A network administrator is looking for a way to automatically update company browsers so they import a list of root certificates from an online source. This online source will then be responsible for tracking which certificates are to be trusted or not trusted. Which of the following BEST describes the service that should be implemented to meet these requirements?

A. Trust model
B. Key escrow

C. OCSP
D. PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 562
A quality assurance analyst is reviewing a new software product for security, and has complete access to the code and data structures used by the developers. This is an example of which of the following types of testing?

A. Black box
B. Penetration
C. Gray box
D. White box

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 563
The security consultant is assigned to test a client's new software for security, after logs show targeted attacks from the Internet. To determine the weaknesses, the consultant has no access to the application program interfaces, code, or data structures. This is an example of which of the following types of testing?

A. Black box
B. Penetration
C. Gray box
D. White box

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 564
Which of the following types of cryptography should be used when minimal overhead is necessary for a mobile device?

A. Block cipher
B. Elliptical curve cryptography
C. Diffie-Hellman algorithm
D. Stream cipher

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 565
The server administrator has noted that most servers have a lot of free disk space and low memory utilization. Which of the following statements will be correct if the server administrator migrates to a virtual server environment?

A. The administrator will need to deploy load balancing and clustering.
B. The administrator may spend more on licensing but less on hardware and equipment.
C. The administrator will not be able to add a test virtual environment in the data center.
D. Servers will encounter latency and lowered throughput issues.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 566
Configuring key/value pairs on a RADIUS server is associated with deploying which of the following?

A. WPA2-Enterprise wireless network
B. DNS secondary zones
C. Digital certificates
D. Intrusion detection system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 567
A security analyst performs the following activities: monitors security logs, installs surveillance cameras and analyzes trend reports. Which of the following job responsibilities is the analyst performing? (Select TWO).

A. Detect security incidents
B. Reduce attack surface of systems
C. Implement monitoring controls
D. Hardening network devices
E. Prevent unauthorized access

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 568
A certificate used on an ecommerce web server is about to expire. Which of the following will occur if the certificate is allowed to expire?

A. The certificate will be added to the Certificate Revocation List (CRL).
B. Clients will be notified that the certificate is invalid.
C. The ecommerce site will not function until the certificate is renewed.
D. The ecommerce site will no longer use encryption.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 569
An administrator needs to segment internal traffic between layer 2 devices within the LAN. Which of the following types of network design elements would MOST likely be used?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 570
The security administrator needs to restrict traffic on a layer 3 device to support FTP from a new remote site. Which of the following secure network administration principles will need to be implemented?

A. Implicit deny
B. VLAN management
C. Port security
D. Access control lists

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 571
After a network outage, a PC technician is unable to ping various network devices. The network administrator verifies that those devices are working properly and can be accessed securely. Which of the following is the MOST likely reason the PC technician is unable to ping those devices?

A. ICMP is being blocked
B. SSH is not enabled
C. DNS settings are wrong
D. SNMP is not configured properly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 572
The security administrator has been tasked to update all the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections?

A. WEP
B. WPA2 CCMP
C. Disable SSID broadcast and increase power levels
D. MAC filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 573
After a recent security breach, the network administrator has been tasked to update and backup all router and switch configurations. The security administrator has been tasked to enforce stricter security policies. All users were forced to undergo additional user awareness training. All of these actions are due to which of the following types of risk mitigation strategies?

A. Change management
B. Implementing policies to prevent data loss
C. User rights and permissions review
D. Lessons learned

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 574
Various network outages have occurred recently due to unapproved changes to network and security devices. All changes were made using various system credentials. The security analyst has been tasked to update the security policy. Which of the following risk mitigation strategies would also need to be implemented to reduce the number of network outages due to unauthorized changes?

A. User rights and permissions review
B. Configuration management
C. Incident management
D. Implement security controls on Layer 3 devices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 575
A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered?

A. Symmetric encryption
B. Non-repudiation
C. Steganography
D. Hashing

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 576
Which of the following concepts describes the use of a one way transformation in order to validate the integrity of a program?

A. Hashing
B. Key escrow
C. Non-repudiation
D. Steganography

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 577
Recent data loss on financial servers due to security breaches forced the system administrator to harden their systems. Which of the following algorithms with transport encryption would be implemented to provide the MOST secure web connections to manage and access these servers?

A. SSL
B. TLS
C. HTTP
D. FTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 578
Which of the following provides a static record of all certificates that are no longer valid?

A. Private key
B. Recovery agent
C. CRLs
D. CA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 579
A company requires that a user's credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentication is being described?

A. Biometrics
B. Kerberos

C. Token
D. Two-factor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 580
A company wants to ensure that all credentials for various systems are saved within a central database so that users only have to login once for access to all systems. Which of the following would accomplish this?

A. Multi-factor authentication
B. Smart card access
C. Same Sign-On
D. Single Sign-On

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 581
Physical documents must be incinerated after a set retention period is reached. Which of the following attacks does this action remediate?

A. Shoulder Surfing
B. Dumpster Diving
C. Phishing
D. Impersonation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 582
All executive officers have changed their monitor location so it cannot be easily viewed when passing by their offices. Which of the following attacks does this action remediate?

A. Dumpster Diving
B. Impersonation
C. Shoulder Surfing
D. Whaling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 583
Which of the following protocols is vulnerable to man-in-the-middle attacks by NOT using end to end TLS

encryption?

A. HTTPS
B. WEP
C. WPA
D. WPA 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 584
A security administrator has been tasked with setting up a new internal wireless network that must use end to end TLS. Which of the following may be used to meet this objective?

A. WPA
B. HTTPS
C. WEP
D. WPA 2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 585
A server administrator notes that a legacy 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 describe?

A. Zero-day
B. Buffer overflow
C. Cross site scripting
D. Malicious add-on

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 586
Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?

A. Bollards
B. Video surveillance
C. Proximity readers
D. Fencing

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 587
After running into the data center with a vehicle, attackers were able to enter through the hole in the building and steal several key servers in the ensuing chaos. Which of the following security measures can be put in place to mitigate the issue from occurring in the future?

A. Fencing
B. Proximity readers
C. Video surveillance
D. Bollards

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 588
A CA is compromised and attacks start distributing maliciously signed software updates. Which of the following can be used to warn users about the malicious activity?

A. Key escrow
B. Private key verification
C. Public key verification
D. Certificate revocation list

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 589
After encrypting all laptop hard drives, an executive officer's laptop has trouble booting to the operating system. Now that it is successfully encrypted the helpdesk cannot retrieve the data.

Which of the following can be used to decrypt the information for retrieval?

A. Recovery agent
B. Private key
C. Trust models
D. Public key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 590
Which of the following devices is MOST likely being used when processing the following?

1 PERMIT IP ANY ANY EQ 80
2 DENY IP ANY ANY

A. Firewall
B. NIPS
C. Load balancer
D. URL filter

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 591
The security administrator at ABC company received the following log information from an external party:

10:45:01 EST, SRC 10.4.3.7:3056, DST 8.4.2.1:80, ALERT, Directory traversal
10:45:02 EST, SRC 10.4.3.7:3057, DST 8.4.2.1:80, ALERT, Account brute force
10:45:03 EST, SRC 10.4.3.7:3058, DST 8.4.2.1:80, ALERT, Port scan

The external party is reporting attacks coming from abc-company.com. Which of the following is the reason the ABC company's security administrator is unable to determine the origin of the attack?

A. A NIDS was used in place of a NIPS.
B. The log is not in UTC.
C. The external party uses a firewall.
D. ABC company uses PAT.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 592
The security administrator is implementing a malware storage system to archive all malware seen by the company into a central database. The malware must be categorized and stored based on similarities in the code. Which of the following should the security administrator use to identify similar malware?

A. TwoFish
B. SHA-512
C. Fuzzy hashes
D. HMAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 593
The security administrator installed a newly generated SSL certificate onto the company web server. Due to a mis-configuration of the website, a downloadable file containing one of the pieces of the key was available to the public. It was verified that the disclosure did not require a reissue of the certificate.
Which of the following was MOST likely compromised?

A. The file containing the recovery agent's keys.
B. The file containing the public key.
C. The file containing the private key.
D. The file containing the server's encrypted passwords.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 594
Which of the following was launched against a company based on the following IDS log?

122.41.15.252 - - [21/May/2012:00:17:20 +1200] "GET
/index.php?
username=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA HTTP/1.1"
200 2731 "http://www.company.com/cgibin/
forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar
4.4.7.0)"

A. SQL injection
B. Buffer overflow attack
C. XSS attack
D. Online password crack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 595
The security administrator is analyzing a user's history file on a Unix server to determine if the user was attempting to break out of a rootjail. Which of the following lines in the user's history log shows evidence that the user attempted to escape the rootjail?

A. cd ../../../../bin/bash
B. whoami
C. ls /root
D. sudo -u root

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 596
A software development company has hired a programmer to develop a plug-in module to an existing proprietary application. After completing the module, the developer needs to test the entire application to ensure that the module did not introduce new vulnerabilities. Which of the following is the developer performing when testing the application?

A. Black box testing
B. White box testing
C. Gray box testing

D. Design review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 597
A security administrator must implement all requirements in the following corporate policy: Passwords shall be protected against offline password brute force attacks. Passwords shall be protected against online password brute force attacks. Which of the following technical controls must be implemented to enforce the corporate policy? (Select THREE).

A. Account lockout
B. Account expiration
C. Screen locks
D. Password complexity
E. Minimum password lifetime
F. Minimum password length

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 598
Which of the following is a best practice for error and exception handling?

A. Log detailed exception but display generic error message
B. Display detailed exception but log generic error message
C. Log and display detailed error and exception messages
D. Do not log or display error or exception messages

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 599
A team of firewall administrators have access to a `master password list' containing service account passwords. Which of the following BEST protects the master password list?

A. File encryption
B. Password hashing
C. USB encryption
D. Full disk encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 600
An SSL/TLS private key is installed on a corporate web proxy in order to inspect HTTPS requests. Which of the following describes how this private key should be stored so that it is protected from theft?

A. Implement full disk encryption
B. Store on encrypted removable media
C. Utilize a hardware security module
D. Store on web proxy file system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 601
An insurance company requires an account recovery process so that information created by an employee can be accessed after that employee is no longer with the firm. Which of the following is the BEST approach to implement this process?

A. Employee is required to share their password with authorized staff prior to leaving the firm
B. Passwords are stored in a reversible form so that they can be recovered when needed
C. Authorized employees have the ability to reset passwords so that the data is accessible
D. All employee data is exported and imported by the employee prior to them leaving the firm

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 602
A small company has a website that provides online customer support. The company requires an account recovery process so that customers who forget their passwords can regain access.

Which of the following is the BEST approach to implement this process?

A. Replace passwords with hardware tokens which provide two-factor authentication to the online customer support site.
B. Require the customer to physically come into the company's main office so that the customer can be authenticated prior to their password being reset.
C. Web-based form that identifies customer by another mechanism and then emails the customer their forgotten password.
D. Web-based form that identifies customer by another mechanism, sets a temporary password and forces a password change upon first login.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 603
A new MPLS network link has been established between a company and its business partner.

The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link?

A. MPLS should be run in IPVPN mode.
B. SSL/TLS for all application flows.
C. IPSec VPN tunnels on top of the MPLS link.
D. HTTPS and SSH for all application flows.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 604
Which of the following authentication services should be replaced with a more secure alternative?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 605
A financial company requires a new private network link with a business partner to cater for realtime and batched data flows.

Which of the following activities should be performed by the IT security staff member prior to establishing the link?

A. Baseline reporting
B. Design review
C. Code review
D. SLA reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 606
Which device monitors network traffic in a passive manner?

A. Sniffer
B. IDS
C. Firewall
D. Web browser

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 607
What is a system that is intended or designed to be broken into by an attacker?

A. Honeypot
B. Honeybucket
C. Decoy
D. Spoofing system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 608
How must user accounts for exiting employees be handled?

A. Disabled, regardless of the circumstances
B. Disabled if the employee has been terminated
C. Deleted, regardless of the circumstances
D. Deleted if the employee has been terminated

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 609
Human Resources (HR) would like executives to undergo only two specific security training programs a year. Which of the following provides the BEST level of security training for the executives? (Select TWO).

A. Acceptable use of social media
B. Data handling and disposal
C. Zero day exploits and viruses
D. Phishing threats and attacks
E. Clean desk and BYOD
F. Information security awareness

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 610
Which of the following provides data the best fault tolerance at the LOWEST cost?

A. Load balancing
B. Clustering
C. Server virtualization
D. RAID 6

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 611
The librarian wants to secure the public Internet kiosk PCs at the back of the library. Which of the following would be the MOST appropriate? (Select TWO).

A. Device encryption
B. Antivirus
C. Privacy screen
D. Cable locks
E. Remote wipe

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 612
A system administrator wants to enable WPA2 CCMP. Which of the following is the only encryption used?

A. RC4
B. DES
C. 3DES
D. AES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 613
Two programmers write a new secure application for the human resources department to store personal identifiable information. The programmers make the application available to themselves using an uncommon port along with an ID and password only they know. This is an example of which of the following?

A. Root Kit
B. Spyware
C. Logic Bomb
D. Backdoor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 614
Everyone in the accounting department has the ability to print and sign checks. Internal audit has asked that only one group of employees may print checks while only two other employees may sign the checks. Which of the following concepts would enforce this process?

A. Separation of Duties
B. Mandatory Vacations
C. Discretionary Access Control
D. Job Rotation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 615
The security department has implemented a new laptop encryption product in the environment. The product requires one user name and password at the time of boot up and also another password after the operating system has finished loading. This setup is using which of the following authentication types?

A. Two-factor authentication
B. Single sign-on
C. Multifactor authentication
D. Single factor authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 616
The Human Resources department has a parent shared folder setup on the server. There are two groups that have access, one called managers and one called staff. There are many sub folders under the parent shared folder, one is called payroll. The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission. Which of the following is the quickest way to prevent the staff group from gaining access to the payroll folder?

A. Remove the staff group from the payroll folder
B. Implicit deny on the payroll folder for the staff group
C. Implicit deny on the payroll folder for the managers group
D. Remove inheritance from the payroll folder

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 617
The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank's certificates are still valid?

A. Bank's CRL
B. Bank's private key
C. Bank's key escrow
D. Bank's recovery agent

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 618
Which of the following are examples of network segmentation? (Select TWO).

A. IDS
B. IaaS
C. DMZ
D. Subnet
E. IPS

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 619
Which of the following provides the strongest authentication security on a wireless network?

A. MAC filter
B. WPA2
C. WEP
D. Disable SSID broadcast

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 620
Which of the following provides the BEST explanation regarding why an organization needs to implement IT security policies?

A. To ensure that false positives are identified
B. To ensure that staff conform to the policy
C. To reduce the organizational risk
D. To require acceptable usage of IT systems

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 621
An incident response team member needs to perform a forensics examination but does not have the required hardware. Which of the following will allow the team member to perform the examination with minimal impact to the potential evidence?

A. Using a software file recovery disc

B. Mounting the drive in read-only mode
C. Imaging based on order of volatility
D. Hashing the image after capture

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 622
Which of the following allows an organization to store a sensitive PKI component with a trusted third party?

A. Trust model
B. Public Key Infrastructure
C. Private key
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 623
Which of the following security devices can be replicated on a Linux based computer using IP tables to inspect and properly handle network based traffic?

A. Sniffer
B. Router
C. Firewall
D. Switch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 624
A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

A. Integrity of downloaded software.
B. Availability of the FTP site.
C. Confidentiality of downloaded software.
D. Integrity of the server logs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 625
An administrator has successfully implemented SSL on srv4.comptia.com using wildcard certificate

*.comptia.com, and now wishes to implement SSL on srv5.comptia.com. Which of the following files should be copied from srv4 to accomplish this?

A. certificate, private key, and intermediate certificate chain
B. certificate, intermediate certificate chain, and root certificate
C. certificate, root certificate, and certificate signing request
D. certificate, public key, and certificate signing request

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 626
When reviewing security logs, an administrator sees requests for the AAAA record of www.comptia.com. Which of the following BEST describes this type of record?

A. DNSSEC record
B. IPv4 DNS record
C. IPSEC DNS record
D. IPv6 DNS record

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 627
Which of the following practices reduces the management burden of access management?

A. Password complexity policies
B. User account audit
C. Log analysis and review
D. Group based privileges

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 628
Which of the following helps to apply the proper security controls to information?

A. Data classification
B. Deduplication
C. Clean desk policy
D. Encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 629
Which of the following describes purposefully injecting extra input during testing, possibly causing an application to crash?

A. Input validation
B. Exception handling
C. Application hardening
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 630
Which of the following types of security services are used to support authentication for remote users and devices?

A. Biometrics
B. HSM
C. RADIUS
D. TACACS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 631
A Chief Information Security Officer (CISO) is tasked with outsourcing the analysis of security logs. These will need to still be reviewed on a regular basis to ensure the security of the company has not been breached. Which of the following cloud service options would support this requirement?

A. SaaS
B. MaaS
C. IaaS
D. PaaS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 632
A security administrator needs a locally stored record to remove the certificates of a terminated employee. Which of the following describes a service that could meet these requirements?

A. OCSP
B. PKI
C. CA
D. CRL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 633
A security analyst informs the Chief Executive Officer (CEO) that a security breach has just occurred. This results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the CEO asks for further information. Which of the following strategies should be implemented to ensure the Risk Manager and CIO are not caught unaware in the future?

A. Procedure and policy management
B. Chain of custody management
C. Change management
D. Incident management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 634
Which of the following relies on the use of shared secrets to protect communication?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 635
A security administrator wants to test the reliability of an application which accepts user provided parameters. The administrator is concerned with data integrity and availability. Which of the following should be implemented to accomplish this task?

A. Secure coding
B. Fuzzing
C. Exception handling
D. Input validation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 636
Which of the following concepts is a term that directly relates to customer privacy considerations?

A. Data handling policies
B. Personally identifiable information
C. Information classification
D. Clean desk policies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 637
Which of the following is a Data Loss Prevention (DLP) strategy and is MOST useful for securing data in use?

A. Email scanning
B. Content discovery
C. Database fingerprinting
D. Endpoint protection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 638
Which of the following is a concern when encrypting wireless data with WEP?

A. WEP displays the plain text entire key when wireless packet captures are reassembled
B. WEP implements weak initialization vectors for key transmission
C. WEP uses a very weak encryption algorithm
D. WEP allows for only four pre-shared keys to be configured

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 639
A security administrator is tasked with calculating the total ALE on servers. In a two year period of time, a company has to replace five servers. Each server replacement has cost the company $4,000 with downtime costing $3,000. Which of the following is the ALE for the company?

A. $7,000
B. $10,000
C. $17,500
D. $35,000

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 640
ABC company has a lot of contractors working for them. The provisioning team does not always get notified that a contractor has left the company. Which of the following policies would prevent contractors from having access to systems in the event a contractor has left?

A. Annual account review
B. Account expiration policy
C. Account lockout policy
D. Account disablement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 641
The practice of marking open wireless access points is called which of the following?

A. War dialing
B. War chalking
C. War driving
D. Evil twin

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 642
Multi-tenancy is a concept found in which of the following?

A. Full disk encryption
B. Removable media
C. Cloud computing
D. Data loss prevention

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 643
Which of the following is a common coding error in which boundary checking is not performed?

A. Input validation
B. Fuzzing
C. Secure coding
D. Cross-site scripting

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 644
While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are:

A. no longer used to authenticate to most wireless networks.
B. contained in certain wireless packets in plaintext.
C. contained in all wireless broadcast packets by default.
D. no longer supported in 802.11 protocols.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 645
One of the most consistently reported software security vulnerabilities that leads to major exploits is:

A. Lack of malware detection.
B. Attack surface decrease.
C. Inadequate network hardening.
D. Poor input validation.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 646
Public key certificates and keys that are compromised or were issued fraudulently are listed on which of the following?

A. PKI
B. ACL
C. CA
D. CRL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 647
One of the most basic ways to protect the confidentiality of data on a laptop in the event the device is physically stolen is to implement which of the following?

A. File level encryption with alphanumeric passwords
B. Biometric authentication and cloud storage
C. Whole disk encryption with two-factor authentication

D. BIOS passwords and two-factor authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 648
Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them?

A. Whole disk encryption
B. SSH
C. Telnet
D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 649
A malicious user is sniffing a busy encrypted wireless network waiting for an authorized client to connect to it. Only after an authorized client has connected and the hacker was able to capture the client handshake with the AP can the hacker begin a brute force attack to discover the encryption key. Which of the following attacks is taking place?

A. IV attack
B. WEP cracking
C. WPA cracking
D. Rogue AP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 650
Which of the following protocols is used by IPv6 for MAC address resolution?

A. NDP
B. ARP
C. DNS
D. NCP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 651
Which of the following provides dedicated hardware-based cryptographic functions to an operating system

and its applications running on laptops and desktops?

A. TPM
B. HSM
C. CPU
D. FPU

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 652
Which of the following tests a number of security controls in the least invasive manner?

A. Vulnerability scan
B. Threat assessment
C. Penetration test
D. Ping sweep

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 653
When using PGP, which of the following should the end user protect from compromise? (Select TWO).

A. Private key
B. CRL details
C. Public key
D. Key password
E. Key escrow
F. Recovery agent

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 654
Which of the following disaster recovery strategies has the highest cost and shortest recovery time?

A. Warm site
B. Hot site
C. Cold site
D. Co-location site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

http://www.gratisexam.com/

QUESTION 655
In the case of a major outage or business interruption, the security office has documented the expected loss of earnings, potential fines and potential consequence to customer service. Which of the following would include the MOST detail on these objectives?

A. Business Impact Analysis
B. IT Contingency Plan
C. Disaster Recovery Plan
D. Continuity of Operations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 656
After visiting a website, a user receives an email thanking them for a purchase which they did not request. Upon investigation the security administrator sees the following source code in a pop-up window:

<HTML>
<body onload="document.getElementByID('badForm').submit()"> <form id="badForm" action="shoppingsite.company.com/purchase.php" method="post" <input name="Perform Purchase" value="Perform Purchase" /> </form></body></HTML>

Which of the following has MOST likely occurred?

A. SQL injection
B. Cookie stealing
C. XSRF
D. XSS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 657
Which of the following ports should be used by a system administrator to securely manage a remote server?

A. 22
B. 69
C. 137
D. 445

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 658
Which of the following ports is used to securely transfer files between remote UNIX systems?

A. 21
B. 22
C. 69
D. 445

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 659
Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter?

A. Increased availability of network services due to higher throughput
B. Longer MTBF of hardware due to lower operating temperatures
C. Higher data integrity due to more efficient SSD cooling
D. Longer UPS run time due to increased airflow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 660
Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications under which of the following conditions?

A. Unexpected input
B. Invalid output
C. Parameterized input
D. Valid output

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 661
Which of the following types of wireless attacks would be used specifically to impersonate another WAP in order to gain unauthorized information from mobile users?

A. IV attack
B. Evil twin
C. War driving

D. Rogue access point

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 662
Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?

A. Zero-day
B. LDAP injection
C. XML injection
D. Directory traversal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 663
Which of the following is built into the hardware of most laptops but is not setup for centralized management by default?

A. Whole disk encryption
B. TPM encryption
C. USB encryption
D. Individual file encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 664
Which of the following is true about the recovery agent?

A. It can decrypt messages of users who lost their private key.
B. It can recover both the private and public key of federated users.
C. It can recover and provide users with their lost or private key.
D. It can recover and provide users with their lost public key.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 665
Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages?

A. Risk transference
B. Change management
C. Configuration management
D. Access control revalidation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 666
A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose?

A. ACL
B. IDS
C. UTM
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 667
Which of the following would the security engineer set as the subnet mask for the servers below to utilize host addresses on separate broadcast domains?

Server 1: 192.168.100.6
Server 2: 192.168.100.9
Server 3: 192.169.100.20

A. /24
B. /27
C. /28
D. /29
E. /30

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 668
Which of the following offerings typically allows the customer to apply operating system patches?

A. Software as a service
B. Public Clouds
C. Cloud Based Storage
D. Infrastructure as a service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 669
A technician is unable to manage a remote server. Which of the following ports should be opened on the firewall for remote server management? (Select TWO).

A. 22
B. 135
C. 137
D. 143
E. 443
F. 3389

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 670
When designing a new network infrastructure, a security administrator requests that the intranet web server be placed in an isolated area of the network for security purposes. Which of the following design elements would be implemented to comply with the security administrator's request?

A. DMZ
B. Cloud services
C. Virtualization
D. Sandboxing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 671
At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

A. Configure an access list.
B. Configure spanning tree protocol.
C. Configure port security.
D. Configure loop protection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 672
Users report that they are unable to access network printing services. The security technician checks the

router access list and sees that web, email, and secure shell are allowed. Which of the following is blocking network printing?

A. Port security
B. Flood guards
C. Loop protection
D. Implicit deny

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 673
Joe, a security administrator, believes that a network breach has occurred in the datacenter as a result of a misconfigured router access list, allowing outside access to an SSH server. Which of the following should Joe search for in the log files?

A. Failed authentication attempts
B. Network ping sweeps
C. Host port scans
D. Connections to port 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 674
Which of the following firewall types inspects Ethernet traffic at the MOST levels of the OSI model?

A. Packet Filter Firewall
B. Stateful Firewall
C. Proxy Firewall
D. Application Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 675
A security analyst needs to logon to the console to perform maintenance on a remote server. Which of the following protocols would provide secure access?

A. SCP
B. SSH
C. SFTP
D. HTTPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 676
Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group. Which of the following would prevent her from denying accountability?

A. Email Encryption
B. Steganography
C. Non Repudiation
D. Access Control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 677
Ann, a technician, is attempting to establish a remote terminal session to an end user's computer using Kerberos authentication, but she cannot connect to the destination machine. Which of the following default ports should Ann ensure is open?

A. 22
B. 139
C. 443
D. 3389

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 678
Concurrent use of a firewall, content filtering, antivirus software and an IDS system would be considered components of:

A. Redundant systems.
B. Separation of duties.
C. Layered security.
D. Application control.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 679
Which of the following is a security risk regarding the use of public P2P as a method of collaboration?

A. Data integrity is susceptible to being compromised.
B. Monitoring data changes induces a higher cost.
C. Users are not responsible for data usage tracking.

D. Limiting the amount of necessary space for data storage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 680
The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

A. Security awareness training.
B. BYOD security training.
C. Role-based security training.
D. Legal compliance training.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 681
After an audit, it was discovered that the security group memberships were not properly adjusted for employees' accounts when they moved from one role to another. Which of the following has the organization failed to properly implement? (Select TWO).

A. Mandatory access control enforcement.
B. User rights and permission reviews.
C. Technical controls over account management.
D. Account termination procedures.
E. Management controls over account management.
F. Incident management and response plan.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 682
A security technician wishes to gather and analyze all Web traffic during a particular time period.

Which of the following represents the BEST approach to gathering the required data?

A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443.
B. Configure a proxy server to log all traffic destined for ports 80 and 443.
C. Configure a switch to log all traffic destined for ports 80 and 443.
D. Configure a NIDS to log all traffic destined for ports 80 and 443.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 683
A security administrator suspects that an increase in the amount of TFTP traffic on the network is due to unauthorized file transfers, and wants to configure a firewall to block all TFTP traffic.

Which of the following would accomplish this task?

A. Deny TCP port 68
B. Deny TCP port 69
C. Deny UDP port 68
D. Deny UCP port 69

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 684
The network security engineer just deployed an IDS on the network, but the Chief Technical Officer (CTO) has concerns that the device is only able to detect known anomalies. Which of the following types of IDS has been deployed?

A. Signature Based IDS
B. Heuristic IDS
C. Behavior Based IDS
D. Anomaly Based IDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 685
Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems?

A. Acceptable Use Policy
B. Privacy Policy
C. Security Policy
D. Human Resource Policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 686
The Chief Technical Officer (CTO) has tasked The Computer Emergency Response Team (CERT) to develop and update all Internal Operating Procedures and Standard Operating Procedures documentation in order to successfully respond to future incidents. Which of the following stages of the Incident Handling process is the team working on?

A. Lessons Learned
B. Eradication
C. Recovery
D. Preparation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 687
Company XYZ recently salvaged company laptops and removed all hard drives, but the Chief Information Officer (CIO) is concerned about disclosure of confidential information. Which of the following is the MOST secure method to dispose of these hard drives?

A. Degaussing
B. Physical Destruction
C. Lock up hard drives in a secure safe
D. Wipe

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 688
A company has recently implemented a high density wireless system by having a junior technician install two new access points for every access point already deployed. Users are now reporting random wireless disconnections and slow network connectivity. Which of the following is the MOST likely cause?

A. The old APs use 802.11a
B. Users did not enter the MAC of the new APs
C. The new APs use MIMO
D. A site survey was not conducted

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 689
A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless network after entering the correct network information. Which of the following is the MOST likely reason for this issue?

A. The SSID broadcast is disabled.
B. The company is using the wrong antenna type.
C. The MAC filtering is disabled on the access point.
D. The company is not using strong enough encryption.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 690
A company is looking to reduce the likelihood of employees in the finance department being involved with money laundering. Which of the following controls would BEST mitigate this risk?

A. Implement privacy policies
B. Enforce mandatory vacations
C. Implement a security policy
D. Enforce time of day restrictions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 691
A company recently experienced data loss when a server crashed due to a midday power outage. Which of the following should be used to prevent this from occurring again?

A. Recovery procedures
B. EMI shielding
C. Environmental monitoring
D. Redundancy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 692
Joe, a security administrator, is concerned with users tailgating into the restricted areas. Given a limited budget, which of the following would BEST assist Joe with detecting this activity?

A. Place a full-time guard at the entrance to confirm user identity.
B. Install a camera and DVR at the entrance to monitor access.
C. Revoke all proximity badge access to make users justify access.
D. Install a motion detector near the entrance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 693
It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission. They are concerned about which of the following types of security control?

A. Integrity
B. Safety
C. Availability

D. Confidentiality

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 694
A security manager requires fencing around the perimeter, and cipher locks on all entrances. The manager is concerned with which of the following security controls?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 695
A security engineer is reviewing log data and sees the output below:

POST: /payload.php HTTP/1.1
HOST: localhost
Accept: */*
Referrer: http://localhost/
****
HTTP/1.1 403 Forbidden
Connection: close

Log: Access denied with 403. Pattern matches form bypass Which of the following technologies was MOST likely being used to generate this log?

A. Host-based Intrusion Detection System
B. Web application firewall
C. Network-based Intrusion Detection System
D. Stateful Inspection Firewall
E. URL Content Filter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 696
A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

A. Antenna placement
B. Interference
C. Use WEP

D. Single Sign on
E. Disable the SSID
F. Power levels

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 697
An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to integrate the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

A. Unified Threat Management
B. Virtual Private Network
C. Single sign on
D. Role-based management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 698
A company's legacy server requires administration using Telnet. Which of the following protocols could be used to secure communication by offering encryption at a lower OSI layer? (Select TWO).

A. IPv6
B. SFTP
C. IPSec
D. SSH
E. IPv4

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 699
Joe, the Chief Technical Officer (CTO), is concerned about new malware being introduced into the corporate network. He has tasked the security engineers to implement a technology that is capable of alerting the team when unusual traffic is on the network. Which of the following types of technologies will BEST address this scenario?

A. Application Firewall
B. Anomaly Based IDS
C. Proxy Firewall
D. Signature IDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 700
Which of the following describes the purpose of an MOU?

A. Define interoperability requirements
B. Define data backup process
C. Define onboard/offboard procedure
D. Define responsibilities of each party

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 701
The security manager received a report that an employee was involved in illegal activity and has saved data to a workstation's hard drive. During the investigation, local law enforcement's criminal division confiscates the hard drive as evidence. Which of the following forensic procedures is involved?

A. Chain of custody
B. System image
C. Take hashes
D. Order of volatility

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 702
Environmental control measures include which of the following?

A. Access list
B. Lighting
C. Motion detection
D. EMI shielding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 703
Which of the following is the BEST concept to maintain required but non-critical server availability?

A. SaaS site
B. Cold site
C. Hot site
D. Warm site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 704
Prior to leaving for an extended vacation, Joe uses his mobile phone to take a picture of his family in the house living room. Joe posts the picture on a popular social media site together with the message: "Heading to our two weeks vacation to Italy." Upon returning home, Joe discovers that the house was burglarized. Which of the following is the MOST likely reason the house was burglarized if nobody knew Joe's home address?

A. Joe has enabled the device access control feature on his mobile phone.
B. Joe's home address can be easily found using the TRACEROUTE command.
C. The picture uploaded to the social media site was geo-tagged by the mobile phone.
D. The message posted on the social media site informs everyone the house will be empty.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 705
Which of the following technical controls helps to prevent Smartphones from connecting to a corporate network?

A. Application white listing
B. Remote wiping
C. Acceptable use policy
D. Mobile device management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 706
Which of the following would prevent a user from installing a program on a company-owned mobile device?

A. White-listing
B. Access control lists
C. Geotagging
D. Remote wipe

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 707
Which of the following can be used to maintain a higher level of security in a SAN by allowing isolation of mis-configurations or faults?

A. VLAN
B. Protocol security
C. Port security
D. VSAN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 708
The act of magnetically erasing all of the data on a disk is known as:

A. Wiping
B. Dissolution
C. Scrubbing
D. Degaussing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 709
Joe, a network security engineer, has visibility to network traffic through network monitoring tools.

However, he's concerned that a disgruntled employee may be targeting a server containing the company's financial records. Which of the following security mechanism would be MOST appropriate to confirm Joe's suspicion?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 710
Joe, a technician at the local power plant, notices that several turbines had ramp up in cycles during the week. Further investigation by the system engineering team determined that a timed .exe file had been uploaded to the system control console during a visit by international contractors. Which of the following actions should Joe recommend?

A. Create a VLAN for the SCADA
B. Enable PKI for the MainFrame
C. Implement patch management
D. Implement stronger WPA2 Wireless

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 711
A system administrator has been instructed by the head of security to protect their data at-rest. Which of the following would provide the strongest protection?

A. Prohibiting removable media
B. Incorporating a full-disk encryption system
C. Biometric controls on data center entry points
D. A host-based intrusion detection system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 712
An Information Systems Security Officer (ISSO) has been placed in charge of a classified peer-topeer network that cannot connect to the Internet. The ISSO can update the antivirus definitions manually, but which of the following steps is MOST important?

A. A full scan must be run on the network after the DAT file is installed.
B. The signatures must have a hash value equal to what is displayed on the vendor site.
C. The definition file must be updated within seven days.
D. All users must be logged off of the network prior to the installation of the definition file.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 713
Ann has taken over as the new head of the IT department. One of her first assignments was to implement AAA in preparation for the company's new telecommuting policy. When she takes inventory of the organizations existing network infrastructure, she makes note that it is a mix of several different vendors. Ann knows she needs a method of secure centralized access to the company's network resources. Which of the following is the BEST service for Ann to implement?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 714
A group policy requires users in an organization to use strong passwords that must be changed every 15

days. Joe and Ann were hired 16 days ago. When Joe logs into the network, he is prompted to change his password; when Ann logs into the network, she is not prompted to change her password. Which of the following BEST explains why Ann is not required to change her password?

A. Ann's user account has administrator privileges.
B. Joe's user account was not added to the group policy.
C. Ann's user account was not added to the group policy.
D. Joe's user account was inadvertently disabled and must be re-created.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 715
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 716
Several employee accounts appear to have been cracked by an attacker. Which of the following should the security administrator implement to mitigate password cracking attacks? (Select TWO).

A. Increase password complexity
B. Deploy an IDS to capture suspicious logins
C. Implement password history
D. Implement monitoring of logins
E. Implement password expiration
F. Increase password length

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 717
A cafe provides laptops for Internet access to their customers. The cafe is located in the center corridor of a busy shopping mall. The company has experienced several laptop thefts from the cafe during peek shopping hours of the day. Corporate has asked that the IT department provide a solution to eliminate laptop theft. Which of the following would provide the IT department wit the BEST solution?

A. Attach cable locks to each laptop
B. Require each customer to sign an AUP

C. Install a GPS tracking device onto each laptop

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 718
A company hired Joe, an accountant. The IT administrator will need to create a new account for Joe. The company uses groups for ease of management and administration of user accounts. Joe will need network access to all directories, folders and files within the accounting department.

Which of the following configurations will meet the requirements?

A. Create a user account and assign the user account to the accounting group.
B. Create an account with role-based access control for accounting.
C. Create a user account with password reset and notify Joe of the account creation.
D. Create two accounts: a user account and an account with full network administration rights.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 719
Ann, the network administrator, has learned from the helpdesk that employees are accessing the wireless network without entering their domain credentials upon connection. Once the connection is made, they cannot reach any internal resources, while wired network connections operate smoothly.
Which of the following is MOST likely occurring?

A. A user has plugged in a personal access point at their desk to connect to the network wirelessly.
B. The company is currently experiencing an attack on their internal DNS servers.
C. The company's WEP encryption has been compromised and WPA2 needs to be implemented instead.
D. An attacker has installed an access point nearby in an attempt to capture company information.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 720
Ann works at a small company and she is concerned that there is no oversight in the finance department; specifically, that Joe writes, signs and distributes paychecks, as well as other expenditures. Which of the following controls can she implement to address this concern?

A. Mandatory vacations
B. Time of day restrictions
C. Least privilege
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 721
A hospital IT department wanted to secure its doctor's tablets. The IT department wants operating system level security and the ability to secure the data from alteration. Which of the following methods would MOST likely work?

A. Cloud storage
B. Removal Media
C. TPM
D. Wiping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 722
Which of the following common access control models is commonly used on systems to ensure a "need to know" based on classification levels?

A. Role Based Access Controls
B. Mandatory Access Controls
C. Discretionary Access Controls
D. Access Control List

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 723
A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?

A. Install a registration server.
B. Generate shared public and private keys.
C. Install a CA
D. Establish a key escrow policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 724
A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site
B. Block port 23 on the network firewall
C. Block port 25 on the L2 switch at each remote site

D. Block port 25 on the network firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 725
Pete, a security administrator, is informed that people from the HR department should not have access to the accounting department's server, and the accounting department should not have access to the HR department's server. The network is separated by switches. Which of the following is designed to keep the HR department users from accessing the accounting department's server and vice-versa?

A. ACLs
B. VLANs
C. DMZs
D. NATS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 726
Which of the following is BEST utilized to actively test security controls on a particular system?

A. Port scanning
B. Penetration test
C. Vulnerability scanning
D. Grey/Gray box

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 727
Which of the following has serious security implications for large organizations and can potentially allow an attacker to capture conversations?

A. Subnetting
B. NAT
C. Jabber
D. DMZ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 728
Upper management decides which risk to mitigate based on cost. This is an example of:

A. Qualitative risk assessment
B. Business impact analysis
C. Risk management framework
D. Quantitative risk assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 729
Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 730
Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

A. AES
B. Blowfish
C. RC5
D. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 731
Which of the following best practices makes a wireless network more difficult to find?

A. Implement MAC filtering
B. UseWPA2-PSK
C. Disable SSD broadcast
D. Power down unused WAPs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 732
The use of social networking sites introduces the risk of:

A. Disclosure of proprietary information
B. Data classification issues
C. Data availability issues
D. Broken chain of custody

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 733
Which the following flags are used to establish a TCP connection? (Select TWO).

A. PSH
B. ACK
C. SYN
D. URG
E. FIN

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 734
Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

A. Error and exception handling
B. Application hardening
C. Application patch management
D. Cross-site script prevention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 735
Which of the following MUST Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret?

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 736
Visitors entering a building are required to close the back door before the front door of the same entry room is open. Which of the following is being described?

A. Tailgating
B. Fencing
C. Screening
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 737
Which of the following software allows a network administrator to inspect the protocol header in order to troubleshoot network issues?

A. URL filter
B. Spam filter
C. Packet sniffer
D. Switch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 738
Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

A. 21
B. 25
C. 80
D. 3389

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 739
Which of the following would Pete, a security administrator, do to limit a wireless signal from penetrating the exterior walls?

A. Implement TKIP encryption
B. Consider antenna placement
C. Disable the SSID broadcast

D. Disable WPA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 740
Which of the following is where an unauthorized device is found allowing access to a network?

A. Bluesnarfing
B. Rogue access point
C. Honeypot
D. IV attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 741
Which of the following attacks allows access to contact lists on cellular phones?

A. War chalking
B. Blue jacking
C. Packet sniffing
D. Bluesnarfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 742
Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

A. Hashing
B. Transport encryption
C. Digital signatures
D. Steganography

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 743
Which of the following identifies certificates that have been compromised or suspected of being compromised?

A. Certificate revocation list

B. Access control list
C. Key escrow registry
D. Certificate authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 744
Which of the following BEST allows Pete, a security administrator, to determine the type, source, and flags of the packet traversing a network for troubleshooting purposes?

A. Switches
B. Protocol analyzers
C. Routers
D. Web security gateways

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 745
Which of the following is the MOST important step for preserving evidence during forensic procedures?

A. Involve law enforcement
B. Chain of custody
C. Record the time of the incident
D. Report within one hour of discovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 746
Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end- users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

A. SQL Injection
B. Theft of the physical database server
C. Cookies
D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 747
The fundamental information security principals include confidentiality, availability and which of the following?

A. The ability to secure data against unauthorized disclosure to external sources
B. The capacity of a system to resist unauthorized changes to stored information
C. The confidence with which a system can attest to the identity of a user
D. The characteristic of a system to provide uninterrupted service to authorized users

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 748
Which of the following is the MOST likely cause of users being unable to verify a single user's email signature and that user being unable to decrypt sent messages?

A. Unmatched key pairs
B. Corrupt key escrow
C. Weak public key
D. Weak private key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 749
Full disk encryption is MOST effective against which of the following threats?

A. Denial of service by data destruction
B. Eavesdropping emanations
C. Malicious code
D. Theft of hardware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 750
Which of the following may cause Jane, the security administrator, to seek an ACL work around?

A. Zero day exploit
B. Dumpster diving
C. Virus outbreak
D. Tailgating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 751
In order to use a two-way trust model the security administrator MUST implement which of the following?

A. DAC
B. PKI
C. HTTPS
D. TPM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 752
Which of the following would a security administrator use to verify the integrity of a file?

A. Time stamp
B. MAC times
C. File descriptor
D. Hash

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 753
Which of the following is a best practice when securing a switch from physical access?

A. Disable unnecessary accounts
B. Print baseline configuration
C. Enable access lists
D. Disable unused ports

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 754
A security administrator needs to image a large hard drive for forensic analysis. Which of the following will allow for faster imaging to a second hard drive?

A. cp /dev/sda /dev/sdb bs=8k
B. tail -f /dev/sda > /dev/sdb bs=8k
C. dd in=/dev/sda out=/dev/sdb bs=4k
D. locate /dev/sda /dev/sdb bs=4k

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 755
Sara, an employee, tethers her smartphone to her work PC to bypass the corporate web security gateway while connected to the LAN. While Sara is out at lunch her PC is compromised via the tethered connection and corporate data is stolen. Which of the following would BEST prevent this from occurring again?

A. Disable the wireless access and implement strict router ACLs.
B. Reduce restrictions on the corporate web security gateway.
C. Security policy and threat awareness training.
D. Perform user rights and permissions reviews.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 756
Which of the following can be implemented if a security administrator wants only certain devices connecting to the wireless network?

A. Disable SSID broadcast
B. Install a RADIUS server
C. Enable MAC filtering
D. Lowering power levels on the AP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 757
Which of the following malware types typically allows an attacker to monitor a user's computer, is characterized by a drive-by download, and requires no user interaction?

A. Virus
B. Logic bomb
C. Spyware
D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 758
Which of the following malware types may require user interaction, does not hide itself, and is commonly identified by marketing pop-ups based on browsing habits?

A. Botnet
B. Rootkit

C. Adware
D. Virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 759
Which of the following is characterized by an attack against a mobile device?

A. Evil twin
B. Header manipulation
C. Blue jacking
D. Rogue AP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 760
Which of the following application attacks is used against a corporate directory service where there are unknown servers on the network?

A. Rogue access point
B. Zero day attack
C. Packet sniffing
D. LDAP injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 761
Which of the following protocols allows for the LARGEST address space?

A. IPX
B. IPv4
C. IPv6
D. Appletalk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 762
Who should be contacted FIRST in the event of a security breach?

A. Forensics analysis team

B. Internal auditors
C. Incident response team
D. Software vendors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 763
A security administrator examines a network session to a compromised database server with a packet analyzer. Within the session there is a repeated series of the hex character 90 (x90).

Which of the following attack types has occurred?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 764
Which of the following is an example of a false negative?

A. The IDS does not identify a buffer overflow.
B. Anti-virus identifies a benign application as malware.
C. Anti-virus protection interferes with the normal operation of an application.
D. A user account is locked out after the user mistypes the password too many times.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 765
Which of the following access controls enforces permissions based on data labeling at specific levels?

A. Mandatory access control
B. Separation of duties access control
C. Discretionary access control
D. Role based access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 766

Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 767
Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses?

A. Penetration test
B. Code review
C. Vulnerability scan
D. Brute Force scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 768
Which of the following authentication services uses a ticket granting system to provide access?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 769
Matt, a security administrator, wants to configure all the switches and routers in the network in order to securely monitor their status. Which of the following protocols would he need to configure on each device?

A. SMTP
B. SNMPv3
C. IPSec
D. SNMP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 770
Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

A. Disable the wired ports
B. Use channels 1, 4 and 7 only
C. Enable MAC filtering
D. Disable SSID broadcast
E. Switch from 802.11a to 802.11b

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 771
The public key is used to perform which of the following? (Select THREE).

A. Validate the CRL
B. Validate the identity of an email sender
C. Encrypt messages
D. Perform key recovery
E. Decrypt messages
F. Perform key escrow

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 772
Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks?

A. NAT
B. Virtualization
C. NAC
D. Subnetting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 773
Which of the following would BEST be used to calculate the expected loss of an event, if the likelihood of an event occurring is known? (Select TWO).

A. DAC

B. ALE
C. SLE
D. ARO
E. ROI

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 774
An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame.

Which of the following strategies would the administrator MOST likely implement?

A. Full backups on the weekend and incremental during the week
B. Full backups on the weekend and full backups every day
C. Incremental backups on the weekend and differential backups every day
D. Differential backups on the weekend and full backups every day

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 775
Which of the following can be utilized in order to provide temporary IT support during a disaster, where the organization sets aside funds for contingencies, but does not necessarily have a dedicated site to restore those services?

A. Hot site
B. Warm site
C. Cold site
D. Mobile site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 776
Which of the following is BEST utilized to identify common misconfigurations throughout the enterprise?

A. Vulnerability scanning
B. Port scanning
C. Penetration testing
D. Black box

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 777
Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

A. CCTV system access
B. Dial-up access
C. Changing environmental controls
D. Ping of death

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 778
Which of the following policies is implemented in order to minimize data loss or theft?

A. PII handling
B. Password policy
C. Chain of custody
D. Zero day exploits

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 779
Which of the following provides the HIGHEST level of confidentiality on a wireless network?

A. Disabling SSID broadcast
B. MAC filtering
C. WPA2
D. Packet switching

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 780
A security administrator is aware that a portion of the company's Internet-facing network tends to be non-secure due to poorly configured and patched systems. The business owner has accepted the risk of those systems being compromised, but the administrator wants to determine the degree to which those systems can be used to gain access to the company intranet. Which of the following should the administrator perform?

A. Patch management assessment
B. Business impact assessment
C. Penetration test

D. Vulnerability assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 781
Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

A. Single sign on
B. IPv6
C. Secure zone transfers
D. VoIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 782
Sara, the Chief Information Officer (CIO), has requested an audit take place to determine what services and operating systems are running on the corporate network. Which of the following should be used to complete this task?

A. Fingerprinting and password crackers
B. Fuzzing and a port scan
C. Vulnerability scan and fuzzing
D. Port scan and fingerprinting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 783
Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential type authentication method BEST fits these requirements?

A. EAP-TLS
B. EAP-FAST
C. PEAP-CHAP
D. PEAP-MSCHAPv2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 784
Matt, the Chief Information Security Officer (CISO), tells the network administrator that a security company has been hired to perform a penetration test against his network. The security company asks Matt which type of testing would be most beneficial for him. Which of the following BEST describes what the security company might do during a black box test?

A. The security company is provided with all network ranges, security devices in place, and logical maps of the network.
B. The security company is provided with no information about the corporate network or physical locations.
C. The security company is provided with limited information on the network, including all network diagrams.
D. The security company is provided with limited information on the network, including some subnet ranges and logical network diagrams.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 785
Corporate IM presents multiple concerns to enterprise IT. Which of the following concerns should Jane, the IT security manager, ensure are under control? (Select THREE).

A. Authentication
B. Data leakage
C. Compliance
D. Malware
E. Non-repudiation
F. Network loading

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 786
Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Select TWO).

A. Spoofing
B. Man-in-the-middle
C. Dictionary
D. Brute force
E. Privilege escalation

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 787
Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee's credential?

A. Account expiration
B. Password complexity
C. Account lockout
D. Dual factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 788
Pete, the Chief Executive Officer (CEO) of a company, has increased his travel plans for the next two years to improve business relations. Which of the following would need to be in place in case something happens to Pete?

A. Succession planning
B. Disaster recovery
C. Separation of duty
D. Removing single loss expectancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 789
In order to prevent and detect fraud, which of the following should be implemented?

A. Job rotation
B. Risk analysis
C. Incident management
D. Employee evaluations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 790
An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

A. it is being caused by the presence of a rogue access point.
B. it is the beginning of a DDoS attack.
C. the IDS has been compromised.
D. the internal DNS tables have been poisoned.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 791
A customer service department has a business need to send high volumes of confidential information to customers electronically. All emails go through a DLP scanner. Which of the following is the BEST solution to meet the business needs and protect confidential information?

A. Automatically encrypt impacted outgoing emails
B. Automatically encrypt impacted incoming emails
C. Monitor impacted outgoing emails
D. Prevent impacted outgoing emails

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 792
Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

A. Common access card
B. Role based access control
C. Discretionary access control
D. Mandatory access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 793
Which of the following should be done before resetting a user's password due to expiration?

A. Verify the user's domain membership.
B. Verify the user's identity.
C. Advise the user of new policies.
D. Verify the proper group membership.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 794
Establishing a published chart of roles, responsibilities, and chain of command to be used during a disaster is an example of which of the following?

A. Fault tolerance
B. Succession planning
C. Business continuity testing
D. Recovery point objectives

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 795
A software developer is responsible for writing the code on an accounting application. Another software developer is responsible for developing code on a system in human resources. Once a year they have to switch roles for several weeks.

Which of the following practices is being implemented?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 796
A network engineer is designing a secure tunneled VPN. Which of the following protocols would be the MOST secure?

A. IPsec
B. SFTP
C. BGP
D. PPTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 797
Which of the following implementation steps would be appropriate for a public wireless hot-spot?

A. Reduce power level
B. Disable SSID broadcast
C. Open system authentication
D. MAC filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 798
Which of the following is a step in deploying a WPA2-Enterprise wireless network?

A. Install a token on the authentication server

B. Install a DHCP server on the authentication server
C. Install an encryption key on the authentication server
D. Install a digital certificate on the authentication server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 799
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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 800
Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host?

A. Installing anti-malware
B. Implementing an IDS
C. Taking a baseline configuration
D. Disabling unnecessary services

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 801
A security manager must remain aware of the security posture of each system. Which of the following supports this requirement?

A. Training staff on security policies
B. Establishing baseline reporting
C. Installing anti-malware software
D. Disabling unnecessary accounts/services

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 802

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: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 803
Due to limited resources, a company must reduce their hardware budget while still maintaining availability. Which of the following would MOST likely help them achieve their objectives?

A. Virtualization
B. Remote access
C. Network access control
D. Blade servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 804
Encryption used by RADIUS is BEST described as:

A. Quantum
B. Elliptical curve
C. Asymmetric
D. Symmetric

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 805
Which of the following should an administrator implement to research current attack methodologies?

A. Design reviews
B. Honeypot
C. Vulnerability scanner
D. Code reviews

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 806
A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department?

A. Time of day restrictions
B. Group based privileges
C. User assigned privileges
D. Domain admin restrictions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 807
A security administrator has concerns about new types of media which allow for the mass distribution of personal comments to a select group of people. To mitigate the risks involved with this media, employees should receive training on which of the following?

A. Peer to Peer
B. Mobile devices
C. Social networking
D. Personally owned devices

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 808
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 809
Which of the following ports is used for SSH, by default?

A. 23
B. 32
C. 12
D. 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
right answer.

QUESTION 810
A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN?

A. WPA2 CCMP
B. WPA
C. WPA with MAC filtering
D. WPA2 TKIP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 811
A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs show repeated connection attempts from the following IPs:
10.10.3.16
10.10.3.23
212.178.24.26
217.24.94.83

These attempts are overloading the server to the point that it cannot respond to traffic. Which of the following attacks is occurring?

A. XSS
B. DDoS
C. DoS
D. Xmas

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 812
Which of the following ciphers would be BEST used to encrypt streaming video?

A. RSA
B. RC4
C. SHA1
D. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 813
A user attempting to log on to a workstation for the first time is prompted for the following information before being granted access: username, password, and a four-digit security pin that was mailed to him during account registration. This is an example of which of the following?

A. Dual-factor authentication
B. Multifactor authentication
C. Single factor authentication
D. Biometric authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is perfect.

QUESTION 814
After analyzing and correlating activity from multiple sensors, the security administrator has determined that a group of very well organized individuals from an enemy country is responsible for various attempts to breach the company network, through the use of very sophisticated and targeted attacks. Which of the following is this an example of?

A. Privilege escalation
B. Advanced persistent threat
C. Malicious insider threat
D. Spear phishing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 815
Which of the following is true about input validation in a client-server architecture, when data integrity is critical to the organization?

A. It should be enforced on the client side only.
B. It must be protected by SSL encryption.
C. It must rely on the user's knowledge of the application.
D. It should be performed on the server side.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 816
A merchant acquirer has the need to store credit card numbers in a transactional database in a high performance environment. Which of the following BEST protects the credit card data?

A. Database field encryption
B. File-level encryption
C. Data loss prevention system

D. Full disk encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 817
A bank has a fleet of aging payment terminals used by merchants for transactional processing. The terminals currently support single DES but require an upgrade in order to be compliant with security standards. Which of the following is likely to be the simplest upgrade to the aging terminals which will improve in-transit protection of transactional data?

A. AES
B. 3DES
C. RC4
D. WPA2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 818
Which of the following is BEST at blocking attacks and providing security at layer 7 of the OSI model?

A. WAF
B. NIDS
C. Routers
D. Switches

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 819
Which of the following is BEST used to capture and analyze network traffic between hosts on the same network segment?

A. Protocol analyzer
B. Router
C. Firewall
D. HIPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
accurate answer.

QUESTION 820
After a number of highly publicized and embarrassing customer data leaks as a result of social engineering

attacks by phone, the Chief Information Officer (CIO) has decided user training will reduce the risk of another data leak. Which of the following would be MOST effective in reducing data leaks in this situation?

A. Information Security Awareness
B. Social Media and BYOD
C. Data Handling and Disposal
D. Acceptable Use of IT Systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: